การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธกับผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศ

นายดามร คำไตรย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรดุษฎีบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

The Use of New Technologies in Armed Conflict and the Implications on International Humanitarian Law

Mr. Damon Kumtrai

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Juridical Science in Laws
FACULTY OF LAW
Chulalongkorn University
Academic Year 2022

หัวข้อวิทยานิพนธ์	การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธกับผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศ
โดย	นายดามร คำไตรย์
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรดุษฎีบัณฑิต

..... คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปารีณา ศรีวนิชย์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ ดร.ชุมพร ปัจจุสานนท์)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.โชติกา วิทยาวรากุล)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ภาวัฒน์ สัตยานุรักษ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ศุภศิษฏ์ ทวีแจ่มทรัพย์)

..... กรรมการภายนอกมหาวิทยาลัย
(พลอากาศเอก ดร.ปรีชา ประดับมุข)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.สุพรรณวษา โชติกญาณ ถัง)

ดามร คำไตรย์ : การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธกับผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศ. (The Use of New Technologies in Armed Conflict and the Implications on International Humanitarian Law) อ.ที่ปรึกษาหลัก : ผศ. ดร.ศารทูล สันติวาสะ

การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธเปลี่ยนแปลงสถานการณ์การขัดกันทางอาวุธอย่างมีนัยสำคัญ โดยเฉพาะอย่างยิ่งลักษณะของเทคโนโลยีใหม่ที่พัฒนาขึ้นมาเพื่อเป็นอาวุธ เทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพแต่ถูกใช้เยี่ยงอาวุธ เทคโนโลยีที่ใช้ประกอบร่วมกับระบบอาวุธเพื่อเพิ่มประสิทธิภาพการทำงานของระบบอาวุธ ก่อให้เกิดข้อพิจารณาว่ากฎหมายมนุษยธรรมระหว่างประเทศยังสามารถปรับใช้ได้อย่างเหมาะสมและเพียงพอหรือไม่

แม้กฎหมายมนุษยธรรมระหว่างประเทศมีหลักการพื้นฐานที่มีลักษณะเป็นการทั่วไปเพื่อจำกัดวิธีการและปัจจัยในการขัดกันทางอาวุธที่จะต้องไม่ก่อให้เกิดผลกระทบต่อบุคคลและทรัพย์สิ่งของที่กฎหมายมุ่งคุ้มครอง แต่เมื่อพิจารณาถึงความยืดหยุ่นของกฎหมายมนุษยธรรมระหว่างประเทศที่สามารถปรับตัวได้อย่างเหมาะสมโดยไม่ฝ่าฝืนหรือบิดเบือนต่อเจตนารมณ์ของกฎหมาย พบว่ากฎหมายมนุษยธรรมระหว่างประเทศยังมีขีดจำกัดในการปรับตัวของหลักการทำให้ไม่สามารถนำไปปรับใช้กับเทคโนโลยีใหม่ได้อย่างเหมาะสมในบางกรณี เทคโนโลยีมีความเปลี่ยนแปลงอย่างต่อเนื่อง รวดเร็วและไม่สามารถคาดหมายได้ ในขณะที่พัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศไม่สามารถดำเนินไปได้อย่างรวดเร็วให้เท่าทันพัฒนาการของการใช้เทคโนโลยีในการขัดกันทางอาวุธ โดยขณะนี้ยังเร็วไปที่จะสามารถบ่งชี้หลักกฎหมายใหม่ที่ควรจะมีเพิ่มเติมเพื่อให้ปรับใช้ได้กับการใช้เทคโนโลยีใหม่อย่างเหมาะสม อย่างไรก็ตาม การใช้กฎหมายระหว่างประเทศในมิติอื่นเช่นการควบคุมหรือการจำกัดการใช้เทคโนโลยีโดยทั่วไป ซึ่งรวมถึงจริยธรรมในการใช้เทคโนโลยีใหม่เช่นปัญญาประดิษฐ์อาจเป็นประโยชน์ต่อการควบคุมการใช้เทคโนโลยีใหม่ให้สอดคล้องต่อกฎหมายมนุษยธรรมระหว่างประเทศ

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2565 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5986553134 : MAJOR LAWS

KEYWORD: International Humanitarian Law New Technologies Implications

Damon Kumtrai : The Use of New Technologies in Armed Conflict and the Implications on International Humanitarian Law. Advisor: Asst. Prof. SARATOON SANTIVASA, Ph.D.

The use of new technologies in armed conflict has significantly changed the circumstances of armed conflict. In particular, the development of new technologies as a weapon, technologies which are not per se a weapon but being used as a weapon and technologies used to enhance the efficiency of military weapons. These lead to the consideration that whether the international humanitarian law can be appropriately and sufficiently applied to the New Technologies.

Despite the international humanitarian law contains fundamental principles which are general in character limiting the methods and means of warfare to minimize the civilian loss. This general character is apt to the flexibility of its application. However, considering the flexibility of the fundamental principle of international humanitarian law capable to appropriately adapt without distorting the purposes of the law, the study finds that international humanitarian law has a limitation in certain aspects of its use, resulting that the law cannot be appropriately applied to new technologies. Technology is constantly changing. It is fast and unpredictable while the development of international humanitarian law has not been able to keep up with the pace of developments in the use of new technology in armed conflict. It is too early to indicate what new legal principles should be to properly cope with the use of the new technologies. However, other aspects of

Field of Study: Laws Student's Signature .....

Academic Year: 2022 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้โดยคำแนะนำที่ทรงคุณค่าจากคณะกรรมการสอบวิทยานิพนธ์อันประกอบด้วย ศาสตราจารย์ ดร.ชุมพร ปัจจุสานนท์ ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ ผู้ช่วยศาสตราจารย์ ดร.โชติกา วิทยาวรากุล ผู้ช่วยศาสตราจารย์ ดร.ศุภศิษฏ์ ทวีแจ่มทรัพย์ ผู้ช่วยศาสตราจารย์ ดร.ภาวัฒน์ สัตยานุรักษ์ ท่าน ดร.สุพรรณวษา โชติกญาณ ถัง และท่านพลอากาศเอก ดร.ปรีชา ประดับมุข

ผู้เขียนขอกราบขอบพระคุณเป็นพิเศษต่อท่านผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ อาจารย์ที่ปรึกษา ผู้จุดประกายทางปัญญา ให้คำแนะนำที่เป็นประโยชน์ต่อการศึกษาและช่วยสร้างกรอบแนวคิดให้ผู้เขียน วิทยานิพนธ์ฉบับนี้จะเกิดขึ้นไม่ได้และสำเร็จไม่ได้โดยปราศจากท่าน ท่านศาสตราจารย์ ดร.ชุมพร ปัจจุสานนท์ ประธานกรรมการสอบวิทยานิพนธ์ ผู้ประสิทธิ์ประสาทระเบียบวิธีคิดทางกฎหมายและการวิจัย ท่าน ดร.สุพรรณวษา โชติกญาณ ถัง อธิบดีกรมสนธิสัญญาและกฎหมาย กระทรวงการต่างประเทศ สำหรับคำแนะนำในมุมมองที่หลากหลายมากกว่ากรอบความคิดทางกฎหมายโดยทั่วไป ท่านพลอากาศเอก ดร.ปรีชา ประดับมุข สำหรับคำแนะนำที่เป็นประโยชน์อย่างยิ่งในประเด็นการพัฒนาระบบอากาศยานไร้คนขับทางการทหารและระบบปัญญาประดิษฐ์ในอาวุธ ท่านศาสตราจารย์กิตติคุณ วิทิต มันตาภรณ์ อาจารย์ผู้เป็นแรงบันดาลใจในการใช้ชีวิตในวงการกฎหมายของผู้เขียน

ผู้เขียนใคร่ขอรำลึกถึงพระคุณของท่านรองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ ผู้ล่วงลับ ซึ่งเป็นทั้งอาจารย์ ผู้บังคับบัญชาและญาติผู้ใหญ่

ท้ายที่สุด ผู้เขียนขอขอบคุณมารดาของผู้เขียน คุณจันทรา คำไตรย์ ผู้เป็นกำลังใจและส่งเสริมการศึกษาตั้งแต่เด็กจนถึงปัจจุบัน เพื่อนร่วมชั้นเรียนและน้องๆ ที่รักอันประกอบด้วย ดร.ฉัตรชัย เอมราช อาจารย์ปิยอร เปลี่ยนผดุง อาจารย์โศภิต ชีวะพานิชย์ อาจารย์วิลาสินี หมายเจริญศรี และอาจารย์กัณภัค ตัณฑสิทธิ์ คุณธนภร สวัสดิมงคล ผู้เป็นกำลังใจ ที่ปรึกษาและสนับสนุนภารกิจต่างๆ

ดามร คำไตรย์

สารบัญ

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การขัดกันทางอาวุธระหว่างประเทศยูเครนและรัสเซียในปี พ.ศ.2565 (ค.ศ.2022)[1] สะท้อนให้เห็นภาพการทำสงครามในยุคใหม่ว่าการต่อสู้ในสงครามนั้นไม่จำกัดเฉพาะการต่อสู้ทางทหารด้วยอาวุธสงครามแบบในอดีตอีกต่อไป ปฏิบัติการทางทหารระหว่างยูเครนและรัสเซียในความขัดแย้งครั้งนี้ปรากฏทั้งการใช้กองกำลังทางทหารและอาวุธตามแบบโดยปกติควบคู่ไปกับการโจมตีทางไซเบอร์ต่อการสื่อสารและสาธารณูปโภคทั้งทางการทหารและพลเรือน มีการใช้งานอากาศยานไร้คนขับเพื่อการโจมตีอย่างแพร่หลาย[2] การโจมตีทางไซเบอร์หลายกรณีก่อให้เกิดความเสียหายที่ไม่ปรากฏผลทางกายภาพอย่างชัดเจนเหมือนการใช้กำลังทางอาวุธที่เคยเป็นมาในอดีต นอกจากนั้นพลเรือนยังเข้ามามีส่วนเกี่ยวข้องกับการทำสงครามมากขึ้นด้วย[3] เช่นการจัดตั้งกลุ่ม IT Army[4] ของพลเรือนชาวยูเครนเพื่อตอบโต้ปฏิบัติการของกองทัพรัสเซียรวมตลอดถึงการที่พลเมืองชาวยูเครนมีส่วนร่วมในการถ่ายภาพกองกำลังของรัสเซียที่เดินทางเข้าไปยังพื้นที่ต่างๆ[5] เพื่อเป็นการอำนวยความสะดวกให้กองกำลังยูเครนสามารถปฏิบัติการตอบโต้กองทัพรัสเซียได้รวดเร็วขึ้นฯลฯ สิ่งเหล่านี้ล้วนเป็นความเปลี่ยนแปลงของการทำสงครามในยุคปัจจุบันที่ไม่จำกัดการโจมตีและการป้องกันตัวเฉพาะจากการต่อสู้ด้วยอาวุธแต่เพียงอย่างเดียว แต่เทคโนโลยีต่างๆ โดยเฉพาะอย่างยิ่งเทคโนโลยีสารสนเทศในระบบไซเบอร์เข้ามามีส่วนเกี่ยวข้องกับการสงครามมากยิ่งขึ้น

---

[1] Dominika Kunertova, "The war in Ukraine shows the game-changing effect of drones depends on the game," *Bulletin of the Atomic Scientists* 79, no. 2 (2023/03/04 2023), https://doi.org/10.1080/00963402.2023.2178180, https://doi.org/10.1080/00963402.2023.2178180. :95.

[2] Ibid.

[3] Patricia Justino, "The Conflict in Ukraine – The Role of Civilians," UNU Wider. (February 2022) [online] Accessed: March 26, 2022. Available from: https://www.wider.unu.edu/publication/conflict-ukraine-role-civilians

[4] Russell Buchan and Nicholas Tsagourias. "Ukrainian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?" European Journal of International Law. (March 9, 2022) [online] Accessed: March 26, 2023. Available from: https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-inhostilities/?fbclid=IwAR1IL6iWjPKOUQQ4QUvOj3G3aDWK2g7W4Bxy QumJLFoweDtP3YHpiT40wkU

[5] Simon Hogue, "Civilian Surveillance in the war in Ukraine: Mobilizing the Agency of the Observer of War," Surveillance and Society, 21 (1), (2023), p. 109.

เราปฏิเสธไม่ได้ว่าเทคโนโลยีที่มีการใช้งานในความขัดแย้งระหว่างยูเครนและรัสเซียนั้นเป็นผลมาจากพัฒนาการทางวิทยาศาสตร์และเทคโนโลยีในศตวรรษที่ 21 ซึ่งทำให้วิถีการใช้ชีวิตของมนุษย์เปลี่ยนแปลงแตกต่างไปจากเดิมอย่างมีนัยสำคัญ การใช้งานสิ่งอำนวยความสะดวกในชีวิตต่างๆ เช่น เครื่องใช้ไฟฟ้าในครัวเรือน เครื่องมือสื่อสาร และอุปกรณ์เพื่อการทำงานในสำนักงาน ฯลฯ ก้าวผ่านจากระบบอนาล็อก (Analog) ไปสู่ระบบดิจิทัล (Digital) การทำงานของอุปกรณ์ต่างๆ มีระบบการประมวลผลของคอมพิวเตอร์ประกอบกับการทำงานของอินเทอร์เน็ตมากขึ้น[6] การใช้งานโทรศัพท์เคลื่อนที่แทนการทำงานของคอมพิวเตอร์สามารถทำได้สะดวกยิ่งขึ้น ผลของความเปลี่ยนแปลงดังกล่าวเป็นเหตุให้การขัดกันทางอาวุธในปัจจุบันมีใช้งานเทคโนโลยีทางอาวุธบนพื้นฐานของเทคโนโลยีดิจิทัล[7]และการสื่อสารในระบบอินเทอร์เน็ตมากยิ่งขึ้น[8]

การสั่งการระบบอุปกรณ์อำนวยความสะดวกต่างๆ ในยุคปัจจุบันเป็นการสั่งงานผ่านระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตที่เรียกว่าระบบไซเบอร์[9] เช่น การเชื่อมต่อการทำงานของกล้องวงจรปิดเข้ากับโทรศัพท์มือถือหรือการสั่งสตาร์ทรถยนต์ล่วงหน้าด้วยโทรศัพท์มือถือ ฯลฯ ซึ่งการทำงานของคอมพิวเตอร์ในระบบไซเบอร์มีสาระสำคัญที่อุปกรณ์อิเล็กทรอนิกส์ที่เราใช้งานนั้นสามารถรับคำสั่งหรือข้อมูลต่างๆ ที่ส่งผ่านระบบอิเล็กทรอนิกส์ทั้งลักษณะการเชื่อมต่อแบบมีสายและไร้สายได้ ขณะที่การเชื่อมต่อนั้นไม่จำกัดเฉพาะระหว่างอุปกรณ์ชนิดเดียวกันแต่สามารถทำการเชื่อมต่อระหว่างอุปกรณ์ที่แตกต่างกันได้[10] นอกจากนั้นอุปกรณ์ในลักษณะของคอมพิวเตอร์ในปัจจุบันยังมีขอบเขตที่หลากหลาย โดยเฉพาะอย่างยิ่งอุปกรณ์ที่ทำงานโดยมีระบบประมวลผลและหน่วยความจำ ซึ่งอาจมีลักษณะแตกต่างกันไป ได้แก่

1) อุปกรณ์ที่ทำงานในลักษณะเดียวกับเครื่องคอมพิวเตอร์ เช่น แทปเล็ตและโทรศัพท์มือถือเป็นอุปกรณ์ที่มีระบบประมวลผลและหน่วยความจำจึงสามารถทำงานในลักษณะเดียวกับคอมพิวเตอร์ได้ เราจึงสามารถใช้แทปเล็ตและโทรศัพท์มือถือเพื่อการเชื่อมต่อระบบอินเทอร์เน็ต

---

[6] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, (Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018), p. 86.

[7] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26. [online] Accessed April 24, 2023. Available from: https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts.

[8] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

[9] Robert S. Gutzwiller, Sunny Fugate, Benjamin D. Sawyer, and P. A. Hancock, "The Human Factors of Cyber Network Defense," Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting – 2015, p. 322.

[10] Ibid, p. 324.

สามารถรับส่งข้อความผ่านอีเมลและแอปพลิเคชันอื่นๆ ได้[11] นอกจากนั้นยังสามารถใช้งานอุปกรณ์ที่ทำงานในลักษณะเดียวกับคอมพิวเตอร์นี้เชื่อมต่อการทำงานกับอุปกรณ์อื่นๆ ได้ผ่านโปรแกรมสั่งการในรูปแบบแอปพลิเคชันต่างๆ เช่น แอปพลิเคชันสั่งงานระบบเปิด-ปิดไฟฟ้าในบ้าน แอปพลิเคชันสั่งสตาร์ทรถยนต์ล่วงหน้า แอปพลิเคชันสั่งงานและดูภาพจากกล้องวงจรปิดภายในบ้าน แอปพลิเคชันการควบคุมอากาศยานไร้คนขับ (โดรน) เป็นต้น

2) อุปกรณ์อื่นๆ ที่มีระบบการทำงานเชื่อมต่อกับเครือข่ายคอมพิวเตอร์แต่ไม่ได้ทำงานแบบเดียวกับคอมพิวเตอร์ เช่นกล้องวงจรปิดมีระบบการทำงานของหน่วยประมวลผลกลางและหน่วยความจำทำให้กล้องวงจรปิดสามารถบันทึกข้อมูลได้และกล้องวงจรผิดสามารถเชื่อมต่อการทำงานกับคอมพิวเตอร์ โทรศัพท์มือถือหรือแทปเล็ตได้[12] เมื่อกล้องวงจรปิดมีความสามารถในการทำงานบางลักษณะคล้ายคอมพิวเตอร์จึงมีผู้ประสงค์ร้ายสามารถใช้ระบบการทำงานของกล้องวงจรปิดเพื่อทำหน้าที่แบบเดียวกับคอมพิวเตอร์ได้ เช่นการสั่งการให้กล้องวงจรปิดหลายเครื่องส่งคำขอเข้าสู่เว็บไซต์หนึ่งพร้อมกันได้ ลักษณะการทำงานดังกล่าวจะก่อให้เกิดความล้มเหลวของเครือข่ายการสื่อสารของเว็บไซต์ดังกล่าวเนื่องจากมีคำขอเข้าสู่ข้อมูลมากเกินไป วิธีการโจมตีเครือข่ายการสื่อสารลักษณะนี้เป็นการปฏิเสธการเข้าถึงบริการที่เรียกว่า DDoS (Distributed Denial-of-Service)[13] ซึ่งบริษัทผู้ให้บริการทางด้านความปลอดภัยทางอินเทอร์เน็ต Sucuri ของสหรัฐอเมริกากล่าวว่ามีการเจาะเข้าสู่ระบบ cloud ของกล้องวงจรปิด (CCTV) กว่า 105 ประเทศทั่วโลกเพื่อส่ง Botnet เข้าสู่ระบบกล้องวงจรปิด สำหรับทำปฏิบัติการ DDoS โดยพบว่าการโจมตีดังกล่าวร้อยละ 25 มาจากไต้หวัน ร้อยละ 12 มาจากสหรัฐอเมริกาและร้อยละ 10 มาจากอินโดนีเซีย[14]

3) อุปกรณ์ที่ทำงานประกอบร่วมกับคอมพิวเตอร์และช่วยให้คอมพิวเตอร์มีความสามารถสูงขึ้นในการปฏิบัติการ เช่น หน่วยประมวลผลรูปภาพ (GPU: Graphic Processing Unit) โดยทั่วไปหน่วยประมวลผลรูปภาพของคอมพิวเตอร์นี้มีไว้เพื่อประโยชน์ในการแสดงผลทางหน้าจอคอมพิวเตอร์

---

[11] Robert S. Gutzwiller, Sunny Fugate, Benjamin D. Sawyer, and P. A. Hancock, "The Human Factors of Cyber Network Defense,": 324.

[12] Ibid.

[13] "สบายแต่เสี่ยงโดนแฮก กล้อง CCTV ในยุคอินเทอร์เน็ตของทุกสิ่ง," สำนักงานพัฒนารัฐบาลดิจิทัล, (2559), [online] เข้าถึง 20 พฤษภาคม พ.ศ.2565. Available from: https://www.dga.or.th /document-sharing/article/35961/

[14] Iain Thomson, "25,000 malware-riddled CCTV cameras form network-crashing botnet," The Register, 28 June 2016, [online] Accessed: May 20, 2022. Available from: https://www.theregister.com/2016/06/28/25000_compromised_cctv_cameras/

ให้เกิดภาพที่มีความละเอียดสูงหรือภาพที่มีความซับซ้อนมาก ซึ่งการทำงานของระบบประมวลผลกลางในเครื่องคอมพิวเตอร์นั้นไม่เพียงพอต่อการแสดงผลภาพดังกล่าว หน่วยประมวลผลรูปภาพแต่เดิมนั้นมีไว้เพื่อการทำงานเฉพาะอย่าง เช่น งานออกแบบสถาปัตยกรรม งานออกแบบกราฟิก การประมวลผลเพื่อเกมส์คอมพิวเตอร์ ฯลฯ แต่เมื่อเกิดปรากฏการณ์การใช้เงินตราดิจิทัล (Crypto Currency) ก็มีผู้นำเอาหน่วยประมวลผลรูปภาพของคอมพิวเตอร์นี้มาช่วยเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์เพื่อการเข้าถึงการรับรองธุรกรรมทางเงินตราดิจิทัล[15]ในระบบบล็อคเชน (Block Chain)[16] ซึ่งผู้ทำการรับรองธุรกรรมเงินตราดิจิทัลนี้จะได้รับค่าตอบแทนจากการรับรองธุรกรรม (โดยทั่วไปเรียกรูปแบบการกระทำดังกล่าวว่า “การขุดบิดคอยน์” “การทำฟาร์ม” หรือ “การทำเหมือง” ขึ้นอยู่กับขีดความสามารถของคอมพิวเตอร์จากน้อยไปมาก) เมื่อผู้ใช้งานหน่วยประมวลผลรูปภาพมีมากขึ้นก็ส่งผลกระทบหลายประการต่อสังคม ได้แก่ ผลกระทบทางเศรษฐกิจจากราคาหน่วยประมวลผลรูปภาพมีราคาสูงขึ้นหลายเท่าตัว[17] เป็นต้น

ลักษณะการใช้งานคอมพิวเตอร์และการสื่อสารผ่านระบบอินเทอร์เน็ตของคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องดังที่ได้กล่าวมาชี้ให้เห็นว่าเทคโนโลยีคอมพิวเตอร์ที่เกี่ยวข้องกับการสื่อสารผ่านเครือข่ายไซเบอร์ในปัจจุบันพัฒนาไปอย่างมากและมีความซับซ้อน[18] การใช้งานเทคโนโลยีดังกล่าวสามารถใช้ในทางที่เกิดประโยชน์หรือใช้เพื่อก่อความเสียหายก็ได้ เมื่อประกอบร่วมกับการทำงานผ่านเครือข่ายไซเบอร์และอินเทอร์เน็ตซึ่งเป็นพื้นฐานของการติดต่อสื่อสารในปัจจุบัน ทำให้การใช้งาน

[15] Michael Bedford Taylor, “The Evolution of Bitcoin Hardware,” Computer, vol. 50, no. 9, (2017): pp. 59-60.

[16] ในธุรกรรมสินทรัพย์ทางดิจิทัลรูปแบบการซื้อ-ขาย แลกเปลี่ยน เป็นไปโดยเสรี ไม่มีหน่วยงานใดเป็นผู้รับรอง ข้อมูลทั้งหมดจะอยู่ในพื้นที่ทางไซเบอร์ ผู้สร้างสินทรัพย์ดิจิทัลแต่ละบริษัทจะกำหนดค่าตอบแทนการรับรองธุรกรรมสินทรัพย์ดิจิทัลเอาไว้ให้ผู้ใดก็ได้ในพื้นที่ไซเบอร์สามารถเข้าไปรับรองการทำธุรกรรมเพื่อให้มีการบันทึกการทำธุรกรรมนั้นๆ ตามลำดับเวลาของสินทรัพย์ดิจิทัลสกุลต่างๆ การรับรองจะถูกบันทึกเอาไว้เป็นชุดข้อมูลที่เรียกว่าบล็อค (Block) และเชื่อมต่อกันกับชุดข้อมูลอื่นๆ ที่เกิดขึ้นในอดีตเป็นลำดับเหมือนโซ่ (Chain) จึงเรียกการรับรองธุรกรรมสินทรัพย์ดิจิทัลในโลกไซเบอร์นี้ว่า Block chain การเข้าสู่ข้อมูลธุรกรรมสินทรัพย์ดิจิทัลทางไซเบอร์นี้จะกระทำได้ก็ต่อเมื่อผู้ใช้งานคอมพิวเตอร์จะต้องมีโปรแกรมในการค้นหาการเคลื่อนไหวธุรกรรมสินทรัพย์ดิจิทัลนั้นๆ ด้วยระบบประมวลผลที่มีความสามารถระดับสูง โดยปกติการประมวลผลของคอมพิวเตอร์จะกระทำผ่านหน่วยประมวลผลกลาง (CPU: Central Processing Unit) ซึ่งมีข้อจำกัดสำหรับผู้ใช้งานโปรแกรมที่เป็นบุคคลทั่วไปที่ไม่สามารถเข้าถึงระบบประมวลผลที่มีความสามารถสูงได้นำมาสู่การใช้หน่วยประมวลผลทางกราฟฟิค (GPU) เพื่อการประมวลผลแทนหน่วยประมวลผลกลาง เนื่องจากในหน่วยประมวลผลทางกราฟฟิคก็มีหน่วยประมวลผลและหน่วยความจำในตัวเช่นกัน

[17] Michael Bedford Taylor, “The Evolution of Bitcoin Hardware,” pp. 59-60.

[18] Timothe Lopez, L’adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

อุปกรณ์อำนวยความสะดวกหลายอย่างมีการเชื่อมต่อกันอย่างกว้างขวางยิ่งขึ้น ในขณะเดียวกันการใช้งานในทางมิชอบเพื่อก่อความเสียหายก็จะก่อให้เกิดความเสียหายในขอบเขตที่กว้างขวางเช่นกัน

การทำงานของแอปพลิเคชันและโปรแกรมต่างๆ ในคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องนั้น นอกจากลักษณะของการทำงานผ่านเครือข่ายไซเบอร์และอินเทอร์เน็ตดังที่ได้กล่าวมาแล้ว ยังมีปัจจัยสำคัญประการหนึ่งที่ทำให้ระบบประมวลผลของคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องทำงานได้มีประสิทธิภาพมากขึ้นคือการใช้ระบบการวิเคราะห์ซับซ้อนแบบอัลกอริทึ่ม (Algorithm) เข้ามาประกอบร่วมกับการใช้งานอุปกรณ์คอมพิวเตอร์และการทำงานของโปรแกรมคอมพิวเตอร์บนเครือข่ายไซเบอร์[19]

การประมวลผลแบบอัลกอริทึ่มเป็นพื้นฐานการทำงานของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) ก่อให้เกิดการเปลี่ยนแปลงเทคโนโลยีในหลายลักษณะ โดยลักษณะการใช้งานสำคัญ 2 ประการที่นำมาสู่ประเด็นท้าทายทางกฎหมายในปัจจุบัน ได้แก่[20]

ประเด็นที่ 1 การทำงานของระบบไซเบอร์อยู่บนพื้นที่ทางอิเล็กทรอนิกส์และมีการเชื่อมต่อแบบไร้ขอบเขต และสามารถทำงานร่วมกับระบบอัลกอริทึ่มได้

ลักษณะการทำงานของระบบไซเบอร์ในปัจจุบันเป็นการเชื่อมต่ออุปกรณ์และการทำงานของโปรแกรมต่างๆ ทั้งในรูปแบบการใช้อินเทอร์เน็ตเพื่อเชื่อมต่อกับอุปกรณ์ที่ติดต่อกับอินเทอร์เน็ตได้ (IoT: Internet of Things) การจัดเก็บข้อมูลการใช้บริการอินเทอร์เน็ตของบุคคลในทุกเรื่อง (Big Data) และการนำข้อมูลการใช้อินเทอร์เน็ตรวมถึงข้อมูลส่วนบุคคลที่อยู่ในพื้นที่อินเทอร์เน็ตของบุคคลมาทำการวิเคราะห์เพื่อวัตถุประสงค์ทางพาณิชย์ เช่น โปรแกรม google analytics ซึ่งทำการประมวลผลความต้องการสินค้าและบริการของเรา โดยเชื่อมต่อไปยังผู้ให้บริการหรือร้านค้าต่างๆ ที่มีข้อมูลพื้นฐานในระบบอินเทอร์เน็ต เพื่อนำเสนอสินค้าที่เราสนใจผ่านทั้งหน้าต่างโฆษณา อีเมล และช่องทางอื่นๆ ของเราเช่น เฟซบุค (Facebook) ฯลฯ ลักษณะการทำงานของระบบไซเบอร์นี้หากเป็นไปเพื่อการอำนวยความสะดวกก็สามารถทำได้ในวงกว้างในขณะที่หากเป็นการทำเพื่อการประสงค์ร้ายก็สามารถทำได้ในวงกว้างเช่นกันเนื่องจากข้อมูลเหล่านี้อยู่ในพื้นที่ไซเบอร์ซึ่งมีลักษณะเป็นเครือข่ายการเชื่อมต่อกันในพื้นที่อิเล็กทรอนิกส์ (พื้นที่ทางไฟฟ้าและคลื่นแม่เหล็กไฟฟ้า) ทำให้

[19] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p. 26.

[20] Ibid.

การทำงานของโปรแกรมประมวลผลและวิเคราะห์ข้อมูลที่ซับซ้อนสามารถทำงานได้ง่ายเป็นประโยชน์อย่างมากในทางพาณิชย์

ในทำนองกลับกัน หากข้อมูลส่วนบุคคลดังกล่าวไปอยู่ในมือของผู้ประสงค์ร้ายหรือหากรัฐต้องการเข้าถึงข้อมูลของผู้ก่อความไม่สงบเรียบร้อยที่มีในพื้นที่ไซเบอร์ก็สามารถกระทำได้เช่นกัน เช่น กรณีการใช้งานโปรแกรม Pegasus เพื่อการเข้าถึงข้อมูลของบุคคล โดยโปรแกรม Pegasus นี้เป็น Spyware ที่ได้รับการพัฒนาและสร้างขึ้นมาจากบริษัทเอกชนของอิสราเอลในกลุ่ม NSO Group[21] ซึ่งจำหน่ายให้กับเฉพาะหน่วยงานของรัฐบาลประเทศต่างๆ เพื่อวัตถุประสงค์ในการป้องกันการก่อการร้ายและการต่อต้านอาชญากรรม แต่ในอีกมิติหนึ่งก็มีผู้มองว่าการใช้งานโปรแกรม Pegasus Spyware นี้เป็นการละเมิดต่อสิทธิส่วนบุคคลเช่นกัน การเข้าถึงข้อมูลในพื้นที่ไซเบอร์ของบุคคลด้วยโปรแกรม Pegasus เป็นการนำข้อมูลมาจากหลายแหล่ง โดยข้อมูลจากแหล่งต่างๆ เหล่านั้นมักเป็นอุปกรณ์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เมื่อโปรแกรม Pegasus สามารถเข้าถึงระบบ Internet of Things และ Big Data ได้ ก็จะทำให้ผู้ใช้งานโปรแกรม Pegasus สามารถเข้าถึงข้อมูลส่วนบุคคลที่บันทึกไว้ในพื้นที่ไซเบอร์ได้ ในอีกทางหนึ่งจึงมีความวิตกกังวลเกิดขึ้นในสังคมว่าหากมีการใช้งานโปรแกรม Spyware ลักษณะทำนองเดียวกันกับ Pegasus นี้ โดยกลุ่มผู้ก่อการร้าย ความเสียหายที่จะเกิดขึ้นก็จะเป็นวงกว้างได้เช่นกัน[22]

ประเด็นที่ 2 การใช้งานระบบปัญญาประดิษฐ์สามารถใช้ได้ทั้งเพื่อวัตถุประสงค์ทางสันติและการใช้งานเพื่อการทหาร

การใช้งานปัญญาประดิษฐ์ที่อาจปรากฏในรูปแบบของโปรแกรมที่เป็นซอฟท์แวร์และปัญญาประดิษฐ์ในลักษณะเป็นอุปกรณ์ฮาร์ดแวร์ เช่น หุ่นยนต์ส่งอาหารในร้านอาหาร หุ่นยนต์ดูดฝุ่น หุ่นยนต์ที่มีลักษณะเหมือนมนุษย์และสามารถสื่อสารกับมนุษย์ได้ ฯลฯ หุ่นยนต์เหล่านี้มีเป้าหมายในการพัฒนาเพื่ออำนวยความสะดวกในการทำงานและใช้ชีวิตประจำวันของมนุษย์ ในทางตรงข้ามเทคโนโลยีหุ่นยนต์นี้ก็มีการพัฒนาและนำไปใช้งานเพื่อการทหารด้วย เช่น ระบบการรักษาความปลอดภัยในพรมแดนของประเทศเกาหลีใต้ ด้วยระบบอาวุธ SGR A-1 ซึ่งเป็นการทำงานของระบบเซ็นเซอร์ทำงานอัตโนมัติตรวจการเคลื่อนไหวบริเวณชายแดน มีรัศมีในการตรวจตราราว 3 กิโลเมตร

[21] Amnesty International, “Forensic Methodology Report: How to catch NSO Group’s Pegasus,” Amnesty International. July 18, 2021. Accessed: July 19, 2021. Available from: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[22] Ibid.

ทำงานร่วมกับปืนกลขนาด 5.5 มิลลิเมตรและเครื่องยิงลูกระเบิดเพื่อการโจมตีเป้าหมาย เมื่ออาวุธตรวจพบการเคลื่อนไหวจะส่งสัญญาณไปศูนย์บัญชาการ มีทหารประจำศูนย์บัญชาการจะทำการแจ้งเตือนสิ่งที่พบดังกล่าวก่อนตัดสินใจสั่งปฏิบัติในลำดับต่อไป[23] การทำงานรูปแบบดังกล่าวพบในระบบต่อต้านขีปนาวุธ Iron Dome ของกองทัพอิสราเอลเช่นกัน มีทำงานร่วมกันระหว่างระบบเซ็นเซอร์ด้วยเรดาร์และระบบระบุตำแหน่งบนพื้นโลก (Global Positioning System) พร้อมเทคโนโลยีการประมวลผลและระบบยิงจรวดทำลายเป้าหมาย โดยระบบเรดาร์จะตรวจจับภัยคุกคามจากจรวดหรือขีปนาวุธที่เข้ามาในน่านฟ้าอิสราเอล หลังจากนั้นจะมีการส่งข้อมูลกลับมาที่ระบบประมวลผลเพื่อวิเคราะห์ว่าภัยคุกคามดังกล่าวอยู่ในระยะที่สามารถโต้ตอบได้หรือไม่ ภัยคุกคามที่พบเป็นวัตถุที่ต้องทำลายหรือไม่ หากจะตอบโต้จะต้องกระทำในระยะเท่าใด จะสั่งการยิงจรวดต่อต้านเมื่อใด ทำลายในระยะใดจึงจะปลอดภัยต่อประชาชน และควรยิงจรวดต่อต้านเมื่อใด[24] เป็นต้น การประมวลผลของระบบอาวุธดังกล่าวต้องอาศัยการทำงานของอัลกอริทึ่มซึ่งเป็นระบบหนึ่งที่มีความสำคัญต่อการทำงานของปัญญาประดิษฐ์โดยทั่วไป

ความเปลี่ยนแปลงของเทคโนโลยีต่อวิถีการใช้ชีวิตของมนุษย์ไปอย่างมีนัยสำคัญนี้ส่งผลในระดับที่ทำให้หลายคนเชื่อว่าอนาคตนั้นมนุษย์จะถูกแทนที่ด้วยเครื่องจักร หุ่นยนต์และระบบคอมพิวเตอร์ โดยสิ่งเหล่านี้จะเข้ามาแทนที่การทำงานของมนุษย์รวมไปถึงความคิดว่าในอนาคตหุ่นยนต์และปัญญาประดิษฐ์จะมีบทบาทมากขึ้นในการสงครามด้วย[25]

ความก้าวหน้าทางเทคโนโลยีดังกล่าวไม่ได้มีผลเฉพาะต่อความรู้สึกว่าหุ่นยนต์และปัญญาประดิษฐ์จะมาทำหน้าที่แทนมนุษย์แต่เพียงอย่างเดียวเท่านั้นแต่มีผลต่อการใช้ชีวิตมนุษย์ในความเป็นจริงโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลของเรา เช่น ระบบการรับ-ส่งข้อมูลของอินเทอร์เน็ตจะมีการบันทึกข้อมูลกิจกรรมการสื่อสารทั้งหมดไว้ในรูปแบบดิจิทัลเพื่อประโยชน์ในการทำงานของหน่วยประมวลผลคอมพิวเตอร์ในการเรียกแสดงข้อมูลเดิมซ้ำ เพื่อบันทึกประวัติการเข้าถึงข้อมูล และเพื่อเป็นประโยชน์ในการประมวลผลในลักษณะอื่นๆ ที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต ฯลฯ ข้อมูลที่มีการบันทึกไว้เหล่านี้เป็นร่องรอยทางดิจิทัล (Digital footprint)[26] ซึ่งมีทั้งด้านดีและด้านลบ

---

[23] Ugo Pagallo, The law of robot: Crimes, contracts and torts, (London: Springer, 2013), p. xi.

[24] Jeremy M. Sharp, U.S. foreign aid to Israel, (Washington, DC: Congressional Research Service, 2023), pp. 16-19.

[25] Annabelle Quince, "Future Drone Strikes Could See Execution by Algorithm," ABC Online, January 21, 2013., [online] Accessed: July 24, 2020. Available from: https://www.abc.net.au/radionational/programs/rearvision/drones/4703792

[26] Stephen D. Weaver and Mark Gahegan, "Constructing, Visualizing and Analyzing a Digital Footprint," The Geographical Review, 97 (3), (July 2007): 328-331.

ในด้านดีของระบบปัญญาประดิษฐ์ในคอมพิวเตอร์คือโปรแกรมอัลกอริทึ่มของคอมพิวเตอร์จะคัดเลือกข้อมูลที่เราเข้าถึงมาประเมินความสนใจของเราหรือวิเคราะห์พฤติกรรมการใช้งานระบบไซเบอร์เพื่อนำเสนอข้อมูลที่เป็นประโยชน์ในเชิงพาณิชย์และนำเสนอสินค้า บริการและข้อมูลอื่นๆ ที่โปรแกรมคอมพิวเตอร์วิเคราะห์แล้วเห็นว่าเรามีความสนใจ ทำให้เราได้รับข้อมูลข่าวสารและสินค้าจากผู้ให้บริการตรงกับข้อมูลที่เราเคยแสดงพฤติกรรมในโลกไซเบอร์ ซึ่งทำให้ผู้ค้าสินค้าและผู้ให้บริการมีช่องทางในการโฆษณาสินค้าได้ตรงกับเป้าหมายผู้บริโภคมากขึ้น[27]

ในทำนองกลับกันนั้นด้านลบของระบบปัญญาประดิษฐ์ในคอมพิวเตอร์นั้น ผู้ประสงค์ร้ายที่สามารถเข้าถึงข้อมูลของเราที่ถูกบันทึกไว้ในระบบไซเบอร์อาจขโมยข้อมูลเราที่อยู่ในพื้นที่เครือข่ายไซเบอร์ ข้อมูลที่อยู่ในคอมพิวเตอร์และข้อมูลที่บันทึกในอุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์แล้วไปใช้ในทางที่อาจก่อความเสียหายแก่เราได้[28]

ลักษณะการทำงานของระบบไซเบอร์ที่เป็นเครือข่ายเชื่อมต่ออุปกรณ์หลายชนิด เป็นช่องทางทำให้มีผู้ใช้โปรแกรมประสงค์ร้าย (Malware) เพื่อทำลายข้อมูลหรือทำลายอุปกรณ์ของที่เกี่ยวข้องกับระบบไซเบอร์ได้เป็นวงกว้าง ดังนั้นการปล่อยไวรัสคอมพิวเตอร์เพื่อมุ่งให้เกิดความเสียหายต่อข้อมูลหรืออุปกรณ์คอมพิวเตอร์สามารถกระทำได้โดยผู้ประสงค์ร้ายโดยการปล่อยมัลแวร์เข้าสู่เครือข่ายการสื่อสารของคอมพิวเตอร์เพียงเครือข่ายเดียวหรือเครื่องคอมพิวเตอร์เครื่องเดียวที่เชื่อมต่อระบบอินเทอร์เน็ตก็อาจส่งผลให้เครื่องคอมพิวเตอร์เครื่องอื่นๆ และเครือข่ายการติดต่ออื่นๆ ติดมัลแวร์ได้เช่นกัน

ในมิติทางการทหารนั้นเทคโนโลยีที่เกิดขึ้นในปัจจุบันมีส่วนสำคัญในการเพิ่มความแม่นยำในการโจมตีและอำนวยความสะดวกต่อกองทัพมากขึ้น[29] เช่น ในการพัฒนาเครื่องบินรบ F-35 Stealth ของกองทัพสหรัฐอเมริกามีการติดตั้งระบบการทำงานของคอมพิวเตอร์และระบบประมวลผลที่ซับซ้อนเพื่อให้นักบินปฏิบัติภารกิจหลายหน้าที่ได้ในขณะที่เครื่องบินทำการบินด้วยความเร็วสูง [30] เครื่องบินจะต้องมีความสามารถในการหลบการตรวจจับของสัญญาณเรดาร์พร้อมกันนั้นเครื่องบินจะต้องสามารถตรวจจับเป้าหมายและยิงอาวุธนำวิถีได้ด้วยความแม่นยำ การปฏิบัติภารกิจทั้งหมดนี้

---

[27] Stephen D. Weaver and Mark Gahegan, “Constructing, Visualizing and Analyzing a Digital Footprint,”, p.326.

[28] Ibid.

[29] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p. 26.

[30] Philip Ball, “New lessons for stealth technology,” Nature Materials, 20, 4 (January 2021): 2-9.

นักบินเพียงหนึ่งคนไม่สามารถควบคุมระบบที่ซับซ้อนได้จึงต้องมีการพัฒนาระบบประมวลผลทางคอมพิวเตอร์เพื่อช่วยการบินและช่วยนักบินให้ควบคุมปฏิบัติการทั้งหมดเพื่อบรรลุเป้าหมายในการรบได้[31]

ในปัจจุบันการใช้เครื่องบินลาดตระเวนถูกแทนที่ด้วยอากาศยานไร้คนขับ (Unmanned Aerial Vehicles หรือ Drone) โดยกองทัพทหารของหลายรัฐมองว่าเครื่องบินรบแบบเดิมมีต้นทุนการบินแต่ละครั้งค่อนข้างสูง[32] อีกทั้งเครื่องบินก็มีราคาสูงและยังอาจเสี่ยงต่อการเสียชีวิตของทหารผู้ปฏิบัติการ การใช้อากาศยานไร้คนขับเพื่อการลาดตระเวนและเพื่อการโจมตีจึงเป็นการลดต้นทุนการใช้เครื่องบินรบและลดการสูญเสียกำลังพล อากาศยานไร้คนขับช่วยลดความสูญเสียงบประมาณในการรบและเพิ่มขีดความสามารถในการทำการรบได้ค่อนข้างมาก เช่นปฏิบัติการของกองทัพสหรัฐอเมริกาด้วยการใช้อากาศยานไร้คนขับ (Unmanned Arial Vehicle, Drone) เพื่อการระบุเป้าหมายและทำลายเป้าหมายในภารกิจประเทศปากีสถาน[33] อิรัก อัฟกานิสถาน โคโซโว เยเมน โซมาเลีย และลิเบีย[34] จนถึงการใช้อากาศยานไร้คนขับ Bayraktar TB2 ของประเทศยูเครนเพื่อทำลายกองทัพรัสเซีย[35] โดยในสถานการณ์การขัดกันทางอาวุธระหว่างยูเครนและรัสเซียนั้น กองทัพยูเครนใช้อากาศยานไร้คนขับ Bayraktar TB2 ในการโจมตีกองทัพรัสเซีย เป้าหมายหลักในการใช้ Bayraktar TB2 ในการโจมตีคือการทำลายรถถังและการทำลายที่ตั้งของกองทัพรัสเซียที่อยู่ในดินแดนของยูเครน การใช้อากาศยานไร้คนขับในปฏิบัติการดังกล่าวสร้างความได้เปรียบอย่างมากต่อกองทัพ

[31] Husnain Ahmad, Asra Tariq, Amir Shehzad, Muhammad S. Faheem, Muhammad Shafiq, Iqra A. Rashid, Ayesha Afza, Adnan Munir, Muhammad T. Riaz, Hafiz T. Haider, Ali Afzal, Muhammad B. Qadir, and Zubair Khaliq, "Stealth technology: Methods and composite materials—A review," Polymer Composites, (December 2019): 4469.

[32] Thomas G. Pledger, The Roles of Drones in Future Terrorist Attacks, Land Warfare Paper 137, February 2021, The Association of the United States Army, p. 2.

[33] Amnesty International, "Will I be next? US Drone Strikes in Pakistan" Amnesty International Publications, 2013, p.12. [online] Accessed: February 22, 2018. Available from: https://www.amnestyusa.org/files/asa330132013en.pdf.

[34] Craig Martin, "Target Killing, Self-Defense, and the Jus ad Bellum Regime," in Claire Finkelstein, Jens David Ohlin, Andrew Altman, Targeted Killings: Law & Morality in an Asymmetrical World, (Oxford: Oxford University Press, 2012), p. 223.

[35] Stephen Witt, "The Turkish Drone That Changed the Nature of Warfare," The New Yorker, May 16, 2022. [online] Accessed: May 20, 2022) Available from: https://www.newyorker.com/magazine/annals-of-war.

ยูเครนและเป็นการลดความสูญเสียที่จะเกิดขึ้นกับชีวิตทหารยูเครนซึ่งมีจำนวนน้อยกว่าทหารของรัสเซียด้วย[36]

ในปฏิบัติการใช้อากาศยานไร้คนขับโจมตีเป้าหมายนั้น ผู้โจมตีสามารถควบคุมอากาศยานดังกล่าวจากที่ใดก็ได้ขณะที่ผู้ถูกโจมตีสามารถป้องกันตัวได้น้อยมากและการตอบโต้กลับคงทำได้เพียงการทำลายอากาศยานไร้คนขับเท่านั้น แต่อากาศยานไร้คนขับนั้นสามารถทำลายชีวิตของผู้ถูกโจมตีได้ ซึ่งก่อให้เกิดความได้เปรียบเสียเปรียบที่แตกต่างกันอย่างมากระหว่างเป้าหมายกับผู้ปฏิบัติการ[37]

นอกเหนือจากการใช้อากาศยานไร้คนขับเพื่อการโจมตีแล้วการใช้พาหนะไร้คนขับเพื่อการขนส่งทางบกของทหารสำหรับภารกิจช่วยรบหรือการขนส่งยุทโธปกรณ์ยังมีการพัฒนาอย่างแพร่หลายมากขึ้นในปัจจุบันเพื่อทดแทนการใช้รถยนต์ทางการทหาร (ซึ่งปัจจุบันก็ยังคงมีการใช้อยู่) โดยเชื่อว่าจะเป็นการลดความสูญเสียกำลังพลและเพิ่มขีดความสามารถในการช่วยรบได้อย่างมากด้วย[38]

นอกจากการใช้อากาศยานไร้คนขับในปฏิบัติการทางทหารแล้ว ปัจจุบันบทบาทของเทคโนโลยีไซเบอร์ในกองทัพเพื่อปฏิบัติทางทหารยังเป็นที่นิยมอย่างแพร่หลาย ทั้งเพื่อประโยชน์ในการสื่อสารและเพื่อการใช้งานระบบอาวุธ กองทัพของหลายประเทศเริ่มมีความตระหนักในการจัดตั้งหน่วยปฏิบัติการทางไซเบอร์ของตนเองและมีการใช้งานปฏิบัติการทางไซเบอร์ในการขัดกันทางอาวุธมากขึ้น[39] โดยเฉพาะอย่างยิ่งกองทัพอิสราเอลมีการจัดตั้งหน่วยงานความมั่นคงทางไซเบอร์ในกระทรวงกลาโหม[40] ขณะที่ในความขัดแย้งระหว่างประเทศรัสเซียและประเทศยูเครนนั้นมีการโจมตีทั้งตามรูปแบบสงครามปกติด้วยอาวุธและกองกำลังทหารพร้อมไปกับการทำสงครามสารสนเทศ (Information warfare) และการโจมตีทางไซเบอร์ (Cyber Attack) การทำการรบสองรูปแบบไปพร้อมกันนี้มีการเรียกชื่อในทางรัฐศาสตร์การสงครามว่า “สงครามผสมผสาน” (Hybrid warfare)[41]

---

[36] Dominika Kunertova, “The war in Ukraine shows the game-changing effect of drones depend on the game,” Bulletin of the Atomic Scientists, Vol. 79, No. 2, (2023): 98-100.

[37] Ibid., p. 98.

[38] Ibid.

[39] Matthias Schulze, “Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations,” 12th International Conference on Cyber Conflict, Estonia, (2020), pp. 183-197.

[40] Lior Tabansky, “Israel Defense Forces and National Cyber Defense.” Connections 19, no. 1 (2020): 54. [online] Accessed June 20, 2022, Available from: https://www.jstor.org/stable/26934535.

[41] Neil Chuka, and Jean Francoise Born, Hybrid Warfare: Implication for CAF Force Development, Defence Research and Development Canada, Scientific Report, August 2014, p. 1. [online] Accessed June 10, 2022. Available from: https://apps.dtic.mil/sti/pdfs/AD1017608.pdf.

และในสงครามผสมผสานนี้ยังนำมาซึ่งความได้เปรียบ-เสียเปรียบทางการทหารที่แตกต่างจากสงครามรูปแบบเดิม สามารถสร้างข่าวเพื่อทำลายขวัญทหารฝ่ายตรงข้ามได้ง่ายขึ้นและเร็วขึ้น ในขณะที่การใช้ระบบอาวุธในปัจจุบันมีความเกี่ยวข้องกับการสั่งการผ่านระบบไซเบอร์และคอมพิวเตอร์มากขึ้น การทำลายระบบข้อมูลอิเล็กทรอนิกส์ของฝ่ายตรงข้ามได้ย่อมเป็นการทำให้ฝ่ายผู้ปฏิบัติการโจมตีได้เปรียบทางการทหารมากขึ้นด้วย[42]

การโจมตีทางไซเบอร์ร่วมไปกับการรบตามแบบนี้ผู้โจมตีสามารถปฏิบัติการจากพื้นที่ซึ่งอยู่ไกลจากสนามรบได้และสามารถโจมตีเป้าหมายได้ทั้งเป็นการทั่วไปและเป็นการเฉพาะ[43] การโจมตีเป็นการเฉพาะคือการโจมตีเครื่องคอมพิวเตอร์เป้าหมายหรือเครือข่ายคอมพิวเตอร์เป้าหมายเป็นการเฉพาะ เช่น การเจาะระบบรักษาความปลอดภัยของคอมพิวเตอร์เพื่อเข้าไปทำลายข้อมูลหรือระบบประมวลผลของคอมพิวเตอร์เครื่องใดเครื่องหนึ่งทางการทหาร การโจมตีเครือข่ายการสื่อสารทำได้โดยการทำลายระบบสื่อสารหน่วยใดหน่วยหนึ่งหรือทั้งระบบ เช่นการโจมตีด้วยการปฏิเสธการเข้าถึงบริการแบบ DDoS (Distributed Denial-of-Service) โดยการส่งคำขอหลายรายเข้าสู่ระบบผู้ให้บริการอินเทอร์เน็ตหนึ่งรายในเวลาเดียวกันเป็นผลให้ระบบการสื่อสารของเว็บไซต์หนึ่งๆ ล้มเหลว[44]ในขณะที่การโจมตีลักษณะทั่วไปหมายถึงการโจมตีโดยไม่ระบุเป้าหมายสามารถกระทำได้โดยการส่งโปรแกรมไวรัสเข้าไปในระบบไซเบอร์เพื่อให้เกิดกระจายไปในระบบไซเบอร์และอินเทอร์เน็ตที่ทำการเชื่อมต่อกับคอมพิวเตอร์เครื่องต่างๆ ที่สื่อสารผ่านช่องทางดังกล่าว ทำให้คอมพิวเตอร์อาจติดโปรแกรมไวรัสจากการเปิดอีเมลหรือการเข้าถึงเว็บไซต์บางเว็บไซต์ รวมถึงการบันทึกข้อมูลหรือโปรแกรมใดๆ จากอินเทอร์เน็ตเข้าสู่คอมพิวเตอร์ก็อาจนำไปสู่การได้รับโปรแกรมไวรัสเข้าสู่เครื่องคอมพิวเตอร์ได้ การกระทำลักษณะดังกล่าวเป็นปฏิบัติการที่ไม่สามารถระบุเป้าหมายเป็นการเฉพาะได้

การโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่สำคัญได้แก่การโจมตีเครือข่ายระบบอินเทอร์เน็ตของประเทศจอร์เจียในความขัดแย้งที่เมืองเซาท์ออสเซเทียซึ่งมีหลักฐานพิสูจน์ได้ว่ามีความเกี่ยวข้องกับปฏิบัติการของรัสเซีย แม้จะไม่สามารถระบุว่ามีความเกี่ยวข้องกับปฏิบัติการของ

---

[42] Ibid., p. 33.

[43] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), pp. 27-28.

[44] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communication Review, Volume 34, Issue 2, April 1, 2004, p. 40.

กองทัพรัสเซียหรือไม่[45] และการโจมตีโรงงานเพิ่มประสิทธิภาพ (Enrichment) ยูเรเนียมที่เมืองนาธานซ์ (Natanz) ประเทศอิหร่านโดยปฏิบัติการ Stuxnet ด้วยการนำมัลแวร์ Stuxnet เข้าสู่ระบบควบคุมเครื่องคัดแยกธาตุยูเรเนียม (Centrifuge) และสั่งให้ใบพัดเครื่องคัดแยกยูเรเนียมทำงานผิดปกติโดยใบพัดจะหมุนเร็วกว่าปกติระยะหนึ่งและหมุนช้ากว่าปกติระยะหนึ่งก่อให้เกิดการสึกหรอของใบพัดและส่งผลให้การคัดแยกธาตุยูเรเนียมทำได้ช้าลง จากการตรวจสอบและพิสูจน์โดยผู้เชี่ยวชาญพบว่าปฏิบัติการดังกล่าวมีเหตุเชื่อได้ว่ามาจากการกระทำโดยฝ่ายสหรัฐอเมริกา แม้จะไม่สามารถพิสูจน์ตัวผู้กระทำได้และไม่ปรากฏผู้แสดงความรับผิดชอบ[46] ขณะที่การโจมตีเครือข่ายคอมพิวเตอร์นอกสถานการณ์การขัดกันทางอาวุธในเมืองทาลลินน์ ประเทศเอสโตเนียในปี ค.ศ. 2007 ซึ่งเชื่อมโยงไปถึงปฏิบัติการของกลุ่มแฮกเกอร์ชาวรัสเซีย[47] เป็นจุดเริ่มต้นสำคัญที่ทำให้องค์กรสนธิสัญญาเพื่อการป้องกันแอตแลนติกเหนือตั้งคณะทำงานเพื่อจัดทำคู่มือทาลลินน์ว่าด้วยเรื่องการปรับใช้กฎหมายระหว่างประเทศกับสงครามไซเบอร์ (2013 Tallinn Manual on the International Law Applicable to Cyber Warfare)[48]

การขัดกันทางอาวุธในปัจจุบันยังปรากฏการใช้ระบบอาวุธที่สามารถตัดสินใจได้ด้วยตนเองหรือระบบอาวุธอิสระ (Autonomous Weapon Systems) ทั้งที่ปรากฏในรูปแบบของระบบจรวดและขีปนาวุธเพื่อป้องกันภัยทางอากาศและภาคพื้นดินและการใช้งานหุ่นยนต์สังหาร (Killer Robot)[49] ระบบป้องกันภัยทางอากาศที่ปรากฏ ได้แก่ ระบบจรวดป้องกันภัยทางอากาศ MIM-104 Patriot ของกองทัพสหรัฐที่ใช้ในปฏิบัติการอ่าวเปอร์เซียในปี ค.ศ.2003 เพื่อป้องกันการโจมตีทางอากาศจากขีปนาวุธ Scud ของกองทัพอิรัก[50] และระบบป้องกันภัยทางอากาศ Iron Dome ซึ่งเป็นที่

---

[45] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, On cyber warfare, A Chatham House Report, November 2010, p. 2.

[46] Andrew C. Foltz, "Stuxnet Schmitt Analysis, and the Cyber 'Use of Force' Debate", Joint Force Quarterly. Issue 67 (4), (2012): 44.

[47] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, On cyber warfare, p.2.

[48] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013), Introduction, p. 1. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2013).

[49] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, December 8-10, 2015. p. 44.

[50] Eliot A. Cohen, Gulf War Air Power Survey, Washington, D.C.: U.S. Government Printing, 1993). p.30.

รู้จักอย่างกว้างขวางของประเทศอิสราเอล[51] ระบบป้องกันภัยทางอากาศทั้งสองแบบแม้จะมีการใช้งานมาอย่างยาวนานแต่ก็มีพัฒนาการมาโดยตลอด ทำให้ระบบป้องกันภัยทางอากาศทั้งสองแบบมีความทันสมัยและมีความซับซ้อนมากขึ้น ในขณะที่การใช้งานหุ่นยนต์ทหารคุ้มกัน (Sentry Robot) สำหรับการป้องกันภัยภาคพื้นดินก็ปรากฏการใช้งานระบบ SGR A-1 ของประเทศสาธารณรัฐเกาหลี (ใต้) SGR A-1 เป็นระบบป้องกันภัยคุกคามภาคพื้นดินซึ่งได้ถูกนำมาติดตั้งในเขตปลอดทหารตลอดแนวพรมแดนประเทศสาธารณรัฐเกาหลี (ใต้) และประเทศสาธารณรัฐประชาธิปไตยประชาชนเกาหลี (เหนือ) ตั้งแต่ปี ค.ศ.2010 เพื่อทำหน้าที่แทนทหารในเขตดังกล่าว[52] ระบบป้องกันภัยคุกคามของ SGR A-1 สามารถปฏิบัติการได้ตลอดเวลา จึงช่วยเพิ่มขีดความสามารถแก่ทหารในการป้องกันภัยแนวพรมแดนของทั้งสองประเทศ ขณะที่ประเทศอิสราเอลมีการใช้งานหุ่นยนต์ทหารคุ้มกันในเขตพรมแดนฉนวนกาซา[53] เพื่อป้องกันภัยคุกคามภาคพื้นดินที่อาจมาจากกลุ่มผู้ประสงค์ร้ายปาเลสไตน์ ระบบป้องกันภัยภาคพื้นดินที่กล่าวมาทั้งหมดนี้ไม่ใช่หุ่นยนต์ในรูปแบบเหมือนร่างกายมนุษย์ แต่เป็นการทำงานของระบบประมวลผลทางคอมพิวเตอร์ร่วมกับระบบอาวุธให้ระบบการใช้งานอาวุธสามารถค้นหา ระบุเป้าหมายและดำเนินการโจมตีเป้าหมายแทนมนุษย์ได้

แม้จะปรากฏว่ามีความพยายามในการพัฒนาหุ่นยนต์รูปแบบเหมือนมนุษย์ (Android or Cyborg) เพื่อวัตถุประสงค์ในปฏิบัติการทางทหารแต่ยังไม่พบรายงานอย่างเป็นทางการของหุ่นยนต์สังหารรูปแบบเหมือนมนุษย์[54] ในสื่อสังคมออนไลน์อาจปรากฏภาพหรือคลิปวิดีโอการพัฒนาหุ่นยนต์ลักษณะคล้ายมนุษย์หรือสัตว์แต่หุ่นยนต์รูปแบบดังกล่าวยังไม่มีการนำมาใช้จริงในการรบ หุ่นยนต์ที่ใช้งานเพื่อปฏิบัติการทางทหารที่ปรากฏในปัจจุบันมีลักษณะเป็นพาหนะควบคุมระยะไกลซึ่งปฏิบัติการค้นหาเป้าหมายสำหรับการกู้ภัยภาคพื้นดิน หุ่นยนต์เก็บกู้วัตถุระเบิด พาหนะควบคุมระยะไกลทางทะเลและพาหนะควบคุมระยะไกลทางอากาศ[55] ฯลฯ กล่าวโดยสรุปหุ่นยนต์ทางการทหารอาจถูก

---

[51] Emily B. Landau, and Azriel Bermant. "Iron Dome protection: missile defense in Israel's security concept." In Anat Kurz and Shlomo Brom (eds.) The lessons of operation protective edge, (Tel Aviv: Institute for national Security Studies, 2014), p. 37.

[52] Cecilia Anderson, Killer Robot-Autonomous Weapons and Their Compliance with IHL, Master of Law Thesis, Faculty of Law, Lund University, 2014, p. 25.

[53] Ibid.

[54] Ibid.

[55] Ibid.

สร้างขึ้นมาทั้งเพื่อทดแทนทหารในการรบและรวมถึงการปฏิบัติการอื่นๆ เพื่อเหตุผลทางมนุษยธรรมด้วย

ในอีกมุมมองหนึ่ง เทคโนโลยีที่ใช้ในการรบทางการทหารมีความสัมพันธ์บางประการที่เกี่ยวข้องกับการใช้เทคโนโลยีในก่อการร้ายด้วย เช่นในการก่อการร้ายวันที่ 11 กันยายน ค.ศ. 2001 (เหตุการณ์ 911) มีการเชื่อมโยงถึงอาวุธที่ผู้ก่อการร้ายใช้ในการยึดเครื่องบินของสายการบิน American Airline จำนวน 2 ลำ และเครื่องบินของสายการบิน United Airline อีกจำนวน 2 ลำเพื่อโจมตีอาคาร World Trade Center และอาคารกระทรวงกลาโหมของสหรัฐอเมริกา ว่าอาจเกี่ยวข้องกับการใช้อาวุธที่ไม่สามารถตรวจจับได้ในสนามบินซึ่งเป็นผลมาจากการพัฒนาทางเทคโนโลยีในขณะนั้นที่ทำให้ผู้ก่อการร้ายสามารถเลือกวัตถุที่ไม่ใช่อาวุธไปประกอบเป็นอาวุธบนเครื่องบินเพื่อทำการก่อการร้ายได้[56]

ในการสืบสวนคดีเกี่ยวกับการก่อการร้ายในเหตุการณ์ 911 นั้นไม่พบข้อสรุปที่ชัดเจนว่าอาวุธที่ผู้ก่อการร้ายใช้ในการยึดเครื่องบินคือสิ่งใด (แต่มีข้อสันนิษฐานว่าอาจเป็นมีดเนื่องจากในช่วงเวลาดังกล่าวข้อกำหนดการบินยังอนุญาตให้ผู้โดยสารสามารถนำมีดขนาดไม่เกิน 4 นิ้วขึ้นเครื่องบินได้) แต่การก่อการร้ายในเหตุการณ์ 911 นั้นส่งผลต่อองค์การบริหารการบินแห่งชาติของสหรัฐอเมริกา (The Federal Aviation Administration: FAA) ที่จะต้องพิจารณากฎเกณฑ์และเงื่อนไขในการโดยสารอากาศยานพลเรือนใหม่และกำหนดให้มาตรการตรวจผู้โดยสารก่อนขึ้นเครื่องบินจะต้องมีการดำเนินการโดยละเอียด เช่นการตรวจสอบรองเท้า กระเป๋าเงิน เครื่องคอมพิวเตอร์พกพาทุกชนิดและอุปกรณ์ที่เกี่ยวข้องจะต้องถูกนำออกจากกระเป๋าเดินทางทั้งหมดเพื่อผ่านเครื่องตรวจสอบ ในขณะที่กระเป๋าเดินทางที่พกติดตัวขึ้นเครื่องบินนั้นจะต้องมีการตรวจสอบผ่านเครื่องสแกน 3 มิติ รวมถึงการห้ามนำของเหลวที่เกิน 3.4 ออนซ์ (100 มิลลิลิตร) ติดตัวขึ้นเครื่องบินด้วย[57]

มาตรการต่างๆ เหล่านี้เป็นผลมาจากเหตุการณ์ก่อการร้ายในหลายเหตุการณ์รวมกัน เช่น การก่อวินาศกรรมด้วยระเบิดในรองเท้าเกิดในวันที่ 22 ธันวาคม ค.ศ.2001 จากการที่นาย Richard Reid ผู้โดยสารสายการบิน American Airline ซึ่งเดินทางจากปารีสมาที่สนามบินไมอามี ทำการ

---

[56] Katherine Huiskes, “The September 11 Terrorist Attack,” UAV/Miller Center, [online] Accessed: January 30, 2022. Available from: https://millercenter.org/remembering-september-11/september-11-terrorist-attacks,

[57] David Schaper, “It was shoes on, no boarding pass or ID but airport security forever changed on 9/11.” NPR, September 10, 2021. Accessed: January10, 2022, Available from: https://www.npr.org/2021/09/10/1035131619/911-travel-timeline-tsa#:~:text=It's%20not%20 clear%20what%20exactly, it%20wouldn't%20have%20mattered.

บรรจุวัตถุระเบิดในรองเท้าก่อนจะจุดชนวนระเบิดขณะที่เครื่องอยู่ในการบินแต่ไม่สำเร็จเนื่องจากรองเท้าเปียกฝนจนทำให้ตัวจุดชนวนไม่สามารถทำงานได้ จากการสืบสวนพบว่าในรองเท้าของนาย Richard มีวัตถุระเบิดมากพอที่จะทำให้เครื่องบินเกิดความเสียหายได้[58] ขณะที่การห้ามนำของเหลวขึ้นเครื่องบินนั้นเป็นเหตุมาจากการที่เจ้าหน้าที่อังกฤษได้ทำการตรวจพบว่ามีผู้วางแผนการก่อการร้ายด้วยการจุดชนวนระเบิดชนิดเหลวซึ่งปลอมแปลงมาในรูปของน้ำอัดลมขนาด 500 มิลลิลิตร บรรจุในขวดพลาสติก โดยระเบิดชนิดเหลวเหล่านี้มีการบรรทุกไว้ในเครื่องบินจำนวน 10 ลำซึ่งจอดอยู่ที่สนามบินในลอนดอนและมีเป้าหมายในการเดินทางไปยังเมืองต่างๆ ในประเทศสหรัฐอเมริกาและแคนาดา เหตุการณ์ดังกล่าวเกิดขึ้นในเดือนสิงหาคม ค.ศ. 2006 เป็นผลให้หน่วยงานด้านความปลอดภัยในการเดินทางของสหรัฐอเมริกา (Transportation Security Administration: TSA) ห้ามผู้โดยสารนำของเหลว เจล และวัสดุอัดแก๊สขึ้นเครื่องบิน แต่ต่อมาในเดือนกันยายน ค.ศ.2006 TSA ก็ยอมให้ผู้โดยสารสามารถนำของเหลวที่มีปริมาณไม่เกิน 3.4 ออนซ์ (100 มิลลิลิตร) ขึ้นเครื่องบินได้โดยจะต้องนำออกแสดงให้เจ้าหน้าที่ตรวจสอบก่อนขึ้นเครื่องบินด้วย[59]

ในเดือนธันวาคม ค.ศ.2009 นาย Umar Farouk Abdulmutallab ผู้ก่อการร้ายของกลุ่ม Al-Qaeda ได้ถูกจับกุมเนื่องจากพยายามนำสารผลิตระเบิดที่แอบซ่อนในชุดชั้นในไปผสมในห้องน้ำเครื่องบินระหว่างโดยสารไปกับสายการบิน Northwest Airlines ซึ่งเดินทางจากเมืองอัมสเตอร์ดัมไปเมืองดีทรอยต์แต่ระเบิดไม่ทำงานเนื่องจากมีความชื้นมากเกินไป ทำให้ TSA ประกาศมาตรการสแกนร่างกายบุคคลก่อนการโดยสารเครื่องบินทุกครั้ง ตั้งแต่เดือนมีนาคม ค.ศ.2010 เป็นต้นมา[60]

เหตุการณ์ก่อการร้ายโดยการนำสิ่งที่สามารถนำไปผสมหรือประกอบเพื่อเป็นวัตถุระเบิดในเหตุการณ์ก่อการร้ายหลายเหตุการณ์สะท้อนให้เห็นว่าผู้ก่อการร้ายมีการประยุกต์เอาเทคโนโลยีต่างๆ และนำเอาวัสดุที่มิใช่อาวุธโดยสภาพมาใช้ให้เป็นอาวุธเพื่อการทำลายได้[61] ทำให้มาตรการในการต่อต้านการก่อการร้ายในการบินพาณิชย์ระหว่างประเทศต้องเข้มงวดมากขึ้น

ความตื่นตัวของคณะกรรมการกาชาดระหว่างประเทศเรื่องเทคโนโลยีใหม่ที่มีบทบาทต่อการขัดกันทางอาวุธ เริ่มต้นปรากฏในปี ค.ศ.2011 โดยคณะกรรมการกาชาดระหว่างประเทศได้จัดการประชุมครั้งที่ 31 มีการพิจารณาประเด็นเกี่ยวกับบทบาทของเทคโนโลยีใหม่ในการขัดกันทางอาวุธ และ

---

[58] David Schaper, “It was shoes on, no boarding pass or ID but airport security forever changed on 9/11.”

[59] Ibid.

[60] Ibid.

[61] Christopher Coker, Waging War Without Warriors?: The Changing Culture of Military Conflict. (London: Lynne Rienner Publisher, 2002) p.3.

ข้อท้าทายที่เกิดขึ้นต่อกฎหมายมนุษยธรรมระหว่างประเทศ ในที่ประชุมดังกล่าวได้มีการพิจารณาเทคโนโลยีสองรูปแบบคือปฏิบัติการสงครามทางไซเบอร์ (Cyber warfare) และการใช้ระบบอาวุธที่สามารถตัดสินใจได้ด้วยตนเองหรือระบบอาวุธอิสระ (Autonomous Weapons Systems) โดยประเด็นดังกล่าวได้ถูกหยิบยกขึ้นมาพิจารณาอีกครั้งในการประชุมครั้งที่ 32 ใน ค.ศ. 2015[62]

ที่ประชุมของคณะกรรมการกาชาดระหว่างประเทศมีความเห็นว่าการใช้งานระบบไซเบอร์ในการขัดกันทางอาวุธก่อให้เกิดข้อท้าทายต่อหลักกฎหมายมนุษยธรรมระหว่างประเทศหลายประการ ได้แก่

ประการที่ 1 ปัญหาของการใช้ระบบเครือข่ายทางไซเบอร์ที่ส่งผลต่อการแยกแยะเป้าหมายการโจมตี เนื่องจากพื้นที่ไซเบอร์โดยปกติไม่มีการแบ่งแยกพื้นที่เฉพาะของทหารกับพลเรือน แม้จะสามารถแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ได้ (เช่น ระบบอินเทอร์เน็ตและอินทราเน็ต) แต่เมื่อไรก็ตามที่มีการสื่อสารผ่านระบบอินเทอร์เน็ตแบบ world wide web ทุกเครือข่ายคอมพิวเตอร์จะอยู่ในพื้นที่ไซเบอร์เดียวกัน ยิ่งไปกว่านั้น เว็บไซต์ต่างๆ ที่จำเป็นต่อการใช้งานระบบบริการสาธารณะอันเป็นประโยชน์ต่อทั้งพลเรือนและทหารอาจตกเป็นเป้าหมายในการโจมตีได้ เพราะอาจเกี่ยวข้องกับขีดความสามารถในการทำการรบทางการทหาร หากมีการโจมตีระบบดังกล่าวย่อมส่งผลกระทบต่อทั้งขีดความสามารถในปฏิบัติการทางทหารและการใช้งานของพลเรือน[63]

ประการที่ 2 ปัญหาของการแยกแยะผู้ใช้ปฏิบัติการทางไซเบอร์ เนื่องจากในโลกไซเบอร์มีลักษณะของความเป็นโลกเสมือน (virtual reality)[64] การระบุตัวตนของผู้ใช้งานกับตัวตนที่ปรากฏในพื้นที่ไซเบอร์ไม่สามารถกระทำได้ในทันที แม้จะระบุที่มาของข้อมูลและ IP address ของเครื่องมือสื่อสารที่ใช้งานได้ก็ตาม แต่การระบุว่าใครเป็นผู้ใช้งานและการพิสูจน์ว่าตัวตนที่ปรากฏในโลกไซเบอร์สัมพันธ์กับตัวตนของผู้ใช้งานจริงเป็นเรื่องที่ยาก ทั้งนี้เหตุการณ์ที่เกิดขึ้นที่เมืองทาลลินน์ในปี ค.ศ. 2007 สะท้อนให้เห็นปัญหานี้เป็นอย่างดี แม้จะมีการตรวจสอบได้ว่าการปฏิบัติการโจมตีทางไซเบอร์มีหลักฐานเชื่อได้ว่ามาจากประเทศรัสเซียและน่าจะเป็นผู้กระทำการชาวรัสเซีย แต่การจะระบุว่าเป็นผู้ใดมีสถานะเป็นทหารหรือพลเรือนไม่สามารถทำได้ง่าย แม้จะมีการกล่าวหารัฐบาลรัสเซียแต่ก็ไม่สามารถใช้หลักฐานใดยืนยันตัวบุคคลผู้กระทำการอย่างชัดเจนได้[65]

---

[62] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, December 8-10, 2015. p. 44.

[63] Ibid., p. 44.

[64] Ibid.

[65] Ibid.

ปฏิบัติการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธที่อาจเกิดขึ้นได้จากทั้งการกระทำของพลเรือนและโดยทหารนี้ก่อให้เกิดข้อท้าทายต่อทั้งการปฏิบัติการตอบโต้ต่อเป้าหมายและการให้ความคุ้มครองต่อพลเรือน การพิจารณาความได้สัดส่วนในการโจมตีและการระมัดระวังล่วงหน้าก่อนการโจมตี เพราะปฏิบัติการแต่ครั้งมีเงื่อนไขที่จะต้องพิจารณาอย่างถี่ถ้วนเป็นอย่างมาก หากเกิดความผิดพลาดอาจเกิดความเสียหายแก่พลเรือนที่ไม่เกี่ยวข้องโดยตรงในการรบและอาจเกิดความเสียหายต่อระบบสาธารณูปโภคของพลเรือนที่เกี่ยวข้องกับเครือข่ายการทำงานคอมพิวเตอร์ด้วย[66] ซึ่งความเสียหายแก่พลเรือนที่มากกว่าความจำเป็นทางการทหารจะนำไปสู่การละเมิดต่อหลักความได้สัดส่วนตามกฎหมายมนุษยธรรมระหว่างประเทศ

นอกเหนือจากการใช้งานเทคโนโลยีไซเบอร์ในการขัดกันทางอาวุธแล้ว ระบบอาวุธที่ตัดสินใจได้ด้วยตนเองหรือระบบอาวุธอิสระ (Autonomous Weapon Systems) ที่มีบทบาททางการทหารอย่างมากในปัจจุบันถือได้ว่ามีองค์ประกอบของการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence) ร่วมกับระบบอาวุธมากขึ้น[67] เมื่อเกี่ยวข้องกับระบบปัญญาประดิษฐ์นี้ก็ย่อมเกี่ยวข้องกับอัลกอริที่มในระบบประมวลผลของคอมพิวเตอร์ การควบคุมหรือจำกัดพัฒนาการโปรแกรมคอมพิวเตอร์ อัลกอริที่มและระบบปัญญาประดิษฐ์โดยรวมจึงเป็นเรื่องที่มีความซับซ้อนเพราะต้องพิจารณาความเหมาะสมระหว่างการใช้งานเพื่อประโยชน์ทางสันติและการใช้งานเพื่อประโยชน์ทางทหารในการรบ

การใช้งานปัญญาประดิษฐ์ก่อให้เกิดข้อวิพากษ์เกี่ยวกับปัญหาต่อหลักความได้สัดส่วนในการโจมตีในกรณีที่ระบบอาวุธสามารถทำงานด้วยตัวเองได้เต็มรูปแบบซึ่งอาจนำไปสู่ปัญหาในการจำกัดความเสียหายที่เกิดจากปฏิบัติการของระบบอาวุธ รวมตลอดถึงมีข้อวิพากษ์ทั้งในการใช้งานปัญญาประดิษฐ์เกี่ยวกับปัญหาทางด้านจริยธรรมในปฏิบัติการทางทหาร[68] เพราะมนุษย์จะมีส่วนเกี่ยวข้องในสนามรบน้อยลง ในขณะที่ระบบอาวุธตัดสินใจได้ด้วยตนเองนั้นมีแนวโน้มที่จะปฏิบัติการเป็นอิสระด้วยตัวเองมากขึ้น

สถานการณ์การใช้เทคโนโลยีในการขัดกันทางอาวุธในปัจจุบันสร้างความเคลื่อนไหวในสังคมนักกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งแนวคิดว่ากฎหมายมนุษยธรรมระหว่างประเทศตามที่ปรากฏใน

---

[66] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, (2015), pp. 39-44.

[67] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p.26.

[68] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, (2015), p. 44.

อนุสัญญาเจนีวา ค.ศ. 1949 พิธีสารเพิ่มเติม ค.ศ.1977 และอนุสัญญาอื่นๆ ที่เกี่ยวข้องซึ่งมีอยู่แต่เดิมนั้นมีความล้าหลังเกินไปหรือไม่ ควรมีการสร้างกฎหมายใหม่เพื่อการควบคุมอาวุธเฉพาะอย่างให้มากขึ้นหรือไม่เพียงใด

ทั้งนี้ หากพิจารณาจากหลักกฎหมายมนุษยธรรมระหว่างประเทศที่มุ่งควบคุมและจำกัดปฏิบัติการต่างๆ ในกรณีที่เกิดข้อพิพาททางอาวุธนั้นอาจพิจารณาได้ในหลากหลายมิติด้วยกัน ได้แก่

ประการที่ 1 หลักกฎหมายมนุษยธรรมระหว่างประเทศมีหลักการพื้นฐานที่ครอบคลุมปฏิบัติการทางทหาร กฎหมายมนุษยธรรมระหว่างประเทศ มีเป้าหมายในการสร้างสมดุลระหว่างความมีมนุษยธรรมและความรุนแรงที่เกิดขึ้นในการขัดกันทางอาวุธที่เป็นไปเพื่อวัตถุประสงค์ทางการทหาร หลักการทางกฎหมายมนุษยธรรมระหว่างประเทศจึงมิได้มีหลักการเฉพาะแต่เรื่องการคุ้มครองบุคคลแต่ยังมีหลักการจำกัดการใช้อาวุธ ซึ่งมีความครอบคลุมถึงการจำกัดการใช้วิธีและปัจจัยต่างๆ ในการขัดกันทางอาวุธให้เป็นไปเพียงเพื่อความได้เปรียบทางการรบเท่าที่จำเป็นสำหรับปฏิบัติการทางทหารภายใต้หลักเกณฑ์พื้นฐานเพื่อคุ้มครองพลเรือนจากผลกระทบที่เกิดขึ้นจากปฏิบัติการทางทหารด้วย โดยหลักการในการจำกัดอาวุธ วิธีและปัจจัยในการรบนั้นเป็นหลักการที่มีขอบเขตกว้างขวางและครอบคลุมปฏิบัติการทางทหารเกือบทุกประการ การใช้เทคโนโลยีใดๆ ก็ตามเพื่อประโยชน์ในการขัดกันทางอาวุธย่อมตกอยู่ภายใต้หลักการนี้เสมอ ไม่ว่าการใช้เทคโนโลยีนั้นจะอยู่ในรูปแบบของการใช้อาวุธหรือการใช้เป็นวิธีการในการรบก็ตามและไม่ว่าเทคโนโลยีนั้นจะมีพัฒนาการขึ้นในช่วงระยะเวลาใดๆ ก็ตาม

ประการที่ 2 กฎหมายมนุษยธรรมระหว่างประเทศมีข้อจำกัดการใช้อาวุธทั้งหลักทั่วไปและกฎหมายเฉพาะ กฎหมายมนุษยธรรมระหว่างประเทศซึ่งมีข้อจำกัดในการใช้อาวุธ ปรากฏในสองรูปแบบ คือ ข้อจำกัดทั่วไปที่ปรากฏในข้อ 35 ของพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ.1977 ของอนุสัญญาเจนีวา ค.ศ. 1949 เรื่องการจำกัดอาวุธ วิธีและปัจจัยในการขัดกันทางอาวุธและการห้ามใช้อาวุธในอนุสัญญาระหว่างประเทศเฉพาะเรื่อง ดังนั้น การใช้เทคโนโลยีต่างๆ เพื่อเป็นอาวุธและการใช้เทคโนโลยีต่างๆ ประกอบร่วมกับการใช้อาวุธหรือประกอบร่วมกับปฏิบัติการทางทหารในการรบ ย่อมตกอยู่ภายใต้ข้อจำกัดทั่วไปทั้งตามข้อ 35 ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ. 1977 ของอนุสัญญาเจนีวา และโดยอนุสัญญาจำกัดการใช้อาวุธเฉพาะอย่าง ทางใดทางหนึ่งหรือทั้งสองทางอยู่ไม่มากก็น้อย

อย่างไรก็ดี นักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายคนยังมีความเห็นที่หลากหลายเกี่ยวกับประเด็นเรื่องความเพียงพอของกฎหมายมนุษยธรรมระหว่างประเทศเช่นอนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติมที่จะนำมาปรับใช้กับเทคโนโลยีใหม่ ทั้งมุมมองว่ากฎหมายที่สร้างขึ้นมาแต่เดิมนั้นมีวัตถุประสงค์ที่จะใช้กับสงครามรูปแบบเดิมที่ทหารของสองรัฐคู่ภาคีทำการรบกันใน

ภาคพื้นดิน น้ำและอากาศ แต่ไม่มีหลักการใดที่จะปรับใช้กับพื้นที่ทางไซเบอร์ได้ สิ่งที่กฎหมายมนุษยธรรมระหว่างประเทศต้องการคุ้มครองรูปแบบดั้งเดิมคือชีวิตพลเรือนและผู้ที่กฎหมายมุ่งคุ้มครองรวมตลอดถึงทรัพย์สินที่มีลักษณะทางกายภาพแต่ความเสียหายในปัจจุบันอาจเกิดได้ทั้งทางกายภาพและที่ไม่ใช่ทางกายภาพเช่นความเสียหายต่อข้อมูลดิจิทัล ความพยายามในการแยกพลเรือนออกจากพลรบเพื่อคุ้มครองพลเรือนไม่ให้ตกเป็นเป้าหมายในการโจมตีตามแนวคิดเดิมกำลังถูกท้าทายด้วยสงครามในปัจจุบันที่พลเรือนมีส่วนเกี่ยวข้องกับการรบมากขึ้น รวมตลอดถึงการใช้งานเทคโนโลยีในรูปแบบที่ไม่ใช่อาวุธแต่อาจเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธได้ก็นำไปสู่ทั้งปัญหาการแยกแยะเป้าหมายในการโจมตี ความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตีในขณะที่กฎหมายมนุษยธรรมระหว่างประเทศแบบดั้งเดิมอาจให้ความสำคัญกับสิ่งที่เป็นอาวุธหรือวิธีการใช้อาวุธมากกว่า ข้อท้าทายเหล่านี้ส่งผลกระทบไม่มากก็น้อยต่อความเคลื่อนไหวของสังคมนักกฎหมายมนุษยธรรมระหว่างประเทศในปัจจุบันที่ยังคงหาข้อสรุปไม่ได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศสามารถปรับใช้กับเทคโนโลยีใหม่ได้ทุกกรณีหรือไม่

การศึกษาวิจัยนี้จะเป็นการชี้ให้เห็นว่าประเด็นปัญหาเกี่ยวกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นยังไม่เป็นที่ยุติเนื่องจากความซับซ้อนของเทคโนโลยีในการสู้รบและผลกระทบที่เกิดจากการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับปรากฏการณ์ของการขัดกันทางอาวุธในปัจจุบัน

1.2 วัตถุประสงค์ในการศึกษาวิจัย

1) เพื่อศึกษานัยสำคัญของเทคโนโลยีใหม่ในการขัดกันทางอาวุธกับกฎหมายระหว่างประเทศและกฎหมายมนุษยธรรมระหว่างประเทศ

2) เพื่อศึกษาวิเคราะห์ปัญหาและข้อท้าทายต่างๆ ที่เกิดจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธที่สร้างผลกระทบต่อหลักการของกฎหมายมนุษยธรรมระหว่างประเทศ

3) เพื่อศึกษาวิเคราะห์แนวทางในการพัฒนาการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศที่มีความครอบคลุมต่อพัฒนาการการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธในปัจจุบัน ซึ่งจะเป็นประโยชน์ในการแก้ไขปัญหาและข้อท้าทายต่างๆ ที่เกิดขึ้น

1.3 สมมติฐาน

หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมีลักษณะเป็นการทั่วไปที่สามารถนำไปปรับใช้กับสถานการณ์ที่เปลี่ยนแปลงไปได้ โดยทั่วไปการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศดังกล่าวนี้สะท้อนให้เห็นถึงการเป็นระบบกฎหมายที่ปรับใช้กับสถานการณ์การขัดกันทางอาวุธในปัจจุบันที่เปลี่ยนไปจากเดิมโดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีใหม่ในฐานะเป็นวิธีการหรือปัจจัยในการสู้รบ กระนั้น กฎหมายมนุษยธรรมระหว่างประเทศยังคงมีขีดจำกัดของความสามารถในการปรับตัวของหลักการที่ทำให้ไม่สามารถนำไปปรับใช้กับกรณีที่มีการใช้เทคโนโลยีใหม่ได้อย่างเหมาะสม

1.4 ขอบเขตของการวิจัย

การศึกษาวิจัยในวิทยานิพนธ์ฉบับนี้เป็นการศึกษาแนวทางการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับกรณีการใช้เทคโนโลยีในปัจจุบันทางการทหารเพื่อการขัดกันทางอาวุธ โดยให้ความสำคัญกับเทคโนโลยีไซเบอร์ พาหนะไร้คนขับ ระบบอาวุธอิสระ เทคโนโลยีการสื่อสารผ่านดาวเทียมเพื่อประกอบการทำงานของอาวุธและเทคโนโลยีนาโนเพื่อการทหารที่มีการใช้งานในปัจจุบัน การศึกษาเน้นการวิเคราะห์ผลกระทบที่เกิดขึ้นจากการใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายมนุษยธรรมระหว่างประเทศ ปัญหาและข้อท้าทายต่างๆ ที่เกิดขึ้นจากการใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธ และการศึกษาแนวทางในการพัฒนากฎหมายมนุษยธรรมระหว่างประเทศที่จะนำไปสู่การปรับใช้กฎหมายที่ครอบคลุมต่อสถานการณ์การขัดกันทางอาวุธซึ่งเปลี่ยนแปลงไปในบริบทของการใช้เทคโนโลยีในปัจจุบัน โดยการศึกษาแบ่งเป็นส่วนต่างๆ ดังนี้

1. ศึกษาที่มาและความสำคัญของปัญหาของการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ ความสัมพันธ์ระหว่างเทคโนโลยีที่ใช้ในการขัดกันทางอาวุธและกฎหมายมนุษยธรรมระหว่างประเทศ นัยสำคัญของการใช้เทคโนโลยีทางการทหารในปัจจุบันซึ่งส่งผลกระทบต่อรูปแบบการขัดกันทางอาวุธอันอาจส่งผลต่อการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศ

2. ศึกษาข้อท้าทาย หรือประเด็นปัญหาที่อาจเกิดขึ้นจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายมนุษยธรรมระหว่างประเทศ

3. ศึกษาแนวทางในการพัฒนากฎหมายมนุษยธรรมระหว่างประเทศเพื่อให้มีความครอบคลุมถึงการปรับใช้กับพัฒนาการทางเทคโนโลยี

1.5 วิธีการศึกษาและวิจัย

การศึกษาวิจัยในวิทยานิพนธ์ฉบับนี้เป็นการวิจัยเชิงเอกสาร (Documentary Research) ทั้งภาษาไทยและภาษาต่างประเทศ เกี่ยวกับเรื่องแนวทางในการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศต่อกรณีการใช้เทคโนโลยีใหม่ในปัจจุบันเมื่อเกิดการขัดกันทางอาวุธ ปัญหาและข้อท้าทายต่อหลักกฎหมายมนุษยธรรมระหว่างประเทศที่เกิดจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ และแนวทางในการแก้ไขปัญหาและข้อท้าทายที่เกิดจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ โดยใช้ข้อมูลในสองระดับคือ

ข้อมูลระดับปฐมภูมิ (Primary Resource) โดยการศึกษาจากอนุสัญญาเจนีวา ค.ศ. 1949 ทั้ง 4 ฉบับ และพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1977 ฉบับที่ 1 และฉบับที่ 2 และอนุสัญญากรุงเฮก ค.ศ.1899 และ ค.ศ.1907 รวมตลอดถึงกฎหมายระหว่างประเทศอื่นที่เกี่ยวข้อง

ข้อมูลระดับทุติยภูมิ (Secondary Resource) ทำการศึกษาจากบทความทางวิชาการ หนังสือ งานวิจัย วิทยานิพนธ์ ความคิดเห็นของนักกฎหมาย และข้อมูลจากแหล่งอื่นๆ เกี่ยวกับปัญหาที่เกิดจากการใช้เทคโนโลยีในปัจจุบันในการขัดกันทางอาวุธและผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศ รวมตลอดถึงข้อท้าทายต่างๆ เพื่อนำไปสู่แนวทางในการพัฒนาการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศ

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษาวิจัย

1) ทราบนัยสำคัญของเทคโนโลยีใหม่ในการขัดกันทางอาวุธกับกฎหมายระหว่างประเทศและกฎหมายมนุษยธรรมระหว่างประเทศ

2) ทราบปัญหาและข้อท้าทายต่างๆ ที่เกิดจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธที่สร้างผลกระทบต่อหลักการของกฎหมายมนุษยธรรมระหว่างประเทศ

3) สามารถนำเสนอแนวทางในการพัฒนาการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศที่มีความครอบคลุมต่อพัฒนาการการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธในปัจจุบัน ซึ่งจะเป็นประโยชน์ในการแก้ไขปัญหาและข้อท้าทายต่างๆ ที่เกิดขึ้น

1.7 ทบทวนวรรณกรรม

ในการศึกษาวิจัยนี้ได้มีการทบทวนวรรณกรรมที่เกี่ยวข้องกับการปรับใช้กฎหมายกับการใช้เทคโนโลยีชนิดต่างๆ และพบว่างานวรรณกรรมที่เกี่ยวข้องกับกฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่ ปรากฏในวิทยานิพนธ์ งานวิจัย และบทความทางวิชาการมีอยู่ค่อนข้างหลากหลาย ส่วนใหญ่มักเป็นการศึกษาเทคโนโลยีเฉพาะอย่างในหนึ่งงาน เช่น การศึกษาประเด็นทางกฎหมายเกี่ยวกับการโจมตีทางไซเบอร์กับกฎหมายมนุษยธรรมระหว่างประเทศ การศึกษาประเด็นการใช้ระบบอาวุธอิสระ (Autonomous Weapon Systems) กับกฎหมายมนุษยธรรมระหว่างประเทศ การศึกษาประเด็นการใช้อากาศยานไร้คนขับกับกฎหมายมนุษยธรรม ฯลฯ ส่วนงานที่กล่าวถึงเทคโนโลยีใหม่กับกฎหมายมนุษยธรรมระหว่างประเทศในภาพรวมนั้น ปรากฏในงานประชุมทางวิชาการ และบทความทางวิชาการเท่านั้น ยังไม่มีการศึกษาวิจัยประเด็นเทคโนโลยีใหม่ในภาพรวม จึงยังขาดการศึกษาวิจัยลักษณะร่วมกันของเทคโนโลยีชนิดต่างๆ ซึ่งก่อให้เกิดข้อท้าทายต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ งานวิจัยชิ้นนี้จึงเป็นส่วนเติมเต็มการศึกษาวิจัยงานชิ้นต่างๆ

งานศึกษาวิจัยทางวิชาการที่เกี่ยวข้องกับเทคโนโลยีใหม่กับกฎหมายมนุษยธรรมระหว่างประเทศที่มีความสำคัญและเกี่ยวข้องกับการศึกษาวิจัยฉบับนี้ ปรากฏดังนี้

(1) งานวิชาการที่เกี่ยวข้องกับการปรับใช้หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศกับปฏิบัติการทางไซเบอร์

ผู้วิจัยได้รวบรวมงานชิ้นสำคัญที่เกี่ยวข้องกับการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศกับกรณีการใช้ปฏิบัติการทางไซเบอร์ และลักษณะของสงครามไซเบอร์ที่เปลี่ยนแปลงรูปแบบของสงครามดั้งเดิม โดยปรากฏงานวิชาการดังต่อไปนี้

(1.1) สงครามทางไซเบอร์กับกฎหมายสงคราม

งานดุษฎีนิพนธ์ของ Dinniss ซึ่งตีพิมพ์เป็นหนังสือในปี ค.ศ.2012 ในชื่อ Cyber Warfare and the Laws of War เป็นผลมาจากความสนใจในสถานการณ์การโจมตีทางไซเบอร์ซึ่งเกิดขึ้นที่เมือง Tallinn ประเทศเอสโตเนีย ในปี ค.ศ.2007 และการใช้การโจมตีด้วยมัลแวร์ Stuxnet ต่อเครื่องคัดแยกนิวเคลียร์ในประเทศอิหร่าน[69] อันสังเกตได้จากบทนำของงานศึกษาวิจัยเรื่องนี้ที่ให้ลำดับความสำคัญกับสองกรณีดังกล่าว

[69] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, (New York: Cambridge University Pres, 2012), p. 3.

ระเบียบวิธีวิจัยของงานนี้ใช้การศึกษาวิจัยเชิงเอกสารเป็นสำคัญ โดยให้ความสำคัญกับกฎหมายระหว่างประเทศที่สามารถปรับใช้กับปฏิบัติการทางไซเบอร์ได้ ซึ่งกฎหมายระหว่างประเทศที่นำมาใช้พิจารณาประกอบด้วยกฎหมายระหว่างประเทศทั้งที่เป็น Lex Lata และ Lex Ferenda เนื่องจากการพิจารณากฎหมายระหว่างประเทศที่จะปรับใช้กับเรื่องปฏิบัติการทางไซเบอร์โดยตรงนั้นไม่มีในขณะนั้น สิ่งที่ Dinniss พิจารณาว่าสิ่งที่จำเป็นต่อการนำมาปรับใช้คือ หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศ หลักกฎหมายที่ศาลยุติธรรมระหว่างประเทศได้นำมาใช้เพื่อการพิจารณาคดี รวมถึงการตีความของศาลยุติธรรมระหว่างประเทศ เช่นกรณี Nuclear Weapons case รวมตลอดถึงหลักการที่ปรากฏใน Hague Regulations สิ่งที่งานวิจัยนี้ยังค้นพบค่อนข้างน้อยคือกฎเกณฑ์ในรูปแบบ Soft Law หรือ Lex Ferenda[70]

นอกจากนี้ Dinniss มีความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศที่ปรากฏตามหลักการพื้นฐาน เช่น หลักการห้ามใช้วิธีการทางสงครามที่จะก่อให้เกิดความทุกข์ทรมานเกินความจำเป็น หลักการแยกแยะระหว่างพลเรือนและพลรบ รวมตลอดถึงหลักความได้สัดส่วนในปฏิบัติการทางทหาร เป็นพื้นฐานสำคัญที่สามารถปรับใช้ได้เสมอ เพราะเป็นหลักการที่อยู่บนแนวคิดว่าลักษณะของสงครามไม่เคยเปลี่ยนแปลงไป ในขณะที่อนุสัญญาระหว่างประเทศเฉพาะเรื่องที่เกี่ยวข้องกับการควบคุมอาวุธนั้นมักจะให้ความสำคัญกับลักษณะเฉพาะของสงครามในแต่ละช่วงเวลาที่แตกต่างกัน กฎหมายจึงเกิดขึ้นมากมายจากอาวุธแต่ละชนิดในสงครามแต่ละครั้ง รวมถึงยุทธวิธีที่เกิดขึ้นหลากหลายในการทำสงครามแต่ละครั้ง แต่หากพิจารณาเหตุผลของหลักพื้นฐานทางกฎหมายมนุษยธรรมระหว่างประเทศแล้ว จะพบว่าหลักการพื้นฐานเหล่านั้นสามารถปรับใช้กับอาวุธทุกชนิด นอกจากนั้นกฎหมายมนุษยธรรมระหว่างประเทศยังสามารถปรับใช้กับเทคโนโลยีต่างๆ ได้เช่นกัน[71]

งานวิจัยของ Dinniss แบ่งการนำเสนอเป็น 2 ส่วน คือกฎหมายระหว่างประเทศที่ว่าด้วยเรื่องหลักเกณฑ์ที่ใช้ก่อนการขัดกันทางอาวุธ (Jus ad Bellum) และหลักเกณฑ์ที่ใช้ระหว่างที่เกิดการขัดกันทางอาวุธ (Jus in Bello) ซึ่งตามเนื้อหาดังกล่าวค่อนข้างมีความคล้ายคลึงกับ Tallinn Manual ทั้งฉบับที่ 1 และฉบับที่ 2 แต่งานวิจัยฉบับนี้ไม่ได้กล่าวอ้างถึงหลักการตาม Tallinn Manual โดยเหตุที่ Tallinn Manual ฉบับที่ 1 นั้นอยู่ระหว่างการดำเนินการก่อนเผยแพร่ในปี ค.ศ. 2013 งานวิจัยนี้จึงไม่มีความสัมพันธ์กับหลักการที่ปรากฏตาม Tallinn Manual โดยตรง แต่กลับมี

[70] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, pp. 30-31.

[71] Ibid., p. 31.

พื้นฐานแนวคิดที่สอดคล้องกันกับ Tallinn Manual คือความพยายามในการนำกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่แล้วมาปรับใช้กับปฏิบัติการโจมตีทางไซเบอร์

เนื้อหาของงานวิจัยฉบับนี้ไม่ได้ให้ความสำคัญกับรายละเอียดของเทคโนโลยีไซเบอร์ แต่ให้ความสำคัญกับกฎหมายมนุษยธรรมระหว่างประเทศเป็นแกนหลักในการศึกษา แล้วนำเอาลักษณะของปฏิบัติการทางไซเบอร์ที่ก่อให้เกิดปัญหาหรือข้อท้าทายต่อกฎหมายมนุษยธรรมระหว่างประเทศมาพิจารณา โดยแบ่งการพิจารณาผลทางกฎหมายของปฏิบัติการทางไซเบอร์ตั้งแต่ประเด็นการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีจะเทียบเท่าการใช้กำลังทางทหารหรือไม่ และจะนำไปสู่การจำแนกว่าเป็นการขัดกันทางอาวุธได้หรือไม่ การใช้ปฏิบัติการทางไซเบอร์อย่างไรจึงจะถือว่าเป็นการปฏิบัติการของพลรบ หรือเป็นการมีส่วนร่วมโดยตรงของพลเรือนในการขัดกันทางอาวุธ การจำแนกเป้าหมายการโจมตีทางไซเบอร์ การปรับใช้หลักการคุ้มครองสิ่งแวดล้อมและการคุ้มครองทรัพย์สินทางวัฒนธรรมระหว่างที่เกิดการขัดกันทางอาวุธ รวมตลอดถึงการพิจารณาหลักการเรื่องปัจจัยและวิธีการในการขัดกันทางอาวุธกับการใช้ไซเบอร์เพื่อการโจมตี

ผลการศึกษาวิจัยของ Dinniss สรุปว่ากฎหมายมนุษยธรรมระหว่างประเทศโดยเฉพาะอย่างยิ่งหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศนั้นสามารถปรับใช้กับปฏิบัติการทางไซเบอร์ในการขัดกันทางอาวุธได้ แต่ยังคงทิ้งประเด็นท้าทายเอาไว้บางประการ เนื่องจากกฎหมายมนุษยธรรมระหว่างประเทศดั้งเดิมนั้นให้ความสำคัญกับความเสียหายทางกายภาพเป็นสำคัญ อันได้แก่ ความตาย การบาดเจ็บ หรือความเสียหายทางทรัพย์สิน ฯลฯ ที่ปรากฏเด่นชัด แต่ความเสียหายจากปฏิบัติการทางไซเบอร์นั้นอาจมีขอบเขตที่กว้างขวางกว่ามาก เพราะเป็นไปได้ทั้งความเสียหายทางกายภาพและความเสียหายต่อระบบการสื่อสารและสารสนเทศที่ไม่ปรากฏผลทางกายภาพ[72]

ประเด็นเรื่องความเสียหายทางกายภาพนี้ส่งผลต่อการพิจารณาการโจมตีทางไซเบอร์ที่มีผลเทียบเท่าการใช้อาวุธยังจำเป็นต้องคำนึงถึงผลกระทบในระดับที่ใกล้เคียงกับผลที่เกิดจากการโจมตีด้วยอาวุธตามแบบ[73] การโจมตีและการป้องกันตนเองด้วยปฏิบัติการทางไซเบอร์จึงยังคงต้องอยู่บนพื้นฐานของหลักการใช้กำลังแบบดั้งเดิม

ประเด็นสำคัญที่ปฏิบัติการทางไซเบอร์สร้างความเปลี่ยนแปลงต่อการขัดกันทางอาวุธคือการชี้ให้เห็นความสำคัญของข้อมูลสารสนเทศซึ่งเป็นทรัพย์สินที่จับต้องไม่ได้ และสร้าง

---

[72] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 279.

[73] Ibid., p. 279.

ผลกระทบต่อการปรับใช้หลักการปฏิบัติที่เป็นปฏิปักษ์ (Conduct of Hostilities) โดยเฉพาะอย่างยิ่งการกำหนดเป้าหมายในการโจมตี และการปกป้องทรัพย์สินทางวัฒนธรรม[74]

อย่างไรก็ดีงานของ Dinniss ไม่ได้ให้ความสำคัญกับเรื่องการฟื้นฟูระบบไซเบอร์หลังการถูกโจมตี ประเด็นที่งานนี้ทิ้งไว้จึงเป็นไปเพื่อให้มีการศึกษาวิจัยต่อไปเกี่ยวกับประเด็นลักษณะทรัพย์สินดิจิทัล (digital property) การปกป้องและการคุ้มครองทรัพย์สินดิจิทัล รวมตลอดถึงการกู้คืนข้อมูลดิจิทัล การทำสำเนาดิจิทัล และการสร้างข้อมูลดิจิทัล[75]

แม้งานของ Dinniss จะได้ทำการศึกษาวิจัยผลทางกฎหมายมนุษยธรรมระหว่างประเทศต่อปฏิบัติการทางไซเบอร์ในหลากหลายมิติแต่สิ่งที่เปลี่ยนแปลงไปหลังจากการตีพิมพ์ผลงานคือการเผยแพร่คู่มือทาลลินน์ว่าด้วยปฏิบัติการทางไซเบอร์ขององค์กรสนธิสัญญาเพื่อป้องกันแอตแลนติกเหนือ (NATO) ในปี ค.ศ.2013 หลังจากการตีพิมพ์ผลงานของ Dinniss เพียง 1 ปี ซึ่งแม้ใจความสำคัญของงาน Dinniss จะมีสาระสำคัญคล้ายคลึงกับคู่มือทาลลินน์อยู่บ้าง แต่คู่มือทาลลินน์ก็สร้างแนวทางในการปรับใช้กฎหมายระหว่างประเทศที่เกี่ยวข้องกับปฏิบัติการทางไซเบอร์ในการขัดกันทางอาวุธอย่างมาก หลักเกณฑ์หลายประการก็เป็นเพียงการรวบรวมแนวทางกฎหมายระหว่างประเทศที่มีอยู่แล้วเป็นสำคัญก็ตาม แต่การศึกษาแนวทางที่เกิดขึ้นในคู่มือทาลลินน์ก็จะช่วยให้เกิดความเข้าใจวิธีคิดและความพยายามขององค์กรสนธิสัญญาเพื่อป้องกันแอตแลนติกเหนือ (NATO) ในการปรับใช้กฎหมายระหว่างประเทศกับการปฏิบัติการทางไซเบอร์ในการขัดกันทางอาวุธได้

นอกจากนั้นงานของ Dinniss ซึ่งให้ความสำคัญกับประเด็นเฉพาะเกี่ยวกับปฏิบัติการทางไซเบอร์ยังคงไม่ใช่งานที่ตอบคำถามต่อปัญหาที่เกิดขึ้นจากการใช้งานเทคโนโลยีอื่นๆ ในการขัดกันทางอาวุธได้ทุกกรณีเสมอไป จึงยังเป็นประเด็นที่ผู้ศึกษาวิจัยจะได้นำเอาประเด็นที่ Dinniss ศึกษาไว้เป็นข้อมูลเพื่อการวิเคราะห์จุดร่วมและจุดที่ต่างกันของเทคโนโลยีใหม่ที่เกิดขึ้นในการขัดกันทางอาวุธในปัจจุบันว่าเทคโนโลยีเหล่านี้สร้างข้อท้าทายต่อกฎหมายมนุษยธรรมระหว่างประเทศอย่างไร

[74] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 280.

[75] Ibid., p, 280.

(1.2) โฉมหน้าของสงครามรูปแบบใหม่ในลักษณะสงครามไซเบอร์

งานศึกษาของ Erendor and Tamer เรื่อง The New Face of The War: Cyber Warfare แสดงทัศนะว่าไซเบอร์จะมีบทบาทอย่างมากในอนาคต[76] และเขาเห็นว่ากฎหมายระหว่างประเทศที่มาจำกัดหรือควบคุมการใช้ระบบไซเบอร์เป็นเรื่องจำเป็น แต่เขาก็แสดงข้อคิดบางประการว่าการควบคุมการทำสงครามทางไซเบอร์นั้นยังคงเป็นเรื่องที่ยาก เพราะมีข้อท้าทายหลายประการ

Erendor and Tamer ให้ความเห็นว่าสงครามดั้งเดิมนั้นมีลักษณะเป็นการกระทำทางกายภาพที่ปรากฏผลเป็นรูปธรรม นอกจากนั้น Erendor and Tamer ยังเห็นว่าการสร้างระบบการควบคุมและตรวจสอบการใช้งานไซเบอร์ในระดับระหว่างประเทศเป็นเรื่องที่ยากมาก เนื่องจากประเทศต่างๆ ไม่ต้องการเปิดเผยข้อมูลสารสนเทศของประเทศตนเอง ยิ่งกรณีประเทศที่ต้องการควบคุมสารสนเทศของตนเองอย่างมากเช่นประเทศรัสเซียหรือประเทศจีน ยิ่งไม่มีความเป็นไปได้ในการเปิดเผยข้อมูลสารสนเทศของตนเองสู่สาธารณะ โดยเหตุที่ประเทศดังกล่าวมีการจำกัดเสรีภาพในการเข้าถึงข้อมูลข่าวสารของบุคคลภายในประเทศเพื่อนโยบายความมั่นคงของข้อมูลข่าวสารภายในประเทศ แตกต่างจากประเทศในโลกเสรีประชาธิปไตยที่ประชาชนสามารถเข้าถึงข้อมูลสารสนเทศได้อย่างกว้างขวาง ความแตกต่างของแนวคิดทางการเมืองระหว่างประเทศนี้ย่อมนำไปสู่ปัญหาในการสร้างความสมดุลของนโยบายความมั่นคงทางไซเบอร์ระหว่างประเทศอย่างหลีกเลี่ยงไม่ได้[77]

นอกจากแนวคิดว่าการสร้างกฎหมายระหว่างประเทศเป็นเรื่องยากแล้ว Erendor and Tamer มองว่าการจะทำให้ปฏิบัติการทางไซเบอร์มีผลเท่ากับการใช้อาวุธในการขัดกันทางอาวุธจะต้องใช้ลักษณะการเทียบเคียงผลกระทบที่เกิดขึ้น โดยพิจารณาว่าการใช้ปฏิบัติการทางไซเบอร์อาจนำไปสู่ผลในทางกายภาพได้ เช่น การโจมตีระบบปฏิบัติการทางคอมพิวเตอร์ของโรงไฟฟ้าย่อมนำไปสู่การหยุดจ่ายกระแสไฟฟ้า การไม่มีกระแสไฟฟ้าอาจนำไปสู่การที่กองทัพไม่สามารถสั่งระบบยิงอาวุธป้องกันตนเองได้ จึงตกเป็นเป้าหมายของการโจมตีฝ่ายเดียว หรือในกรณีเลวร้ายที่สุดการโจมตีระบบปฏิบัติการทางคอมพิวเตอร์ของโรงปฏิกรณ์นิวเคลียร์อาจนำไปสู่การระเบิดของพลังงาน

[76] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare.” Cyberpolitik Journal. 2 (4). (2018),: 58-75.

[77] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare,”: 58-75.

นิวเคลียร์ในเตาปฏิกรณ์ได้ ความเสียหายที่เกิดขึ้นจากปฏิบัติการทางไซเบอร์ก็จะไม่ต่างจากการทิ้งระเบิดที่โรงปฏิกรณ์นิวเคลียร์ เป็นต้น[78]

Erendor and Tamer เห็นว่าผู้มีหน้าที่ในการจัดการกับสงครามทางไซเบอร์ควรเป็นกองทัพ เพราะปัจจุบันไม่สามารถแยกหน้าที่ของกองทัพออกจากการรักษาความมั่นคงทางไซเบอร์ได้ แต่กระนั้นก็ดี เขามองว่าการโจมตีทางไซเบอร์ หรือสงครามทางไซเบอร์มีผลรุนแรงเฉพาะในประเทศที่มีการพัฒนาด้านไซเบอร์อย่างมาก แต่ในประเทศที่ไม่มีพัฒนาการทางไซเบอร์ขั้นสูงย่อมไม่ต้องวิตกกังวลในเรื่องสงครามทางไซเบอร์มากนัก[79]

ประเด็นที่ Erendor and Tamer เห็นว่าเป็นอุปสรรคหรือข้อท้าทายต่อกฎหมายระหว่างประเทศคือประเด็นเรื่องเป้าหมายการโจมตีที่ชอบด้วยกฎหมาย อันได้แก่[80]

ประการที่ 1 การแยกแยะระหว่างพลเรือนและพลรบ ตั้งแต่สาธารณูปโภครวมตลอดถึงการแยกแยะเครื่องแบบพลรบ และสัญลักษณ์เพื่อความคุ้มครอง ไม่สามารถทำได้ในระบบไซเบอร์ เพราะในโลกไซเบอร์ไม่มีการปรากฏตัวบุคคลเลย

ประการที่ 2 การแยกแยะพื้นที่สนามรบและพื้นที่ที่ได้รับความคุ้มกันระหว่างพลรบกับพลเรือนเป็นไปได้ยาก และหาความชัดเจนของพื้นที่ทั้งสองยาก เพราะพื้นที่ไซเบอร์เป็นพื้นที่ทางอิเล็กทรอนิกส์ที่พลเรือนและทหารใช้ร่วมกัน การโจมตีระบบปฏิบัติการทางคอมพิวเตอร์อันใดอันหนึ่งที่มีผลเท่ากับการโจมตีทางกายภาพต่อกองบัญชาการทางทหารโดยแยกส่วนออกจากการโจมตีที่ส่งผลกระทบต่อที่อยู่อาศัยของพลเรือนเป็นเรื่องที่อธิบายได้ยาก

ทั้งนี้ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศหลายคนให้ความเห็นว่าการโจมตีทางไซเบอร์นั้นไม่สามารถจำกัดความเสียหายได้ชัดเจน ความเสียหายส่วนใหญ่มักเป็นความเสียหายทางเศรษฐกิจไม่ทางตรงก็ทางอ้อม[81] เช่น การโจมตีเว็บไซต์หน่วยงานราชการก็จะมีผลทำให้คนทั่วไปไม่สามารถเข้าถึงข้อมูลหรือการบริการของหน่วยงานได้ ในขณะที่หน่วยงานต้องแก้ไขปัญหาดังกล่าวหรือต้องวางระบบความปลอดภัยให้กับเว็บไซต์ของตนเอง ก็จะต้องใช้งบประมาณและกำลังบุคลากรหรือการโจมตีระบบสาธารณูปโภคของพลเรือนทำให้พลเรือนไม่สามารถใช้สาธารณูปโภคต่างๆ ได้ ขณะที่หน่วยงานที่เกี่ยวข้องก็ต้องหาแนวทางแก้ไขและป้องกันปัญหาในอนาคตต่อไป ฯลฯ ขอบเขต

---

[78] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare,”: 61.

[79] Ibid., p. 69-72.

[80] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 67.

[81] Ibid., p. 65.

ความเสียหายเหล่านี้ไม่สามารถจำกัดความเสียหายเฉพาะทางการทหารได้และหลายครั้งเป็นความเสียหายที่เกิดขึ้นกับทั้งทางทหารและพลเรือน

อย่างไรก็ดีมีหลายฝ่ายเชื่อว่าการโจมตีทางไซเบอร์อาจก่อให้เกิดความเสียหายโดยตรงแก่ชีวิตและร่างกายของมนุษย์ได้และความเสียหายเช่นว่าย่อมเทียบได้กับการโจมตีด้วยอาวุธ เพราะความเสียหายนั้นเป็นผลสืบเนื่องจากการใช้ปฏิบัติการทางไซเบอร์ ตัวอย่างเช่น หากเปรียบเทียบการยิงจรวดทำลายเขื่อนเก็บน้ำก็จะมีผลคล้ายกับการใช้ปฏิบัติการทางไซเบอร์เพื่อสั่งเปิดเขื่อนเก็บน้ำ ซึ่งผลของการกระทำทั้งสองกรณีจะนำไปสู่ความเสียหายต่อชีวิต ร่างกาย และทรัพย์สินของพลเรือน หรือการยิงจรวดทำลายโรงไฟฟ้าพลังนิวเคลียร์ก็จะไม่แตกต่างจากการใช้มัลแวร์ควบคุมเตาปฏิกรณ์นิวเคลียร์ให้ทำงานผิดพลาดจนเกิดการระเบิด[82] เป็นต้น

ประเด็นที่ยังอธิบายได้ยากคือแนวคิดของกฎหมายทุกเรื่องจะต้องเกี่ยวข้องกับหลักอำนาจอธิปไตยที่อยู่บนพื้นฐานของหลักดินแดนทางกายภาพ ดังสังเกตได้จากข้อ 2 ของกฎบัตรสหประชาชาติซึ่งห้ามการกระทำที่ “คุกคามต่อบูรณภาพแห่งรัฐ ดินแดนของประเทศ สิทธิอธิปไตยและเสรีภาพของดินแดน” ปัญหานี้จึงอาจจำเป็นต้องมีการนิยามขอบเขตพื้นที่ทางไซเบอร์ว่าควรใช้หลักการทางกฎหมายอย่างไรมากำหนดจึงจะมีความเหมาะสมและสามารถรองรับกับการกระทำหรือปฏิบัติการที่เกิดขึ้นในพื้นที่ทางไซเบอร์ได้

ประเด็นทางด้านการทหารที่จะต้องพิจารณาคือ กองทัพจะต้องมีหลักการเพิ่มเติมเกี่ยวกับการโจมตีทางไซเบอร์ แต่ปฏิบัติการทางไซเบอร์เป็นเรื่องทางเทคนิค มีสภาพแวดล้อมลักษณะเฉพาะ และเป็นเรื่องค่อนข้างซับซ้อน จะต้องอาศัยผู้มีความรู้เฉพาะทางและมีบุคลากรปฏิบัติงานในปริมาณที่เหมาะสม

นอกจากนี้ Erendor and Tamer ยังเสนอประเด็นที่น่าพิจารณา 3 ประการสำคัญ ได้แก่[83]

ประการที่ 1 การค้นหาตัวผู้กระทำการโจมตีทางไซเบอร์ทำได้มากน้อยแค่ไหนเพียงไร โดยเฉพาะอย่างยิ่งกรณีเหตุการณ์ที่เกิดขึ้นในประเทศตุรกี และซีเรีย ซึ่งมีการโจมตีทางไซเบอร์โดยกลุ่มผู้กระทำที่ไม่ใช่รัฐแต่ได้รับการสนับสนุนจากรัฐ หรือการทำการโจมตีทางไซเบอร์ในลักษณะของตัวแทน การพิสูจน์ความสัมพันธ์ระหว่างผู้กระทำ ผู้สนับสนุนกับการกระทำนั้นค่อนข้างยาก

---

[82] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare,” p. 62.

[83] Ibid., p. 65 - 67.

ประการที่ 2 การตรวจสอบความเสียหายซึ่งเกิดจากการโจมตีทางไซเบอร์ควรมีการสร้างเป็นหลักการเฉพาะ รวมตลอดถึงผลกระทบที่เกิดขึ้นจากการโจมตีทางไซเบอร์ เพื่อประเมินว่าความเสียหายโดยตรงที่จะเกิดขึ้นจากการโจมตีทางไซเบอร์ได้แก่สิ่งใดบ้าง

ประการที่ 3 ผลกระทบจากการโจมตีทางไซเบอร์ต่อหลักความได้สัดส่วน และความรับผิดชอบของผู้ที่เกี่ยวข้องกับการโจมตีทางไซเบอร์จะกระทำอย่างไร

Erendor และ Tamer มีความคิดมากไปกว่านั้นอีกว่าควรจะกำหนดให้พื้นที่การสงครามรวมถึงพื้นที่ทางไซเบอร์ด้วย ซึ่งจะเป็นพื้นที่ที่ 4 คือ บก เรือ อากาศ และไซเบอร์ โดยมีเหตุผลสนับสนุนว่าการสงครามเชิงสารสนเทศเกิดขึ้นมาตั้งแต่หลังสงครามโลกครั้งที่ 2 แล้ว สะท้อนให้เห็นว่าการสงครามเชิงข้อมูลสารสนเทศเป็นพื้นที่ทางการรบประการหนึ่ง[84]

ข้อจำกัดของงานวิจัย Erendor และ Tamer คือเนื้อหาที่ไม่ครอบคลุมทุกมิติของการปฏิบัติการทางไซเบอร์ได้ งาน Erendor และ Tamer จึงเป็นส่วนขยายเพิ่มเติมแนวคิดเกี่ยวกับข้อท้าทายบางประการที่ Dinniss ไม่ได้ให้ความสำคัญเอาไว้ นอกจากนั้นงานของ Erendor และ Tamer ยังเป็นการสนับสนุนแนวคิดของ Dinniss ที่มองว่ากฎหมายมนุษยธรรมระหว่างประเทศให้ความสำคัญกับสงครามและการใช้อาวุธที่เป็นรูปธรรมมีผลในเชิงกายภาพ ซึ่งเป็นข้อจำกัดอย่างมาก หากจะนำเอากฎหมายมนุษยธรรมระหว่างประเทศแบบดั้งเดิมนี้มาพิจารณาลักษณะของปฏิบัติการทางไซเบอร์

ประเด็นที่ Erendor และ Tamer ยังไม่ชัดเจนนักคือการยอมรับลักษณะของสงครามทางไซเบอร์ว่าผลของปฏิบัติการทางไซเบอร์ที่เทียบเท่าการโจมตีด้วยอาวุธตามแบบนั้นมีความเหมาะสมแล้วหรือไม่ เนื่องจาก Erendor และ Tamer มองว่าปฏิบัติการทางไซเบอร์มีความซับซ้อนหลายประการ[85] แต่ท้ายสุด Erendor และ Tamer กลับเห็นว่าควรรับรองให้พื้นที่ไซเบอร์เป็นพื้นที่หนึ่งทางสงครามนอกเหนือจากพื้นที่ทางบก เรือ และ อากาศด้วย[86] โดยให้มองว่าการรบทางไซเบอร์ควรเป็นสมรภูมิทางสารสนเทศรูปแบบหนึ่ง ซึ่งแนวคิดดังกล่าวค่อนข้างจะย้อนแย้งกับข้อท้าทายที่เกิดขึ้นจากลักษณะของปฏิบัติการทางไซเบอร์อยู่พอสมควร เพราะหากการพิจารณาผลทางกายภาพของปฏิบัติการทางไซเบอร์ยังมีปัญหา การนิยามพื้นที่การสู้รบก็อาจมีปัญหาตามไปด้วย

[84] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare,” p. 62.

[85] Ibid., p. 59.

[86] Ibid., p. 62.

รับรองพื้นที่ไซเบอร์ให้เป็นสมรภูมิที่ 4 และกำหนดยุทธศาสตร์เพื่อรับมือกับปฏิบัติการทางไซเบอร์โดยกองทัพทางทหารอาจเป็นการรวบรัดเกินไป แม้ว่าแนวคิดดังกล่าวอาจเป็นข้อเสนอสำหรับแนวทางในการรับมือกับการโจมตีทางไซเบอร์ในอนาคตได้ แต่ก่อนจะถึงขั้นตอนดังกล่าวควรมีการแก้ไขแนวทางในการปรับใช้กฎหมายซึ่งยังไม่ปรากฏในปัจจุบันเสียก่อนน่าจะมีความเหมาะสมมากกว่า

(1.3) การทำให้พื้นที่ทางไซเบอร์เป็นพื้นที่ทางทหาร

งานศึกษาของ Cavelty ในชื่อเรื่อง The Militarisation of Cyberspace: Why Less May Be Better มีมุมมองที่แตกต่างไปจากนักวิชาการหลายคน ท่ามกลางแนวคิดว่าควรมีการพัฒนาแนวทางการปรับใช้กฎหมาย สร้างกฎหมาย หรือสร้างนโยบายในการรับมือกับภัยคุกคามทางไซเบอร์ในการขัดกันทางอาวุธ Cavelty กลับนำเสนอว่าแนวคิดเหล่านั้นเสนอในสิ่งที่มากเกินความจำเป็น[87]

Cavelty นำเสนอว่าการสร้างกฎหมายใหม่เพื่อการควบคุมเทคโนโลยีไซเบอร์ในการขัดกันทางอาวุธไม่มีความจำเป็น Cavelty ใช้แนวคิดเรื่อง “ความเสียหาย” เป็นหลักในการพิจารณา โดย Cavelty มีข้อโต้แย้งเกี่ยวกับการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีว่าเทคโนโลยีเหล่านี้อาจไม่ได้สร้างความเสียหายอย่างร้ายแรงเท่าที่คิด และผลที่เกิดขึ้นโดยมากมักเป็นความวิตกกังวลจากข้อมูลข่าวสารที่มีการนำเสนอซ้ำๆ มากกว่า

Cavelty มีความเห็นว่าปรากฏการณ์ของคำว่า “อาวุธไซเบอร์” มีมิติเกี่ยวข้องเชิงทางการเมืองและสังคมด้วย เช่น มาตรการด้านความมั่นคงย่อมเกี่ยวข้องกับแนวคิดของทหาร ดังนั้นมีประเด็นเรื่องยุทธศาสตร์ด้านความมั่นคงทางไซเบอร์ ทหารก็จะเข้ามามีส่วนเกี่ยวข้องเสมอ ยุทธศาสตร์ทางการทหารอยู่บนพื้นฐานของการทำลายขีดความสามารถของฝ่ายตรงข้ามเพื่อสร้างความได้เปรียบแก่ฝ่ายตน และมาตรการป้องกันภัยคุกคามที่อาจเกิดขึ้นแก่ฝ่ายตนเอง การต่อสู้ทุกครั้งจึงต้องมีสภาวะการชนะและความพ่ายแพ้ มาตรการเกี่ยวกับความมั่นคงทางไซเบอร์ที่เกิดขึ้นจึงต้องมองไซเบอร์ในฐานะเป็นปัจจัยและเป็นวิธีการในการต่อสู้ การรักษาความมั่นคงทางไซเบอร์จึงมักมีลักษณะที่เกินจากความเป็นจริง และมีการสร้างความเชื่อในรูปแบบ “วาทะกรรม” (Discourse) หรือ

[87] Myriam Dunn Cavelty, “The Militarisation of Cyberspace: Why Less May Be Better,” 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis and K. Ziolkowski (Eds.), Tallinn, (2012), p. 142.

ชุดข้อมูลบางอย่างขึ้นมาเพื่อให้คนคล้อยตาม ซึ่งส่งผลต่อความตื่นตระหนก ทำลายขวัญและกำลังใจของประชาชนหรือกองทัพฝ่ายตรงข้ามเป็นสำคัญ

Cavelty อธิบายว่าความเชื่อในรูปแบบ “วาทะกรรม” เกี่ยวกับภัยคุกคามทางไซเบอร์ อาจแบ่งเป็น 3 ลักษณะด้วยกัน คือ[88]

วาทะกรรมที่ 1 ไวรัส หนอน และ Bugs คอมพิวเตอร์

เหตุที่ Cavelty ใช้คำว่า “วาทะกรรมทางเทคนิค” (Technical Discourse) เนื่องมาจากมุมมองของ Cavelty ที่เห็นว่าภัยคุกคามทางไซเบอร์ เช่น ไวรัส หนอน (worm) และ bugs คอมพิวเตอร์ เป็นถ้อยคำที่สร้างขึ้นมาจากสิ่งที่ไม่มีความหมายทางวิทยาการคอมพิวเตอร์ แต่เป็นการนำเอาชื่อสิ่งที่มนุษย์รู้จักมาใช้เรียกลักษณะการทำงานของชุดคำสั่งทางคอมพิวเตอร์ (โปรแกรมประสงค์ร้ายหรือมัลแวร์) ที่คล้ายคลึงกับลักษณะของเชื้อไวรัสที่ติดต่อในสิ่งมีชีวิต การเคลื่อนที่และการใช้ชีวิตของหนอน และลักษณะบางประการของแมลงมาสร้างเป็นคำใหม่ในวงการคอมพิวเตอร์ ซึ่งมีผลต่อความรู้สึกและเปลี่ยนแปลงพฤติกรรมการใช้งานคอมพิวเตอร์ของผู้ใช้งานโดยทั่วไป โดยที่ผู้ใช้งานคอมพิวเตอร์ซึ่งไม่มีความเชี่ยวชาญหรือความรู้เกี่ยวกับที่มาของมัลแวร์เหล่านี้จำเป็นต้องปฏิบัติตามคำแนะนำที่มีการประชาสัมพันธ์กันอย่างแพร่หลาย และเป็นช่องทางในการตลาดเพื่อเสนอขายผลิตภัณฑ์เกี่ยวกับการตรวจหาและกำจัดโปรแกรมมัลแวร์ต่างๆ เหล่านี้

ตัวอย่างของการสร้าง “วาทกรรม” เกี่ยวกับมัลแวร์คอมพิวเตอร์ เกิดขึ้นในราวปี ค.ศ.1988 เมื่อหน่วยงาน The U.S. Advanced Research Projects Agency Network หรือ ARPANET ค้นพบหนอนคอมพิวเตอร์ที่ชื่อว่า “Morris” อันเป็นต้นเหตุของความเสียหายทางระบบอินเทอร์เน็ตในหลายประเทศ ทำให้ประเทศสหรัฐอเมริกาได้มอบหมายหน่วยงานวิจัยระดับสูงของกระทรวงกลาโหมหรือ The Defense Advanced Research Projects Agency: DARPA ทำการศึกษาค้นคว้าแนวทางในการป้องกันความเสียหายทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต หน่วยงานย่อยใน DARPA ที่ทำหน้าที่โดยตรงในเรื่องนี้คือหน่วยปฏิบัติการฉุกเฉินทางคอมพิวเตอร์ หรือ The Computer Emergency Response Team (CERT) ผลจากการปฏิบัติงานของหน่วยงานดังกล่าวก่อให้เกิดบริษัทสร้างโปรแกรมกำจัดไวรัสขึ้นมากมาย ทำให้เรารู้จักไวรัสหลากหลายขึ้น สามารถใช้ป้องกันและทำลายไวรัสได้มากขึ้น[89]

---

[88] Myriam Dunn Cavelty. “The Militarisation of Cyberspace: Why Less May Be Better,”: 141-153.

[89] Ibid., p. 145.

การ “รู้จัก” ไวรัสคอมพิวเตอร์ของบุคคลทั่วไปแสดงออกผ่านความหวาดกลัวว่าไวรัสคอมพิวเตอร์นี้จะทำลายอุปกรณ์คอมพิวเตอร์หรือสร้างความเสียหายต่อข้อมูลในคอมพิวเตอร์ของเรา นอกจากนี้ยังเชื่อว่าไวรัสคอมพิวเตอร์ยังอาจสร้างความเสียหายต่อระบบการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตของคอมพิวเตอร์ด้วย ในบางกรณีนั้นผู้ที่ไม่เคยมีประสบการณ์โดยตรงเกี่ยวกับความเสียหายจากไวรัสคอมพิวเตอร์จึงต้องแสวงหาโปรแกรมตรวจสอบและกำจัดไวรัสมาติดตั้งในเครื่องคอมพิวเตอร์ของตนเอง

คำว่า “ไวรัสคอมพิวเตอร์” ส่งผลในเชิงพาณิชย์ค่อนข้างมาก โดยในยุคแรกที่มีความตื่นตัวเรื่องไวรัสคอมพิวเตอร์ โปรแกรมตรวจจับไวรัสและกำจัดไวรัสได้รับความนิยมอย่างมาก ขณะที่ในปัจจุบันความนิยมในโปรแกรมกำจัดไวรัสเริ่มมีการพูดถึงน้อยลง ส่วนหนึ่งอาจเป็นผลมาจากบริษัท Microsoft ได้พัฒนาโปรแกรมพื้นฐานใน MS office ให้สามารถป้องกันมัลแวร์ได้ในระดับหนึ่ง อีกส่วนหนึ่งอาจมาจากความนิยมในการใช้และแพร่ไวรัสไม่ปรากฏอย่างชัดเจนในยุคปัจจุบัน[90] คำว่า “ไวรัสคอมพิวเตอร์” จึงมีผลต่อความรู้สึกของผู้ใช้งานคอมพิวเตอร์และการตลาดของโปรแกรมกำจัดไวรัสในช่วงเวลาหนึ่งเท่านั้น

“หนอนคอมพิวเตอร์” (Worms) เป็นอีกคำหนึ่งในเทคโนโลยีคอมพิวเตอร์ที่ส่งผลกระทบต่อความรู้สึกของบุคคลทั่วไป และการสร้างนโยบายของรัฐเพื่อความมั่นคงทางอินเทอร์เน็ต ทั้งที่วิศวกรคอมพิวเตอร์ในยุคปี ค.ศ.1960 เคยใช้หนอนคอมพิวเตอร์เป็นวิธีการสำคัญในการเข้าถึงข้อมูล (Hack) คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ นอกจากนั้นหนอนคอมพิวเตอร์ยังถูกใช้งานเพื่อการตรวจสอบ (Investigate) ระบบคอมพิวเตอร์ได้[91]

เมื่อถึงช่วงทศวรรษ ค.ศ.1980 คอมพิวเตอร์กลายเป็นส่วนหนึ่งของชีวิตประจำวันของคนทั่วไปและเป็นปัจจัยสำคัญในการติดต่อสื่อสารทางธุรกิจ หนอนคอมพิวเตอร์กลายเป็นเครื่องมือของผู้ประสงค์ร้ายในการเจาะเข้าสู่ระบบคอมพิวเตอร์เพื่อวัตถุประสงค์บางประการซึ่งอาจเป็นได้ตั้งแต่การจารกรรมข้อมูล รวมถึงการทำลายระบบปฏิบัติการคอมพิวเตอร์ ความเสียหายที่เกิดขึ้นจากมัลแวร์เหล่านี้จึงมีสภาพเป็นรูปธรรมในความเข้าใจของบุคคลทั่วไปมากขึ้น สังคมเกิดความตระหนักในภัยคุกคามจากมัลแวร์คอมพิวเตอร์มากขึ้น และพัฒนามาจนเกิดเป็นวาทะกรรมเรื่องความมั่นคงทางไซเบอร์ (Cyber Security Discourse) ซึ่งก่อให้เกิดผลทั้งในเชิงการพาณิชย์ในการสร้างโปรแกรมกำจัดมัลแวร์จำหน่ายและการสร้างมาตรการของรัฐในการควบคุมการจราจรทาง

---

[90] Myriam Dunn Cavelty. “The Militarisation of Cyberspace: Why Less May Be Better,” p. 145.

[91] Ibid., p. 147.

อินเทอร์เน็ตของผู้ใช้งานคอมพิวเตอร์เพื่อวัตถุประสงค์ในการรักษาความมั่นคงและความปลอดภัยทางอินเทอร์เน็ตในปัจจุบัน[92]

วาทะกรรมที่ 2 อาชญากรรมทางคอมพิวเตอร์และการจารกรรมทางดิจิทัล

อาชญากรรมทางไซเบอร์และอาชญากรรมทางคอมพิวเตอร์ เป็นสิ่งที่มีความหมายใกล้เคียงกันเป็นอย่างมาก ประเทศที่มีพัฒนาการทางด้านเทคโนโลยีสารสนเทศหลายประเทศมีบทบาทในการสร้างวาทะกรรมเรื่องอาชญากรรมทางไซเบอร์ โดยจุดเริ่มต้นมาจากการกระทำในลักษณะการเข้าถึงแหล่งข้อมูลทางคอมพิวเตอร์ของผู้อื่น[93]

อาชญากรรมทางไซเบอร์มีความหมายรวมถึงอาชญากรรมที่เกิดขึ้นแก่ทั้งคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ เช่น การปล่อยมัลแวร์ การใช้สแปม (spam) การหลอกหลวง และการกระทำในลักษณะอื่นๆ เพื่อวัตถุประสงค์ในการสร้างความเสียหายแก่บุคคลอื่น การกระทำที่ยกระดับอาชญากรรมทางไซเบอร์เริ่มต้นที่กลุ่มวัยรุ่นในเมืองมิลวอคกี้ 6 คน ในชื่อ “414s” ทำการเข้าไปในระบบฐานข้อมูลคอมพิวเตอร์ของหน่วยงานรัฐบาลสหรัฐอเมริกาและทำการเปลี่ยนแปลงข้อมูลของหน่วยงานสำคัญหลายหน่วยงาน ก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานภาครัฐ เป็นผลให้หน่วยงานของรัฐบาลสหรัฐอเมริกาต้องสร้างนโยบายความมั่นคงทางไซเบอร์ที่รัดกุมมากขึ้น โดยคำนึงถึงประเด็นเรื่องความสามารถของบุคคลว่าหากกลุ่มวัยรุ่นทั่วไปยังสามารถก่อความเสียหายได้ในระดับนี้ หน่วยงานที่ใหญ่กว่าและมีทรัพยากรที่มากกว่าอาจสร้างความเสียหายได้เป็นทวีคูณ [94]

ความตระหนักถึงภัยคุกคามดังกล่าวทำให้หน่วยงานภาครัฐให้ความสำคัญกับนโยบายความมั่นคงทางไซเบอร์มากขึ้นและใช้งบประมาณจำนวนมากเพื่อต่อต้านการโจมตีทางไซเบอร์ สถานการณ์ดังกล่าวสร้างภาพของความจำเป็นในการต่อต้านภัยคุกคามทางไซเบอร์ให้ปรากฏแก่สาธารณชนโดยทั่วไป และเป็นการสร้างชุดความเชื่อที่มีพื้นฐานจากนโยบายของรัฐ ทำให้ภัยคุกคามทางไซเบอร์เป็นเรื่องที่มีความสำคัญมากยิ่งขึ้นในสังคมระหว่างประเทศ

[92] Myriam Dunn Cavelty. “The Militarisation of Cyberspace: Why Less May Be Better,” p. 147.

[93] Ibid.

[94] Ibid.

วาทะกรรมที่ 3 สงครามข้อมูลข่าวสารและวิกฤติทางด้านสาธารณูปโภค

ความสัมพันธ์ระหว่างเทคโนโลยีข้อมูลข่าวสารและความมั่นคงของชาติเป็นสิ่งที่เกิดขึ้นมาตั้งแต่หลังยุคสงครามโลกครั้งที่ 2 (สงครามเย็น) โดยในช่วงเวลาสงครามเย็นนั้นมีการเปลี่ยนรูปแบบยุทธศาสตร์ทางทหารจากการโจมตีด้วยอาวุธเป็นการทำสงครามจิตวิทยาด้านข้อมูลข่าวสาร ปฏิบัติการทางทหารของกองทัพนั้นมีแนวคิดว่าข้อมูลข่าวสารถือเป็นเป็นองค์ประกอบหนึ่งในกระบวนการกำหนดเป้าหมาย (Targeting) เพื่อทำลายขีดความสามารถของฝ่ายตรงข้ามในความขัดแย้ง เนื่องจากข้อมูลข่าวสารจะส่งผลต่อความรู้สึกของพลเรือนและทหารซึ่งจะมีผลอย่างมากต่อเสถียรภาพของรัฐบาลและกองทัพ การปฏิบัติการด้านข้อมูลข่าวสารย่อมก่อให้เกิดความได้เปรียบเสียเปรียบในปฏิบัติการทางทหารทั้งนี้ขึ้นอยู่กับลักษณะของข้อมูลข่าวสารดังกล่าวด้วยว่ามีความสำคัญและสัมพันธ์กับความมั่นคงของรัฐมากเพียงใด[95]

ปฏิบัติการทางข้อมูลข่าวสาร (Information Operation: IO) ในยุคสงครามเย็นนิยมใช้การโฆษณาชวนเชื่อ (Propaganda) ผ่านสื่อสิ่งพิมพ์ โทรทัศน์และวิทยุเพื่อสร้างความเชื่อถือหรือทำลายความเชื่อถือในประเด็นใดประเด็นหนึ่งแก่สาธารณะชน แต่ในปัจจุบันปฏิบัติการทางข้อมูลข่าวสารเปลี่ยนสภาพมาเป็นปฏิบัติการทางไซเบอร์[96] ตั้งแต่สถานการณ์สงครามอ่าวเปอร์เซีย ในปี ค.ศ.1991 โดยปฏิบัติการทางข้อมูลข่าวสารนี้ทำโดยกองทัพสหรัฐอเมริกาในแนวคิดว่าการทำสงครามทางกายภาพนั้นเป็นการไม่เพียงพอ หากมีการทำสงครามเชิงข้อมูลข่าวสารร่วมไปด้วยจะทำให้มีความได้เปรียบในการรบมากยิ่งขึ้น ความคิดนี้นำไปสู่การพัฒนาหลักการในการทำลายขีดความสามารถฝ่ายตรงข้ามด้วยการทำลายทั้งความน่าเชื่อถือของฝ่ายตรงข้ามและการทำลายระบบการสื่อสารของฝ่ายตรงข้ามด้วย

ยุคกลางทศวรรษ ค.ศ.1990 ความแพร่หลายในการใช้เทคโนโลยีสารสนเทศ มิได้เป็นเพียงสิ่งสำคัญที่ขับเคลื่อนการปฏิวัติกิจการทหารอย่างที่ไม่เคยปรากฏมาก่อนเท่านั้น แต่ปฏิบัติการทางข้อมูลข่าวสารยังมีผลอย่างมากต่อพัฒนาการของเหล่ารัฐผู้ก่อความไม่สงบ (Malicious State) และกลุ่มตัวตนที่ไม่ใช่รัฐ (Non-state actors) และผู้ก่อการร้ายในการนำเทคโนโลยีทางข้อมูลข่าวสารดังกล่าวมาใช้เพื่อประโยชน์ของฝ่ายตนเองด้วย[97]

---

[95] Myriam Dunn Cavelty. “The Militarisation of Cyberspace: Why Less May Be Better,” p. 151.

[96] Ibid.

[97] Ibid.

ลักษณะทั่วไปของปฏิบัติการทางเครือข่ายไซเบอร์ที่อยู่บนพื้นที่ทางอิเล็กทรอนิกส์ทำให้การสืบหาตัวตนของผู้ปฏิบัติการทางข้อมูลข่าวสารที่แท้จริงจากตัวตนที่ปรากฏในโลกไซเบอร์ไม่ใช่เรื่องที่กระทำได้ง่าย[98] นอกจากนั้นการระบุตัวตนและที่ตั้งของผู้กระทำการในระบบสารสนเทศทางไซเบอร์ก็เป็นไปได้ยาก[99] ปฏิบัติการทางข้อมูลข่าวสารเหล่านี้จึงเป็นเครื่องมือสำคัญในการทำลายขีดความสามารถของฝ่ายตรงข้ามอย่างมีประสิทธิภาพ และอาจมีผลถึงขั้นทำลายกองทัพฝ่ายตรงข้ามได้

ลักษณะของการปฏิบัติการทางข้อมูลข่าวสารที่นอกจากจะเป็นยุทธวิธีสงครามแบบผสมผสาน (Hybrid Warfare)[100] แล้ว ยังมีลักษณะเป็นยุทธวิธีสงครามอสมมาตร (Asymmetric warfare)[101] ด้วย สงครามอสมมาตรนี้หมายถึงคู่พิพาทในสงครามมีความได้เปรียบเสียเปรียบแตกต่างกันอย่างชัดเจน หากฝ่ายใดกุมความได้เปรียบในการสื่อสารและปฏิบัติการทางข้อมูลข่าวสารได้มากกว่าหรือสามารถใช้ข้อมูลข่าวสารทำลายความน่าเชื่อถือฝ่ายตรงข้ามได้มากกว่าก็จะได้เปรียบในความขัดแย้งนั้นอย่างมาก ในขณะที่การตอบโต้ปฏิบัติการทางข้อมูลข่าวสารโดยการกระทำต่อตัวบุคคลนั้นเป็นไปได้ยากมากจากลักษณะของความซับซ้อนในการระบุตัวบุคคลผู้ปฏิบัติการดังที่ได้กล่าวมา การตอบโต้ปฏิบัติการทางข้อมูลข่าวสารจึงต้องกระทำผ่านปฏิบัติการทางข้อมูลข่าวสารเท่านั้น และการต่อสู้ในลักษณะข้อมูลข่าวสารดังที่ได้กล่าวมาทั้งหมดเป็นเรื่องยากแก่การพิสูจน์ความน่าเชื่อถือ จึงเป็นปัญหาต่อประชาชนผู้ได้รับข้อมูลด้วยเพราะประชาชนผู้รับข้อมูลข่าวสารจะไม่มีทางเข้าถึงข้อมูลที่ถูกต้องและเป็นจริงเลย

สงครามทางข้อมูลข่าวสารดำเนินต่อมาและยกระดับขึ้น ใน ค.ศ.1999 เมื่อองค์กรสนธิสัญญาเพื่อป้องกันแอตแลนติกเหนือหรือ NATO ส่งกองกำลังเข้าไปในอดีตประเทศยูโกสลาเวีย และมีการใช้ปฏิบัติการโฆษณาชวนเชื่อ ปล่อยข่าวลวงในสื่อต่างๆ รวมถึงการสร้างเว็บไซต์ปลอม และการโจมตีการเข้าถึงเว็บไซต์ด้วยวิธีการ DDoS (A Distributed Denial-of-Service) นอกจากนั้นกองทัพสหรัฐอเมริกายังใช้วิธีการเจาะระบบ ข้อมูลธนาคาร เพื่อโยกย้ายเงินในบัญชีของนายพลสโลโบ

[98] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, (Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018), p. 98-99.

[99] Myriam Dunn Cavelty. "The Militarisation of Cyberspace: Why Less May Be Better," p. 151.

[100] Mehmet Emin Erendor and Gurkan Tamer. "The New Face of The War: Cyber Warfare,": 65.

[101] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better,": 145.

ดัน มิโลเซวิช ปฏิบัติการณ์ดังกล่าวถือเป็นต้นแบบของปฏิบัติการ “สงครามทางอินเทอร์เน็ต” แบบเบ็ดเสร็จในปฏิบัติการทางทหารในยุคต่อมา[102]

Cavelty เห็นว่าสิ่งสำคัญที่ควรกระทำคือการประเมินความเสียหายที่เกิดขึ้นจริงจากการโจมตีทางไซเบอร์ และสร้างความสมดุลระหว่างมาตรการในการป้องกันการโจมตีทางไซเบอร์และต้นทุนที่ต้องจ่ายกับผลประโยชน์ที่จะได้รับมากกว่าที่จะสร้างนโยบายเพื่อความมั่นคงทางไซเบอร์หรือพัฒนาระบบอาวุธทางไซเบอร์ของกองทัพ เพราะผู้โจมตีทางไซเบอร์ ลักษณะการโจมตีทางไซเบอร์และสภาพแวดล้อมทางไซเบอร์เป็นเรื่องที่ยากต่อการจำกัดขอบเขต การลงทุนกับเรื่องดังกล่าวเป็นเรื่องที่ยาก ใช้เวลามากและมีต้นทุนที่สูง[103]

นอกจากนั้นแล้วการป้องกันการโจมตีทางไซเบอร์ยังไม่ควรเป็นบทบาทของกองทัพแต่เพียงฝ่ายเดียว เพราะพื้นที่ทางไซเบอร์เป็นพื้นที่เสมือน กองทัพจึงไม่อาจป้องกันพรมแดนทางไซเบอร์ได้ เมื่อพื้นที่ทางไซเบอร์ไม่ใช่แผ่นดินทางกายภาพการใช้อาวุธปกติจึงไม่สามารถใช้ได้ มาตรการเกี่ยวกับความมั่นคงทางไซเบอร์จึงน่าจะเป็นบทบาทของผู้เชี่ยวชาญทางด้านคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์[104]

อย่างไรก็ดี เราไม่สามารถปฏิเสธได้ว่าการโจมตีทางเทคโนโลยีสารสนเทศอาจก่อให้เกิดความเสียหายรุนแรงได้ในอนาคต ดังนั้น จึงควรมีมาตรการในการดำเนินการดังนี้[105]

ประการที่ 1 กองทัพควรให้ความสำคัญกับการปกป้อง และการกู้คืนข้อมูล เครือข่ายและสาธารณูปโภคทางสารสนเทศของตนเองในกรณีวิกฤติ

ประการที่ 2 รัฐบาลและกองทัพควรรับรู้ถึงข้อจำกัดของตนเองในบทบาทการสร้างความมั่นคงทางไซเบอร์ การรักษาความมั่นคงทางไซเบอร์เป็นบทบาททั้งของรัฐและปัจเจก รัฐมีหน้าที่รักษาสาธารณูปโภคที่จำเป็นในภาวะวิกฤติ สนับสนุนและช่วยพัฒนาระบบความมั่นคง และการกู้คืนฐานข้อมูลเครือข่ายทางไซเบอร์ให้กับภาคเอกชนเป็นสำคัญ

อาจกล่าวได้ว่างานของ Cavelty ต่อต้านแนวคิดกระแสหลักในการให้ความสำคัญกับเรื่องการรับมือกับภัยคุกคามทางไซเบอร์ด้วยการพัฒนากฎหมาย โดยเปลี่ยนไปให้ความสำคัญกับการทำความเข้าใจและแสวงหาความเสียหายที่แท้จริงจากปฏิบัติการทางไซเบอร์ และการสร้าง

---

[102] Myriam Dunn Cavelty, “The Militarisation of Cyberspace: Why Less May Be Better,”: 144.

[103] Ibid., p. 145.

[104] Ibid., p. 144.

[105] Ibid., p. 149.

มาตรการทางปฏิบัติเพื่อป้องกันความเสียหายที่เกิดขึ้นจากปฏิบัติการทางไซเบอร์[106] ซึ่งมาตรการเหล่านี้อาจเป็นแนวทางแก้ไขปัญหาในช่วงเวลาที่ยังไม่สามารถสร้างความชัดเจนทางกฎหมายได้

นอกจากนั้นการมองว่าการจัดการที่น้อยที่สุดกับปัญหาทางไซเบอร์จะก่อให้เกิดความเหมาะสมมากกว่าวิธีการอื่นนี้ก็อาจเป็นแนวคิดที่ยังมีข้อโต้แย้งอยู่พอสมควร ประการที่หนึ่ง แม้ Cavelty จะมองว่าภัยคุกคามทางไซเบอร์เป็นเรื่องไม่จริง แต่ข้อมูลจากการศึกษาของ Cavelty ก็ปรากฏกรณีความเสียหายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์หลายกรณี ภัยคุกคามทางไซเบอร์จึงเป็นเรื่องจริง มีความเสียหายจริง ส่วนมาตรการทางกฎหมายที่เหมาะสมในการจัดการควรอยู่ในระดับใดเป็นอีกเรื่องหนึ่งที่ต้องพิจารณา ประการที่สอง Cavelty เสนอข้อเท็จจริงว่าปฏิบัติการข้อมูลข่าวสารในการสงครามมีอยู่จริง และมีผลกระทบที่เกิดขึ้นอยู่จริง แล้วเหตุใดการพิจารณากฎหมายที่เหมาะสมต่อการรับมือกับปัญหาดังกล่าวจึงไม่ควรเกิดขึ้น ประการที่สาม แม้ Cavelty จะใช้คำว่า “วาทะกรรม” (Discourse) กับภัยคุกคามทางไซเบอร์ แต่ข้อเท็จจริงที่ Cavelty นำเสนอนั้นก็ไม่ได้น้อยไปกว่างานศึกษาของนักวิชาการคนอื่นๆ ด้วยสัดส่วนปัญหาที่นำเสนอในงานของ Cavelty นี้น่าจะแสดงให้เห็นได้ว่า ปัญหาเกี่ยวกับภัยคุกคามทางไซเบอร์เป็นเรื่องที่เกิดขึ้นจริง เพียงแต่ไม่ใช่เรื่องที่น่าตื่นตระหนกมากเกินสมควรเท่านั้น[107]

สิ่งที่งานของ Cavelty ศึกษานั้นอาจเป็นมุมมองของการพิจารณาความสำคัญกับภัยคุกคามทางไซเบอร์ในภาพรวม ไม่ได้เฉพาะเจาะจงกับปัญหาการใช้ปฏิบัติการทางไซเบอร์ในการขัดกันทางอาวุธเป็นหลักจึงไม่มีการวิเคราะห์ตามกฎหมายมนุษยธรรมระหว่างประเทศเท่าไรนัก แต่งานของ Cavelty ก็สร้างคุณูปการแก่วงการวิชาการในการนำเสนอแนวคิดอีกมุมหนึ่งให้เราได้กลับมาไตร่ตรองว่าความเสียหายที่แท้จริงของปฏิบัติการทางไซเบอร์มีความรุนแรงอย่างที่ปรากฏในสื่อต่างๆ หรือข้อมูลต่างๆ ที่เรารับทราบจริงหรือไม่ โดยที่เราอาจไม่ได้ยึดแนวทางของข้อมูลกระแสหลักหรือข้อมูลในมุมมองของ Cavelty เป็นบทสรุปทั้งหมด แต่งานของ Cavelty ก็ช่วยสร้างสมดุลในการศึกษาวิจัยปัญหาเกี่ยวกับภัยคุกคามทางไซเบอร์และเป็นประโยชน์ต่อผู้ศึกษาวิจัยอยู่ไม่น้อย

(1.4) การก่อวินาศกรรมทางไซเบอร์

งานศึกษาของ Solis แสดงทัศนะต่อการก่อวินาศกรรมทางไซเบอร์ว่า “การก่อวินาศกรรม หรือการกระทำอื่นๆ ที่มิได้ใช้อาวุธแต่ส่งผลในทำนองเดียวกัน หากเป็นไปเพื่อการ

---

[106] Myriam Dunn Cavelty, “The Militarisation of Cyberspace: Why Less May Be Better,”: 150.

[107] Ibid., 151.

ขัดขวาง รบกวนการขนส่งหรือการสื่อสารของคู่พิพาทฝ่ายตรงข้าม รวมถึงการโจมตีทางไซเบอร์ก็ถือว่าอยู่ในลักษณะการก่อวินาศกรรมเช่นกัน การกระทำรุนแรงในลักษณะอื่นๆ ที่ก่อให้เกิดผลโดยตรงต่อพลเรือนและทรัพย์สินของพลเรือน เช่น การโจมตีด้วยพลซุ่มยิง การทิ้งระเบิดในพื้นที่พักอาศัยของพลเรือนก็ถือว่าเข้าลักษณะการกระทำในทำนองเดียวกัน”[108]

แนวคิดของ Solis ไม่ได้แสดงทัศนะที่แตกต่างจากแนวคิดของนักกฎหมายระหว่างประเทศทั่วไปที่มองว่าปฏิบัติการทางไซเบอร์ก็มีผลเทียบเท่าการก่อวินาศกรรมตามแบบปกติเช่นกัน ทั้งนี้ด้วยเหตุที่การศึกษาของ Solis นี้เป็นส่วนหนึ่งในงานหนังสือของเขาเท่านั้น

(2) งานวิชาการที่เกี่ยวข้องกับระบบอาวุธอิสระ (Autonomous Weapon Systems)

นอกจากประเด็นปัญหาเกี่ยวข้องกับการโจมตีทางไซเบอร์ คณะกรรมการกาชาดระหว่างประเทศได้ทำการศึกษาการใช้งานปัญญาประดิษฐ์ในระบบอาวุธอิสระที่เกี่ยวข้องกับการขัดกันทางอาวุธมาระยะหนึ่งและพบว่าการใช้งานปัญญาประดิษฐ์ในระบบอาวุธอิสระทางการทหารนั้นมีทั้งด้านบวกและลบ ด้านบวกคือเทคโนโลยีทำให้การโจมตีมีความแม่นยำมากขึ้น ลดความสูญเสียทางการทหารของกองทัพในการสงคราม[109] เป็นประโยชน์แก่การคุ้มครองพลเรือนให้สอดคล้องกับกฎเกณฑ์ในการทำสงคราม ด้านลบมักมาจากการใช้งานของบุคคล เช่น การสั่งงานหรือการโปรแกรมการทำงานให้แก่ปัญญาประดิษฐ์ที่อาจก่อให้เกิดความผิดพลาดในดารทำงานของปัญญาประดิษฐ์ซึ่งอาจนำไปสึความเสียหายรวมถึงปัญหาที่ อาจเกิดจากการประเมินความแม่นยำในการทำงานของปัญญาประดิษฐ์ที่ยังไม่สามารถทำได้ในปัจจุบัน[110]

---

[108] Gary D. Solis. The Law of Armed Conflict: International Humanitarian Law in War. (Cambridge: Cambridge University Press, 2010), p. 203.

[109] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p.26.

[110] International Committee of the Red Cross, “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.” International Committee of the Red Cross, Paper, June 6, 2019. pp. 4-5. [online] Accessed: May 26, 2022. Available from: https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach

(2.1) ปัญหาการพิจารณาความสัมพันธ์ระหว่างระบบอาวุธอิสระกับผู้ควบคุม

กลุ่มผู้เชี่ยวชาญของคณะกรรมการกาชาดระหว่างประเทศให้ความเห็นว่าปัญญาประดิษฐ์ที่ใช้ในระบบอาวุธซึ่งสามารถตัดสินใจได้ด้วยตนเองนั้นควรอยู่ภายใต้การพิจารณาความเหมาะสมในเกณฑ์ดังต่อไปนี้[111]

1) การพิจารณาความสัมพันธ์ระหว่างมนุษย์กับการทำงานของปัญญาประดิษฐ์ โดยพิจารณาว่าระดับการควบคุมของมนุษย์ต่อปัญญาประดิษฐ์นั้นมีอยู่เพียงใด ขั้นตอนไหน สามารถตรวจสอบการทำงานของปัญญาประดิษฐ์อย่างไรได้บ้าง

2) การคาดหมายได้และความเชื่อถือได้ของระบบอาวุธดังกล่าว ทั้งนี้การใช้งานระบบอาวุธอิสระที่มีการทำงานของปัญญาประดิษฐ์เป็นส่วนประกอบสำคัญควรเป็นไปเพื่อการสร้างความแม่นยำในการขัดกันทางอาวุธและลดความสูญเสียที่ไม่จำเป็น

3) เงื่อนไขในการปฏิบัติการของระบบอาวุธอิสระดังกล่าวจะต้องมีความชัดเจน เช่น ภาระกิจค้นหาเป้าหมายอะไร สภาพแวดล้อมที่ใช้เป็นอย่างไร ระยะเวลาปฏิบัติการนานเพียงใด พื้นที่ปฏิบัติการกว้างขวางแค่ไหน กรณีที่เกิดสถานการณ์วิกฤติหรือเหตุแทรกแซงขึ้นทำให้การใช้งานระบบอาวุธอิสระอาจเกิดความคลาดเคลื่อนได้ ผู้ใช้ระบบอาวุธอิสระดังกล่าวจะมีมาตรการในการดำเนินการอย่างไร

เงื่อนไขที่กล่าวทั้งหมดนี้จะต้องพิจารณาปัจจัยเพิ่มเติมด้วยว่าระบบปฏิบัติการของอาวุธอิสระนั้นเป็นระบบตัดสินใจด้วยตนเองทั้งหมดหรือไม่ (Fully autonomous) ปัจจัยเรื่องนี้จะสัมพันธ์กับเกณฑ์ในข้อ 1 คือ มนุษย์ผู้ควบคุมอาวุธมีความสัมพันธ์กับการทำงานของระบบอาวุธอย่างไร การที่มนุษย์ยังมีส่วนร่วมในการสั่งการไม่ว่าจะเป็นขณะที่เริ่มต้นปฏิบัติการใช้ระบบอาวุธระหว่างเวลาที่ใช้ระบบอาวุธหรือมนุษย์เกี่ยวข้องในลักษณะการตัดสินใจในขั้นสุดท้ายก่อนการทำลายเป้าหมายย่อมนำไปสู่ข้อพิจารณาทางกฎหมายที่แตกต่างจากกรณีที่ระบบอาวุธสามารถทำงานได้ด้วยตนเองอย่างสมบูรณ์ เนื่องจากกรณีที่มนุษย์เกี่ยวข้องกับการปฏิบัติการ อาจมีการสั่งยุติการทำงานของระบบอาวุธในขั้นตอนต่างๆ ได้ ในขณะที่ระบบอาวุธอิสระที่ทำงานได้ด้วยตัวเองอย่างสมบูรณ์นั้นมนุษย์อาจไม่สามารถสั่งยุติการทำงานของระบบอาวุธได้[112]

---

[111] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach." International Committee of the Red Cross, Paper, June 6, 2019, p. 3.

[112] Ibid., p. 6.

คณะกรรมการกาชาดระหว่างประเทศมีความเชื่อว่าแนวคิดในการนำเอาหลักความสัมพันธ์ระหว่างมนุษย์กับการทำงานของปัญญาประดิษฐ์ (Human-Centred Approach) มาประเมินความรับผิดตามกฎหมายเป็นสิ่งที่มีความเหมาะสม[113] เนื่องจากพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศจะต้องปรับใช้กับการกระทำของบุคคลซึ่งกระทำการในนามของรัฐ ไม่ว่าจะอยู่ในฐานะของผู้มีอำนาจในการสั่งการกองทัพ ผู้นำ หรือทหารเฉพาะรายบุคคลที่ละเมิดต่อข้อกฎหมาย และไม่มีความจำเป็นที่จะเปลี่ยนวิธีการบังคับใช้กฎหมายกับเครื่องจักรกล ซอฟท์แวร์ หรือระบบอัลกอริทึ่มเพราะสิ่งเหล่านี้เกิดจากการประดิษฐ์ของมนุษย์เพื่อการใช้งานของมนุษย์ทั้งสิ้น การพิจารณาความสัมพันธ์ระหว่างบุคคลผู้ควบคุมหรือผู้สั่งการระบบอาวุธและการทำงานของระบบอาวุธจึงมีความสอดคล้องต่อกฎหมายมนุษยธรรมระหว่างประเทศ

ปัญหาประการหนึ่งที่มีการกล่าวถึงในที่ประชุมของคณะกรรมการกาชาดระหว่างประเทศคือจริยธรรมในการใช้ปัญญาประดิษฐ์ ซึ่งเป็นประเด็นที่มีการกล่าวถึงโดยทั่วไปในสังคมในลักษณะว่าเมื่อมีการพัฒนาระบบปัญญาประดิษฐ์ขึ้นมาแล้ว ปัญญาประดิษฐ์ควรทำงานแทนมนุษย์มากเพียงใด ความรับผิดชอบของมนุษย์ต่อการทำงานของปัญญาประดิษฐ์ควรอยู่ในลักษณะใด ใช้เกณฑ์ใดในการพิจารณาระดับความรับผิดชอบของมนุษย์ต่อความเสียหายที่เกิดขึ้นจากปัญญาประดิษฐ์ ในขณะที่หากเป็นการใช้ปัญญาประดิษฐ์ในระบบอาวุธอิสระก็จะต้องคำนึงถึงจริยธรรมที่เกี่ยวข้องได้แก่ การพัฒนาระบบอาวุธอิสระควรทำในขอบเขตเพียงใด การใช้งานระบบอาวุธอิสระในลักษณะใดที่ควรใช้ได้และลักษณะใดที่ควรต้องห้าม ความรับผิดชอบของผู้ที่เกี่ยวข้องกับการออกแบบ การผลิต การใช้งาน การสั่งการระบบอาวุธอิสระควรมีการกำหนดเอาไว้อย่างไร[114] เป็นต้น

คณะกรรมการกาชาดระหว่างประเทศเห็นว่าการเรียนรู้ของปัญญาประดิษฐ์ (Machine Learning) ในปัจจุบันยังอยู่บนพื้นฐานของการสอนโดยมนุษย์เป็นสำคัญ[115] การสอนโดยมนุษย์หมายความรวมตั้งแต่ การเขียนโปรแกรมสั่งการ การกำหนดเงื่อนไขในระบบอัลกอริทึ่ม และการป้อนข้อมูลให้ระบบปัญญาประดิษฐ์จดจำเพื่อใช้ในการประมวลผลในขั้นต่อไป เนื่องจากระบบปัญญาประดิษฐ์ไม่สามารถเรียนรู้ด้วยตนเองทั้งหมดได้ อย่างไรก็ดีในอนาคตระบบปัญญาประดิษฐ์ที่มี

---

[113] International Committee of the Red Cross. “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.”: p. 6.

[114] Ibid., p. 8.

[115] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts. (2019), p. 28.

ความซับซ้อนมากขึ้นอาจมีการเรียนรู้ที่มากขึ้น สามารถตัดสินใจบนเงื่อนไขที่ซับซ้อนมากขึ้นและอาจนำไปสู่ปัญหาหลายประการต่อการปรับใช้กฎหมาย คณะกรรมการกาชาดระหว่างประเทศมองว่าหากรัฐหรือองค์กรผู้เกี่ยวข้องกับพัฒนาระบบอาวุธอิสระหรือการพัฒนาระบบปัญญาประดิษฐ์ได้เปิดเผยข้อมูลความก้าวหน้าของปัญญาประดิษฐ์ในปัจจุบัน จะก่อให้เกิดความชัดเจนในการสร้างแนวทางปรับใช้กฎหมายมากขึ้น

คณะกรรมการกาชาดระหว่างประเทศมองว่าหลักการทั่วไปของกฎหมายมนุษยธรรมระหว่างประเทศยังสามารถปรับใช้ได้กับระบบอาวุธอิสระที่มีปัญญาประดิษฐ์ประกอบรวมอยู่ด้วยแต่อาจจะต้องมีการสร้างหลักเฉพาะเพื่อเสริมหลักทั่วไป ซึ่งอาจอยู่ในรูปแบบของแนวทาง (Guideline) หรือกฎเกณฑ์การใช้ปัญญาประดิษฐ์หรือกฎเกณฑ์เกี่ยวกับการเรียนรู้ของจักรกล (Machine Learning) ในสถานการณ์การขัดกันทางอาวุธ โดยจะต้องสอดคล้องกับหลักการพิจารณาความรับผิดชอบของบุคคลต่อการใช้งานระบบอาวุธในการขัดกันทางอาวุธด้วย[116]

อาจกล่าวได้ว่าแนวทางการศึกษาของคณะกรรมการกาชาดระหว่างประเทศเป็นการศึกษาการใช้งานระบบอาวุธอิสระ (Autonomous Weapons System) ที่สอดคล้องกับแนวทางการพิจารณาความรับผิดที่เกิดจากการใช้งานปัญญาประดิษฐ์ โดยให้ความสำคัญกับเรื่องระดับความสัมพันธ์ระหว่างมนุษย์กับจักรกล แต่คณะกรรมการกาชาดระหว่างประเทศไม่ได้ให้ความสำคัญกับปัญหาทางกฎหมายที่จะเกิดขึ้น และยังขาดรายละเอียดเกี่ยวกับข้อท้าทายหลายประการเกี่ยวกับการใช้งานระบบอาวุธอิสระ

(2.2) ระบบอาวุธอิสระกับกฎหมายมนุษยธรรมระหว่างประเทศ

งานศึกษาของ Egeland เรื่อง Autonomous Weapon Systems under International Humanitarian Law ได้อธิบายความสำคัญของหุ่นยนต์อิสระทางการทหาร (Autonomous Military Robot) หรือหุ่นยนต์สังหาร (Killer Robot) ซึ่งมีการนำมาพิจารณาในแผนงานของอนุสัญญาว่าด้วยการห้ามอาวุธตามแบบบางชนิด (Convention on Certain Conventional Weapons) ในเดือนพฤษภาคม ค.ศ.2014

งานศึกษาของ Egeland ยังคงใช้กรอบแนวคิดแบบเดียวกับคณะกรรมการกาชาดระหว่างประเทศว่าการพิจารณาความสัมพันธ์ระหว่างการควบคุมโดยมนุษย์กับเครื่องจักรกลเป็นเรื่อง

---

[116] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts. (2019), p. 28.

สำคัญ (Meaningful Human Control) และควรเป็นเกณฑ์ในการพิจารณาความรับผิดชอบที่เกิดจากการใช้งานระบบอาวุธ[117]

Egeland เห็นว่าการใช้งานระบบอาวุธอิสระ (Autonomous Weapon Systems) จะต้องคำนึงถึงหลักการแยกแยะระหว่างพลรบและคนที่ไม่ใช่พลรบ หลักความได้สัดส่วนในการโจมตี ซึ่งสามารถพิจารณาได้จากผลที่เกิดขึ้นจากการใช้และปัจจัยที่ใช้ นอกจากนั้นยังต้องสอดคล้องกับหลักความระมัดระวังล่วงหน้าในการโจมตี

ประเด็นสำคัญคือ Egeland เสนอว่าระบบอาวุธสังหารอิสระที่ไม่มีมนุษย์ควบคุมเลยควรเป็นสิ่งต้องห้ามตามกฎหมาย และเสนอว่าแม้กฎหมายมนุษยธรรมจะสามารถปรับใช้กับระบบอาวุธสังหารอิสระได้ก็ควรมีอนุสัญญาเฉพาะเรื่องที่ห้ามการใช้อาวุธดังกล่าวด้วยเช่นกัน

Egeland อ้างถึงการให้นิยามความหมายของคำว่า Autonomous Weapons Systems ของคณะกรรมการกาชาดระหว่างประเทศนิยามคำว่าระบบอาวุธอิสระ หมายถึง อาวุธที่สามารถคัดเลือกเป้าหมายและโจมตีเป้าหมายได้โดยอิสระ[118] แต่โดยนิยามนี้มีข้อน่าสังเกตหลายประการ ได้แก่[119]

ประการที่ 1 คำว่า “เป้าหมาย” ในยุทธวิธีทางการทหารนั้นแตกต่างจาก “เป้าหมาย” ของหลักการแยกแยะตามกฎหมายมนุษยธรรม เพราะเป้าหมายทางการทหารย่อมหมายถึงการโจมตีเป้าหมายที่จะก่อให้เกิดความได้เปรียบทางการรบทั้งหมดซึ่งกว้างขวางมาก แต่ตามกฎหมายมนุษยธรรมระหว่างประเทศหมายถึงเป้าหมายที่แยกระหว่างทหารและพลเรือนรวมถึงทรัพย์สิ่งของพลเรือน โดยเป้าหมายที่สามารถโจมตีได้ต้องเป็นเป้าหมายทางการทหารเท่านั้น คำว่าเป้าหมายจึงไม่ชัดเจนเสียทีเดียว นอกจากนั้นยังน่าสงสัยว่าหุ่นยนต์สังหารนั้นจะสามารถแยกแยะเป้าหมายพลเรือนและทหารได้เพียงใด

ประการที่ 2 คำว่า “เลือกเป้าหมาย” ไม่ชัดเสียทีเดียวว่าเลือกจากอะไร ระหว่างการเลือกตามโปรแกรมสั่งการที่มนุษย์ผู้เขียนโปรแกรมกำหนดเอาไว้ หรือการเลือกจากการคำนวณเองโดยเจตจำนงอิสระของหุ่นยนต์

---

[117] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law", Nordic Journal of International Law, 85, 2 (2016): 90.

[118] International Committee of the Red Cross, ‘Report of the ICRC Expert Meeting on ‘Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects’, 26–28 March 2014, Geneva, p. 1.

[119] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law", Nordic Journal of International Law, 85, 2 (2016): 94.

ประการที่ 3 หากเกิดกรณีที่การเลือกเป้าหมายนั้นเป็นความเข้าใจผิด หุ่นยนต์จะสามารถเปลี่ยนใจในตอนหลังก่อนการโจมตีได้หรือไม่ กรณีที่อาวุธสังหารอิสระไม่สามารถจำแนกระหว่างพลเรือนและทหารได้ อาวุธเหล่านี้ก็จะไม่แตกต่างจากทุ่นระเบิดสังหารบุคคลโดยปกติเลย

ขณะที่คำว่า “Autonomy” เองก็มีปัญหาในตัวเอง เพราะความหมายโดยทั่วไป Autonomy ย่อมหมายความถึงการคิด ตัดสินใจโดยเจตจำนงเสรี (Free Will) แต่คำว่า Autonomy ในเชิงหุ่นยนต์นั้นไม่ได้หมายความถึงเจตจำนงเสรีดังกล่าว แต่มีความหมายถึงการทำงานของหุ่นยนต์ที่สามารถตัดสินใจทำงานโดยปราศจากการควบคุมของมนุษย์ในสถานการณ์ดังกล่าวเท่านั้น ดังนั้นเมื่อนักกฎหมายพูดถึงประเด็น Autonomy ก็น่าคิดว่า Autonomy ในลักษณะใด ยังไม่แน่ชัด[120] แม้กระทั่งการให้นิยามโดย Corn ที่เห็นว่า ระบบอาวุธสังหารอิสระคือระบบอาวุธที่อาศัยการทำงานของปัญญาประดิษฐ์ซึ่งสามารถจำแนกสิ่งต่างๆ ได้โดยใช้เหตุผลแบบเดียวกับที่มนุษย์ใช้[121] นิยามดังกล่าวนี้อาจมีประโยชน์เพียงกรณีการแบ่งแยกระดับความเป็นอิสระแต่ก็ไม่ได้แยกแยะไปไกลถึงการทำงานของหุ่นยนต์ในลักษณะไซบอร์กหรือหุ่นยนต์สังหารเช่นที่ปรากฏในภาพยนตร์ The Terminator แต่อย่างใด[122]

ประเด็นน่าพิจารณาตามหลักกฎหมายมนุษยธรรมระหว่างประเทศคือ

ประเด็นที่ 1 อาวุธบางประเภทต้องห้ามตามกฎหมายเฉพาะ และขัดกับหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศด้วย เช่น อาวุธเคมี อาวุธชีวภาพ อาวุธเลเซอร์ ทุ่นระเบิดสังหารบุคคล ฯลฯ ส่วนหนึ่งเป็นเพราะอาวุธเหล่านี้ขัดต่อหลักความเสียหายเกินขนาดด้วย

ประเด็นที่ 2 อาวุธบางชนิดไม่ได้ขัดต่ออนุสัญญาเฉพาะเรื่องแต่ขัดต่อหลักความเสียหายเกินขนาด เช่น อาวุธนิวเคลียร์ แต่ก็ไม่ได้หมายความว่าจะใช้ไม่ได้ในสถานการณ์อื่นๆ นอกการขัดกันทางอาวุธ

ประเด็นที่ 3 อาวุธบางชนิดอาจใช้แล้วผิดกฎหมายแม้จะไม่ได้เป็นการขัดต่อหลักความเสียหายเกินขนาด เช่น นิวเคลียร์ไม่ได้ผิดกฎหมายในตัวมันเองแต่เป็นการยากที่จะใช้อาวุธนิวเคลียร์โดยแบ่งแยกเป้าหมายการทำลายได้

---

[120] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law," : 95.

[121] Geoffrey S. Corn, ‘Autonomous Weapon Systems: Managing the Inevitability of “Taking the Man out of the Loop,”’ Chapter, in Autonomous Weapons Systems: Law Ethics, Policy, edited by Nehal Bhuta, Susanne Beck, Robin Geib, Hin-Yan Liu and Claus Kreb, (Cambridge: Cambridge University Press, 2016), p. 210.

[122] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law": 97.

จากปัญหาเกี่ยวกับความหมายที่ชัดเจนของระบบอาวุธอิสระ (Autonomous Weapon Systems) ทำให้ Egeland เห็นว่าความหมายของระบบอาวุธอิสระ (Autonomous Weapon Systems) ควรหมายถึงการทำงานของระบบอาวุธที่ตัดความสัมพันธ์ระหว่างบุคคลผู้ใช้อาวุธออกจากการทำงานของอาวุธในขณะที่มีการสั่งการโจมตี[123]

กรณีการใช้งานอากาศยานไร้คนขับแบบติดอาวุธของกองทัพสหรัฐอเมริกาที่มีการกล่าวอ้างว่ามีระบบการจำแนกเป้าหมายได้นั้น มีการยืนยันว่าอากาศยานไร้คนขับจะทำการค้นหาเป้าหมายผู้ต้องสงสัยจากกล้องซึ่งติดตั้งอยู่กับอากาศยานและทำการจำแนกเป้าหมายโดยพิจารณาจากตำแหน่งที่ตั้ง เพศของเป้าหมายและพฤติกรรมที่น่าสงสัยของเป้าหมาย ดังนั้นหากการแต่งตัวของบุคคลดังกล่าวตรงกับข้อมูลที่ถูกโปรแกรมว่าเป็นผู้ต้องสงสัย อากาศยานไร้คนขับก็อาจระบุเป้าหมายดังกล่าวว่าเป็นผู้ก่อการร้ายได้ ในปัจจุบันยังไม่พบรายงานอย่างเป็นทางการว่าอากาศยานไร้คนขับมีความสามารถการจำแนกเป้าหมายระหว่างทหารและพลเรือนได้ ระบบอากาศยานไร้คนขับในปัจจุบันจึงเป็นระบบการตัดสินใจโดยมนุษย์ก่อนเป็นหลัก (Predetermined)[124]

อากาศยานไร้คนขับแบบ RQ-9 Reaper เป็นอากาศยานที่สามารถใช้ระบบนำทางและค้นหาเป้าหมายได้ด้วยตัวเองแต่การตัดสินใจขั้นสุดท้ายหากจะมีการทำลายเป้าหมายจะอยู่บนพื้นฐานของการควบคุมทางไกลของมนุษย์[125] อย่างไรก็ดี เป็นไปได้ว่าในอนาคตนั้นอากาศยานรูปแบบดังกล่าวอาจไม่ต้องควบคุมโดยมนุษย์แต่ใช้คอมพิวเตอร์และระบบปัญญาประดิษฐ์ควบคุมแทนทั้งหมด[126]

การกล่าวอ้างว่าอากาศยานไร้คนขับในปัจจุบันพัฒนาไปอย่างมาก ได้แก่ อากาศยานไร้คนขับแบบ MQ-1 Predator นั้นสามารถอยู่ในอากาศได้นานถึง 14 ชั่วโมง ในขณะที่เครื่องบินรบ F-16 และเครื่องบินรบ A-10 สามารถอยู่ในอากาศได้นานที่สุดเพียง 4 ชั่วโมงเท่านั้น โอกาสในการที่อากาศยานไร้คนขับจะใช้เวลาตรวจสอบเป้าหมายก่อนการโจมตีจึงมีมากกว่าและมีโอกาสที่จะแยกแยะเป้าหมายทางการทหารและพลเรือนมากกว่าเครื่องบินรบ และหากเปรียบเทียบกับการยิงจรวดร่อน (Cruise Missiles) รวมถึงขีปนาวุธข้ามทวีป (Intercontinental Ballistic Missiles)

---

[123] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law": 99.

[124] Ibid., p. 100.

[125] Noel Sharkey, "Cassandra or False Prophet of Doom: AI Robots and War," IEEE Intelligent Systems, vol. 23, no. 4, July-Aug. 2008, p. 16.

[126] Annabelle Quince, "Future Drone Strikes Could See Execution by Algorithm," ABC Online, January 21, 2013., [online] Accessed: July 24, 2020. Available from: https://www.abc.net.au/radionational/programs/rearvision/drones/4703792

อากาศยานไร้คนขับจะยิงอาวุธในระยะที่ใกล้เป้าหมายได้มากกว่า มีโอกาสตัดสินใจเมื่ออยู่ใกล้เป้าหมายมากกว่าจรวดและขีปนาวุธ ทำให้ความแม่นยำในการโจมตีและการจำกัดขอบเขตความเสียหายย่อมมีความชัดเจนมากกว่าจรวดและขีปนาวุธ[127]

Kilcullen และ Exum ผู้เชี่ยวชาญทางการทหารเห็นว่าปัญหาไม่ได้อยู่ที่เทคโนโลยีอากาศยานไร้คนขับแต่ปัญหาเกิดขึ้นจากการใช้งาน จากการศึกษาพบว่าการใช้งานอากาศยานไร้คนขับนั้นก่อให้เกิดความเสียหายในลักษณะเดียวกับเครื่องบินรบ แต่สิ่งที่แตกต่างอย่างมากคือระบบปัญญาประดิษฐ์ที่ติดตั้งในอากาศยานไร้คนขับซึ่งไม่ใช่สิ่งที่ปรากฏทางกายภาพเลย[128]

จากงานศึกษาของ Egeland จะเห็นได้ว่ามีการกล่าวถึงประเด็นความจำเป็นในการมีอนุสัญญาระหว่างประเทศเฉพาะเรื่องเพื่อการควบคุมอาวุธสังหารอิสระ[129] ซึ่งมีข้อน่าพิจารณาสำคัญว่าโดยทั่วไปอนุสัญญาระหว่างประเทศที่เกี่ยวข้องกับอาวุธเฉพาะอย่างนั้นมักเป็นกฎหมายที่ควบคุมอาวุธนอกสถานการณ์การขัดกันทางอาวุธ มีอนุสัญญาระหว่างประเทศน้อยเรื่องมากที่จะมีข้อกำหนดห้ามใช้อาวุธเฉพาะอย่างในการขัดกันทางอาวุธ และแม้ว่าอนุสัญญาเหล่านั้นจะมีข้อกำหนดห้ามการใช้อาวุธเฉพาะอย่างในการขัดกันทางอาวุธ ข้อกำหนดเหล่านั้นก็มักจะเกี่ยวข้องกับหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศตามที่ปรากฏในข้อ 35 ของพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 เช่น หลักการห้ามใช้ปัจจัยหรือวิธีการในการขัดกันทางอาวุธที่ก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น การห้ามใช้วิธีการหรือปัจจัยที่ไม่สามารถแยกแยะเป้าหมายการทำลายได้ แม้กระทั่งการใช้วิธีการดัดแปลงสภาพแวดล้อมเพื่อการทำลายเป้าหมาย

อนุสัญญาระหว่างประเทศหลายฉบับมักเป็นการควบคุมอาวุธเฉพาะอย่างเกี่ยวกับเรื่องการห้ามผลิต ห้ามสะสม ห้ามโอน ห้ามพัฒนา ฯลฯ ซึ่งอยู่ในกรอบกฎหมายว่าด้วยการลดอาวุธ (Disarmament) แต่มิได้ว่าด้วยเรื่องความชอบด้วยกฎหมายในการใช้อาวุธในการขัดกันทางอาวุธ ในขณะที่เทคโนโลยีที่เกิดขึ้นใหม่เช่นระบบอาวุธสังหารอิสระ (Autonomous Weapon Systems) นั้น เป็นการใช้งานอาวุธควบคู่ไปกับเทคโนโลยีอื่นที่ไม่ใช่อาวุธโดยตรง เช่น การใช้งานหุ่นยนต์สังหารย่อมประกอบด้วยการประมวลผลของคอมพิวเตอร์ โปรแกรมประมวลผลแบบอัลกอริทึ่ม ระบบการคิดและตัดสินใจแบบปัญญาประดิษฐ์ ร่วมกับระบบการใช้อาวุธของหุ่นยนต์ หากตัดองค์ประกอบ

---

[127] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law", p. 101.

[128] Ibid., p. 102.

[129] Ibid.

เทคโนโลยีส่วนอื่นที่ไม่ใช่การใช้อาวุธของหุ่นยนต์ออกไป ก็แทบจะไม่มีการใช้งานระบบอาวุธที่แตกต่างไปจากการใช้งานอาวุธเดิมเลย องค์ประกอบของเทคโนโลยีส่วนที่ประกอบรวมกันจนก่อให้เกิดความสามารถในการใช้อาวุธได้เหล่านี้ล้วนแล้วแต่ไม่ใช่อาวุธทั้งสิ้น แต่เทคโนโลยีเหล่านี้เป็นวิธีการที่ก่อให้เกิดการใช้งานอาวุธที่เปลี่ยนแปลงไป การสร้างกฎหมายเฉพาะเพื่อควบคุมเทคโนโลยีย่อมอาจเป็นการไม่เหมาะสม เพราะหากควบคุมเทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพเหล่านี้ ย่อมกระทบการใช้งานเทคโนโลยีของพลเรือนที่เกี่ยวข้องด้วย

(3) ประเด็นเรื่องประสิทธิผลของการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

Kennedy เห็นว่าแม้กฎหมายมนุษยธรรมระหว่างประเทศจะพยายามสร้างกฎเกณฑ์เพื่อการการปกป้องความเสียหายของพลเรือนแต่ในความเป็นจริงการหวังผลเช่นนั้นเป็นเรื่องที่ยากมาก[130] และแทบสร้างตัวชี้วัดความสำเร็จของการใช้กฎหมายที่เป็นรูปธรรมไม่ได้ เพราะในสงครามนั้นทุกกองทัพต่างหวังผลสำเร็จคือความแพ้-ชนะ ปฏิบัติการทางทหารในสงครามย่อมเลือกยุทธวิธีในการทำลายขีดความสามารถของกองทัพฝ่ายตรงข้ามให้ได้มากที่สุด และยิ่งคำนึงถึงกระบวนการเกี่ยวกับการกำหนดเป้าหมายในการรบซึ่งเป็นหลักนิยมของกองทัพแล้วจะยิ่งเห็นว่าการทำลายขีดความสามารถของฝ่ายศัตรูย่อมก่อให้เกิดผลกระทบต่อพลเรือนไม่มากก็น้อย แม้ว่าหลักความจำเป็นทางการทหารจะห้ามการก่อความเสียหายทางพลเรือนโดยตรงก็ตาม แต่สงครามหลายครั้งก็ปรากฏความเสียหายแก่พลเรือนอยู่เสมอ

นอกจากนั้นยังปรากฏว่าบทบาทที่กองทัพควรจะทำคือการส่งเสริมความรู้ความเข้าใจในการคุ้มครองความมีมนุษยธรรมในการทำสงครามยังเป็นเพียงฉากบังหน้าการค้าอาวุธสงครามเท่านั้น Kennedy อ้างถึงข้อเท็จจริงในการอบรมเกี่ยวกับปฏิบัติการทางทหารให้แก่กองกำลังเซเนกัล โดยผู้ให้การอบรมคือหน่วยงาน U.S. Naval Justice School (โดยการอบรมนี้มีการจัดขึ้นทั้งหมดกับกองทัพชาติต่างๆ ราว 53 ประเทศ) สิ่งที่ควรจะเน้นในการอบรมนี้คือหลักกฎหมายมนุษยธรรมระหว่างประเทศ การคุ้มครองบุคคลในการขัดกันทางอาวุธและการปฏิบัติต่อกันอย่างมีมนุษยธรรม แต่ในความเป็นจริงหลักการด้านมนุษยธรรมกลับไม่ใช่ประเด็นหลักที่มีการส่งเสริม ตรงกันข้าม เวทีนี้

[130] David Kennedy, Reassessing International Humanitarianism: The Dark Side, (Oxford: Princeton University Press, 2004), p.3.

กลายเป็นพื้นที่ในการเสนอขายอาวุธทันสมัยของอเมริกา และการเสนอหลักการที่กองทัพอเมริกันใช้ในการสงครามเพื่อเป็นแนวทางให้กองทัพชาติต่างๆ ได้นำหลักนิยมของกองทัพอเมริกันไปใช้[131]

Kennedy มีความเห็นว่าในทางปฏิบัตินั้นหลักการป้องกันตนเอง หลักความได้สัดส่วน และหลักความจำเป็นทางการทหารมักจะถูกขยายขอบเขตออกไปมากจนเกิดความบิดเบือน ซึ่งในหลายกรณีการป้องกันตนเองถูกขยายขอบเขตไปจนเป็นการคุกคาม และปฏิบัติการทางทหารที่ควรคำนึงถึงหลักความจำเป็นทางการทหารกลายเป็นการสร้างความเสียหายมากกว่าการจำกัดการก่อความเสียหาย [132]

Kennedy กล่าวว่า ครั้งหนึ่งเขาเคยบรรยายหลักกฎหมายทหารและหลักการเข้าปะทะให้กับโรงเรียนนายเรือ หลังจากเสร็จสิ้นการบรรยายและนักกฎหมายที่เข้ามาฟังการบรรยายออกจากห้องประชุมไปแล้ว ผู้บังคับบัญชารายหนึ่งเข้ามาในห้องอบรมเพื่อสรุปหลักการว่า “พวกคุณไม่ต้องทำอะไร พวกคุณไม่ต้องคิดถึงเรื่องความจำเป็น แค่ปกป้องตัวเองให้ได้ก็พอ ที่สำคัญคือพยายามอย่าให้ถูกฆ่าเวลาออกรบ” ประโยคนี้เป็นตลกร้ายอย่างมาก แต่สะท้อนให้เห็นว่าสิ่งที่ทหารมองว่าเป็นเรื่องสำคัญในสงครามคือการรักษาชีวิตของตน การจะไปคุ้มครองผู้อื่นอาจเป็นเรื่องสำคัญรองลงมา เพราะเป้าหมายในการทำสงครามคือเพื่อชันชนะของกองทัพตนเอง หากทหารฝ่ายตนไม่เสียชีวิตและสามารถทำลายชีวิตทหารฝ่ายตรงข้ามได้มากกว่า ก็ย่อมแสดงว่ากองทัพมีศักยภาพเพียงพอที่จะชนะในการสงครามนั้นได้[133]

การโจมตีที่ก่อให้เกิดความเสียหายเกินความจำเป็นทางการทหารที่ Kennedy เสนอตัวอย่างได้แก่กรณีสงครามอ่าวเปอร์เซียซึ่งไม่ได้มีการโจมตีเฉพาะเป้าหมายทางการทหารเท่านั้น แต่ปรากฏการโจมตีโรงงานผลิตกระแสไฟฟ้า การโจมตีระบบประปา ฯลฯ การโจมตีสาธารณูปโภคเหล่านี้หากมองในมุมของกระบวนการกำหนดเป้าหมายซึ่งเป็นยุทธวิธีทางการทหารอาจสะท้อนให้เห็นว่าสาธารณูปโภคเช่นไฟฟ้ามีความเกี่ยวข้องกับการใช้งานระบบอาวุธของกองทัพ หากทำลายระบบไฟฟ้าได้กองทัพฝ่ายตรงข้ามย่อมสูญเสียความได้เปรียบในการทำการรบ ในขณะที่เมื่อระบบประปาถูกทำลายก็จะส่งผลต่อการสนับสนุนการรบของกองทัพ เมื่อกองทัพขาดอาหารและน้ำก็จะมีโอกาสเป็นฝ่ายแพ้มากขึ้น แต่ในทำนองกลับกันความเสียหายที่เกิดขึ้นกับระบบไฟฟ้าและประปานี้ก็ส่งผลกระทบต่อพลเรือนที่ควรได้รับความคุ้มครองตามกฎหมายด้วย ความเสียหายที่เกิดขึ้นแก่การพลเรือนอย่าง

---

[131] David Kennedy, Reassessing International Humanitarianism: The Dark Side, p.5.

[132] Ibid., p. 5.

[133] Ibid., p.7.

เกินความจำเป็นในวงกว้างนี้ เป็นสิ่งที่สังคมระหว่างประเทศประณามเพราะไม่สอดคล้องต่อหลักกฎหมาย อย่างไรก็ดีกองทัพผู้กระทำการก็มักจะมีปฏิกิริยาตอบสนองต่อสังคมระหว่างประเทศโดยการออกมาแสดงความรับผิดชอบโดยกล่าวว่าเป็นความผิดพลาดในปฏิบัติการ[134] การจะพิสูจน์ว่าความเสียหายนั้นมาจากความตั้งใจหรือความผิดพลาดย่อมทำได้ยาก คงทำได้เพียงพิจารณาจากระดับความเสียหายที่เกิดขึ้นจากปฏิบัติการดังกล่าวเท่านั้น

Kennedy สรุปว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่ได้เป็นอิสระจากการเมืองและยุทธศาสตร์ทางการทหารในการปฏิบัติเพื่อหวังชัยชนะในสงคราม ในการทำสงครามจึงมักพบการกระทำที่ขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศอยู่เสมอในขณะที่อำนาจทางการเมืองระหว่างประเทศที่เหนือกว่าจะเป็นสิ่งที่ทำให้รัฐใดรัฐหนึ่งได้เปรียบจากทั้งการใช้ยุทธวิธีที่เหนือกว่าและการปฏิเสธความรับผิดชอบทางกฎหมายในกรณีที่มีการละเมิดต่อกฎหมายระหว่างประเทศ[135]

ความเป็นจริงคือเมื่อใดก็ตามที่เกิดสงครามก็จะนำไปสู่ความเสียหายแก่ชีวิตของพลเรือนเสมอ การโยนภาระทั้งหมดไปให้กฎหมายมนุษยธรรมระหว่างประเทศอาจไม่ใช่ทางออกของปัญหาด้วยเหตุและปัจจัยที่กล่าวมาทั้งหมด การทำให้หลักมนุษยธรรมยังคงปรากฏในการทำสงครามย่อมเป็นหน้าที่ของกองทัพคู่พิพาทเพราะจะเป็นการป้องกันไม่ให้เกิดปัญหาขึ้นแต่ต้น แต่ในทางปฏิบัติคงทำได้ยากเนื่องจากการเกิดสงครามแต่ละครั้งอาจมีเหตุที่แตกต่างกันและนำไปสู่การตัดสินใจของคู่พิพาทในการเลือกวิธีการทำลายฝ่ายตรงข้ามที่แตกต่างกันด้วย

อย่างไรก็ดี สิ่งที่ยังคงต้องคำนึงถึงเสมอคือความรับผิดชอบทางการเมืองของรัฐเพราะปฏิสัมพันธ์ระหว่างการเมืองและสงครามในปัจจุบันแทบจะไม่สามารถแยกออกจากกันได้[136]

อาจกล่าวได้ว่างานของ Kennedy เป็นงานที่สร้างมุมมองเชิงรัฐศาสตร์เป็นสำคัญโดยมีทัศนะว่ากฎหมายแต่เพียงอย่างเดียวอาจไม่ใช่คำตอบในการแก้ไขปัญหาทุกประการและหลายกรณีก็ปรากฏชัดเจนว่าการมีกฎหมายแต่เพียงอย่างเดียวยังนำไปสู่การละเมิดอยู่บ่อยครั้ง ยิ่งเมื่อเป็นกฎหมายระหว่างประเทศด้วยแล้วยิ่งสัมพันธ์กับอำนาจทางการเมืองระหว่างประเทศขึ้นไปอีก การจะบังคับใช้กฎหมายระหว่างประเทศจึงต้องพิจารณาความเป็นจริงในสังคมระหว่างประเทศประกอบไปด้วย แต่ไม่ได้หมายความว่ากฎหมายไม่มีความสำคัญเสียเลยเพราะอย่างน้อยที่สุดกฎหมายระหว่างประเทศก็

---

[134] David Kennedy, Reassessing International Humanitarianism: The Dark Side, p. 10.

[135] Ibid., p. 12.

[136] David Kennedy, "Modern War and Modern Law," University of Baltimore Law Review, Vol. 36, Issue 2, (2007): 472.

สร้างแนวทางและมาตรฐานในการปฏิบัติเอาไว้ เพียงแต่การจะทำตามกฎหมายอย่างเคร่งครัดเพื่อให้เกิดผลสัมฤทธิ์นั้นย่อมขึ้นอยู่กับปัจจัยหลายประการและนักกฎหมายจะต้องตระหนักถึงปัจจัยเหล่านี้นอกเหนือจากการให้ความสำคัญกับกฎหมายแต่เพียงอย่างเดียวด้วย

งานของ Kennedy จึงเป็นงานที่สร้างมุมมองที่กว้างขวางกว่างานนิติศาสตร์ทั่วไปและสร้างแนวทางในการวิเคราะห์ปัญหาประเด็นการบังคับใช้กฎหมายที่ไม่ได้พิจารณาแต่หลักเกณฑ์ที่ปรากฏแต่ให้ความสำคัญกับปรากฏการณ์ที่เกิดขึ้นจริงในสังคมระหว่างประเทศด้วย

(4) ข้อท้าทายของอาวุธไซเบอร์และความจำเป็นในการสร้างกฎหมายระหว่างประเทศเพื่อควบคุมอาวุธไซเบอร์

งานศึกษาของ Tasdemmir และ Albayrak เห็นว่าโลกไซเบอร์ถูกนำมารวมเป็นส่วนหนึ่งของปัจจัยในการขัดกันทางอาวุธยุคใหม่แต่การใช้ปฏิบัติการทางไซเบอร์ในฐานะอาวุธกลับไม่ได้ถูกห้ามตามกฎหมาย ซึ่งปฏิบัติการทางไซเบอร์ควรจะต้องอยู่ภายใต้หลักการแยกแยะและความได้สัดส่วน แม้ว่าสถานะของพื้นที่ทางไซเบอร์จะแตกต่างจากพื้นที่ของโลกทางกายภาพก็ตาม สิ่งที่ยากประการหนึ่งคือการระบุตัวผู้ปฏิบัติการทางไซเบอร์ ซึ่งจะทำให้การปรับใช้หลักกฎหมายว่าด้วยการขัดกันทางอาวุธนั้นยากขึ้นไปอีก โดยเฉพาะอย่างยิ่งในยุคปัจจุบันพลเรือนมีบทบาทมากขึ้นในการใช้งานระบบไซเบอร์ ยิ่งทำให้การกำหนดเป้าหมายการโจมตีที่ชอบด้วยกฎหมายนั้นยากขึ้นด้วย[137]

Tasdemmir และ Albayrak ยอมรับในแนวทางการตีความว่า การพิจารณาการมีส่วนร่วมโดยตรงในการขัดกันทางอาวุธนั้นจะต้องสอดคล้องกับความสัมพันธ์โดยตรงระหว่างการกระทำและผลด้วย (Direct Causal Link) โดยเปรียบเทียบว่า การพัฒนาและการใช้โปรแกรมคอมพิวเตอร์เพื่อการทำลายเป้าหมายทางการทหาร ถือเป็นผลโดยตรงระหว่างการกระทำและผลในการสู้รบ จึงเข้าข่ายการมีส่วนร่วมในการสู้รบ เช่นเดียวกับการที่พลเรือนขับรถขนส่งระเบิดเข้าไปในพื้นที่สงครามแต่การเขียนโปรแกรมคอมพิวเตอร์ทั่วไปไม่ถือว่ามีความสัมพันธ์โดยตรงต่อการทำสงคราม เทียบได้กับการที่พลเรือนขับรถขนส่งระเบิดจากโรงงานผลิตไปยังท่าเรือก่อนที่เรือจะขนส่งระเบิดไปยังพื้นที่สงครามต่อไป[138]

---

[137] Fatma Tasdemmir and Gokhan Albayrak, “The Law of Cyber Warfare In Terms of Jus Ad Bellum and Jus In Bello: Application of International Law to the Unknown.” E-journal of Law, Vol 3 (2), (2017): 6. [online] accessed May 10, 2021. Available from: https://papers.ssrn. com/sol3/papers.cfm?abstract_id=3092654

[138] Ibid.

กล่าวโดยสรุป การปรับใช้กฎหมายในปฏิบัติการโจมตีทางไซเบอร์ในปัจจุบันนั้นเป็นความพยายามใช้กฎหมายกับสิ่งที่ไม่เป็นรูปธรรมเพราะสภาพแวดล้อมที่เปลี่ยนไปในพื้นที่ทางไซเบอร์ทำให้การระบุตัวผู้ปฏิบัติการทำได้ยากขึ้นและการระบุที่ตั้งของกลุ่มปฏิบัติการก็ยังเป็นไปได้ยาก ดังนั้น การสร้างกฎหมายระหว่างประเทศเฉพาะด้านในเรื่องการโจมตีทางไซเบอร์จึงเป็นเรื่องจำเป็นเพื่อรับมือของรูปแบบการทำสงครามที่เปลี่ยนแปลงไป

ขณะที่ Piatkowski เห็นว่านิยามของการขัดกันทางอาวุธควรจะมีการเปลี่ยนแปลงไป โดยคำนึงถึงองค์ประกอบเพิ่มเติมอันได้แก่ น้ำหนักการกระทำ สัดส่วนการกระทำ ความรุนแรงของการกระทำ และองค์ประกอบอื่นๆ ที่แสดงออกซึ่งเจตนาในการก่อสงครามระหว่างคู่พิพาท ทั้งนี้จะต้องคิดถึงการโจมตีทางไซเบอร์ฝ่ายเดียวด้วยว่าการกระทำระดับใดจึงถือว่ามีผลเท่ากับการใช้กำลัง โดยแนวคิดนี้ปรากฏใน Tallinn Manual ฉบับที่ 2 ด้วย Piatkowski จึงเสนอนิยามใหม่ว่าการขัดกันทางอาวุธในพื้นที่ไซเบอร์ควรหมายถึง “การใช้กำลังระหว่างรัฐที่ถึงระดับและความรุนแรงโดยเจตนาเพื่อก่อให้เกิดการโจมตีและการป้องกัน”[139]

Piatkowski เห็นว่าเหตุการณ์เดียวของปฏิบัติการทางไซเบอร์ที่เทียบเท่ากับการใช้กำลังทางอาวุธคือการโจมตีทางไซเบอร์ต่อโรงไฟฟ้าที่ยูเครนโดยปฏิบัติการดังกล่าวไม่มีการตอบโต้จากกองกำลังของรัฐแต่อย่างใดเนื่องจากไม่สามารถพิสูจน์ที่ตั้งของผู้ปฏิบัติการและเขตอำนาจของรัฐต่างประเทศซึ่งเป็นที่ตั้งของผู้ปฏิบัติการได้[140]

กล่าวโดยสรุป Piatkowski เห็นควรให้มีการสร้างนิยามใหม่ของการโจมตีทางไซเบอร์นอกเหนือจากนิยามที่เกิดขึ้นในศาล ICTY คดี Tadic ซึ่งเกิดมานานกว่า 20 ปีแล้ว เพื่อให้นิยามของการโจมตีทางไซเบอร์ครอบคลุมเพียงพอต่อเหตุการณ์ในอนาคตที่อาจมีผลเท่ากับการโจมตีด้วยกำลังอาวุธจริง และสอดคล้องกับหลักการกระทำที่เป็นปรปักษ์ และการสร้างกฎหมายระหว่างประเทศใหม่นี้จะยังทำให้เกิดแนวทางปฏิบัติระหว่างคู่พิพาทในการขัดกันทางอาวุธที่ชัดเจนขึ้นด้วย

งานศึกษาของ Mills อ้างว่าการโจมตีทางไซเบอร์ในสนามรบปัจจุบันอาจแบ่งได้เป็น 3 ลักษณะ ได้แก่[141]

---

[139] Mateusz Piatkowski, “The Definition of the Armed Conflict in the Conditions of Cyber Warfare,” Polish Political Science Yearbook, vol. 46 (1), (2017): 271-280.

[140] Ibid., p. 276.

[141] Ivoty Mills, “Emergent International Humanitarian Law in the Context of Cyber Warfare,” Transmission: The Journal of Film and Media Studies, Vol 2, No.1. (2017): 78-99.

ประการที่ 1 Syntactic Attacks คือการเข้าถึงระบบเครือข่ายทางไซเบอร์เพื่อเปลี่ยนแปลง แก้ไข ขัดขวาง ทำลายระบบปฏิบัติการทางคอมพิวเตอร์ซึ่งอาจไม่สามารถคาดหมายวิธีการได้เช่นการใช้ malware, DDoS การ Hack ข้อมูล

ประการที่ 2 Semantic Attacks เป็นปฏิบัติการโจมตีต่อเป้าหมายเฉพาะ เช่นการเข้าถึงระบบปฏิบัติการหรือข้อมูลทางการทหารหรือรัฐบาลเพื่อทำลายระบบการสื่อสารและการเชื่อมต่อข้อมูล โดยที่ขณะปฏิบัติการนั้นเป้าหมายจะยังสามารถปฏิบัติการได้ตามปกติ นอกจากนั้นยังหมายถึงการเข้าไปเปลี่ยนแปลงฐานข้อมูลเพื่อให้ระบบปฏิบัติการของเป้าหมายเกิดความผิดพลาดในการทำงาน เช่น การเปลี่ยนข้อมูลคอมพิวเตอร์ให้โรงไฟฟ้าหยุดทำงาน การทำลายระบบคมนาคมทางอากาศหรือทำลายระบบเตือนภัยฉุกเฉิน

ประการที่ 3 Mixed Attacks คือการใช้วิธีการโจมตีทั้งสองรูปแบบขั้นต้นรวมกัน ซึ่งจะก่อให้เกิดความเสียหายในวงกว้าง ทั้งเป้าหมายเฉพาะและผู้ที่ไม่ใช่เป้าหมายการโจมตีโดยตรงด้วยการโจมตีทางไซเบอร์นี้จึงก่อให้เกิดความเสียหายทั้งทางกายภาพต่อบุคคล สังคม เศรษฐกิจ และการเมือง โดยไม่จำกัดผลแค่เพียงในสนามรบเท่านั้น

Mills ประเมินว่าจากการถกเถียงในวงวิชาการแล้วข้อสรุปค่อนข้างชัดว่าปัจจุบันไม่มีกฎหมายมนุษยธรรมระหว่างประเทศที่เพียงพอต่อการกำหนดความชอบด้วยกฎหมายในการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตี การขาดการตีความที่ชัดเจน ไม่มีกลไกในการบังคับใช้หลักการจึงควรมีการสร้างกฎหมายระหว่างประเทศเฉพาะด้านเรื่องการโจมตีทางไซเบอร์[142]

Iasiello สนับสนุนว่าการใช้ปฏิบัติการทางไซเบอร์มีบทบาทสำคัญในการเปลี่ยนแปลงรูปแบบการรบของกองทัพเพราะเทคโนโลยีไซเบอร์เป็นอาวุธของสงครามอสมมาตร (Asymmetric warfare) วิธีการในการโจมตีด้วยปฏิบัติการทางไซเบอร์นั้นทั้งพลเรือนและพลรบสามารถเข้าถึงได้ในขณะที่ผลเสียหายที่เกิดขึ้นจากการโจมตีนั้นมีความหลากหลายมาก[143] ทั้งการทำลายระบบคอมพิวเตอร์และผลที่อาจเกิดทั้งทางกายภาพต่อชีวิต ร่างกายและทรัพย์สิน ดังนั้นประเทศที่มีเทคโนโลยีซับซ้อนย่อมสามารถสร้างระบบป้องกันตนเองได้มาก ในขณะที่ประเทศที่มีพัฒนาการทางเทคโนโลยีน้อย ก็จะเป็นกลุ่มที่เสี่ยงต่อการถูกโจมตีทางไซเบอร์มาก

---

[142] Ivoty Mills, "Emergent International Humanitarian Law in the Context of Cyber Warfare,": 78-99.

[143] Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?" Military and Strategic Affair, Vol. 7 No.1. (March 2015): 23-40.

นอกจากนั้น Iasiello ยังอ้างถึงสถานการณ์ต่างๆ ซึ่งมีการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีเพื่อแสดงให้เห็นว่าปฏิบัติการทางไซเบอร์มีนัยสำคัญอย่างไรต่อการรบของกองทัพ และการขัดกันทางอาวุธรวมตลอดถึงการก่อการร้ายในปัจจุบัน[144]

Eilstrup-Sangiovanni เห็นว่าการสร้างอนุสัญญาระหว่างประเทศว่าด้วยสงครามทางไซเบอร์เป็นเรื่องจำเป็น โดยเทียบกับอนุสัญญาระหว่างประเทศอื่นๆ ที่สร้างขึ้นมาเพื่อจำกัดหรือควบคุมการใช้อาวุธเฉพาะอย่าง Eilstrup-Sangiovanni ระบุว่าแม้ NATO จะมีการใช้ Tallinn Manual on the International Law Applicable to Cyber Warfare แต่คู่มือดังกล่าวได้รับการยอมรับในกลุ่มแคบ เฉพาะประเทศสมาชิก NATO ยิ่งไปกว่านั้น Tallinn Manual ไม่ได้สร้างแนวทางใหม่ใดๆ ในเชิงกฎหมายระหว่างประเทศ เพราะเป็นการตีความกฎหมายระหว่างประเทศที่มีอยู่แล้วเพื่อปรับใช้แก่การทำสงครามทางไซเบอร์ แม้กระทั่งนักกฎหมายที่อยู่เบื้องหลังการทำงานเพื่อสร้างคู่มือดังกล่าวยังมองว่าการตีความกฎหมายที่มีอยู่แล้วนั้นยังคงมีปัญหาอยู่อีกมาก เนื่องจากต้องอาศัยการเกิดขึ้นของปรากฏการณ์ปัจจุบันโดยไม่มีหลักการที่ชัดเจนใดๆ รองรับ ยิ่งไปกว่านั้นการปฏิบัติของรัฐต่างๆ ในแนวทางเดียวกันยังไม่สามารถเกิดขึ้นได้ ลักษณะความเห็นว่าแนวทางปฏิบัตินั้นเป็นกฎหมาย (Opinio Juris) ก็จะไม่เกิดขึ้น และกฎหมายเท่าที่มีอยู่ก็ไม่เพียงพอต่อสถานการณ์การใช้งานไซเบอร์เพื่อการขัดกันทางอาวุธแล้ว[145]

Eilstrup-Sangiovanni ยังนำเสนอว่าการขาดกฎหมายเฉพาะย่อมนำไปสู่ปัญหาต่างๆ อันได้แก่ ปัญหาในการระบุฐานความผิดในการใช้งานไซเบอร์เพื่อการโจมตี และปัญหาในการทำงานขององค์กรต่างๆ และหน่วยงานต่างๆ อย่างเป็นระบบเพื่อจัดการกับปัญหาการใช้งานไซเบอร์เพื่อการโจมตี เขาจึงเสนอแนวทางในการสร้างอนุสัญญาเฉพาะด้านเพื่อการจัดการกับปัญหาการทำสงครามทางไซเบอร์[146]

อาจกล่าวได้ว่างานศึกษาหลายชิ้นนั้นได้ศึกษาเฉพาะเรื่องเทคโนโลยีแต่ละชนิดเป็นสำคัญ แต่ยังไม่ได้มีงานชิ้นใดศึกษาประเด็นร่วมกันของเทคโนโลยีใหม่ที่มีการใช้งานในการขัดกันทางอาวุธว่าเทคโนโลยีเหล่านั้นมีจุดร่วมกันในประเด็นท้าทายเรื่องใด แม้ว่าการศึกษาประเด็นเฉพาะจะเป็นเรื่องที่มีความจำเป็น แต่สิ่งที่เป็นผลตามมาคือความเห็นที่หลากหลายในการปรับใช้กฎหมาย ทั้งความพยายามในการใช้

---

[144] Emilio Iasiello, “Are Cyber Weapons Effective Military Tools?”: 23-40.

[145] Mette Eilstrup-Sangiovanni, “Why the World Needs an International Cyberwar Convention.” Philosophy and Technology. Vol. 31. (2018): 379-407.

[146] Ibid., pp. 379-407.

กฎหมายมนุษยธรรมระหว่างประเทศเท่าที่มีอยู่และความพยายามในการสร้างกฎหมายใหม่ ซึ่งหากให้ความสำคัญประเด็นเฉพาะเหล่านี้เป็นรายกรณีไปก็อาจก่อให้เกิดแนวคิดในการสร้างกฎหมายใหม่เพื่อจำกัดการใช้งานเทคโนโลยีต่างๆ ในการขัดกันทางอาวุธอยู่เรื่อยไป ขณะที่การศึกษาประเด็นร่วมกันบางประการของเทคโนโลยีใหม่จะทำให้เห็นความชัดเจนของลักษณะการใช้งานเทคโนโลยีใหม่บางประการและนำไปสู่การแสวงหาแนวทางกลางที่สามารถแก้ไขปัญหาการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธโดยไม่จำเป็นต้องคิดถึงการสร้างกฎหมายใหม่เพื่อจัดการกับปัญหาทุกกรณีได้

ลักษณะประการสำคัญของความเป็นเทคโนโลยีไม่ว่าจะเป็นไซเบอร์ อากาศยานไร้คนขับ เทคโนโลยีอวกาศและการสื่อสารผ่านดาวเทียมหรือเทคโนโลยีอื่นๆ ที่มีการใช้งานในปัจจุบันมีจุดร่วมสำคัญบางประการ เช่น การเป็นเทคโนโลยีที่ใช้ร่วมกันระหว่างพลเรือนและทหาร การเป็นเทคโนโลยีที่ไม่ได้ออกแบบมาให้เป็นอาวุธตั้งแต่ต้น[147] แต่เทคโนโลยีเหล่านี้ถูกนำมาใช้ประกอบกับอาวุธ โดยสภาพเทคโนโลยีเองเมื่อไม่ใช่อาวุธ การจะไปพิจารณาเรื่องการสร้างกฎหมายใหม่ในการควบคุมการใช้งานในการขัดกันทางอาวุธจึงอยู่นอกเหนือจากขอบเขตของกฎหมายมนุษยธรรมระหว่างประเทศและเมื่อพิจารณาจากกฎหมายมนุษยธรรมระหว่างประเทศที่ปรากฏในพิธีสารฉบับที่ 1 ค.ศ.1977 เพิ่มเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 แล้วจะพบว่าข้อกำหนดการห้ามใช้วิธีการ (Methods) และปัจจัย (Means) ในการขัดกันทางอาวุธนั้นก็แทบจะครอบคลุมทั้งอาวุธและวิธีการในการขัดกันทางอาวุธทุกกรณีแล้ว การใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธจึงต้องอยู่ภายใต้หลักการนี้ด้วย

อย่างไรก็ดี เทคโนโลยีใหม่นั้นสร้างประเด็นท้าทายหลายประการต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศทั้งต่อหลักการแยกแยะเป้าหมาย โดยเหตุที่เทคโนโลยีเหล่านี้เป็นสิ่งที่ใช้งานได้ทั้งการทหารและเพื่อประโยชน์พลเรือน[148] การพิจารณาการกระทำที่เป็นปฏิปักษ์ (Conduct of Hostilities) จึงมีความซับซ้อนขึ้น ทั้งในมิติของผู้ใช้งานเทคโนโลยี และผลกระทบที่จะเกิดขึ้นกับทรัพยากรที่เกี่ยวข้องกับทั้งทหารและพลเรือน การโจมตีและการป้องกันตัวในกรณีของเทคโนโลยีไซเบอร์ที่ไม่ปรากฏผลทางกายภาพในบางกรณี ซึ่งลักษณะร่วมกันประการสำคัญเหล่านี้จะเป็นประโยชน์ต่อการพิจารณาแนวทางในการปรับใช้กฎหมายมนุษยธรรมีระหว่างประเทศให้เกิดความเหมาะสมต่อปัญหาและข้อท้าทายที่อาจเกิดขึ้นในอนาคต ซึ่งศาลยุติธรรมระหว่างประเทศและศาลอาญาระหว่างประเทศย่อมจะต้องมีบทบาทในการนำกฎหมายเหลานี้มาปรับใช้อย่างเหมาะสมต่อสถานการณ์ในปัจจุบัน

---

[147] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 96.

[148] Ibid.

การศึกษาวิจัยในวิทยานิพนธ์ฉบับนี้มีเป้าหมายในการนำเสนอขอบเขตเรื่องเทคโนโลยีใหม่ที่มีการใช้ในการขัดกันทางอาวุธในปัจจุบัน ข้อพิจารณาเกี่ยวกับนิยามของเทคโนโลยีใหม่ในการขัดกันทางอาวุธ นัยสำคัญของเทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายระหว่างประเทศ ข้อพิจารณาในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศและข้อท้าทายต่างๆ ที่อาจเกิดขึ้น เพื่อค้นหาคำตอบว่ากฎหมายมนุษยธรรมระหว่างประเทศเท่าที่มีอยู่ในปัจจุบันสามารถปรับใช้กับกรณีการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธได้เพียงใดและมีช่องว่างทางกฎหมายใดหรือไม่ที่จะก่อให้เกิดปัญหาในการปรับใช้กฎหมาย โดยการศึกษาวิเคราะห์นั้นจะพิจารณาทั้งตามหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศในเรื่องการก่อให้เกิดการขัดกันทางอาวุธโดยการใช้เทคโนโลยีใหม่ว่าจะเป็นไปได้หรือไม่ เพียงใด ความชอบด้วยกฎหมายในการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ การบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่ หลักปฏิบัติการทางทหารในขณะที่เกิดสถานการณ์การขัดกันทางอาวุธ ทั้งหลักการเกี่ยวกับเรื่องการกำหนดเป้าหมายในการโจมตี การแยกแยะเป้าหมายในการโจมตี ความได้สัดส่วนในการใช้กำลัง หลักความระมัดระวังในการโจมตี เพื่อพิสูจน์ว่าแท้จริงแล้วหลักเกณฑ์ของกฎหมายมนุษยธรรมระหว่างประเทศมีความครอบคลุมมากน้อยเพียงไร พัฒนาการของเทคโนโลยีที่เกิดขึ้นนี้อาจนำไปสู่ข้อท้าทายประการใดบ้างต่อกฎหมายมนุษยธรรมระหว่างประเทศและควรจะสร้างแนวทางในการรับมือกับข้อท้าทายต่างๆ อย่างไร เพื่อให้หลักการของกฎหมายมนุษยธรรมระหว่างประเทศสามารถปรับใช้แก่เทคโนโลยีใหม่ที่มีบทบาทสำคัญในการขัดกันทางอาวุธได้อย่างครอบคลุม

บทที่ 2

การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ

การศึกษาแนวทางการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับ “เทคโนโลยีใหม่” ในการขัดกันทางอาวุธมีประเด็นที่ต้องทำความเข้าใจเบื้องต้นหลายประการ เช่น เทคโนโลยีคืออะไร เทคโนโลยีใหม่แตกต่างอย่างไรกับเทคโนโลยีเก่า อะไรคือสิ่งที่ใช้ในการจำแนกความเก่าความใหม่ของเทคโนโลยี เทคโนโลยีมีความสัมพันธ์อย่างไรกับการขัดกันทางอาวุธ การขัดกันทางอาวุธคืออะไร ตลอดจนถึงประเด็นที่ต้องทำความเข้าใจว่าเทคโนโลยีใหม่มีบทบาทในการขัดกันทางอาวุธในระดับใด เหตุใดจึงมีความสำคัญถึงขนาดที่จะทำการศึกษาปัญหาการปรับใช้กฎหมาย

ในบทที่ 2 นี้ ผู้ศึกษาวิจัยจะได้นำเสนอข้อมูลและการวิเคราะห์ประเด็นความสัมพันธ์ระหว่างเทคโนโลยีใหม่กับการขัดกันทางอาวุธ โดยทำการคลี่คลายประเด็นต่างๆ ที่ได้กล่าวไว้ตอนต้น เพื่อชี้ให้เห็นข้อเท็จจริงเกี่ยวกับการใช้เทคโนโลยีใหม่ซึ่งก่อให้เกิดผลที่เปลี่ยนแปลงไปในการสงครามอย่างมีนัยสำคัญ ก่อนที่จะนำไปสู่ประเด็นข้อกฎหมายระหว่างประเทศเรื่องต่างๆ ที่สามารถปรับใช้ได้กับกรณีปัญหาที่เกิดขึ้น

2.1 ความหมายของเทคโนโลยีและเทคโนโลยีใหม่ในการขัดกันทางอาวุธ

การอธิบายความหมายของคำว่าเทคโนโลยีและเทคโนโลยีใหม่ในการศึกษานี้ มีเป้าหมายเพื่อกำหนดขอบเขตของคำว่าเทคโนโลยีและเทคโนโลยีใหม่ให้เกิดความชัดเจนในการศึกษาและการทำความเข้าใจโดยความหมายของคำทั้งสองในการศึกษาวิจัยปรากฏดังนี้

2.1.1 ความหมายของเทคโนโลยี

“เทคโนโลยี” เป็นคำที่ไม่มีความหมายเฉพาะในกฎหมายมนุษยธรรมระหว่างประเทศ การอธิบายความหมายของคำว่า “เทคโนโลยี” ในงานวิจัยนี้จึงใช้ความหมายทั่วไปของคำว่า “เทคโนโลยี” เพื่ออธิบายสิ่งที่นำมาใช้ในการขัดกันทางอาวุธ คำว่า “เทคโนโลยี” โดยทั่วไปหมายถึง “การประยุกต์ใช้องค์ความรู้ทางวิทยาศาสตร์เพื่อประโยชน์ในทางปฏิบัติ (โดยเฉพาะอย่างยิ่งเพื่อประโยชน์ในทางอุตสาหกรรม)”[149] คำจำกัดความนี้ชี้ให้เห็นว่าเทคโนโลยีย่อมเป็นได้ทั้งสิ่งประดิษฐ์ที่มีสถานะ

[149] Oxford Dictionary, “The application of scientific knowledge for practical purposes, especially in industry”, Cambridge Dictionary, “the study and knowledge of the practical, especially industrial, use of scientific discoveries.”

เป็นวัตถุทางกายภาพ และรวมถึงกระบวนการหรือวิธีการในการปฏิบัติ[150] ซึ่งเป็นองค์ความรู้แต่มิได้มีสถานะเป็นวัตถุทางกายภาพ

ตัวอย่างของเทคโนโลยีซึ่งเป็นสิ่งประดิษฐ์ที่เกี่ยวข้องกับการทหารในการรบได้แก่ อาวุธปืนซึ่งเป็นการนำเอาดินระเบิดมาบรรจุใส่ในกระสุนและใช้กลไกการยิงด้วยอาวุธปืนที่ทำหน้าที่เป็นตัวจุดชนวนระเบิดโดยเข็มแทงชนวน เทคโนโลยีเครื่องบินซึ่งเป็นการนำเครื่องร่อนมาติดตั้งเครื่องยนต์ให้ทำการบินได้เร็วขึ้น ไกลขึ้น ใช้เพื่อวัตถุประสงค์การลาดตระเวนหรือการโจมตีทางการทหาร รถถังซึ่งเป็นการนำเอาความรู้ในการผลิตรถยนต์มาประกอบรวมกับการสร้างตัวถังรถยนต์ที่สามารถทนทานต่อแรงระเบิดหรือกระสุนปืนได้และมีการติดตั้งอาวุธปืนในรถถังทำให้รถถังกลายเป็นยานพาหนะที่ใช้ทำการโจมตีไปได้พร้อมกับการเคลื่อนที่ จรวดนำวิถีซึ่งเป็นการนำเอาความรู้เกี่ยวกับระบบค้นหาเป้าหมายและนำทางซึ่งอาจทำได้ทั้งระบบเรดาร์ ระบบการติดตามคลื่นความร้อนอินฟราเรด และระบบการกำหนดตำแหน่งบนพื้นโลก (GPS) มาประยุกต์ติดตั้งในระบบจรวดเพื่อการทำลายหรือระบบจรวดเพื่อการป้องกันภัยทางอากาศ ทำให้การยิงจรวดมีความแม่นยำในการทำลายเป้าหมายมากขึ้น เป็นต้น

ในขณะที่เทคโนโลยีซึ่งไม่ใช่สิ่งประดิษฐ์ที่เกี่ยวข้องกับการทหารในการรบได้แก่ การประยุกต์เอาความรู้ในการสร้างฝนเทียมมาใช้ในการเปลี่ยนแปลงสภาพแวดล้อมให้กลายเป็นอาวุธฝนเหลืองเพื่อใช้ในการโจมตีในยุคสงครามเวียดนาม การนำข้อมูลพิกัดทางภูมิศาสตร์ที่สามารถบอกตำแหน่งที่ตั้งของอาคาร สถานที่ ยานพาหนะ หรือบุคคล (Global Positioning System; GPS) มาใช้เพื่อประโยชน์ในการกำหนดเป้าหมายของระบบอาวุธนำวิถี การนำความรู้เกี่ยวกับการทำงานของมัลแวร์คอมพิวเตอร์และความรู้เกี่ยวกับการรบกวนการสื่อสารผ่านช่องทางอินเทอร์เน็ตมาใช้เพื่อการโจมตีทางไซเบอร์ต่อเว็บไซต์ เครือข่ายคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์เป้าหมาย เครื่องใดเครื่องหนึ่งหรือหลายเครื่อง เป็นต้น

พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ.2554 “วิทยาการที่นำเอาความรู้ทางวิทยาศาสตร์มาใช้ให้เกิดประโยชน์ในทางปฏิบัติ อุตสาหกรรม เป็นต้น”

[150] Wilbert E. Moore, “Introduction,” in Wilbert E. Moore (ed.), Technology and Social Change, (Chicago: Quadrangle Books, 1972), p. 5.

2.1.2 ความหมายของเทคโนโลยีใหม่

ความหมายของคำว่า “เทคโนโลยี” ตามกฎหมายมนุษยธรรมระหว่างประเทศนั้นไม่มีการนิยามไว้อย่างเป็นทางการ แต่ปรากฏการใช้คำว่า “เทคโนโลยีใหม่” (New Technology) ในที่ประชุมทางด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายครั้ง เช่น ในการประชุมของคณะกรรมการกาชาดระหว่างประเทศเพื่อพิจารณาข้อท้าทายใหม่ของกฎหมายมนุษยธรรมระหว่างประเทศในปี ค.ศ.2011 และ ค.ศ.2015 มีการพิจารณาข้อท้าทายทางกฎหมายมนุษยธรรมระหว่างประเทศที่เกิดจากเทคโนโลยีใหม่ในการสงคราม (New technologies of warfare)[151]

การประชุมของคณะกรรมการกาชาดระหว่างประเทศครั้งที่ 31 ในปี ค.ศ.2011 และการประชุมครั้งที่ 32 ในปี ค.ศ.2015 มีการกล่าวถึงข้อท้าทายจากเทคโนโลยีใหม่ 2 ลักษณะ คือ ปฏิบัติการทางไซเบอร์เพื่อการสงคราม (Cyber warfare)[152] และการใช้ระบบอาวุธที่ตัดสินใจได้ด้วยตนเองหรือระบบอาวุธอิสระ (Autonomous Weapon Systems)[153] เหตุที่มีการยกประเด็นทั้งสองเป็นข้อท้าทายของกฎหมายมนุษยธรรมระหว่างประเทศนั้น เนื่องจากมีสถานการณ์การใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีปรากฏหลายครั้ง ได้แก่ การโจมตีทางไซเบอร์ซึ่งเกิดขึ้นที่ประเทศเอสโตเนีย การโจมตีทางไซเบอร์ที่เกิดขึ้นที่ประเทศจอร์เจีย การโจมตีโรงงานเพิ่มประสิทธิภาพแร่ยูเรเนียมที่เมือง Natanz ประเทศอิหร่านด้วยปฏิบัติการ Stuxnet ฯลฯ ส่วนการใช้ระบบอาวุธอิสระนั้นคาดว่าน่าจะเป็นผลมาจากการใช้งานอากาศยานไร้คนขับซึ่งเป็นที่นิยมอย่างแพร่หลาย เช่น การใช้อากาศยานไร้

[151] International Committee of the Red Cross, (2015), International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015, p. 2., and International Committee of the Red Cross, (2011), International Humanitarian Law and the challenges of contemporary armed conflicts, 31th International Conference of the Red Cross and Red Crescent, (31IC/11/5.1.2), November 28-December 1, 2011., p. 2.

[152] คณะกรรมการกาชาดระหว่างประเทศมีทัศนะว่า Cyber warfare หมายถึง ปฏิบัติการต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ผ่านช่องทางการเดินทางของข้อมูลระหว่างคอมพิวเตอร์ โดยหากมีการใช้เป็นวิธีหรือปัจจัยในการรบย่อมถือว่าอยู่ในบริบทของการขัดกันทางอาวุธ, (International Committee of the Red Cross, (2015), International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015, p. 39.)

[153] คณะกรรมการกาชาดระหว่างประเทศไม่มีคำจำกัดความสำหรับคำว่า “Autonomous Weapon Systems” แต่หมายความถึงระบบอาวุธที่สามารถค้นหา คัดเลือกเป้าหมาย และโจมตีได้อย่างอิสระ ไม่ว่าจะเป็นทางบก ทางทะเล หรือทางอากาศ (International Committee of the Red Cross, (2015), International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015, p. 44.

คนขับของกองทัพสหรัฐอเมริกาเพื่อการค้นหาเป้าหมาย การโจมตี และการลอบสังหารบุคคล ซึ่งพบการใช้งานอากาศยานไร้คนขับของกองทัพสหรัฐอเมริกาทั้งปฏิบัติการในประเทศอิรัก อิหร่าน อัฟกานิสถาน ซีเรีย ลิเบีย ฯลฯ และประเด็นหนึ่งมาจากแนวโน้มการพัฒนาทางการทหารที่ต้องการสร้างอุปกรณ์เพื่อช่วยการรบทางการทหารในรูปแบบของหุ่นยนต์สังหาร (Killer Robot) ซึ่งเชื่อว่าอาจมีการนำมาใช้งานในปฏิบัติการทางทหารในอนาคต

ที่ประชุมของคณะกรรมการกาชาดระหว่างประเทศทั้งใน ค.ศ.2011 และ ค.ศ.2015 เห็นว่ารูปแบบการใช้งานเทคโนโลยีทั้งสองประการนั้นมีประเด็นที่น่าสนใจที่การใช้งานเทคโนโลยีไซเบอร์และการใช้งานระบบที่เกี่ยวข้องกับอุปกรณ์ตัดสินใจอิสระ (Autonomous) ซึ่งมีลักษณะการใช้งานที่ทับซ้อนกับทั้งพลเรือนและกองทัพทหาร[154] ทั้งนี้หมายความว่าทั้งความรู้ที่ใช้พัฒนาเทคโนโลยี ลักษณะการใช้งานเทคโนโลยี พื้นที่การใช้งานของทหารและพลเรือนอยู่บนพื้นฐานเดียวกัน แตกต่างกันเพียงเป้าหมายของการใช้งานเทคโนโลยีแต่ละชิดเท่านั้น เช่น เทคโนโลยีไซเบอร์ซึ่งหมายถึงการทำงานในระบบและเครือข่ายของคอมพิวเตอร์นั้น มีการพัฒนาและใช้อย่างแพร่หลายในการติดต่อสื่อสารเพื่อประโยชน์ในทางสันติของพลเรือน ในขณะที่ทางการทหารมีการใช้ระบบไซเบอร์เพื่อการโจมตีระบบการสื่อสารของเป้าหมาย การควบคุมระบบอาวุธทางไกล การใช้ระบบป้องกันภัยทางไซเบอร์เพื่อการต่อต้านการโจมตีระบบสาธารณูปโภคของประเทศ การสร้างโปรแกรมคอมพิวเตอร์เพื่อสร้างความแม่นยำในการใช้อาวุธโจมตี ฯลฯ

ส่วนเทคโนโลยีตัดสินใจอิสระนั้นมีความเกี่ยวข้องกับการพัฒนาระบบปัญญาประดิษฐ์ (Artificial Intelligence) เพื่อวัตถุประสงค์ในการให้เครื่องจักรสามารถทำงานช่วยเหลือมนุษย์ได้ โดยส่วนสำคัญของการทำให้ปัญญาประดิษฐ์สามารถทำงานได้คือการใช้ระบบอัลกอริทึ่มเพื่อการวิเคราะห์ข้อมูลพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคคล การใช้หุ่นยนต์เพื่อการประกอบผลิตภัณฑ์ในโรงงานอุตสาหกรรม การใช้ระบบประมวลผลในการนำทางและการควบคุมระบบเบรคอัตโนมัติในรถยนต์ เป็นต้น ในขณะเดียวกันเทคโนโลยีเหล่านี้ก็สามารถนำไปใช้เป็นวิธีการในการขัดกันทางอาวุธได้ ทั้งรูปแบบการนำไปใช้เป็นอาวุธเพื่อการโจมตีทางการทหาร การใช้งานเพื่อการป้องกันภัยและการใช้เพื่อประโยชน์ในการให้ความช่วยเหลือทางมนุษยธรรม ฯลฯ

---

[154] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015, p. 45.

ระบบอาวุธอิสระในปฏิบัติการทางทหารที่สำคัญซึ่งสะท้อนให้เห็นความพยายามในการใช้ระบบอัลกอริทึ่มเพื่อประมวลผลในระบบป้องกันภัยทางอากาศ ได้แก่ ระบบป้องกันภัยทางอากาศ Iron Dome ของอิสราเอลและระบบป้องกันภัยทางอากาศ Patriot ของกองทัพสหรัฐอเมริกา ในขณะที่ระบบป้องกันภัยภาคพื้นดินที่มีความพยายามใช้ระบบอัลกอริทึ่มเพื่อการประมวลผลของอาวุธ ได้แก่ ระบบป้องกันภัยภาคพื้นดิน SGR-A1 ของกองทัพเกาหลีใต้บริเวณพรมแดนเกาหลีเหนือ-เกาหลีใต้[155]

ระบบป้องกันภัยทั้งทางอากาศและภาคพื้นดินนี้ต้องอาศัยการทำงานร่วมกันของระบบการค้นหาเป้าหมายและกำหนดเป้าหมาย ระบบอาวุธยิง และระบบสั่งปฏิบัติการโจมตี ในการทำงานของระบบทั้งหมดจะต้องอาศัยการประมวลผลข้อมูลที่ซับซ้อนก่อนที่จะมีการโจมตีเป้าหมายเกิดขึ้น[156] โปรแกรมคอมพิวเตอร์ซึ่งประเมินเงื่อนไขและทางเลือกที่ดีที่สุดในการปฏิบัติการจึงอยู่ในรูปแบบการทำงานระบบอัลกอริทึ่ม การทำงานของระบบอัลกอริทึ่มจึงเป็นสาระสำคัญของการตัดสินใจของระบบอาวุธอิสระ พัฒนาการของระบบอัลกอริทึ่มทางการทหารนี้เป็นพัฒนาการเดียวกับระบบอัลกอริทึ่มของพลเรือน เนื่องจากการเขียนโปรแกรมประมวลผลแบบอัลกอริทึ่มรูปแบบหลักเป็นสากลอยู่แล้ว การแบ่งแยกการใช้งานระหว่างทหารและพลเรือนจึงเกิดขึ้นในขั้นตอนการเปลี่ยนแปลงเงื่อนไขและชุดข้อมูลในการประมวลผลและทำงานของโปรแกรมอัลกอริทึ่มและอุปกรณ์ที่เกี่ยวข้องเท่านั้น

เมื่อพิจารณาจากรูปแบบการใช้งานเทคโนโลยีดังกล่าว จะเห็นได้ว่าเทคโนโลยีที่พลเรือนใช้งานโดยปกติสามารถนำมาใช้หรือนำมาประกอบร่วมเข้าไปในระบบการใช้อาวุธ ทำให้ในบางกรณีเทคโนโลยีเหล่านี้ไม่ใช่อาวุธโดยสภาพแต่สามารถนำมาใช้งานระบบอาวุธได้ เช่น โปรแกรมคอมพิวเตอร์ในลักษณะมัลแวร์หรือโปรแกรมประสงค์ร้ายนั้นไม่มีลักษณะของการเป็นอาวุธโดยสภาพ ทั้งนี้หากพิจารณาสาระสำคัญซึ่งเป็นที่มาของการสร้างไวรัสคอมพิวเตอร์เป็นเพียงการแสดงให้เห็นความสามารถของโปรแกรมคอมพิวเตอร์ที่ทำซ้ำตัวเองได้ เช่นเดียวกับหนอนคอมพิวเตอร์ (worm) แต่หากมีการเพิ่มคำสั่งแทรกเข้าไปในไวรัสคอมพิวเตอร์หรือหนอนคอมพิวเตอร์ดังกล่าว โปรแกรมไวรัสคอมพิวเตอร์หรือโปรแกรมหนอนคอมพิวเตอร์นั้นจะสามารถทำงานในหน้าที่อื่นเพิ่มได้ด้วย เช่น

---

[155] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 10. [online] Accessed: August 2, 2019. Available from: https://icrcndresourcecentre.org/wp-content/uploads/2017/11/4283_002_Autonomus-Weapon-Systems_WEB.pdf

[156] Ibid.

การควบคุมคอมพิวเตอร์เป้าหมายให้ทำงานตามคำสั่ง ซึ่งคำสั่งนั้นอาจนำไปสู่การทำลายระบบควบคุมอาวุธสงครามและก่อให้เกิดความเสียหายทางกายภาพจากอาวุธที่ทำงานผิดพลาดดังกล่าวได้

กรณีของระบบอัลกอริที่มนั้นก็เป็นโปรแกรมทางคอมพิวเตอร์ลักษณะหนึ่ง โดยโปรแกรมอัลกอริที่มเพื่อการประมวลผลซับซ้อนนี้อาจทำงานได้กับข้อมูลที่อยู่ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่งหรือประมวลผลจากข้อมูลที่อยู่ในระบบอินเทอร์เน็ตก็ได้ หากมีการใช้โปรแกรมอัลกอริที่มในทางสันติก็จะเป็นประโยชน์ต่อการตัดสินใจในการเข้าถึงสินค้าและบริการที่ผู้บริโภคต้องการ เช่น การโปรแกรม Google Analytics[157] ซึ่งเป็นโปรแกรมประมวลผลข้อมูลการใช้งานอินเทอร์เน็ตของบุคคล โดยนำเอาข้อมูลพฤติกรรมการสืบค้นของบุคคลที่กระทำผ่านแพลตฟอร์ม google และเครือข่ายอื่นๆ เพื่อประมวลผลว่าบุคคลที่ใช้งานคอมพิวเตอร์สนใจเรื่องใดและเชื่อมโยงการโฆษณาสินค้ามานำเสนอในแพลตฟอร์มต่างๆ ที่เราใช้บริการในระบบอินเทอร์เน็ต เป็นต้น ในขณะที่หากเปลี่ยนเงื่อนไขสำหรับการตัดสินใจของโปรแกรมอัลกอริที่ม โปรแกรมก็สามารถทำงานเพื่อการคัดเลือกเป้าหมายทางการทหารเพื่อการสั่งการระบบอาวุธได้ เช่น การใช้โปรแกรมอัลกอริที่มในระบบจรวดเพื่อการป้องกันภัยทางอากาศซึ่งจะมีการนำข้อมูลระยะทางของเป้าหมาย ตำแหน่งของเป้าหมาย ความเร็วในการเคลื่อนที่ของเป้าหมาย ที่มาจากการทำงานของระบบเรดาร์หรือระบบอินฟราเรดมาคำนวณในคอมพิวเตอร์เพื่อกำหนดระยะยิงทำลายภัยคุกคามดังกล่าวที่เหมาะสมโดยจะต้องสัมพันธ์กับระยะปลอดภัยของพลเรือน หรือการใช้ระบบการเรียนรู้ของอัลกอริที่มในระบบป้องกันภัยภาคพื้นดินซึ่งอาจทำงานร่วมกับระบบการจดจำภาพเป้าหมาย โปรแกรมอัลกอริที่มจะต้องสามารถเรียนรู้เป้าหมายพลเรือนและเป้าหมายทางการทหารและแยกแยะได้ว่าเป้าหมายใดเป็นเป้าหมายที่อาจโจมตีได้ เป็นต้น

การทำงานของโปรแกรมอัลกอริที่มทั้งสองกรณีมีองค์ประกอบสำคัญแบบเดียวกันคือจะต้องมี องค์ประกอบที่ 1 ระบบจัดเก็บข้อมูล ไม่ว่าการจัดเก็บข้อมูลนั้นจะมาจากการนำข้อมูลเข้าไปในระบบของมนุษย์เอง เช่นการสืบค้นข้อมูลทางอินเทอร์เน็ตของเราที่จะมีการบันทึกในการจราจรทางอินเทอร์เน็ตเสมอและระบบอินเทอร์เน็ตจะมีการจัดเก็บเอาไว้ในพื้นที่ไซเบอร์ หรือการให้ระบบคอมพิวเตอร์เรียนรู้ด้วยตัวเอง (Machine Learning) โดยการให้มนุษย์สอนหรือให้คอมพิวเตอร์เรียนรู้เองจากภาพที่บันทึกผ่านกล้อง และมีการจัดเก็บข้อมูลนั้นเอาไว้ในหน่วยความจำของระบบ

---

[157] Westley Chai, “Google Analytics,” TechTarget, April 2021, [online] Accessed Feb 15, 2022. Available from: https://www.techtarget.com/searchbusinessanalytics/definition /Google-Analytics,

องค์ประกอบที่ 2 การประมวลผลข้อมูลที่มีการจัดเก็บไว้ผ่านระบบการวิเคราะห์ที่ซับซ้อนซึ่งจะกระทำผ่านระบบอัลกอริทึ่ม โดยสามารถทำได้ทั้งการวิเคราะห์ความสัมพันธ์ของข้อมูล แยกแยะเนื้อหาที่ผู้เขียนโปรแกรมต้องการใช้ประโยชน์ได้ รวมถึงสามารถนำข้อมูลที่วิเคราะห์แล้วไปนำเสนอยังเป้าหมายได้ นอกเหนือจากการเขียนโปรแกรมประมวลผลแล้วกระบวนการทำงานของอัลกอริทึ่มเหล่านี้อาจมีมนุษย์เข้าไปเกี่ยวข้องหรือไม่มีเลยก็ได้[158]

เครือข่ายการทำงานของคอมพิวเตอร์ที่มักเรียกรวมว่าระบบไซเบอร์นี้ (หมายถึงการทำงานทั้งหมดที่เกี่ยวข้องกับคอมพิวเตอร์ไม่ว่าจะผ่านระบบอินเทอร์เน็ตหรือไม่) โดยทั่วไปแล้วพลเรือนใช้ระบบไซเบอร์เพื่อการสื่อสาร การบันเทิง การทำงาน และสันทนาการ ในขณะที่ผู้ประสงค์ร้ายก็สามารถนำวิธีการเข้าถึงข้อมูล (Hack) หรือการใช้มัลแวร์เพื่อก่อความเสียหายได้ ในขณะที่วิธีการของผู้ประสงค์ร้ายใช้ทั้งการเจาะเข้าสู่ระบบและการใช้มัลแวร์เพื่อก่อความเสียหายนั้นสามารถนำมาใช้ทางการทหารได้ด้วย เช่น การเจาะเข้าสู่ข้อมูลสำคัญของรัฐบาลเพื่อหวังผลในความได้เปรียบทางสงคราม การเจาะเข้าสู่ระบบปฏิบัติการของอาวุธเพื่อเปลี่ยนแปลงคำสั่งปฏิบัติการ หรือการใช้มัลแวร์ทำลายระบบการสื่อสารของเครือข่ายคอมพิวเตอร์ทางการทหาร เป็นต้น การใช้งานระบบไซเบอร์ทางการทหารนี้ย่อมเป็นวิธีการหรือปัจจัยในการขัดกันทางอาวุธได้ ในขณะที่การใช้อากาศยานไร้คนขับโดยทั่วไปมีวัตถุประสงค์เพื่อการบันทึกภาพมุมสูงของพลเรือน แต่หากนำไปใช้ในการลาดตระเวนทางการทหารภาพมุมสูงดังกล่าวก็จะเป็นประโยชน์ต่อการค้นหาและระบุเป้าหมายของฝ่ายศัตรู การกระทำดังกล่าวย่อมเป็นวิธีในการขัดกันทางอาวุธ หากมีการติดตั้งอาวุธยิงเข้ากับอากาศยานไร้คนขับเพื่อการทำลาย อากาศยานดังกล่าวก็จะกลายเป็นปัจจัยหรืออาวุธในการทำสงคราม เป็นต้น

ในขณะที่ความเคลื่อนไหวขององค์การสหประชาชาติ ซึ่งมักแสดงบทบาทในการควบคุมการใช้อาวุธในทางระหว่างประเทศนั้นมีคณะผู้เชี่ยวชาญเพื่อศึกษาในประเด็นตามอนุสัญญาว่าด้วยการห้ามและจำกัดการใช้อาวุธในบางลักษณะที่จะก่อให้เกิดความบาดเจ็บเกินขนาดหรือมีผลกระทบที่ไม่สามารถจำกัดขอบเขตได้ ให้ความสำคัญกับเรื่องระบบอาวุธที่ตัดสินใจได้ด้วยตัวเองมากกว่าเทคโนโลยีประการอื่น[159]

---

[158] Jeff Erickson, Algorithms, (Illinois: Illinois University Press, 2019), p. 192-193. [online] accessed May 10, 2022. Available from: https://jeffe.cs.illinois.edu/teaching/algorithms/book/Algorithms-JeffE.pdf,

[159] CCW, Report of the informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), (CCW/MSP/2014/3, CCW/MSP/2015/3 and CCW/CONF.V/2)

นอกเหนือจากการพิจารณาเทคโนโลยีสองประการดังที่ปรากฏในที่ประชุมคณะกรรมการกาชาดระหว่างประเทศและองค์การสหประชาชาติแล้ว ในที่ประชุมกลุ่ม International Law Association เมื่อวันที่ 22-23 พฤศจิกายน ค.ศ.2013 ได้ทำการพิจารณาข้อท้าทายของสงครามในศตวรรษที่ 21 โดยกล่าวถึงเทคโนโลยีหลายประการ ได้แก่ Cyber warfare, Armed Drones, Autonomous Weapon Systems และ Outer space technologies[160] และในการประชุมวิชาการที่ Australian National University ในปี ค.ศ. 2012 อันเป็นที่มาของการจัดทำหนังสือในชื่อเรื่อง "New Technologies and the Law of Armed Conflict" ได้มีการระบุถึงเทคโนโลยีที่อาจก่อให้เกิดข้อท้าทายต่อกฎหมายมนุษยธรรมระหว่างประเทศ 5 ประการด้วยกันคือ 1) Cyber Technology, 2) Outer Space Technology, 3) Nanotechnology 4) Autonomous Weapons System และ 5) Unmanned Technology[161] แม้การประชุมทั้งสองที่กล่าวถึงนี้จะไม่มีนัยสำคัญต่อการเปลี่ยนแปลงหลักการของกฎหมายมนุษยธรรมระหว่างประเทศ แต่ก็แสดงให้เห็นแนวคิดของนักกฎหมายต่อข้อท้าทายที่เกิดขึ้นกับกฎหมายมนุษยธรรมระหว่างประเทศได้ในระดับหนึ่ง

จากการกล่าวถึงเทคโนโลยีใหม่ในการขัดกันทางอาวุธในที่ประชุมระหว่างประเทศหลายเวทีพบว่าสิ่งที่ยังไม่ได้ข้อสรุปชัดเจนคือคำว่าเทคโนโลยีใหม่ควรจะหมายถึงสิ่งใดบ้าง ผู้ศึกษาวิจัยมีข้อพิจารณาบางประการเกี่ยวกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธดังนี้

ข้อพิจารณาที่ 1 ขอบเขตความใหม่ของเทคโนโลยีจะใช้เกณฑ์ใดในการวัด

การประชุมของคณะกรรมการกาชาดระหว่างประเทศซึ่งใช้ถ้อยคำว่า "เทคโนโลยีใหม่ในการสงคราม" (New technologies of warfare)[162] ในการประชุมครั้งที่ 31 ในปี ค.ศ.2011 และการประชุมครั้งที่ 32 ในปี ค.ศ.2015 ระบุข้อท้าทายจากเทคโนโลยีใหม่ 2 ลักษณะ คือการใช้

[160] ILA, "The Conduct of Hostilities and International Humanitarian Law," ILA study group document, pp. 5-10.

[161] Hitoshi Nasu. and Robert McLaughlin, (eds), New Technologies and the Law of Armed Conflict, (The Hague: T.M.C. Asser Press, 2014), p. 16.

[162] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015. p.2., and International Committee of the Red Cross, (2011), International Humanitarian Law and the challenges of contemporary armed conflicts, 31th International Conference of the Red Cross and Red Crescent, (31IC/11/5.1.2), November 28-December 1, 2011., p.2.

ระบบไซเบอร์เพื่อปฏิบัติการทางสงคราม (Cyber warfare)[163] และการใช้ระบบอาวุธที่ตัดสินใจได้ด้วยตนเอง (Autonomous Weapon Systems)[164] ในขณะที่ที่ประชุม International Law Association ให้ความสำคัญกับเทคโนโลยี Cyber warfare, Armed Drones, Autonomous Weapon Systems และ Outer space technologies[165] และในการประชุมวิชาการที่ Australian National University ในปี ค.ศ. 2012 ให้ความสำคัญกับ Cyber Technology, Outer Space Technology, Nanotechnology, และ Unmanned Technology[166] จึงอาจสรุปในเบื้องต้นได้ในสองลักษณะดังต่อไปนี้

ลักษณะที่ 1 เกณฑ์พิจารณาด้านเวลา ในมิติของนักกฎหมายมนุษยธรรมระหว่างประเทศนั้นมองที่ปรากฏการณ์การใช้งานเทคโนโลยีที่มีในปัจจุบัน (ช่วงเวลา 15 ปี ที่ผ่านมา) เป็นสำคัญ อันสังเกตได้จากการให้ความสำคัญกับเรื่องการโจมตีทางไซเบอร์ ซึ่งกรณีสำคัญที่ต้องกล่าวถึงคือการโจมตีระบบอาวุธอิสระที่ประเทศเอสโตเนียในปี ค.ศ.2007 อันเป็นเหตุให้องค์กรสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) ต้องสร้างคู่มือทาลินน์เพื่อการปรับใช้กฎหมายระหว่างประเทศกับการทำสงครามทางไซเบอร์ (Tallinn Manual on the International Law Applicable to Cyber Warfare) ในปี ค.ศ.2009 และคู่มือดังกล่าวได้มีการแก้ไขใหม่เป็นฉบับที่ 2 ในปี ค.ศ.2017 การให้ความสำคัญกับระบบการทำงานของอุปกรณ์ไร้มนุษย์ (Unmanned Technology) เช่น Drone หรือ Autonomous Weapon Systems ก็เป็นผลมาจากการใช้งาน drone เพื่อการโจมตีประเทศปากีสถานและอัฟกานิสถาน ซึ่งเริ่มมาตั้งแต่ปี ค.ศ.2004[167] ในขณะที่ระบบการใช้งานเทคโนโลยี

---

[163] คณะกรรมการกาชาดระหว่างประเทศมีทัศนะว่า Cyber warfare หมายถึง ปฏิบัติการต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ผ่านช่องทางการเดินทางของข้อมูลระหว่างคอมพิวเตอร์ โดยหากมีการใช้เป็นวิธีหรือปัจจัยในการรบย่อมถือว่าอยู่ในบริบทของการขัดกันทางอาวุธ, (International Committee of the Red Cross, (2015), *International Humanitarian Law and the challenges of contemporary armed conflicts,* 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015.p.39.)

[164] คณะกรรมการกาชาดระหว่างประเทศไม่มีคำจำกัดความสำหรับคำว่า “Autonomous Weapon Systems” แต่หมายความถึงระบบอาวุธที่สามารถค้นหา คัดเลือกเป้าหมาย และโจมตีได้อย่างอิสระ ไม่ว่าจะเป็นทางบก ทางทะเล หรือทางอากาศ (International Committee of the Red Cross, (2015), International Humanitarian Law and the challenges of contemporary armed conflicts, 32th International Conference of the Red Cross and Red Crescent, (32IC/15/11), December 8-10, 2015.p.44.)

[165] ILA, “The Conduct of Hostilities and International Humanitarian Law,” ILA study group document, pp. 5-10.

[166] Hitoshi Nasu and Robert McLaughlin, (eds), New Technologies and the Law of Armed Conflict, p. 16.

[167] Craig Martin, (2012), “Target Killing, Self-Defense, and the Jus ad Bellum Regime,” in Claire Finkelstein, Jens David Ohlin, Andrew Altman (eds), Targeted Killings: Law & Morality in an Asymmetrical World, Oxford: Oxford University Press, 2012), p. 223.

อวกาศและนาโนเทคโนโลยีไม่ปรากฏแน่ชัดว่าเริ่มมีการใช้งานในปฏิบัติการทางทหารเมื่อใด แต่ระบบการสื่อสารผ่านดาวเทียมนั้นมีมายาวนานแล้ว เช่นเดียวกับเทคโนโลยี Stealth ซึ่งเป็นลักษณะหนึ่งของเทคโนโลยีนาโนในการสร้างอากาศยานที่มีสถาปัตยกรรมโครงสร้างและพื้นผิวที่สามารถหลบการตรวจจับของเรดาร์ได้

ลักษณะที่ 2 เกณฑ์พิจารณาด้านลักษณะการใช้งานเทคโนโลยีที่เปลี่ยนแปลงไปจากเดิม นอกเหนือจากการพิจารณาความใหม่ของเทคโนโลยีในการขัดกันทางอาวุธโดยพิจารณาระยะเวลาการเกิดขึ้นของเทคโนโลยีแล้ว ลักษณะการใช้งานเทคโนโลยีในการขัดกันทางอาวุธก็ถือเป็นปัจจัยสำคัญในการจำแนกความเปลี่ยนแปลงการใช้เทคโนโลยีจากเดิมได้ โดยการใช้งานเทคโนโลยีที่เปลี่ยนแปลงไปจากเดิมอาจพิจารณาได้จากมุมมองดังต่อไปนี้

มุมมองที่ 1 เทคโนโลยีใหม่คือการประยุกต์ใช้ความรู้และนวัตกรรมที่พลเรือนและทหารใช้ร่วมกันได้ สังเกตได้จากการกล่าวถึงการปฏิบัติการทางไซเบอร์และการใช้อากาศยานไร้คนขับในที่ประชุมระหว่างประเทศหลายครั้ง ผู้เกี่ยวข้องและนักวิชาการมองว่าเทคโนโลยีทั้งสองประการนี้เป็นสิ่งที่ทั้งพลเรือนและทหารสามารถใช้ได้ เพราะการปฏิบัติการทางไซเบอร์คือการทำงานผ่านระบบเครือข่ายคอมพิวเตอร์ซึ่งไม่มีการแบ่งพื้นที่เฉพาะ ไม่มีพรมแดนทางกายภาพ การกำหนดเขตแดนระหว่างพื้นที่สนามรบและพื้นที่พลเรือนทางไซเบอร์จึงทำได้ยาก ในขณะที่อากาศยานไร้คนขับเป็นสิ่งที่แยกประเภทการใช้งานระหว่างทหารและพลเรือนได้ก็จริง แต่พื้นฐานการใช้งานเทคโนโลยีทั้งทางทหารและพลเรือนไม่มีความแตกต่างกัน การเปลี่ยนแปลงองค์ประกอบบางประการเช่นการควบคุมอากาศยานไร้คนขับโดยผู้สังกัดในกองทัพจึงทำให้อากาศยานนั้นถูกใช้งานในฐานะเป็นวิธีการหรือปัจจัยในการขัดกันทางอาวุธ

มุมมองที่ 2 เทคโนโลยีใหม่หมายถึงการนำเอาสิ่งที่ไม่ใช่อาวุธมาใช้งานในลักษณะอาวุธ สังเกตได้จากเทคโนโลยีที่มีการกล่าวถึงในที่ประชุมระหว่างประเทศหลายประการมีลักษณะของการนำเอาสิ่งที่ไม่ได้ออกแบบมาให้เป็นอาวุธโดยสภาพมาประกอบรวมเข้ากับระบบการใช้อาวุธ และการใช้งานเทคโนโลยีที่ไม่ได้ออกแบบมาเพื่อการเป็นอาวุธให้กลายเป็นอาวุธเพื่อการทำลาย[168] เช่น การใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตี เป็นการนำเอาลักษณะการทำงานของเครือข่ายคอมพิวเตอร์มาใช้เป็นประโยชน์ในการทำให้ฝ่ายตรงข้ามเสียหายทั้งในเชิงข้อมูลข่าวสาร การสื่อสาร

[168] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p.26.

และความเสียหายทางกายภาพ ฯลฯ การใช้อากาศยานไร้คนขับ เป็นการควบคุมพาหนะที่ไม่มีมนุษย์เป็นผู้ขับขี่พาหนะดังกล่าวเพื่อวัตถุประสงค์ตามแต่ผู้ควบคุมซึ่งอยู่นอกพาหนะนั้นสั่งการ เช่น การนำพาหนะดังกล่าวติดระบบอาวุธยิง หรือระเบิดเพื่อการทำลายเป้าหมาย ฯลฯ จากที่พาหนะดังกล่าวไม่มีลักษณะเป็นอาวุธโดยการออกแบบขั้นต้น กลายเป็นอาวุธโดยการดัดแปลง การใช้งานระบบป้องกันภัยคุกคามทางอากาศเดิมใช้มนุษย์เป็นผู้ยิงอาวุธต่อต้านภัยทางอากาศ แต่เมื่อสามารถใช้การประมวลผลแบบอัลกอริทึ่มในโปรแกรมสั่งการค้นหาเป้าหมาย ระบุเป้าหมายและระบบการทำลายเป้าหมายได้ ก็ทำให้ระบบการป้องกันภัยทางอากาศนั้นมีความแม่นยำและสะดวกต่อการป้องกันภัยได้มากขึ้น การใช้งานระบบการกำหนดตำแหน่งบนพื้นโลก (GPS) เป็นระบบสัญญาณดาวเทียมที่สามารถใช้งานประกอบการนำทางของอุปกรณ์หลายชนิด[169] เช่น ระบบนำทางรถยนต์ ระบบนำทางอากาศยาน ระบบนำทางนาฬิกาอัจฉริยะ ฯลฯ แต่เมื่อนำเอาระบบนำทางซึ่งไม่ใช่อาวุธโดยสภาพนี้มาใช้ประกอบรวมกับระบบอาวุธนำวิถีก็ทำให้ระบบอาวุธนำวิถีนั้นมีความแม่นยำในการทำลายเป้าหมายมากขึ้น เป็นต้น

ลักษณะการใช้เทคโนโลยีในรูปแบบที่เปลี่ยนแปลงในการใช้อาวุธย่อมสะท้อนให้เห็นว่าสิ่งที่ไม่ได้ออกแบบมาเพื่อเป็นอาวุธก็อาจนำมาใช้เป็นอาวุธได้

ข้อพิจารณาที่ 2 ความจำเป็นในการสร้างคำจำกัดความ หรือขอบเขตของคำว่าเทคโนโลยีใหม่

เป็นที่น่าพิจารณาว่าหากมีการสร้างคำจำกัดความ หรือขอบเขตของคำว่า “เทคโนโลยีใหม่” แล้วจะเกิดผลอย่างไรในทางกฎหมาย และจะมีความจำเป็นหรือไม่ในการสร้างขอบเขตนิยามของ “เทคโนโลยีใหม่” เพราะหากพิจารณาจากกฎหมายระหว่างประเทศที่ปรากฏมาโดยตลอดนั้นจะพบว่าโดยมากเป็นการสร้างอนุสัญญาเฉพาะเรื่องที่ใช้บังคับกับอาวุธเฉพาะอย่างไปโดยไม่มีการศึกษาถึงความเก่าหรือความใหม่ของอาวุธชนิดต่างๆ อาจเป็นไปได้ว่ากฎหมายระหว่างประเทศถูกสร้างขึ้นมาเพื่อป้องกันหรือแก้ไขปัญหาที่เกิดขึ้นในแต่ละกรณีที่นักกฎหมายระหว่างประเทศเห็นว่าเป็นเรื่องสำคัญ หากพิจารณาในบริบทดังกล่าวนี้ การสร้างนิยามหรือขอบเขตของเทคโนโลยีใหม่ก็แทบจะไม่มีความจำเป็น หากเทคโนโลยีใดสร้างปัญหาขึ้นกับการบังคับใช้กฎหมาย

[169] Ibid., p. 27.

มนุษยธรรมระหว่างประเทศก็สามารถสร้างกฎหมายระหว่างประเทศฉบับใหม่เพื่อป้องกันหรือแก้ไขปัญหาดังกล่าวได้เลย

ในขณะที่การพิจารณาขอบเขตคำว่า “เทคโนโลยีใหม่” แทบไม่เกิดขึ้นเลยในกฎหมายระหว่างประเทศ เมื่อพิจารณาจากการประชุมต่างๆ และงานวิชาการที่เกิดขึ้น อาจเนื่องจากการจำกัดขอบเขตของคำว่า “เทคโนโลยีใหม่” ไม่ใช่เรื่องง่ายและอาจไม่ใช่เรื่องจำเป็นถึงขนาดที่ต้องมีความชัดเจน ในทางตรงข้าม คำว่า “เทคโนโลยีใหม่” ที่ไม่มีนิยามขอบเขตนี้อาจใช้เป็นคำทั่วไป และเปิดโอกาสให้หมายถึงสิ่งของที่เป็นรูปธรรมรวมถึงความรู้ที่เป็นนามธรรมในการประยุกต์ใช้งานอุปกรณ์ต่างๆ อาจเป็นประโยชน์ในการรวมเอาเทคโนโลยีที่ยังไม่เกิดขึ้นในปัจจุบันมาอยู่ในขอบเขตของคำว่า “เทคโนโลยีใหม่” นี้ได้

อย่างน้อยที่สุด การใช้คำว่า “เทคโนโลยีใหม่” ในที่ประชุมระหว่างประเทศรวมตลอดถึงผลงานวิชาการทางกฎหมายระหว่างประเทศหลายชิ้น แสดงให้เห็นว่า “เทคโนโลยีใหม่” (New Technology) เป็นคำที่นักกฎหมายระหว่างประเทศเข้าใจกันโดยทั่วไป เพียงแต่ยังไม่มีการสร้างขอบเขตที่ชัดเจนเท่านั้น

การศึกษาวิจัยเพื่อระบุขอบเขตหรือลักษณะของ “เทคโนโลยีใหม่” จึงเป็นการสร้างความชัดเจนของถ้อยคำที่แม้จะไม่มีผลต่อการสร้างนิยามของคำว่า “เทคโนโลยีใหม่” ให้ปรากฏในกฎหมายระหว่างประเทศ แต่ย่อมก่อให้เกิดความชัดเจนว่าความ “ใหม่” ของเทคโนโลยีคืออะไร และความใหม่ของเทคโนโลยีเช่นว่านั้นก่อให้เกิดข้อท้าทายหรือปัญหาอย่างไรในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ ซึ่งหากเทคโนโลยีดังกล่าวไม่ก่อให้เกิดข้อท้าทายใดหรือปัญหาใดในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศเลย ก็น่าพิจารณาว่าความ “ใหม่” ที่กล่าวกันนั้นเป็นจริงหรือไม่ และเมื่อสามารถจำกัดขอบเขตหรือนิยามของเทคโนโลยีใหม่ได้ย่อมนำไปสู่แนวทางในการพิจารณาบทบาทของกฎหมายมนุษยธรรมระหว่างประเทศว่าจะต้องปรับใช้บทบัญญัติที่มีอยู่แล้วอย่างไรต่อเทคโนโลยีใหม่ที่มีการใช้งานในการขัดกันทางอาวุธ และมีช่องว่างของกฎหมายอย่างไรหรือไม่ที่จะนำไปสู่การแก้ไข หรือเพิ่มเติมกฎหมาย หรืออาจจำต้องมีการสร้างอนุสัญญาเฉพาะเรื่องเพื่อตอบสนองต่อปัญหาการใช้งานเทคโนโลยีใหม่ดังกล่าวหรือไม่ อย่างไร

2.2 ความหมายของการขัดกันทางอาวุธ

ประเด็นเรื่องเงื่อนไขและองค์ประกอบของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ ผู้วิจัยจะอธิบายโดยละเอียดในบทที่ 3 อย่างไรก็ดีในตอนต้นนี้จะเป็นคำอธิบายความหมายของคำว่า “การขัดกันทางอาวุธ” โดยสังเขปสำหรับการทำความเข้าใจเนื้อหาในงานวิจัยฉบับนี้ เนื่องจากการขัดกันทางอาวุธตามกฎหมายมนุษยธรรมระหว่างประเทศมีความสำคัญในการจำแนกสถานการณ์ที่สามารถบังคับใช้อนุสัญญาเจนีวา ค.ศ. 1949 และพิธีสารเพิ่มเติม ค.ศ.1977 ลักษณะของการขัดกันทางอาวุธจึงมีความสำคัญในการจำแนกช่วงเวลาและสถานการณ์ที่กฎหมายมีผลใช้บังคับ

อนุสัญญาเจนีวา ค.ศ.1949 ซึ่งเป็นกฎหมายระหว่างประเทศที่กำหนดให้ใช้บังคับเมื่อเกิด “การขัดกันทางอาวุธ” (armed conflict) ไม่มีการนิยามความหมายของคำว่าการขัดกันทางอาวุธเอาไว้แต่มีการอธิบายโดยศาลอาญาระหว่างประเทศของอดีตประเทศยูโกสลาเวียอธิบายความหมายของการขัดกันทางอาวุธว่า “...การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐ...”[170]

การขัดกันทางอาวุธในอนุสัญญาเจนีวา ค.ศ.1949 มีหลักการในข้อ 2 ร่วมและข้อ 3 ร่วมของอนุสัญญาเจนีวาทั้ง 4 ฉบับ แบ่งสถานการณ์ในการบังคับใช้อนุสัญญาเจนีวาเป็น 2 กรณี คือ การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ ดังนี้

1) การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ หมายถึง กรณีสงครามที่มีการประกาศหรือกรณีการพิพาทกันด้วยอาวุธอย่างอื่นระหว่างคู่ภาคีสองฝ่ายหรือกว่านั้น แม้จะไม่มีการรับรองสถานะสงครามก็ตาม และกรณีการยึดครองอาณาเขตบางส่วนแม้ไม่มีการต่อต้านด้วยอาวุธ[171]

---

[170] The Prosecutor v. Dusko Tadic, The Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, The Appeal Chamber (ICTY) 2 October 1995 para.70.

[171] Article 2, Geneva Convention 1949 “In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.
The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

หลักการดังกล่าวอธิบายได้ว่าอนุสัญญาเจนีวาส่วนที่เกี่ยวข้องกับการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศนั้นบังคับใช้ในสองกรณีได้แก่

กรณีที่ 1 เมื่อเกิดการพิพาทกันด้วยอาวุธระหว่างรัฐคู่ภาคีสองฝ่ายหรือมากกว่านั้น ตัวอย่างเช่น รัฐ A ใช้กองกำลังทหารพร้อมอาวุธต่อสู้กับกองกำลังทางทหารของรัฐ B หรือกรณีที่รัฐ A รัฐ B รัฐ C ใช้กองกำลังทางทหารพร้อมอาวุธปฏิบัติการร่วมกันเพื่อต่อสู้กับรัฐ D รัฐ E และรัฐ F เป็นต้น

กรณีที่ 2 เมื่อเกิดการยึดครองอาณาเขตบางส่วนของรัฐแม้จะไม่มีการต่อต้านด้วยอาวุธก็ตาม ตัวอย่างเช่น การที่รัฐ A ใช้กองกำลังทางทหารเคลื่อนที่เข้าไปพื้นที่ของรัฐ B ยึดครองบางส่วนของรัฐ B ไว้ โดยที่รัฐ B ยังไม่มีการตอบโต้ใดๆ เป็นต้น

2) การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ ในอนุสัญญาเจนีวา ค.ศ.1949 อธิบายไว้เพียงว่าหมายถึงการขัดกันทางอาวุธที่เกิดขึ้นในอาณาเขตของภาคีผู้ทำสัญญาฝ่ายหนึ่งฝ่ายใด [172] อย่างไรก็ดี ในพิธีสารเพิ่มเติมฉบับที่ 2 ค.ศ.1977 กำหนดขอบเขตการบังคับใช้กฎหมายในกรณีข้อพิพาททางอาวุธที่เกิดขึ้นในอาณาเขตของภาคีระหว่างกองทัพของตนและกองกำลังของฝ่ายต่อต้านหรือกลุ่มกองกำลังที่ได้มีการจัดตั้งขึ้นอื่นๆ ซึ่งอยู่ภายใต้อำนาจการบังคับบัญชาที่รับผิดชอบและสามารถควบคุมอาณาเขตส่วนหนึ่งของภาคีนั้น จนทำให้กองกำลังดังกล่าวสามารถปฏิบัติการทางทหารได้อย่างต่อเนื่องและพร้อมเพรียง สถานการณ์ดังกล่าวจะอยู่ในบังคับของพิธีสารเพิ่มเติมฉบับที่ 2 ค.ศ.1977 ทั้งนี้ไม่รวมสถานการณ์ความยุ่งยากภายในและความตึงเครียดต่างๆ เช่น การจลาจล การใช้กำลังรุนแรงที่เกิดขึ้นเป็นครั้งคราวและไม่ต่อเนื่อง[173] [174]

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof."

172 Common Article 3 of Geneva Convention 1949

173 Article 1 of Additional Protocol II of the Geneva Convention 1977

174 นิยามที่กล่าวมานี้เป็นความหมายที่มาจากฎหมายสองฉบับคือ ข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ซึ่งนิยามคำว่า การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ หมายถึง "...การพิพาทกันด้วยอาวุธอันมิได้มีลักษณะเป็นกรณีระหว่างประเทศเกิดขึ้นในอาณาเขตของอัครภาคีผู้ทำสัญญาฝ่ายหนึ่งฝ่ายใด..." และข้อ 1 ของพิธีสารฉบับที่ 2 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 ซึ่งนิยามว่าการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ หมายถึง "ข้อพิพาททางอาวุธที่เกิดขึ้นในอาณาเขตของภาคี ระหว่างกองทัพของตนและกองกำลังของฝ่ายต่อต้าน หรือกลุ่มกองกำลังที่ได้มีการจัดตั้งขึ้นอื่นๆ ซึ่งอยู่ภายใต้อำนาจการบังคับบัญชาที่รับผิดชอบ และ

อนุสัญญาเจนีวา ค.ศ.1949 ทั้ง 4 ฉบับใช้บังคับแยกจากพิธีสารเพิ่มเติมอนุสัญญาเจนีวาโดยเป็นไปตามการลงนามผูกพันของชาติสมาชิกแต่ละประเทศ ข้อ 3 ร่วมของอนุสัญญาเจนีวาจึงสามารถใช้ได้กับชาติที่ลงนามผูกพันในอนุสัญญาเจนีวา เช่นเดียวกับเงื่อนไขที่ปรากฏในพิธีสารเพิ่มเติมอนุสัญญาเจนีวานั้นก็จะมีผลผูกพันเฉพาะชาติที่ลงนามผูกพันเช่นกัน การบังคับใช้ข้อกำหนดที่ปรากฏในพิธีสารเพิ่มเติมฉบับที่ 2 จึงต้องผ่านการพิจารณาองค์ประกอบในข้อ 1 ของพิธีสารนี้ก่อน เช่น หากประเทศ A มีพันธกรณีตามอนุสัญญาเจนีวาเท่านั้น ข้อพิพาททางอาวุธที่เกิดขึ้นภายในรัฐ A ย่อมเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศและใช้อนุสัญญาเจนีวาบังคับได้กับกรณีการกระทำที่เกิดขึ้นภายในรัฐ ในขณะที่หากจะบังคับใช้ข้อกฎหมายในพิธีสารเพิ่มเติมฉบับที่ 2 ได้นั้น รัฐ A จะต้องลงนามยอมรับความผูกพันตามพิธีสารฉบับที่ 2 นี้ก่อน

หากพิจารณาตามข้อ 2 ร่วมและข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ทั้งสี่ฉบับจะพบคำสำคัญในความหมายของการขัดกันทางอาวุธ ได้แก่ “สงครามที่มีการประกาศ” (...all cases of declared war...)[175] และ “การขัดกันทางอาวุธประการอื่น” (...any other armed conflict...)[176] โดยความเข้าใจทั่วไป “สงคราม” (war) เป็นคำที่บุคคลทั่วไปเข้าใจได้ว่าหมายถึงการต่อสู้ในลักษณะการรบของฝ่ายที่มีความขัดแย้ง แต่สงครามตามกฎหมายระหว่างประเทศหมายถึงการต่อสู้ระหว่างรัฐด้วยกองกำลังทางทหาร ในขณะที่คำว่า “การขัดกันทางอาวุธ” (armed conflict) เป็นคำสำคัญที่ชี้ว่าในการใช้กำลังทางทหารของสองฝ่ายต้องมีอาวุธเป็นเครื่องมือในการต่อสู้รวมอยู่ด้วย ไม่ว่าการขัดกันทางอาวุธนั้นจะเป็นสงครามรูปแบบดั้งเดิมหรือการต่อสู้กันในลักษณะที่แตกต่างจากสงครามรูปแบบเดิมก็ตาม

ในนิยามของการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศนั้นรวมถึงกรณีการยึดครองอาณาเขตบางส่วนแม้ไม่มีการต่อต้านด้วยอาวุธ น่าสังเกตว่าในวรรคสองของข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 นี้กำหนดในข้อความตอนต้นว่า “อนุสัญญาฉบับนี้ให้ใช้บังคับแก่กรณี...”[177] และเนื้อความในตอนหลังประกอบด้วยเงื่อนไขของสองกรณีคือสงครามที่มีการประกาศรวมถึงการขัดกันทางอาวุธรูปแบบอื่นและการยึดครองอาณาเขตบางส่วน ซึ่งมีความหมายว่าในสองกรณีดังกล่าวคือ

สามารถควบคุมอาณาเขตส่วนหนึ่งของภาคีนั้น จนทำให้กองกำลังดังกล่าวสามารถปฏิบัติการทางทหารได้อย่างต่อเนื่องและพร้อมเพรียง”

[175] Common Article 2 of Geneva Convention 1949

[176] Ibid.

[177] Ibid.

ขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศตามอนุสัญญาเจนีวา ค.ศ.1949 แต่หากจะอนุมานว่าการยึดครองอาณาเขตบางส่วนมีความหมายเท่ากับการขัดกันทางอาวุธก็เห็นจะแปลกอยู่ เพราะเมื่อการต่อสู้ยังไม่เกิดขึ้นก็ยังไม่น่าจะเรียกว่าการขัดกันทางอาวุธได้

อย่างไรก็ดี หากพิจารณาจากพัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศที่มีมาอย่างยาวนานนั้นผู้ร่างกฎหมายย่อมมองว่าการยึดครองอาณาเขตบางส่วนนั้นอาจนำไปสู่การขัดกันทางอาวุธได้ ดังนั้นแม้ไม่มีการต่อสู้ด้วยอาวุธแต่สถานการณ์ใกล้เคียงกับการเกิดการขัดกันทางอาวุธกฎหมายมนุษยธรรมระหว่างประเทศก็ควรมีผลบังคับใช้แล้ว ทั้งนี้มิได้หมายความว่าในสถานการณ์ดังกล่าวกองกำลังทางทหารของรัฐจะไม่มีอาวุธ เพราะหากไม่มีอาวุธก็น่าสงสัยว่าการต่อสู้ของสองรัฐจะดำเนินไปได้อย่างไรโดยปราศจากเครื่องมือทำลายขีดความสามารถทางการทหารที่ถือว่าเป็นเป้าหมายหลักในปฏิบัติการทางทหาร ดังนั้นอาวุธยังน่าจะเป็นเครื่องมือสำคัญสำหรับการต่อสู้ในสงคราม เพียงแต่กฎหมายมนุษยธรรมระหว่างประเทศจำเป็นต้องกำหนดขอบเขตการปรับใช้กฎหมายที่มีความกว้างขวางเพื่อรองรับสถานการณ์ที่หลากหลายอย่างเหมาะสม

เมื่อพิจารณาจากนิยามคำว่าการขัดกันทางอาวุธตามอนุสัญญาเจนีวาแล้วอาจอธิบายให้เข้าใจได้ง่ายๆ ว่า การขัดกันทางอาวุธมีความหมายกว้างขวางทั้งการทำสงครามที่มีการประกาศและการต่อสู้ด้วยอาวุธในลักษณะอื่นๆ ระหว่างสองรัฐหรือมากกว่า ในขณะที่การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศหมายถึงการต่อสู้ด้วยอาวุธระหว่างรัฐกับกลุ่มซึ่งมิใช่รัฐภายในดินแดนของตนนั่นเอง

2.3 พัฒนาการของเทคโนโลยีในการขัดกันทางอาวุธและพัฒนาการของกฎหมายระหว่างประเทศ

พัฒนาการของเทคโนโลยีในการขัดกันทางอาวุธมีผลกระทบต่อขอบเขตของกฎหมายมนุษยธรรมระหว่างประเทศในสองลักษณะ ได้แก่ 1) พัฒนาการทางเทคโนโลยีที่เกี่ยวข้องกับอาวุธใหม่ และ 2) พัฒนาการทางเทคโนโลยีที่ไม่ใช่การพัฒนาอาวุธใหม่โดยตรงแต่เป็นการนำเอาเทคโนโลยีมาใช้เป็นวิธีการทางทหารหรือประกอบร่วมกับการใช้อาวุธในการรบ

ในขณะที่กฎหมายระหว่างประเทศที่เกี่ยวข้องกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธอาจแบ่งได้เป็น 2 ขอบเขต คือ 1) กฎหมายมนุษยธรรมระหว่างประเทศที่จำกัดการใช้วิธีการและปัจจัยซึ่งรวมถึงการใช้อาวุธในการขัดกันทางอาวุธ และ 2) กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธ (Disarmament) ซึ่งควบคุมการผลิต สะสม พัฒนา ถ่ายโอนอาวุธ ซึ่งมีขอบเขตการบังคับใช้นอกเหนือ

สถานการณ์การขัดกันทางอาวุธ แม้กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธจะไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศในตัวเองแต่ก็มีบทบาทนอกสถานการณ์การขัดกันทางอาวุธ ทั้งเป็นการป้องกันไม่ให้มีการนำอาวุธเหล่านี้มาใช้ในการรบและอาจเป็นมาตรการในการทำลายอาวุธเหล่านี้เมื่อการขัดกันทางอาวุธสิ้นสุดลง โดยสถานการณ์ทั้งสองนั้นไม่อยู่ในช่วงเวลาการขัดกันทางอาวุธ แต่การบังคับใช้กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธในช่วงเวลาก่อนและหลังการขัดกันทางอาวุธนี้ย่อมทำให้กฎหมายมนุษยธรรมระหว่างประเทศได้รับการปฏิบัติตามมากขึ้น

2.3.1 พัฒนาการของเทคโนโลยีในการขัดกันทางอาวุธ

ในการขัดกันทางอาวุธ ประเทศคู่พิพาทมักจะมีการใช้อาวุธที่ได้เปรียบฝ่ายตรงข้ามรวมตลอดถึงวิธีการรบใหม่ๆ เพื่อหวังผลชนะในสงคราม นอกจากอาวุธที่ดีกว่าจะก่อให้เกิดความได้เปรียบในการทำสงครามแล้ว อาวุธที่ดีกว่าและยุทธวิธีทางทหารที่เหนือกว่ายังมีประโยชน์ในการป้องกันประเทศจากการถูกรุกรานด้วย ตั้งแต่ยุคแรกที่มนุษย์เริ่มทำสงครามกันจนถึงปัจจุบันจึงมีการพัฒนาเทคโนโลยีทางอาวุธและการใช้ความรู้ใหม่ๆ เพื่อประโยชน์ในการทำสงครามเสมอมา

พัฒนาการทางเทคโนโลยีทางอาวุธและวิธีการในการทำสงครามมีลักษณะคล้ายกับพัฒนาการทางอุตสาหกรรม แม้จะไม่สามารถเทียบกันได้โดยตรง ตัวอย่างเช่น ในระยะแรกสงครามยุคดั้งเดิมตั้งแต่สมัยที่เริ่มปรากฏการใช้อาวุธจนถึงก่อนสงครามโลกครั้งที่ 1 มักเป็นการใช้อาวุธที่มีอำนาจทำลายขั้นพื้นฐานที่สุดและซับซ้อนน้อยที่สุด เช่น ดาบ หอก ธนู กระบอง เครื่องทุ่มหรือเครื่องเหวี่ยงหิน ฯลฯ ในขณะที่ระยะที่ 2 ก่อนสงครามโลกครั้งที่ 1 จนถึงสงครามโลกครั้งที่ 1 เป็นต้นมาก็เริ่มมีการใช้อาวุธปืน ซึ่งเปลี่ยนแปลงโฉมการทำสงครามไปค่อนข้างมาก เพราะอาวุธปืน และปืนใหญ่ช่วยให้การทำลายเป้าหมายในระยะไกลทำได้ง่ายขึ้น[178] ความรุนแรงจากอาวุธมีมากขึ้น เช่นเดียวกับความเสียหายที่เพิ่มมากขึ้นเช่นกัน ระยะที่ 3 คือก่อนสงครามโลกครั้งที่ 2 เล็กน้อยจนถึงช่วงสงครามโลกครั้งที่ 2 เป็นต้นมา เริ่มมีพัฒนาการของเทคโนโลยีทางอาวุธที่มากขึ้นกว่าสงครามโลกครั้งที่ 1 ทั้งวิธีการทำสงครามแบบสนามเพลาะ การใช้ปืนประจำกายพลรบที่มีเทคโนโลยีที่ดีขึ้นคือสามารถหวังผลได้ไกลขึ้น บรรจุกระสุนได้มากขึ้น มีการใช้งานรถถังซึ่งเป็นพาหนะยานเกราะที่สร้างความได้เปรียบในการรบ จากทหารราบเดินเท้าที่จะต้องต่อสู้ในภาคพื้นดินก็เปลี่ยนเป็นการใช้รถถังเพื่อลดความสูญเสียชีวิตทหารและเพิ่มอำนาจในการทำลายล้างศัตรูฝ่ายตรงข้ามมากขึ้น ระบบการยิง

[178] Williams Boothby, Weapons and the Law of Armed Conflict, (Oxford: Oxford University Press, 2009), p. 9.

ปืนใหญ่ก็เปลี่ยนแปลงไปจากเดิมที่ยิงได้ในระยะจำกัดก็เพิ่มขีดความสามารถให้ยิงได้ไกลขึ้น รวมตลอดจนถึงการปรากฏตัวของเครื่องบินรบเช่นในสงคราม Pearl Harbor ระหว่างสหรัฐอเมริกากับประเทศญี่ปุ่นก็มีการใช้ยุทธวิธีการรบทางอากาศของญี่ปุ่น ที่รู้จักกันในชื่อปฏิบัติการ Kamikaze โดยใช้เครื่องบินรบและนักบินเป็นอาวุธในการโจมตีกองทัพสหรัฐอเมริกา ทำให้การโจมตีของกองทัพญี่ปุ่นส่งผลกระทบอย่างมากต่อความเสียหายของกองทัพสหรัฐอเมริกา[179] หรือแม้กระทั่งการใช้ปฏิบัติการเรือดำน้ำซึ่งมีพัฒนาการมากขึ้นในยุคสงครามโลกครั้งที่ 2 ก็เป็นผลทำให้การรบทางทะเลแตกต่างจากสงครามรูปแบบเดิมอย่างมีนัยสำคัญ คือแทนที่จะทำการรบทางเรือที่สามารถมองเห็นได้อย่างชัดเจน เรือดำน้ำก็สามารถซ่อนตัวในน้ำได้ ทำการโจมตีเป้าหมายทั้งทางน้ำด้วยการโจมตีเรือรบของข้าศึกและเป้าหมายทางอากาศโดยการโจมตีเครื่องบินรบ โดยเป้าหมายการโจมตีดังกล่าวอาจไม่เห็นเรือดำน้ำเลยหรือกว่าจะรู้ว่าตนเองตกเป็นเป้าหมายการโจมตีก็เหลือเวลาในการป้องกันตัวได้น้อย[180]

อาวุธสำคัญที่แสดงบทบาทมากที่สุดในสงครามโลกครั้งที่สองคือระเบิดปรมาณูที่มีอานุภาพทำลายล้างสูงกว่าอาวุธใดๆ ที่เคยมีการใช้มาในโลก บทบาทสำคัญของอาวุธปรมาณูคือการทำให้สงครามโลกครั้งที่ 2 ยุติลงจากการที่ประเทศญี่ปุ่นต้องยอมแพ้สงคราม และเยอรมันที่ไม่มีญี่ปุ่นสนับสนุนก็ไม่สามารถทำสงครามต่อไปได้ นอกจากนั้น การเกิดขึ้นของอาวุธเคมี ตั้งแต่การใช้ Agent Orange หรือฝนกรด[181] โดยกองทัพสหรัฐอเมริกาในสงครามเวียดนาม และการพัฒนาอาวุธชีวภาพในช่วงเวลาต่อมา ทำเกิดกระแสของกฎหมายระหว่างประเทศในการห้ามการใช้อาวุธเหล่านี้ โดยใช้คำเรียกอาวุธที่ก่อให้เกิดความเสียหายในปริมาณมากนี้ว่า “อาวุธที่มีอานุภาพทำลายล้างสูง” (Weapon of Mass Destruction) ซึ่งแนวโน้มในการสร้างความตระหนักต่อการจำกัดการพัฒนา การผลิต และการใช้งานอาวุธที่มีอานุภาพทำลายล้างสูงนี้ยังคงส่งผลกระทบต่อมาตรการในการควบคุมอาวุธในสังคมระหว่างประเทศ ด้วยเกรงว่าหากอาวุธที่มีอานุภาพทำลายล้างสูงเหล่านี้ตกไปอยู่ในมือของกลุ่มผู้ก่อการร้ายจะทำให้การโจมตีโดยผู้ก่อการร้ายในเหตุการณ์ต่างๆ มีความรุนแรงมากขึ้น

---

[179] Nathaniel Patch, “Kamikazes: When Japanese Planes Attacked the U.S. Submarine Devilfish,” Prologue, Vol.46, No. 1 (Spring 2014): 19. [online] accessed April 19, 2021. Available from: https://www.archives.gov/files/publications/ prologue/2014/spring/kamikazes.pdf,

[180] Ibid., p. 19.

[181] George Black, “The Victims of Agent Orange The U.S. Has Never Acknowledged,” The New York Times Magazine, March 16, 2021, [online] accessed April 10, 2021. Available from: https://www.nytimes.com/2021/03/16/magazine/laos-agent-orange-vietnam-war.html,

ความหวาดกลัวต่อการใช้งานอาวุธที่มีอานุภาพทำลายล้างสูงไม่ได้มีผลเพียงการจำกัดการใช้อาวุธในการทหารแต่ยังยกระดับมาจนถึงมาตรการในการจำกัดการส่งออกสินค้าที่อาจนำไปใช้เป็นส่วนประกอบในการผลิตอาวุธที่มีอานุภาพทำลายล้างสูง ตามกรอบของอนุสัญญาระหว่างประเทศว่าด้วยอาวุธตามแบบบางชนิด (The Convention on Certain Conventional Weapons) ก่อให้เกิดกรอบความร่วมมือระหว่างประเทศในหลายรูปแบบเพื่อจำกัดการเคลื่อนไหวของสินค้าผ่านแดน ว่าจะต้องไม่ได้เป็นไปเพื่อการขนส่งสิ่งที่อาจนำไปผลิตอาวุธที่มีอานุภาพทำลายล้างสูงได้ ทำให้มาตรการในการควบคุมอาวุธทางการทหารเริ่มมีผลกระทบต่อการค้าสินค้าทางระหว่างประเทศมากขึ้น[182]

เทคโนโลยีทางการทหารที่ส่งผลกระทบสำคัญอย่างมากต่อสังคมระหว่างประเทศจึงมักเป็นเทคโนโลยีที่เกิดขึ้นระหว่างสงครามโลกครั้งที่ 2 อันสังเกตได้จากความเคลื่อนไหวในระดับสากลขององค์การสหประชาชาติที่พยายามสร้างกฎหมายระหว่างประเทศในรูปแบบของอนุสัญญาระหว่างประเทศเพื่อควบคุมการใช้และการพัฒนาอาวุธในหลายรูปแบบ

ในขณะที่ระยะที่ 4 ของพัฒนาการทางด้านอาวุธ คือหลังสงครามโลกครั้งที่ 2 ถึงปัจจุบัน พัฒนาการที่เปลี่ยนแปลงไปอย่างมากคือ การใช้ระบบอาวุธนำวิถี ซึ่งหมายถึงการใช้ระบบยิงจรวดและขีปนาวุธพิสัยใกล้และพิสัยไกลที่ทำงานประกอบร่วมกับระบบการระบุเป้าหมายภาคพื้นดินด้วยระบบกำหนดตำแหน่งบนพื้นโลก (Global Positioning System: GPS) รวมถึงการใช้ระบบตรวจจับความร้อนของเป้าหมายแบบ infrared ซึ่งมีการทำงานร่วมกับการส่งสัญญาณของระบบดาวเทียม ระบบการกำหนดตำแหน่งบนพื้นโลกนี้มีชื่อเรียกระบบแตกต่างกันตามประเทศที่เป็นผู้ใช้เทคโนโลยีและดาวเทียมซึ่งเป็นของตนเอง ระบบอาวุธนำวิถีถูกนำมาใช้ทั้งทางบก ติดตั้งในเรือและเรือดำน้ำเพื่อใช้กับการรบทางทะเล และติดตั้งกับเครื่องบิน มีผลทำให้การทำลายเป้าหมายมีความแม่นยำมากขึ้น ซึ่งมีผลในสองลักษณะ คือ ลักษณะที่ 1 เป้าหมายที่ถูกโจมตีมีความคลาดเคลื่อนน้อยลงหากการตัดสินใจทำลายเป้าหมายไม่มีความผิดพลาด โอกาสสูญเสียทางพลเรือนก็อาจเกิดขึ้นได้น้อยมาก ลักษณะที่ 2 เป้าหมายการโจมตีมีโอกาสถูกทำลายสูงและมีอัตรารอดต่ำ เพราะระบบอาวุธนำวิถีจะติดตามเป้าหมายจนกว่าการทำลายจะเกิดขึ้น โอกาสรอดพ้นจากการถูกทำลายของเป้าหมายจะต้องใช้ระบบการต่อต้านอาวุธนำวิถี จึงเป็นที่มาในระยะหลังที่หลายกองทัพเริ่มมีการใช้งานระบบการต่อต้านจรวด ขีปนาวุธ และระบบอาวุธนำวิถีมากขึ้น

---

[182] Piyanat Uamduang, Export Control of Dual-Use Items: A Comparative Study of Thai and Foreign Laws, Thesis Master of Laws in Business Law, Faculty of Law, Thammasat University, 2016. P. 4.

นอกเหนือจากระบบอาวุธนำวิถีแล้ว การใช้ระบบการสื่อสารผ่านสัญญาณดาวเทียม การใช้เครื่องบินความเร็วเหนือเสียง การใช้เครื่องบินที่มีเทคโนโลยีลดการตรวจจับ การใช้อากาศยานไร้คนขับยังปรากฏมากขึ้นอย่างมีนัยสำคัญ เพราะเทคโนโลยีเหล่านี้สร้างความได้เปรียบแก่กองทัพเป็นอย่างมาก หากกองทัพใดมีเทคโนโลยีทางการรบเหล่านี้ในความครอบครองและใช้งานในการรบก็แทบจะสามารถชนะสงครามได้

ขณะที่พัฒนาการในช่วง 20 ปีที่ผ่านมามีการใช้งานระบบไซเบอร์ทางการหทารมากขึ้น ทั้งการหวังผลเพื่อการเข้าถึง การโจมตี การจารกรรมทางข้อมูลข่าวสาร และการโจมตีระบบเครือข่ายการทำงานของคอมพิวเตอร์และอุปกรณ์ที่ทำงานเชื่อมต่อกับคอมพิวเตอร์ รวมตลอดถึงการใช้งานระบบอัลกอริทึ่มในการประมวลผล และการใช้งานระบบปัญญาประดิษฐ์ ทั้งที่ปรากฏในการใช้ระบบอาวุธต่อต้านขีปนาวุธ จรวด และระบบอาวุธนำวิถี รวมถึงการพัฒนาระบบหุ่นยนต์ (Robot) ทั้งเพื่อวัตถุประสงค์ในการช่วยเหลือทางมนุษยธรรมและการโจมตีทางการทหาร เทคโนโลยีเหล่านี้เปลี่ยนแปลงรูปแบบการรบไปอย่างมากจนถึงขนาดที่มีการใช้ถ้อยคำอธิบายปรากฏการณ์การรบในสงครามยุคหลังว่าเป็น “สงครามอสมมาตร” (Asymmetric Warfare)

สงครามอสมมาตร (Asymmetric Warfare) เป็นคำที่ใช้เรียกการทำสงครามที่ก่อให้เกิดความได้เปรียบเสียเปรียบกันอย่างมาก เพราะคู่พิพาทฝ่ายหนึ่งมักจะอาศัยความได้เปรียบอย่างมากในขณะที่อีกฝ่ายเสียเปรียบอย่างมาก[183] ความได้เปรียบและเสียเปรียบนี้เป็นผลมาจากรูปแบบของเทคโนโลยีและวิธีการในการใช้งานเทคโนโลยีที่เปลี่ยนแปลงไป จากที่ทหารควรจะเผชิญหน้ากันโดยตรง ก็เปลี่ยนเป็นการใช้เทคโนโลยีที่ควบคุมด้วยระยะไกลมากขึ้น การควบคุมไกลขึ้นหมายความว่าผู้ใช้งานระบบอาวุธมีความเสี่ยงน้อยต่อความสูญเสีย ในขณะที่ผู้ถูกโจมตีเสี่ยงภัยต่อความเสียหายมากกว่า เช่นการโจมตีด้วยอากาศยานไร้คนขับ ซึ่งผู้ควบคุมอาจอยู่ไกลออกไปหลายกิโลเมตร ในขณะที่ผู้ถูกโจมตีอาจทำการป้องกันตัวได้ โดยการทำลายอากาศยานดังกล่าว แต่การทำลายอากาศยานไร้คนขับดังกล่าวก็ไม่ได้ทำให้ทหารของฝ่ายตรงข้ามมีปริมาณลดลง นั่นหมายความว่า ผู้ควบคุมอากาศยานไร้คนขับคนเดิมนั้นสามารถกระทำการโจมตีกี่ครั้งก็ได้ และสามารถโจมตีได้ทั้งต่อเป้าหมายเดิมหรือเป้าหมายใหม่ รวมถึงความสามารถในการโจมตีเป้าหมายหลายเป้าหมายในเวลาเดียวกันได้ ในขณะที่การควบคุมระบบอาวุธดังกล่าวสามารถทำโดยผู้ใดก็ได้ รูปแบบการโจมตีเช่นนี้สร้างความ

[183] Wolff Heintschel von Heinegg, “Asymmetric Warfare: How to Respond?” International Law Studies, Vol 87, (2011): 464-465.

ได้เปรียบแก่กองทัพผู้ใช้เทคโนโลยีเป็นอย่างมาก จึงมีผู้เรียกว่าเป็นยุทธวิธีของสงครามที่ไม่เท่าเทียมหรือสงครามอสมมาตร

มิติหนึ่งของเทคโนโลยีวัสดุศาสตร์ที่มีผลต่อการออกแบบเครื่องบินเพื่อหลบหนีการตรวจจับของสัญญาณเรดาร์ ซึ่งมีชื่อเรียกว่าเทคโนโลยี Stealth คือการสร้างพื้นผิวเครื่องบินให้มีการหักเหการตกกระทบของเรดาร์ที่เปลี่ยนแปลงไปทำให้เรดาร์ตรวจจับการบินไม่สามารถระบุเป้าหมายซึ่งเป็นอากาศยานได้อย่างชัดเจน นอกจากการออกแบบเครื่องบินรบแล้วเทคโนโลยีลดการตรวจจับนี้ยังมีการนำมาพัฒนาเครื่องแบบทหาร ยานพาหนะทางบก และการผลิตอาวุธ เพื่อให้สิ่งของเหล่านี้รอดพ้นจากการมองเห็นและการตรวจจับด้วยอุปกรณ์ชนิดต่างๆ เป็นการสร้างความได้เปรียบต่อกองทัพผู้ใช้งานเทคโนโลยีมากขึ้น[184]

อาจกล่าวได้ว่าเทคโนโลยีทางการรบที่ปรากฏในช่วงยุคหลังสงครามโลกครั้งที่ 2 เป็นต้นมานี้เปรียบเสมือนยุค 4.0 ของเทคโนโลยีทางการทหารในการรบเช่นเดียวกับเทคโนโลยี 4.0 ทางอุตสาหกรรม ที่มีพัฒนาการของเทคโนโลยีไร้สายและการทำงานเชื่อมต่อหลายอุปกรณ์มากยิ่งขึ้น โดยไม่ได้ก่อให้เกิดความเสียหายลักษณะรุนแรงเหมือนการใช้อาวุธทำลายล้างสูงในสมัยสงครามโลกครั้งที่ 2 แต่ในทางตรงข้าม การโจมตีด้วยเทคโนโลยีบางประการกลับไม่ได้ก่อให้เกิดความเสียหายต่อชีวิตโดยตรง แต่ก่อให้เกิดความเสียหายต่อระบบการสื่อสารมากกว่า เช่นการโจมตีทางไซเบอร์ แต่สิ่งที่เปลี่ยนแปลงโฉมหน้าในการทำสงครามไปอย่างมากคือ การสร้างความได้เปรียบเสียเปรียบทางการทหารมากขึ้น การสร้างความแม่นยำในการโจมตีที่มากขึ้น และการลดความสูญเสียทางการทหารของฝ่ายผู้โจมตีมากขึ้น[185] ปรากฏการณ์เหล่านี้เป็นสิ่งที่อธิบายการเกิดขึ้นของเทคโนโลยีใหม่ในการขัดกันทางอาวุธหรือในยามสงครามที่สร้างผลกระทบอย่างมากในทางปฏิบัติ และในเชิงความคิดของผู้ที่เกี่ยวข้องทั้งทางทหารและนักกฎหมายระหว่างประเทศ

การศึกษาพัฒนาการของเทคโนโลยีใหม่ในการขัดกันทางอาวุธที่ใช้งานในสงครามยุคปัจจุบันและเทคโนโลยีที่คาดว่าจะมีการนำมาใช้งานในอนาคตอันใกล้จะทำให้เราเข้าใจสาระสำคัญของเทคโนโลยีแต่ละรูปแบบมากขึ้น และการพิจารณาผลกระทบที่เกิดขึ้นจากเทคโนโลยีเหล่านี้จะทำให้

---

[184] Vivek Kapul, “Stealth Technology and Its Effect on Aerial Warfare,” IDSA Monograph Series, No.33, March 2014, pp. 18-24. Accessed: June 20, 2021. Available from: https://www.idsa.in/system/files/monograph33.pdf

[185] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p.26.

เราเห็นรูปแบบการใช้งานเทคโนโลยีในการรบมากยิ่งขึ้น ข้อมูลการใช้เทคโนโลยีเหล่านี้จะทำให้เข้าใจข้อท้าทายที่เกิดขึ้นในการรบและสิ่งที่อาจเป็นปัญหาในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ และการเตรียมความพร้อมในการรับมือสถานการณ์ดังกล่าวในทางระหว่างประเทศ ก่อนเข้าสู่การพิจารณาประเด็นทางกฎหมายในบทที่ 3 ต่อไป

2.3.2 พัฒนาการของกฎหมายระหว่างประเทศเกี่ยวกับเทคโนโลยีทางอาวุธ

พัฒนาการของกฎหมายระหว่างประเทศเกี่ยวกับเทคโนโลยีทางอาวุธอาจแบ่งได้เป็น 2 ลักษณะ คือ 1) กฎหมายที่จำกัดใช้วิธีการและปัจจัยในการสงครามหรือกฎหมายมนุษยธรรมระหว่างประเทศ และ 2) กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธซึ่งควบคุมการพัฒนา การผลิต การจำหน่ายจ่ายโอน การถ่ายทอดเทคโนโลยีเกี่ยวกับอาวุธ ดังที่ได้กล่าวมา โดยพัฒนาการของกฎหมายทั้งสองลักษณะมีความแตกต่างกันเนื่องจากเป็นกฎหมายที่ใช้บังคับในขอบเขตที่แตกต่างกันดังนี้

1) พัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศที่จำกัดการใช้วิธีการและปัจจัยในการรบซึ่งรวมตลอดถึงการใช้อาวุธในการรบนี้พัฒนามาจากหลักการห้ามใช้วิธีการและปัจจัยในการรบที่จะก่อให้เกิดความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็น (Superfluous Injuries and Unnecessary Suffering) ซึ่งมีวัตถุประสงค์ในการจำกัดวิธีการรบไม่ให้ไร้ขอบเขตมากเกินความจำเป็นทางการทหาร[186] หลักการนี้ปรากฏในกฎหมายว่าด้วยการขัดกันทางอาวุธ (Law of Armed Conflict) ก่อนหน้าอนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติม ค.ศ.1977 เช่นใน Liber Code ซึ่งปรากฏข้อจำกัดการใช้อาวุธที่จะก่อให้เกิด “ความเสียหายเกินขนาด” (Superfluous injury)[187] ข้อจำกัดการใช้อาวุธดังกล่าวยังปรากฏในปฏิญญาเซนต์ปีเตอร์สเบิร์ก[188] คู่มือออกซ์ฟอร์ด (Oxford

[186] Williams Boothby, Weapons and the Law of Armed Conflict, (Oxford: Oxford University Press, 2009), p. 5.

[187] Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863, Art 14. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863

[188] International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874, Art 12 and 13 (a) and (e). [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874

Manual 1880)[189]รวมถึงในอนุสัญญาเฮก ค.ศ.1907[190] จนกระทั่งหลังสงครามโลกครั้งที่ 2 คณะกรรมการกาชาดระหว่างประเทศได้รวบรวมหลักการต่างๆ ที่ปรากฏในกฎหมายระหว่างประเทศหลายฉบับโดยตระหนักถึงสถานการณ์ที่เกิดขึ้นในสงครามโลกครั้งที่ 2 และได้สร้างข้อจำกัดเรื่องการห้ามใช้วิธีการและปัจจัยที่จะก่อให้เกิดความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นขึ้นมา[191]

2) พัฒนาการของกฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธได้รับอิทธิพลไม่มากก็น้อยจากแนวคิดในการจำกัดความเสียหายที่เกิดจากการใช้อาวุธในการขัดกันทางอาวุธ โดยเริ่มต้นจากกฎหมายห้ามใช้อาวุธในการรบ เช่น ปฏิญญาเซ็นต์ปีเตอร์สเบิร์กว่าด้วยการห้ามใช้กระสุนปืนที่มีน้ำหนักต่ำกว่า 400 กรัม ค.ศ.1868 อนุสัญญากรุงเฮก ค.ศ. 1899 ซึ่งมีปฏิญญาประกอบ 3 ฉบับ ฉบับที่ 1 ว่าด้วยเรื่องการห้ามใช้กระสุนและวัตถุระเบิดที่ปล่อยจากบอลลูน ฉบับที่ 2 ว่าด้วยเรื่องการห้ามใช้กระสุนแก๊สพิษ ฉบับที่ 3 ว่าด้วยเรื่องการห้ามใช้กระสุนที่แตกกระจายเมื่อเข้าสู่ร่างกายมนุษย์ พิธีสารเจนีวาว่าด้วยเรื่องการห้ามใช้แก๊สพิษและแบคทีเรียในการทำสงคราม ค.ศ.1925 อนุสัญญาแห่งสหประชาชาติว่าด้วยการห้ามใช้อาวุธตามแบบที่อาจก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น ค.ศ.1980 ซึ่งมีพิธีสารเพิ่มเติม 5 ฉบับ อันได้แก่ พิธีสารฉบับที่ 1 ว่าด้วยเรื่องการห้ามใช้วัตถุที่แตกกระจายในร่างกายมนุษย์และไม่สามารถตรวจพบได้ด้วยรังสีเอ็กซ์ ค.ศ.1980 พิธีสารฉบับที่ 2 ว่าด้วยการห้ามและจำกัดการใช้ทุ่นระเบิดสังหารบุคคล ค.ศ.1980 พิธีสารฉบับที่ 3 ว่าด้วยการห้ามและจำกัดการใช้อาวุธเพลิง ค.ศ.1980 พิธีสารฉบับที่ 4 ว่าด้วยการห้ามใช้อาวุธเลเซอร์ ค.ศ.1995 พิธีสารฉบับที่ 5 ว่าด้วยเรื่องวัตถุระเบิดที่เหลือจากการสงคราม ค.ศ.2003 เป็นต้น

องค์การสหประชาชาติมีบทบาทอย่างมากในการพัฒนากฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธในยุคหลังสงครามโลกครั้งที่ 2 ซึ่งเป็นเป็นตามวัตถุประสงค์การจัดตั้งองค์การ

---

[189] The Laws of War on Land, Manual published by the Institute of International Law (Oxford Manual), Adopted by the Institute of International Law at Oxford, September 9, 1880. Art 3 and art 4. [online] Accessed: June 9, 2022. Available from: http://hrlibrary.umn.edu/instree/1880a.htm

[190] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, Art. 22. [online] Accessed: June 10, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

[191] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 35 (1).

สหประชาชาติเพื่อการรักษาสันติภาพระหว่างประเทศ ในขณะที่กฎหมายมนุษยธรรมระหว่างประเทศมีขอบเขตการปรับใช้ในสถานการณ์การขัดกันทางอาวุธอยู่แล้ว กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธของสหประชาชาติจึงถูกสร้างขึ้นมาเพื่อการการลดอาวุธที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความเสียหายที่ไม่สามารถจำกัดขอบเขตได้ ซึ่งมาตรการที่เกี่ยวข้องกับการลดอาวุธย่อมรวมถึงการควบคุมการพัฒนา การควบคุมการผลิต และการควบคุมการแพร่กระจายอาวุธ[192] มาตรการเหล่านี้ไม่เกี่ยวข้องกับขอบเขตการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศโดยตรงแต่เป็นมาตรการที่เสริมประสิทธิผลการการใช้กฎหมายมนุษยธรรมระหว่างประเทศในสองลักษณะคือการป้องกันไม่ให้มีการพัฒนาและผลิตอาวุธที่จะนำมาใช้ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศและการทำลายอาวุธภายหลังจากที่สถานการณ์ขัดกันทางอาวุธสิ้นสุดลง

นอกจากนั้น กฎหมายระหว่างประเทศเหล่านี้ชี้ให้เห็นถึงแนวโน้มของกฎหมายระหว่างประเทศในการห้ามการใช้อาวุธเฉพาะอย่าง ซึ่งอาวุธที่ปรากฏในช่วงเวลาต่างๆ เป็นตัวแทนของพัฒนาการทางเทคโนโลยีในแต่ละยุค เมื่อมีการพัฒนาอาวุธใหม่ๆ ขึ้น จึงก่อให้เกิดความพยายามในการสร้างกฎหมายในการควบคุมการใช้งานอาวุธเหล่านั้น การบังคับใช้กฎหมายในแต่ละยุคจึงอยู่ในลักษณะของการบังคับกับเทคโนโลยีที่เป็นลักษณะของวัตถุ หรือสิ่งประดิษฐ์ที่เกิดขึ้นมามากกว่าที่จะเป็นการบังคับกับองค์ความรู้หรือวิธีการทำสงคราม ดังสังเกตได้ว่ากฎหมายเฉพาะเรื่องที่เกี่ยวกับการห้ามวิธีการที่มิใช่สิ่งประดิษฐ์เกิดขึ้นมาน้อยมาก เช่น อนุสัญญาสหประชาชาติว่าด้วยการห้ามใช้เทคนิคการดัดแปลงสิ่งแวดล้อมในทางทหารหรือการใช้ที่เป็นปฏิปักษ์อื่นใด ค.ศ.1977[193] เป็นต้น แม้กฎหมายระหว่างประเทศที่เกี่ยวข้องกับการห้ามการใช้ความรู้ในฐานะที่เป็นเทคโนโลยีในการทำการรบจะมีค่อนข้างน้อยก็ตาม แต่จากกฎหมายระหว่างประเทศที่ปรากฏถึงความพยายามในการควบคุมการใช้เทคโนโลยีในทั้งสองลักษณะคือทั้งการใช้วัตถุหรือสิ่งประดิษฐ์เช่นอาวุธและการใช้วิธีการหรือเทคนิคในการทำสงครามในลักษณะความรู้ใหม่ ขอบเขตของ “เทคโนโลยี” ที่ศึกษาในงานวิจัยฉบับนี้จึงมุ่งหมายที่จะพิจารณาเทคโนโลยีที่ใช้ 2 ลักษณะ คืออาวุธที่ใช้เพื่อการขัดกันทางอาวุธและวิธีการที่ใช้ในการขัดกันทางอาวุธ โดยให้ความสำคัญกับเทคโนโลยีในลักษณะที่เป็นการนำเอาวิธีการและอาวุธมาใช้เพื่อประโยชน์ในการขัดกันทางอาวุธ ซึ่งจะมีความครอบคลุมกับกรอบข้อจำกัดในการขัดกันทาง

---

[192] Alyn Ware, eds., Assuring our Common Future: A guide to parliamentary action in support of disarmament for security and sustainable development, (New York: United Nations Secretary general, 2020), p.10.

[193] 1977 United Nations Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques.

อาวุธในเรื่องของ วิธีการ (Methods) และปัจจัย (Means) ที่ปรากฏในพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 ทั้งนี้ การให้ความสำคัญกับผลที่เกิดจากการใช้งานเทคโนโลยีย่อมสอดคล้องกับหลักการขั้นพื้นฐานในการให้ความคุ้มครองบุคคลในกรณีการขัดกันทางอาวุธ

หลายศตวรรษที่ผ่านมาพัฒนาของอาวุธทางการทหารให้ความสำคัญกับเครื่องมือที่เป็นวัตถุ (hardware) เช่น ธนู ปืน ฯลฯ แต่ยุคต่อมาการพัฒนาการรบเริ่มเปลี่ยนแปลงในรูปแบบและวิธีการลักษณะอสมมาตร (Asymmetric warfare) มากขึ้น กล่าวคือเริ่มมีการคำนึงถึงปฏิบัติการที่หวังผล (effects-based approach)[194] โดยให้ความสำคัญกับการพัฒนาอาวุธที่เป็นวัตถุลดลง โดยปรากฏว่ามีประเทศกว่า 100 ประเทศที่จัดตั้งหน่วยปฏิบัติการทางไซเบอร์ของกองทัพขึ้นมา ในขณะที่ประเทศเกือบ 30 ประเทศมีการพัฒนาระบบอากาศยานไร้คนขับ (Unmanned Aerial Vehicle) เพื่อการลาดตระเวน ตรวจตรา และระบุตำแหน่งเป้าหมายแล้ว นอกจากนั้นยังพบการใช้ระบบปัญญาประดิษฐ์ (Artificial Intelligence) และระบบนาโนเทคโนโลยี รวมถึงเทคโนโลยีชีวภาพของกองทัพหลายประเทศ[195] พัฒนาการทางเทคโนโลยีในการขัดกันทางอาวุธจึงเป็นไปเพื่อเพิ่มประสิทธิภาพทางการรบของกองทัพ ให้สามารถทำลายเป้าหมายได้แม่นยำขึ้น ลดการสูญเสียของพลรบและพลเรือนให้มากขึ้น[196] ในขณะเดียวกันก็ยังมีวิธีการในการใช้งานสิ่งที่ไม่ใช่อาวุธให้กลายเป็นอาวุธมากขึ้นด้วยโดยการประยุกต์เอาความรู้และนวัตกรรมที่มีอยู่ในการใช้งานภาคพลเรือนมาเป็นประโยชน์ในการรบมากยิ่งขึ้น

พัฒนาการทางด้านเทคโนโลยีในการขัดกันทางอาวุธนี้ก่อให้เกิดข้อท้าทายต่อกฎหมายหลายประการ ทั้งเรื่องการพิจารณาความรับผิดของปัญญาประดิษฐ์ที่สามารถก่อความเสียหายต่อเป้าหมายที่มีการสั่งงานหรือกำหนดเงื่อนไขไว้ได้ การแยกแยะผู้ปฏิบัติการในการโจมตีทางไซเบอร์ว่าผู้ใดคือพลเรือนและผู้ใดคือพลรบ เช่นเดียวกับอากาศยานไร้คนขับซึ่งแม้ในปัจจุบันจะเป็นการใช้งานเพื่อการลาดตระเวนค้นหาเป้าหมายเป็นสำคัญแต่ก็อาจขัดต่อหลักกฎหมายอื่นๆ เช่นสิทธิส่วนบุคคล การบุก

---

[194] Darren M. Steward, “New Technology and the Law of Armed Conflict.” International Law Studies, Vol 87, (2011): 271.

[195] Rain Liivoja, “Technological Change and the Evolution of the Law of War.” International Review of the Red Cross Review: The evolution of warfare, Volume 97, Number 900, (2015): 1158.

[196] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p.26.

รุกเข้าไปในพื้นที่ของบุคคลหรือดินแดนของรัฐอื่น เทคโนโลยีที่มีการใช้งานในปัจจุบันจึงแสดงผลออกมาทั้งในแง่ของข้อดีและข้อเสียของการใช้งานเทคโนโลยีดังกล่าว

ในมุมมองของสังคมระหว่างประเทศทั้งในเชิงการทหาร เชิงวิทยาศาสตร์และเชิงเศรษฐกิจนั้น พัฒนาการของเทคโนโลยีใหม่ทางการทหารมีทั้งข้อดีในแง่การนำความรู้ทางวิทยาศาสตร์เพื่อต่อยอดการใช้งานอาวุธ ก่อให้เกิดการพัฒนาทางเทคโนโลยีทางอาวุธที่ใช้งานได้แม่นยำและละความสูญเสียทางกำลังพล ซึ่งสอดคล้องต่อกฎหมายมนุษยธรรมระหว่างประเทศมากขึ้น แต่อีกมุมมองหนึ่งเทคโนโลยีเหล่านี้ก็สร้างความเหลื่อมล้ำต่อประเทศผู้ครอบครองเทคโนโลยีที่ทันสมัยและประเทศที่ไม่สามารถเข้าถึงเทคโนโลยีเหล่านี้ได้ด้วยข้อจำกัดด้านการเงินและความรู้

ความเหลื่อมล้ำในการเป็นผู้ครอบครองและใช้เทคโนโลยีใหม่ทมางการทหารนี้ไม่ได้ส่งผลกระทบเฉพาะแต่เพียงการเป็นมหาอำนาจทางการทหารและความได้เปรียบในการรบแต่ยังมีผลต่อการสร้างความร่วมมือระหว่างประเทศที่เกี่ยวข้องกับการสร้างกฎหมายระหว่างประเทศเพื่อควบคุมอาวุธและเทคโนโลยีทางการทหารด้วย เช่นในคณะศึกษาทำงานเพื่อร่างอนุสัญญาระหว่างประเทศเกี่ยวกับระบบอาวุธอิสระ (Autonomous Weapons Systems) ของสหประชาชาติไม่สามารถผลักดันให้ร่างอนุสัญญาดังกล่าวผ่านความเห็นชอบของที่ประชุมแห่งสหประชาชาติได้ เนื่องจากการพัฒนาระบบอาวุธสังหารอิสระยังอยู่ในระหว่างการพัฒนาและไม่แน่ว่าในอนาคตจะเทคโนโลยีเหล่านี้จะเป็นอย่างไร[197]และปัจจัยย่อยประการอื่นทางการเมืองระหว่างประเทศเช่นความแตกต่างระหว่างประเทศที่พัฒนาด้านระบบอาวุธอิสระอย่างมากกับประเทศที่ไม่มีระบบอาวุธอิสระเลยก็เป็นที่มาของการหาข้อยุติในการรับรองอนุสัญญาระหว่างประเทศเกี่ยวกับการควบคุมระบบอาวุธไม่ได้เช่นกัน[198]

2.3.3 บทบาทขององค์การระหว่างประเทศในการแก้ไขปัญหาการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ

เทคโนโลยีใหม่ที่ปรากฏการใช้งานในปัจจุบันนั้นก่อให้เกิดผลทั้งในเชิงบวกและเชิงลบ กล่าวคือ เทคโนโลยีหลายประการที่มีการใช้งานเพื่ออำนวยความสะดวกแก่พลเรือนนั้นทำให้การดำรงชีวิตมีความสะดวกมากขึ้นในขณะที่เทคโนโลยีใหม่ที่ปรากฏการนำมาใช้ทางการทหารนั้นอาจ

---

[197] United Nations, “Report of the 2023 session of the Group of the Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,” CCW/GGE.1/2023/2, 24 May 2023, Para 20.

[198] Afonso Seixas Nunes, “Autonomous Weapons System and Deploying States: making Designers and Programmers Accountable,” Nacao e Defesa, 161 (2022): 72.

นำไปสู่ทั้งการลดความเสียหายแก่กองทัพและพลเรือนและอาจนำไปสู่ความเสียหายในปริมาณที่กว้างขวางก็ได้[199] การใช้เทคโนโลยีในทั้งสองลักษณะจึงนำไปสู่การพิจารณาว่าควรจะต้องมีการควบคุมหรือไม่ และจะควบคุมอย่างไร เพราะเทคโนโลยีเหล่านี้มีทั้งประโยชน์และโทษในเวลาเดียวกัน อย่างไรก็ดี ความเคลื่อนไหวของกฎหมายระหว่างประเทศที่ปรากฏมีทั้งในรูปแบบของความพยายามในการสร้างองค์กรแนวทางปฏิบัติ และกฎหมายเพื่อควบคุมการใช้งานเทคโนโลยีใหม่เหล่านี้ให้อยู่ในระดับที่ไม่ก่อให้เกิดความเสียหายต่อสังคม ความเคลื่อนไหวต่างๆ ที่แสดงนัยสำคัญของเทคโนโลยีใหม่ต่อกฎหมายระหว่างประเทศ ได้แก่

1) การโจมตีทางไซเบอร์ซึ่งนำไปสู่การสร้างคู่มือทาลลินน์ Tallinn Manual 1.0 และ 2.0

เหตุการณ์การโจมตีทางไซเบอร์ต่อระบบการสื่อสารทางอินเทอร์เน็ตของเมืองทาลลินน์ ประเทศเอสโตเนียในปี ค.ศ. 2007 ทำให้ NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) ซึ่งประกอบด้วยกลุ่มผู้เชี่ยวชาญทางด้านกฎหมายมนุษยธรรมระหว่างประเทศ ผู้เชี่ยวชาญทางการทหาร นักวิชาการ และผู้เชี่ยวชาญด้านคอมพิวเตอร์ได้ริเริ่มเสนอแนวทางในการปรับใช้กฎหมายระหว่างประเทศต่อกรณีการโจมตีทางไซเบอร์ โดยจำแนกแนวทางการปรับใช้กฎหมายใน 2 สถานการณ์คือการปรับใช้กฎหมายระหว่างประเทศในสถานการ Jus ad bellum หรือการโจมตีทางไซเบอร์ในสถานการณ์ที่จะนำไปสู่การขัดกันทางอาวุธตามกฎหมายระหว่างประเทศ และการปรับใช้กฎหมายในกรณี Jus in Bello หรือกรณีการโจมตีทางไซเบอร์ที่เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ

คู่มือทาลลินน์ ฉบับที่ 1 ว่าด้วยเรื่องการปรับใช้กฎหมายระหว่างประเทศต่อสงครามทางไซเบอร์ (Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare) หรือที่เรียกว่า Tallinn Manual 1.0 ตีพิมพ์เผยแพร่ในปี ค.ศ.2013 (พ.ศ.2558) มีเนื้อหาครอบคลุมขอบเขตการใช้งานไซเบอร์ในบริบทต่างๆ ของกฎหมายระหว่างประเทศ แต่จะเน้นที่ปฏิบัติการระหว่างไซเบอร์ต่อไซเบอร์ (cyber-to-cyber) หรือปฏิบัติการที่ใช้การทำงานของอุปกรณ์คอมพิวเตอร์ผ่านพื้นที่เครือข่ายคอมพิวเตอร์เพื่อทำลายระบบเครือข่ายคอมพิวเตอร์ของเป้าหมาย แต่ไม่ได้ให้ความสำคัญกับปฏิบัติการทางกายภาพต่อไซเบอร์ (kinetic-to-cyber) เช่นการใช้จรวดยิงทำลายเป้าหมายที่เป็น

---

[199] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 27.

ศูนย์ปฏิบัติการทางไซเบอร์[200] ในขณะที่ประเด็นซึ่งอยู่นอกเหนือสถานการณีการขัดกันทางอาวุธหลายกรณีก็ไม่มีการกล่าวถึงใน Tallinn Manual 1.0 นี้ เช่น แนวทางในการปรับใช้กฎหมายระหว่างประเทศต่อความมั่นคงทางไซเบอร์ การจารกรรมทางไซเบอร์ และอาชญากรรมทางไซเบอร์ แม้ว่าจะเป็นที่เข้าใจได้ว่าประเทศต่างๆ น่าจะมีกฎหมายภายในของตนเองในการจัดการกับปัญหาดังกล่าวก็ตาม แต่ประเด็นของปฏิบัติการทางไซเบอร์มีลักษณะสำคัญอยู่ที่การทำงานแบบไร้พรมแดน กล่าวคือ ผู้ปฏิบัติการจะอยู่ที่ใดก็สามารถทำการโจมตีเครือข่ายไซเบอร์เป้าหมายซึ่งอยู่ในดินแดนประเทศอื่นได้ หากมีแนวทางกฎหมายระหว่างประเทศในการจัดการกับปัญหาดังกล่าวจะเป็นการสอดคล้องกับลักษณะของปฏิบัติการทางไซเบอร์มากกว่า

NATO ยอมรับให้ปฏิบัติการโจมตีทางไซเบอร์ที่สหรัฐอเมริกากระทำต่อประเทศอิหร่าน และปฏิบัติการของ NATO ในการป้องกันทางไซเบอร์ให้กับประเทศเอสโตเนียเป็นการขัดกันทางอาวุธ โดยใน Tallinn Manual 1.0 ให้ความหมายของคำว่า “การใช้กำลัง” (Use of Force) หมายถึง “การฆาตกรรมหรือการทำให้บุคคลได้รับบาดเจ็บ หรือการทำลายหรือทำให้สิ่งของได้รับความเสียหาย”

Tallinn Manual 1.0 กำหนดหลักเกณฑ์ในการปรับใช้กฎหมายระหว่างประเทศทั้งสิ้น 95 ข้อ มีโครงสร้างการจัดหมวดหมู่ดังนี้

ส่วนที่ 1 การปรับใช้กฎหมายระหว่างประเทศกับความมั่นคงทางไซเบอร์ ให้ความสำคัญกับเรื่อง

(ก) ความสัมพันธ์ระหว่างรัฐกับพื้นที่ทางไซเบอร์ โดยเป็นการสร้างความเชื่อมโยงระหว่างอำนาจอธิปไตยของรัฐกับพื้นที่ทางไซเบอร์ ขอบเขตการบังคับใช้กฎหมายตามหลักอำนาจอธิปไตย เขตอำนาจรัฐ และการควบคุมสาธารณูปโภคขั้นพื้นฐานทางไซเบอร์ ความรับผิดชอบของรัฐตามกฎหมายระหว่างประเทศต่อการปฏิบัติการทางไซเบอร์

---

[200] B. Pratama and M. Bamatraf, “Tallinn manual: Cyber warfare in Indonesian regulation,” IOP Conference Series: Earth and Environmental Science, Vol. 729, International Conference on Biospheric Harmony Advanced Research (ICOBAR 2020) 23-24 June 2020, Jakata, Indonesia. (2021): 1-8 [online] Accessed: March 20, 2023. Available from: https://iopscience.iop.org/article/10.1088/1755-1315/729/1/012033/pdf

(ข) หลักการใช้กำลัง ที่สอดคล้องกับกฎบัตรสหประชาชาติ โดยจำแนกการใช้ปฏิบัติการทางไซเบอร์เป็น 2 ประเด็นด้วยกัน คือ 1) ข้อห้ามเรื่องการใช้กำลังทางระหว่างประเทศ 2) หลักการป้องกันตัว

(ค) การกระทำขององค์การระหว่างประเทศ โดยการกำหนดบทาทขององค์การระหว่างประเทศที่ใช้ปฏิบัติการทางไซเบอร์ซึ่งถือเป็นตัวตนหนึ่งของกฎหมายระหว่างประเทศ

ส่วนที่ 2 กฎหมายว่าด้วยการขัดกันทางอาวุธไซเบอร์ ประกอบด้วย

(ก) หลักทั่วไปเกี่ยวกับเรื่องการขัดกันทางอาวุธ ซึ่งกำหนดให้นำกฎหมายมนุษยธรรมระหว่างประเทศมาใช้กับปฏิบัติการทางไซเบอร์ที่เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธทั้งการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ โดยการขัดกันทางอาวุธเป็นไปตามเงื่อนไขของอนุสัญญาเจนีวา ค.ศ.1949[201] นอกจากนั้นยังระบุว่าปฏิบัติการทางไซเบอร์นั้นรวมถึงการโจมตีทางไซเบอร์ด้วย แต่ปฏิบัติการทางไซเบอร์ย่อมไม่จำกัดเฉพาะการโจมตีทางไซเบอร์เท่านั้น และนิยามคำว่าการโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง ปฏิบัติการทางไซเบอร์ไม่ว่าจะเป็นการโจมตีหรือการป้องกัน ซึ่งคาดหมายได้ว่าจะก่อให้เกิดความบาดเจ็บหรือความตายแก่บุคคล หรือความเสียหายแก่ทรัพย์สิน[202]

(ข) หลักการกระทำที่เป็นปรปักษ์ (Conduct of Hostilities) อันได้แก่การมีส่วนร่วมในการขัดกันทางอาวุธ หลักการโจมตีทั่วไป หลักการโจมตีบุคคล หลักการโจมตีวัตถุ หลักวิธีการและปัจจัยในการทำสงคราม หลักการกระทำที่ถือว่าเป็นการโจมตี หลักความระมัดระวังล่วงหน้า หลักการล่อลวง การชี้นำทางที่ผิด และการจารกรรม หลักการปิดล้อมและพื้นที่ต่างๆ ซึ่งหลักการเหล่านี้ปรากฏอยู่ในอนุสัญญาเจนีวา ค.ศ. 1949 และพิธีสารเพิ่มเติมจะต้องนำมาปรับใช้กับปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธด้วย[203]

(ค) หลักการคุ้มครองสำหรับบุคคล วัตถุ และกิจกรรรมกรณีเฉพาะ เช่น การคุ้มครองสถานพยาบาล การคุ้มครองเจ้าหน้าที่ขององค์การสหประชาชาติ การคุ้มครองผู้ต้องขัง การคุ้มครอง

---

[201] Michael N. Schmitt, eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013), Rule 20, p. 68.

[202] Ibid., p. 91. Rule 30.

[203] Ibid., Rule 25-40.

เด็ก การคุ้มครองผู้สื่อข่าว การคุ้มครองสถานที่ติดตั้งวัตถุอันตราย การคุ้มครองพื้นที่และวัตถุทางวัฒนธรรม การคุ้มครองสิ่งแวดล้อมทางธรรมชาติ และการให้ความช่วยเหลือทางมนุษยธรรม[204]

(ง) การครอบครองดินแดน และความคุ้มครองบุคคลที่อยู่ในพื้นที่ครอบครองจะต้องได้รับความคุ้มครองจากปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์[205]

(จ) หลักความเป็นกลาง

หลังจากมีการเผยแพร่คู่มือทาลินน์ฉบับที่ 1 ไปได้ 4 ปี คณะผู้เชี่ยวชาญขององค์การสนธิสัญญาเพื่อการป้องกันแอตแลนติกเหนือหรือนาโต้ ได้ทำการปรับปรุงแก้ไขคู่มือทาลินน์อีกครั้งตามกรอบระยะเวลาที่กำหนดเอาไว้ โดยครั้งนี้ใช้ชื่อว่า คู่มือทาลินน์ฉบับที่ 2 ว่าด้วยกฎหมายระหว่างประเทศที่ปรับใช้แก่ปฏิบัติการทางไซเบอร์ (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations) โดยยังคงใช้แนวทางตามที่เคยใช้กับการสร้าง Tallinn Manual 1.0 คือการนำเอาอนุสัญญาระหว่างประเทศ แนวทางคำพิพากษาศาลระหว่างประเทศและข้อมูลอื่นๆ มาวิเคราะห์ และสังเคราะห์แนวทางในการปรับใช้กฎหมายระหว่างประเทศเหล่านั้นกับกรณีปฏิบัติการทางไซเบอร์

Tallinn Manual 2.0 มีการเผยแพร่ในเดือนมกราคม ค.ศ.2017 โดยมีความต้องการแก้ไขเนื้อหาบางส่วนที่มีอยู่เดิมในฉบับที่ 1 ที่เห็นว่ามีบริบทที่เปลี่ยนแปลงไป เช่นเรื่องอำนาจอธิปไตยและความรับผิดชอบของรัฐ นอกจากนั้นยังมีการเพิ่มเติมเนื้อหาอื่นๆ ที่คณะผู้เชี่ยวชาญเห็นว่าในฉบับแรกมิได้มีการกล่าวถึงและอาจก่อให้เกิดปัญหาต่อการปรับใช้กฎหมาย อันได้แก่ประเด็นเรื่อง การคุ้มครองสิทธิมนุษยชน กฎหมายระหว่างประเทศที่เกี่ยวข้องกับพื้นที่ทางอากาศ อวกาศ และพื้นที่ทางทะเล

อาจกล่าวได้ว่า Tallinn Manual 2.0 นี้ เป็นแนวทางในการปรับใช้กฎหมายระหว่างประเทศกับกรณีปฏิบัติการทางไซเบอร์ที่ให้ความสำคัญกับกิจกรรมทางไซเบอร์ในช่วงเวลาสันติค่อนข้างมาก โดยกฎเกณฑ์ต่างๆ ที่สร้างขึ้นมาใน Tallinn Manual 2.0 ส่วนที่ 1 นั้น เป็นส่วนที่เพิ่มเติมขึ้นมาค่อนข้างมาก แต่หลักการในส่วนที่ 2 ซึ่งเกี่ยวข้องกับกฎหมายมนุษยธรรมระหว่างประเทศไม่ได้เปลี่ยนแปลงไปจากเดิม

เนื้อหาภายในคู่มือทาลินน์ ฉบับที่ 2 นี้มีข้อกำหนดทั้งสิ้น 154 ข้อ มีการจัดโครงสร้างใหม่เล็กน้อย โดยประเด็นเรื่องกฎหมายระหว่างประเทศกับความมั่นคงทางไซเบอร์ เปลี่ยนไปใช้ชื่อ

---

[204] Michael N. Schmitt, eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 70-86.

[205] Ibid., Rule 87-90.

“กฎหมายระหว่างประเทศกรณีทั่วไปกับพื้นที่ทางไซเบอร์” และเน้นเนื้อหาเรื่อง อำนาจอธิปไตยทางไซเบอร์ของรัฐทั้งภายในรัฐและภายนอกรัฐ การละเมิดอำนาจอธิปไตย และความคุ้มกันของรัฐ

นอกจากนั้นยังมีการเพิ่มเติมหลัก Due Diligence หรือหลักการประเมินผลกระทบต่อกรณีการใช้งานไซเบอร์ ขยายคำอธิบายเรื่องเขตอำนาจรัฐ และมีการเพิ่มเติมเนื้อหาเรื่องความรับผิดชอบของรัฐให้ละเอียดขึ้น มีการเพิ่มเติมเรื่องการปฏิบัติการทางไซเบอร์ของกลุ่มที่ไม่ใช่รัฐ เพิ่มเติมเรื่องการคุ้มครองสิทธิมนุษยชนทางไซเบอร์ เพิ่มหลักกฎหมายทะเล กฎหมายอากาศ กฎหมายอวกาศที่จะปรับใช้ต่อปฏิบัติการทางไซเบอร์ หลักกฎหมายเกี่ยวกับการโทรคมนาคม หลักการระงับข้อพิพาท และหลักข้อห้ามเรื่องการใช้กำลัง

อย่างไรก็ดี ปรากฏว่าเนื้อหาของคู่มือส่วนที่ 2 ซึ่งเป็นเรื่องการปฏิบัติการทางไซเบอร์ต่อกรณีการขัดกันทางอาวุธนั้นไม่มีการแก้ไขหรือเปลี่ยนแปลงเลย หมายความว่ากลุ่มผู้เชี่ยวชาญมองว่าปัญหาของปฏิบัติการทางไซเบอร์มีผลกระทบต่อกฎหมายทั่วไปในกรณีที่ไม่ได้เกิดการขัดกันทางอาวุธมากกว่า

ประเด็นที่น่าสังเกตประการหนึ่งคือ ประธานคณะผู้เชี่ยวชาญเพื่อจัดทำคู่มือทาลินน์ทั้งสองฉบับที่ผ่านมาคือ Professor Michael N. Schmitt ซึ่งเป็นอดีตทหารอากาศแห่งกองทัพสหรัฐอเมริกาและปัจจุบันดำรงตำแหน่งที่ปรึกษาอาวุโสด้านการป้องกันภัยทางไซเบอร์ขององค์กรสนธิสัญญาเพื่อการป้องกันแอตแลนติกเหนือ ซึ่ง Schmitt มีงานตีพิมพ์ในปี ค.ศ. 2010 ในประเด็นที่เกี่ยวข้องกับเรื่องหลักการใช้กำลังทางอาวุธและการโจมตีทางไซเบอร์ โดยในงานชิ้นดังกล่าว Schmitt มองว่าปฏิบัติการทางไซเบอร์ไม่มีทางที่จะถือว่าเป็นการใช้กำลังทางอาวุธหรือการคุกคามต่อสันติภาพและบูรณภาพแห่งดินแดน ตามข้อ 2 (4) ของกฎบัตรสหประชาชาติได้เลย แต่ในคู่มือทาลลินน์ ฉบับที่ 1 มีการอธิบายว่าทางปฏิบัติของรัฐทั้งหลายยอมรับเป็นแนวเดียวกันว่าการโจมตีทางไซเบอร์ถือว่าเป็นการโจมตีเช่นเดียวกับอาวุธ ทั้งนี้ให้พิจารณาจากลักษณะของการกระทำที่เทียบเท่ากับลักษณะของการใช้อาวุธ[206] และให้ถือว่าการโจมตีทางไซเบอร์เป็นการละเมิดต่อข้อ 2 (4) ของกฎบัตรสหประชาชาติด้วย ทั้งนี้ การกระทำที่เทียบเท่ากับการใช้อาวุธ หมายถึงการพิจารณาจากสัดส่วนและผลกระทบที่เกิดขึ้น (Scale and effects)[207] มีการอธิบายเพิ่มเติมว่ากรณีการใช้ปฏิบัติการทางไซเบอร์เพื่อข่าวสารปลอมโดยหวังผลความได้เปรียบทางการรบนั้นย่อมไม่เทียบเท่าการใช้กำลังทางอาวุธ โดยเทียบเคียงกับคำ

[206] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, p. 43.

[207] Ibid., p.46.

พิพากษาของศาลยุติธรรมระหว่างประเทศคดี Nicaragua ซึ่งศาลอธิบายว่าการสนับสนุนกองกำลังด้วยงบประมาณนั้น ไม่ถือว่าเป็นการใช้กำลังทางอาวุธ เพราะการใช้กำลังทางอาวุธต้องเป็นเรื่องที่เกี่ยวข้องกับการใช้กำลังโดยตรงเท่านั้น

แม้คำอธิบายดังกล่าวจะเป็นที่ยอมรับได้ของคณะผู้เชี่ยวชาญ แต่ก็ยังมีหลายประเด็นทียังไม่ชัดเจนเช่น การวัดสัดส่วนและผลกระทบที่เทียบเท่ากับกับการใช้อาวุธจะทำได้อย่างไร และกรณีที่มีการใช้ปฏิบัติการทางไซเบอร์ของกลุ่มที่ไม่ใช่รัฐจะใช้หลักเกณฑ์นี้บังคับได้หรือไม่ ดังนั้นหากพิจารณาในภาพรวมของหลักเกณฑ์ที่ปรากฏในคู่มือทาลลินน์ฉบับนี้จะพบว่าค่อนข้างเป็นการด่วนสรุปเพื่อให้ใช้กฎหมายได้ และมีความพยายามสร้างหลักการที่เป็นนามธรรมเพื่อให้เกิดความยืดหยุ่นต่อการปรับใช้กฎหมาย ซึ่งปัญหาน่าจะไปตกอยู่กับศาลระหว่างประเทศในกรณีที่มีข้อพิพาทเกิดขึ้นจากการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตี เพราะคู่มือทาลลินน์นี้ก็ไม่มีสถานะทางกฎหมายระหว่างประเทศแต่อย่างใด จะถือว่าเป็นตัวอย่างของการปฏิบัติในสังคมระหว่างประเทศก็คงไม่ได้ เนื่องจากเป็นแนวทางที่เกิดขึ้นโดย NATO อย่างไรก็ดี คู่มือทาลลินน์นี้ก็ไม่ได้ไร้ประโยชน์เสียทั้งหมด เพราะอย่างน้อยก็เป็นความพยายามในการอธิบายว่ากฎหมายระหว่างประเทศใดจะใช้บังคับต่อกรณีการปฏิบัติการทางไซเบอร์ได้บ้าง

2) พัฒนาการของระบบอาวุธอิสระซึ่งนำไปสู่ความพยายามในการสร้างอนุสัญญาของสหประชาชาติ

ระบบอาวุธอิสระ (Autonomous Weapons System) สร้างความตระหนักต่อกองทัพของรัฐต่างๆ และนักกฎหมายระหว่างประเทศ รวมถึงองค์การสหประชาชาติซึ่งต้องการให้มีบทบัญญัติกฎหมายระหว่างประเทศที่สามารถบังคับหรือควบคุมการใช้งานระบบอาวุธอิสระได้ จึงมีการจัดคณะผู้เชี่ยวชาญของสหประชาชาติขึ้นมาเพื่อศึกษาความเคลื่อนไหวของพัฒนาการระบบอาวุธตัดสินใจได้ด้วยตนเอง การใช้งานที่ปรากฏในการขัดกันทางอาวุธ และความเป็นไปได้ในการสร้างอนุสัญญาระหว่างประเทศเพื่อควบคุมระบบอาวุธอิสระ

แม้ในปัจจุบันการสร้างอนุสัญญาระหว่างประเทศเกี่ยวกับการควบคุมระบบอาวุธอิสระของสหประชาชาติจะยังไม่ได้รับการรับรองจากประเทศสมาชิกของสหประชาชาติให้ประกาศเป็นอนุสัญญาระหว่างประเทศเนื่องจากพัฒนาการในปัจจุบันของเทคโนโลยียังอยู่ในการพัฒนาอย่างต่อเนื่อง

จึงจำเป็นต้องมีการพิจารณาถึงแนวโน้มในอนาคตของระบบอาวุธอิสระที่ยังไม่สามารถสรุปได้[208] แต่กลุ่มผู้เชี่ยวชาญของสหประชาชาติยังคงเห็นว่าการใช้งานระบบอาวุธอิสระนั้นจะต้องสอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศด้วยโดยเฉพาะอย่างยิ่งต่อหลักการพื้นฐาน อันได้แก่หลักการแยกแยะ หลักความได้สัดส่วน และความระมัดระวังล่วงหน้าก่อนการโจมตี[209] นอกจากนั้นรัฐต่างๆ ยังมีหน้าที่ในการพิจารณาว่าระบบอาวุธอิสระที่ตนมีอยู่และใช้งานนั้นจะต้องสามารถจำกัดเป้าหมายในการโจมตีได้ สามารถจำกัดระยะเวลาการใช้งานอาวุธ จำกัดพื้นที่ใช้อาวุธและจำกัดการใช้งานอาวุธ รวมตลอดถึงการจัดการฝึกอบรมอย่างเหมาะสมแก่ผู้ทำหน้าที่ในการควบคุมปฏิบัติการของระบบอาวุธอิสระด้วย[210]

ประเด็นที่น่าสนใจคือแนวโน้มการพัฒนาเทคโนโลยีทางการทหารในปัจจุบันของสังคมระหว่างประเทศให้ความสำคัญกับระบบปัญญาประดิษฐ์เป็นอย่างมาก โดยระบบปัญญาประดิษฐ์เหล่านี้มักเกี่ยวข้องกับเทคโนโลยีเพื่อการป้องกันประเทศและเป็นการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้งานเพื่อระบบอาวุธอิสระ (Autonomous Weapons Systems) เป็นสำคัญ ในขณะที่การพัฒนาในระดับรองลงมาคือการใช้งานเทคโนโลยีไซเบอร์เพื่อการทหารโดยมีความพยายามในการนำเอาระบบ Big Data และการประมวลผลในระบบไซเบอร์ (Analytics) มาทำงานร่วมกับการใช้อาวุธและปฏิบัติการทางทหารมากขึ้น[211] นอกจากนั้นการเชื่อมต่อการทำงานของอุปกรณ์หลายชนิดกับระบบอาวุธไม่ว่าจะเป็นการเชื่อมต่อสัญญาณดาวเทียมของระบบกำหนดตำแหน่งบนพื้นโลกและการเชื่อมต่อการปฏิบัติการทางทหารเข้ากับระบบการใช้งานอินเตอร์เน็ตเพื่อให้การทำงานของระบบอาวุธมีความแม่นยำมากขึ้นและมีระยะการทำการที่ไกลขึ้น ล้วนแล้วแต่เป็นเป้าหมายสำคัญในการพัฒนาเทคโนโลยีทางการทหารในปัจจุบันเป็นอย่างมาก[212]

---

[208] United Nations, “Report of the 2023 session of the Group of the Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,” CCW/GGE.1/2023/2, 24 May 2023, Para 20.

[209] Ibid., para 21.

[210] Ibid., para 22.

[211] “Top 10 Military Technology Trends and Innovations for 2023,” StartUs insights, (2023) [online] accessed July 16, 2023. Available from: https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/

[212] Deeper Looks, “The Future of Battlefield,” in Global Trends, Office of the Director of National Intelligence, (April 2021) [online] accessed: July 16, 2023. Available from: https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield

แนวโน้มการพัฒนาทางด้านเทคโนโลยีเหล่านี้สะท้อนให้เห็นว่าบทบาทของหน่วยงานเอกชนจะมีมากขึ้นในการพัฒนาเทคโนโลยี ประเทศที่มีพัฒนาการด้านเทคโนโลยีปัญญาประดิษฐ์และเทคโนโลยีไซเบอร์มากกว่าอาจมีบทบาทมากขึ้นในการขัดกันทางอาวุธในอนาคต[213] นอกจากนั้นเทคโนโลยีที่เกี่ยวข้องกับการใช้งานร่วมกันของพลเรือนและทหารยังอาจทำให้พลเรือนเข้ามามีส่วนร่วมในการรบมากขึ้นรวมตลอดถึงความเสียหายที่จะเกิดขึ้นกับข้อมูลทางไซเบอร์ของพลเรือนย่อมมีมากขึ้นเช่นกัน

3) บทบาทของสหประชาชาติในการสร้างอนุสัญญาระหว่างประเทศเกี่ยวกับอาชญากรรมทางไซเบอร์

นอกจากบทบาทขององค์กรสนธิสัญญาเพื่อป้องกันแอตแลนติกเหนือ (NATO) ที่มีบทบาทในการสร้างแนวปฏิบัติเกี่ยวกับการใช้กฎหมายระหว่างประเทศกับปฏิบัติการทางไซเบอร์แล้วยังมีองค์การสหประชาชาติที่ให้ความสำคัญกับเรื่องเทคโนโลยีไซเบอร์โดยมุ่งเน้นไปที่การควบคุมอาชญากรรมทางไซเบอร์โดยมีความพยายามสร้างสนธิสัญญาระหว่างประเทศว่าด้วยอาชญากรรมทางไซเบอร์ ความพยายามดังกล่าวเกิดขึ้นในที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติในปี ค.ศ. 2019 โดยคำนึงถึงผลกระทบที่เกิดจากการโจมตีทางไซเบอร์ที่มีมากขึ้นในปัจจุบัน เดือนธันวาคม ค.ศ. 2019 สมัชชาใหญ่แห่งสหประชาชาติจึงมีมติที่ 74/247[214] ให้มีการจัดตั้งคณะกรรมการผู้เชี่ยวชาญเฉพาะกิจระหว่างรัฐบาลเพื่อทำการศึกษาแนวทางความเป็นไปได้ในการสร้างอนุสัญญาระหว่างประเทศว่าด้วยการต่อต้านการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อวัตถุประสงค์ในการก่ออาชญากรรม[215]

ปัจจุบันอนุสัญญาดังกล่าวยังอยู่ในรูปแบบของร่างอนุสัญญา ซึ่งมีเป้าหมายสำคัญในการสร้างความร่วมมือระหว่างรัฐเพื่อจัดการปัญหาอาชญากรรมทางไซเบอร์ การสร้างนิยามคำสำคัญทางไซเบอร์และสื่อสารสนเทศที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ การสร้างความรับผิดชอบของรัฐในการป้องกันและจัดการปัญหาอาชญากรรมทางไซเบอร์ แต่ข้อท้าทายที่เกิดขึ้นกับการสร้างสนธิสัญญาอาชญากรรมทางไซเบอร์ในปัจจุบันคือปัญหาเรื่องปัญหาผลกระทบต่อสิทธิมนุษยชนและการขัดกันแห่งกฎหมาย เนื่องจากผู้ที่มีบทบาทสำคัญในโลกไซเบอร์ในปัจจุบันคือบริษัทเอกชนผู้ให้บริการแฟลตฟอร์มออนไลน์เช่น google และ facebook ซึ่งแถลงว่ามีคำขอจากเจ้าหน้าที่รัฐบาลของหลาย

---

[213] “Top 10 Military Technology Trends and Innovations for 2023,” StartUs insights, (2023)

[214] United Nations General Assembly, Resolution on Countering the use of information and communications technologies for criminal purposes, A/RES/74/247, January 20, 2020.

[215] Ibid., (2).

ประเทศในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการสืบสวนสอบสวนคดีอาชญากรรม ซึ่งสร้างความลำบากใจแก่ผู้ให้บริการเอกชนเหล่านี้ว่าการกระทำดังกล่าวจะเป็นการละเมิดต่อสิทธิในข้อมูลส่วนบุคคลหรือไม่และในบางกรณีก็เกิดปัญหาเรื่องความแตกต่างของกฎหมายภายในของแต่ละประเทศที่มีมาตรฐานแตกต่างกัน[216]

สนธิสัญญาระหว่างประเทศเกี่ยวกับอาชญากรรมทางไซเบอร์นี้ไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศกล่าวคือไม่ใช่กฎเกณฑ์ที่เกี่ยวข้องกับการปฏิบัติต่อกันในฐานะคู่ความขัดแย้งในการสงคราม แต่สนธิสัญญาฉบับนี้มีความสัมพันธ์กับกฎหมายมนุษยธรรมระหว่างประเทศใน 2 ลักษณะ คือ ลักษณะที่ 1 เมื่อเกิดสถานการณ์การขัดกันทางอาวุธขึ้นอาจมีกรณีการกระทำความผิดทางไซเบอร์ที่อยู่ในขอบเขตของอาชญากรรมไซเบอร์แต่ไม่ใช่ความผิดตามกฎหมายมนุษยธรรมระหว่างประเทศ สนธิสัญญานี้จะสร้างพันธกรณีให้รัฐภาคีต้องออกกฎหมายภายในเพื่อรองรับต่อกรณีดังกล่าว การปฏิบัติการทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธจึงไม่ใช่เรื่องที่ทำได้ตามอำเภอใจของบุคคล ลักษณะที่ 2 การมีกฎหมายภายในที่ควบคุมพฤติกรรมทางไซเบอร์ของบุคคลจะช่วยเป็นการป้องกันหรือปรามไม่ให้มีการใช้วิธีการที่ผิดกฎหมายในสถานการณ์การขัดกันทางอาวุธ ซึ่งจะลดบทบาทการมีส่วนร่วมของพลเรือนในปฏิบัติการทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ยิ่งไปกว่านั้นลักษณะของสนธิสัญญาที่สร้างความร่วมมือระหว่างประเทศจะเป็นตัวประสานกฎหมายอาชญากรรมทางไซเบอร์ภายในประเทศต่างๆ ให้เป็นมาตรฐานเดียวกันซึ่งแม้จะไม่ก่อให้เกิดประโยชน์ต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศโดยตรง แต่ทางอ้อมก็อาจช่วยลดภาระข้อท้าทายที่เกิดจากการใช้งานระบบไซเบอร์ของพลเรือนในการขัดกันทางอาวุธที่จะส่งผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศ

2.4 ลักษณะของเทคโนโลยีใหม่ที่ใช้ในการขัดกันทางอาวุธในปัจจุบัน

ขอบเขตของเทคโนโลยีใหม่ในการศึกษาวิจัยนี้ประกอบด้วยเทคโนโลยีหลายประการที่ปรากฏในปัจจุบันและอาจรวมถึงเทคโนโลยีที่อาจมีการใช้งานในอนาคตด้วย โดยสาระสำคัญของเทคโนโลยี

---

[216] Jonathan Greig, “First draft of controversial UN Cyber Crime Treaty slate for June,” The Record, April 28, 2023. [accessed June 10, 2023] Available from: https://therecord.media/first-draft-of-un-cybercrime-treaty-expected-in-june

ใหม่มักมีพื้นฐานหลักร่วมกันบางประการคือเทคโนโลยีเหล่านี้มีการทำงานในระบบดิจิทัล[217]และเกี่ยวข้องกับการทำงานของคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมตลอดถึงการสั่งการด้วยระบบคอมพิวเตอร์เชื่อมต่อกับอุปกรณ์หลายชนิดทำให้เกิดลักษณะร่วมกันบางประการของเทคโนโลยีเหล่านี้ที่จะนำไปสู่การวิเคราะห์ปัญหาและข้อท้าทายที่จะเกิดขึ้นจากการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศ คุณสมบัติเฉพาะของเทคโนโลยีใหม่ทั้งหลายที่มีลักษณะร่วมกัน ได้แก่

2.4.1 เทคโนโลยีใหม่มีลักษณะการใช้งานร่วมกันระหว่างทหารและพลเรือน

จากลักษณะการใช้งานเทคโนโลยีในปัจจุบันที่มีพื้นฐานอยู่บนระบบการทำงานแบบดิจิทัล[218] ทำให้คอมพิวเตอร์และระบบการที่เกี่ยวข้องกับคอมพิวเตอร์มีบทบาทต่อการใช้งานเทคโนโลยีใหม่เป็นอย่างมาก โดยเฉพาะอย่างยิ่งการสื่อสารและการทำงานระหว่างเครือข่ายคอมพิวเตอร์ซึ่งปรากฏการใช้งานเทคโนโลยีที่เกี่ยวข้องกับคอมพิวเตอร์ในหลายรูปแบบ เช่น การใช้งานระบบไซเบอร์ การใช้งานอินเทอร์เน็ต รวมตลอดถึงการใช้งานปัญญาประดิษฐ์ ฯลฯ และเทคโนโลยีประการแรกที่ส่งผลต่อการเปลี่ยนแปลงวิถีชีวิตของผู้คนอย่างมีนัยสำคัญในยุคปัจจุบันคือเทคโนโลยีสารสนเทศและการทำงานของระบบไซเบอร์

การใช้งานเทคโนโลยีสารสนเทศและการใช้งานระบบไซเบอร์ปรากฏทั้งการใช้งานของพลเรือนและการใช้งานทางการทหาร โดยการใช้งานของทั้งกลุ่มพลเรือนและทหารนี้จะมีลักษณะคล้ายกันคือทั้งการใช้งานแพลตฟอร์มเดียวกัน เช่น ระบบอินเทอร์เน็ตที่ใช้ร่วมกันระหว่างทหารและพลเรือน โปรแกรมคอมพิวเตอร์ที่พัฒนาบนพื้นฐานเดียวกัน ทรัพยากรทางคอมพิวเตอร์และทรัพยากรทางดิจิทัลที่อาจมีส่วนร่วมกัน ฯลฯ แต่เป้าหมายหลักในการใช้งานแตกต่างกันในแต่ละกลุ่ม โดยพลเรือนใช้เทคโนโลยีไซเบอร์ในรูปแบบของเทคโนโลยีสารสนเทศเพื่อการติดต่อสื่อสารเป็นหลัก ในขณะที่การใช้งานทางการทหารเพื่อการขัดกันทางอาวุธอาจปรากฏทั้งการใช้งานในรูปแบบของเทคโนโลยีสารสนเทศและการปฏิบัติการทางไซเบอร์เพื่อการโจมตี ทั้งนี้มิได้หมายความว่าพลเรือนไม่มีการใช้การปฏิบัติการทางไซเบอร์เพื่อการโจมตีเพียงแต่การโจมตีทางไซเบอร์โดยพลเรือนมักจะเกิดขึ้นในกรณีเฉพาะที่เป็นการประสงค์ร้าย การใช้งานระบบไซเบอร์จึงสร้างลักษณะร่วมกันของทหารและพลเรือนดังต่อไปนี้

---

[217] Jonathan Greig, “First draft of controversial UN Cyber Crime Treaty slate for June,”

[218] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, p. 26.

2.4.1.1 เทคโนโลยีสารสนเทศกับปฏิบัติการโจมตีทางไซเบอร์

ระบบ “ไซเบอร์” มีความหมายค่อนข้างหลากหลายในเชิงทฤษฎีทางวิชาการ[219] ในความหมายทั่วไป หมายถึง “ลักษณะการทำงานรวมตลอดถึงสิ่งที่เกี่ยวข้องกับการทำงานของคอมพิวเตอร์ เทคโนโลยีสารสนเทศ และโลกเสมือน”[220] และนิยามหนึ่งที่มีการยอมรับคือ “การควบคุมหรือการเชื่อมต่อการสื่อสารระหว่างคนหรือสัตว์กับเครื่องจักรกล”[221] อาจกล่าวได้ว่าไซเบอร์มีความหมายกว้างขวางคือการรวมเอาการทำงานของคอมพิวเตอร์ เครื่องจักรกล โปรแกรมหรือคำสั่งทางคอมพิวเตอร์ การติดต่อสื่อสาร การควบคุมอุปกรณ์ที่เกี่ยวข้องกับระบบ ฯลฯ ซึ่งอาจมีทั้งส่วนที่เป็นองค์ประกอบทางกายภาพที่เป็นมนุษย์ สัตว์ หรืออุปกรณ์เกี่ยวกับคอมพิวเตอร์และเครื่องจักร ในขณะที่อีกส่วนหนึ่งเกี่ยวข้องกับองค์ประกอบที่ไม่มีสาถานะทางกายภาพ เช่น ข้อมูลสารสนเทศ คำสั่งในระบบดิจิทัลและโปรแกรมคอมพิวเตอร์ รวมถึงการทำงานของคอมพิวเตอร์ที่อยู่ในรูปแบบของสัญญาณดิจิทัล ฯลฯ

ในคู่มือทาลลินน์ว่าด้วยกฎหมายระหว่างประเทศซึ่งปรับใช้กับปฏิบัติการสงครามทางไซเบอร์ มีการให้นิยามคำสำคัญบางคำที่เกี่ยวข้องกับปฏิบัติการทางไซเบอร์ว่า ไซเบอร์ (Cyber) หมายถึง สิ่งที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ปฏิบัติการทางไซเบอร์ (Cyber Operations) จึงหมายถึง การใช้ความสามารถทางไซเบอร์เพื่อวัตถุประสงค์ในการบรรลุภารกิจบางประการในพื้นที่ทางไซเบอร์ หรือโดยการใช้พื้นที่ทางไซเบอร์[222]

ขณะที่คู่มือทาลลินน์ให้นิยามคำว่าระบบไซเบอร์ (Cyber System) หมายถึง การเชื่อมต่อระหว่างคอมพิวเตอร์หนึ่งหรือหลายเครื่องร่วมกับซอฟท์แวร์หรืออุปกรณ์ต่อพ่วง โดยรวมถึงการทำงานร่วมกับระบบเซ็นเซอร์หรือโปรแกรมควบคุม การควบคุมเครือข่ายคอมพิวเตอร์อื่นๆ โดยระบบคอมพิวเตอร์เช่นว่ารวมถึงการใช้งานคอมพิวเตอร์เพื่อวัตถุประสงค์ทั่วไปและการใช้งานเพื่อวัตถุประสงค์เฉพาะ[223]

---

[219] Heinz von Foerster, Ethics and second-order cybernetics, in Understanding: Essays on cybernetics and cognition. (New York: Springer-Verlag, 2003), p. 288.

[220] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/cyber, accessed June 15, 2021.

[221] Norbert Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine, (Cambridge: MIT Press, 1948), preface, p. vii-viii.

[222] Michael Schmitt (eds.), Tallinn Manual on The International Law Applicable to Cyber Warfare, p. 211.

[223] Ibid.

นอกจากนั้นในคู่มือทาลลลินน์ยังนิยามคำว่า “สาธารณูปโภคหรือโครงสร้างพื้นฐานทางไซเบอร์ (Cyber infrastructure) หมายถึง ทรัพยากรเกี่ยวกับการสื่อสาร การจัดเก็บข้อมูล และการประมวลผลซึ่งกระทำในระบบสารสนเทศ” “พื้นที่ทางไซเบอร์ (Cyberspace) สภาพแวดล้อมทั้งทางกายภาพและที่ไม่ใช่ทางกายภาพซึ่งประกอบร่วมกันเป็นลักษณะการใช้งานคอมพิวเตอร์ การใช้งานคลื่นแม่เหล็กไฟฟ้า การจัดเก็บข้อมูล การดัดแปลงข้อมูลและการแลกเปลี่ยนข้อมูลระหว่างเครือข่ายคอมพิวเตอร์”[224]

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ของไทยนิยามคำว่า “ไซเบอร์” ในมาตรา 3 ว่าหมายถึง “ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป”[225]

เมื่อพิจารณาจากนิยามที่ปรากฏในแหล่งต่างๆ อาจสรุปความหมายของ “ไซเบอร์” ได้ว่าหมายถึงระบบการทำงานที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งทางกายภาพของอุปกรณ์ต่างๆ ซึ่งก่อให้เกิดระบบการทำงานที่ไม่ใช่ทางกายภาพ เช่น การส่งสัญญาณไฟฟ้า การส่งสัญญาณคลื่นความถี่หรือประการอื่นใดเพื่อให้เกิดการเชื่อมต่อข้อมูลการสื่อสารระหว่างอุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์หรือระบบการทำงานของคอมพิวเตอร์

การทำงานของไซเบอร์ในลักษณะที่เป็นการเชื่อมต่อการสื่อสารดังกล่าวจึงอาศัยองค์ประกอบหลายประการตั้งแต่

1) เครื่องมือที่เกี่ยวข้องกับการสื่อสารเพื่อการรับ-ส่งข้อมูล เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ แทปเล็ต รวมตลอดถึงอุปกรณ์อื่นๆ ที่สามารถทำงานเชื่อมต่อกับระบบอินเทอร์เน็ตได้[226]ลักษณะดังกล่าวนี้การทำงานของระบบไซเบอร์จึงมีส่วนเกี่ยวข้องกับอุปกรณ์ที่เป็นวัตถุทางกายภาพ

---

[224] Michael Schmitt (eds.), Tallinn Manual on The International Law Applicable to Cyber Warfare, p. 211.

[225] มาตรา 3, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562, ราชกิจจานุเบกษา, เล่ม 136, ตอนที่ 69 ก, หน้า 20, 27 พฤษภาคม 2562.

[226] Serkan Savas and Suleyman Karatas, “Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance,” International Cybersecurity Law Review, Vol. 3, (2022): 9-11.

2) เครื่องมือที่ใช้เชื่อมต่อการทำงานของคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์ เช่น อินเทอร์เน็ตหรือระบบการสื่อสารในเครือข่าย www และแอปพลิเคชั่นการใช้งานเครือข่ายคอมพิวเตอร์ในรูปแบบต่างๆ ซึ่งต้องอาศัยระบบการสื่อสารพื้นฐานเช่น เครือข่ายสัญญาณโทรศัพท์ไม่ว่าจะผ่านสายนำสัญญาณ หรือคลื่นความถี่โทรศัพท์เคลื่อนที่ รวมถึงการสื่อสารผ่านสัญญาณดาวเทียม และระบบกำหนดตำแหน่งบนพื้นโลก (GPS) เพื่อให้การเชื่อมต่อการทำงานของคอมพิวเตอร์เกิดขึ้นได้อย่างสมบูรณ์[227] ลักษณะการทำงานประการดังกล่าวนี้เป็นการเชื่อมต่อการทำงานของอุปกรณ์ที่เป็นวัตถุทางกายภาพกับสัญญาณที่มีการส่งผ่านซึ่งไม่มีสถานะทางกายภาพ

3) ข้อมูลที่มีการส่งผ่านระบบหรือข้อมูลที่ส่งผ่านเครือข่ายไม่ว่าจะเป็นถ้อยคำ ภาษา เอกสาร รูปภาพ คำสั่ง ชุดคำสั่ง (โปรแกรม) ฯลฯ จะอยู่ในลักษณะของสัญญาณแม่เหล็กไฟฟ้า (Electro Magnetic) หรือสัญญาณไฟฟ้า ทั้งผ่านสายที่ทำหน้าที่ส่งข้อมูลและที่ส่งผ่านระบบไร้สาย[228] แต่ไม่ว่าจะส่งผ่านระบบใดก็แล้วแต่ข้อมูลดังกล่าวจะมีการเปลี่ยนรูปแบบไปตามอุปกรณ์ที่ข้อมูลนั้นเดินทางออกจาก ระหว่าง หรือถึงเป้าหมาย เช่น ขณะส่งข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งข้อมูลหรือคำสั่งใดๆ จะถูกสั่งการผ่านคีย์บอร์ดซึ่งส่งสัญญาณไฟฟ้าไปที่หน่วยประมวลผลก่อนปรากฏเป็นตัวอักษรที่หน้าจอแสดงผล ขณะที่เมื่อมีการส่งข้อมูลดังกล่าวออกจากคอมพิวเตอร์หรืออุปกรณ์อื่นที่ใช้ส่งข้อมูล ข้อมูลจะเปลี่ยนแปลงเป็นสัญญาณไฟฟ้าเพื่อเดินทางผ่านสายสัญญาณหรือเปลี่ยนแปลงเป็นสัญญาณแม่เหล็กไฟฟ้าก่อนเดินทางผ่านอากาศเข้าสู่ระบบอินเทอร์เน็ตและเดินทางไปสู่เครื่องรับปลายทางก่อนแปลงสัญญาณแม่เหล็กไฟฟ้าหรือสัญญาณไฟฟ้าให้เป็นข้อมูลแสดงที่เครื่องรับปลายทางหรือเป็นคำสั่งให้เครื่องรับปลายทางทำงาน

ลักษณะของข้อมูลที่ส่งผ่านคลื่นแม่เหล็กไฟฟ้าหรือคลื่นไฟฟ้าแล้วแต่กรณีนี้ เราไม่สามารถระบุได้ว่า ณ ช่วงเวลาใดคลื่นดังกล่าวอยู่ที่ใด อยู่ในสถานะใด แต่โดยภาพรวมข้อมูลก่อนการแสดงผล (แม้กระทั่งขณะแสดงผล) ไม่มีสถานะทางกายภาพใดๆ เป็นเพียงสัญญาณคลื่นไฟฟ้าเท่านั้น พื้นที่การเดินทางของข้อมูลและตัวข้อมูลจึงไม่มีตัวตนทางกายภาพ แต่สามารถทำงานได้จริงในทางปฏิบัติ พื้นที่ของการส่งข้อมูลหรือการปฏิบัติการทางไซเบอร์จึงถูกเรียกว่า “โลกเสมือน” (Virtual reality) เพราะการทำงานของระบบไซเบอร์ทั้งหมดอยู่ในพื้นที่ของสัญญาณคลื่นไฟฟ้าแต่สามารถ

---

[227] Serkan Savas and Suleyman Karatas, “Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance,”: 9-11.

[228] Ibid.

ทำงานได้เสมือนการกระทำทางกายภาพและบางกรณีการส่งสัญญาณทางคลื่นไฟฟ้านี้ยังทำให้เกิดผลทางกายภาพได้

(1) ลักษณะการทำงานของไซเบอร์

การทำงานของไซเบอร์ขั้นพื้นฐานมักเกี่ยวข้องกับอุปกรณ์ที่สามารถรับ-ส่งข้อมูลไฟฟ้าและคลื่นแม่เหล็กไฟฟ้าได้ โดยอุปกรณ์พื้นฐานในปัจจุบันที่เกี่ยวข้องกับระบบไซเบอร์มากที่สุดคือคอมพิวเตอร์ เป็นที่ทราบกันดีว่าคำว่า “คอมพิวเตอร์” หรือ “Computer” ในภาษาอังกฤษนั้นหมายถึงเครื่องคำนวณ แต่เป็นการคำนวณ (Compute) ในลักษณะที่ซับซ้อนและหลากหลายกว่าการคำนวณตัวเลข (calculate) โดยอุปกรณ์ที่เป็นที่ยอมรับว่าทำงานได้ใกล้เคียงกับเครื่องคอมพิวเตอร์ในปัจจุบันคือเครื่องมือถอดรหัส Enigma[229] ในยุคสงครามโลกครั้งที่ 2 โดยเครื่องถอดรหัส Enigma นี้ความสามารถในการคำนวณและแปลงข้อมูลที่กองทัพเยอรมันสื่อสารผ่านเครื่อง Enigma เครื่อง Enigma นี้มีรูปร่างเหมือนเครื่องพิมพ์ดีดทำหน้าที่ส่งข้อความที่มีพิมพ์โดยมนุษย์จากเครื่องส่งและทำการส่งข้อมูลดังกล่าวผ่านสัญญาณไฟฟ้าไปยังเครื่องรับ กลไกสำคัญของเครื่อง Enigma คือแกนหมุนในเครื่อง 3 แกน ทำหน้าที่ในการเปลี่ยนข้อมูลที่ส่งจากเครื่องส่งให้ไม่ตรงตามข้อความที่กดก่อนส่งไปเครื่องรับ การทำงานดังกล่าวเรียกว่าการเข้ารหัส (Encryption) การสื่อสารของเครื่องส่งและเครื่องรับเพื่อให้ได้ข้อมูลที่ตรงกันจึงต้องหมุนแกนทั้งสามให้อยู่ในรูปแบบเดียวกันก่อนที่จะมีการส่งและการรับข้อมูล[230]

กองทัพอังกฤษสามารถเข้าถึงข้อมูลรับ-ส่งของกองทัพเยอรมันได้ แต่ปัญหาคือกองทัพอังกฤษไม่สามารถรู้ได้ว่าข้อมูลดังกล่าวมีความหมายอย่างไรเนื่องจากเป็นข้อมูลเข้ารหัสไว้ จึงต้องใช้การคำนวณทางคณิตศาสตร์และนักคณิตศาสตร์คำนวณความเป็นไปได้ของความหมายข้อความที่เข้ารหัสดังกล่าว แต่การคำนวณด้วยมนุษย์ต้องใช้เวลามาก จึงนำไปสู่การสร้างเครื่องคำนวณซึ่งสามารถทำงานได้เร็วกว่ามนุษย์หลายเท่า ทำให้ฝ่ายสัมพันธมิตรเข้าถึงข้อมูลที่ฝ่ายเยอรมันส่งถึงกันในปฏิบัติการสงครามและนำไปสู่ชัยชนะของฝ่ายสัมพันธมิตรในท้ายที่สุด

แม้เครื่องคำนวณจะดูเหมือนเป็นจุดเริ่มต้นของคอมพิวเตอร์ แต่สิ่งที่สามารถคำนวณบางอย่างก็ไม่เรียกว่าคอมพิวเตอร์ เช่น เครื่องคิดเลข หรือลูกคิด ด้วยเหตุที่เครื่องคิดเลขแม้จะใช้ใน

---

[229] Joanne Baker, “Forgotten Heroes of the Enigma Story,” Nature, September 3, 2018, [online] Accessed October 10, 2020. Available from: https://www.nature.com/articles /d41586-018-06149-y

[230] Ibid.

การคำนวณได้ แต่ต้องอาศัยมนุษย์ผู้ใช้งานทำหน้าที่ค่อนข้างมาก (การกดหมายเลขเพื่อการคำนวณ) โดยเครื่องคิดเลขไม่ได้ทำหน้าที่ประมวลผลด้วยตัวเอง อาจเปรียบได้ว่าเครื่องคิดเลขเป็นเพียงกระดาษทดอิเล็กทรอนิกส์เท่านั้น (กระดาษทดที่อาศัยการบันทึกข้อมูลในกระแสไฟฟ้าและหน่วยความจำ) ขณะที่ลูกคิดนั้นไม่มีสถานะเป็นเครื่อง (Machine) เพราะมนุษย์ต้องทำงานแทบตลอดทั้งการคำนวณ แต่ลูกคิดเป็นเพียงเครื่องแสดงสัญลักษณ์เพื่อการจำเท่านั้น

สาเหตุที่ต้องเปรียบเทียบการทำงานของเครื่องคำนวณในลักษณะคอมพิวเตอร์กับเครื่องคำนวณในลักษณะอื่นๆ เนื่องจากลักษณะการในระบบไซเบอร์มีความเกี่ยวข้องกับระบบการคำนวณแบบคอมพิวเตอร์และการทำงานของระบบกระแสไฟฟ้า รวมถึงอุปกรณ์เพื่อการใช้งานและบันทึกข้อมูลในรูปแบบกระแสไฟฟ้า (electronics) แต่การทำงานของสิ่งที่จะเป็นระบบไซเบอร์ในความเข้าใจทางวิทยาศาสตร์คอมพิวเตอร์จะต้องนำเอาการทำงานของระบบกระแสไฟฟ้าในอุปกรณ์ลักษณะคอมพิวเตอร์ไปผนวกเข้ากับการทำงานของอุปกรณ์อื่นด้วย เช่น การใช้งานคอมพิวเตอร์เครื่องเดียวเพื่อการประมวลผล (เช่นที่เคยใช้งานเครื่อง Enigma) ก็ไม่มีลักษณะการทำงานเชื่อมต่อกับอุปกรณ์อื่นจึงไม่เป็นการทำงานในระบบไซเบอร์ เครื่องคิดเลขทั่วไปจึงอาจไม่อยู่ในลักษณะอุปกรณ์ที่จะเรียกว่าเป็นระบบไซเบอร์ ขณะที่คอมพิวเตอร์ที่ทำงานเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น คอมพิวเตอร์ที่สั่งงานเครื่องจักรกล คอมพิวเตอร์ที่ทำหน้าที่บันทึกคำสั่งลงในสิ่งบันทึกข้อมูลอื่นก่อนจะนำสิ่งบันทึกข้อมูลนั้นไปใช้กับอุปกรณ์เพื่อการทำงานตามคำสั่งต่อไป ทั้งนี้รวมถึงการใช้งานคอมพิวเตอร์เพื่อการส่งชุดคำสั่ง (โปรแกรม) เข้าไปในระบบคลื่นไฟฟ้าที่เชื่อมโยงกับการทำงานของเครือข่ายอุปกรณ์ที่เกี่ยวข้องด้วย

การทำงานของระบบไซเบอร์จึงมีลักษณะสำคัญที่เกี่ยวข้องกับการทำงานของ “อุปกรณ์” เพื่อส่ง “ข้อมูล” ผ่านระบบ “ไฟฟ้า” หรือ “คลื่นแม่เหล็กไฟฟ้า” ให้เกิดการทำงานของอุปกรณ์อื่นต่อไป ซึ่งเมื่อพิจารณาจากลักษณะสำคัญนี้จะทำให้เราจำแนกได้ว่า ลูกคิดแม้คำนวณได้แต่ก็ไม่เกี่ยวข้องกับระบบไซเบอร์ เครื่องคิดเลขคำนวณได้แสดงข้อมูลได้ แต่จะเกี่ยวข้องกับระบบไซเบอร์หรือไม่ต้องพิจารณาสาระสำคัญของการทำงานของเครื่องคิดเลขเครื่องนั้นว่ามีลักษณะการทำงานในลักษณะการเชื่อมต่อข้อมูลหรือไม่ ในขณะที่การทำงานของคอมพิวเตอร์ในปัจจุบันมีลักษณะการทำงานในระบบไซเบอร์ค่อนข้างมาก เพราะมักเป็นการทำงานเชื่อมต่อกับเครือข่าย และมีการรับ-ส่งข้อมูลผ่านเครือข่ายระหว่างคอมพิวเตอร์ (Internet) เป็นสำคัญ นอกจากนี้ยังมีอุปกรณ์ต่อพ่วงและเกี่ยวข้องกับการทำงานของคอมพิวเตอร์อีกมากมายที่มีลักษณะการทำงานในระบบไซเบอร์

(2) การใช้งานระบบไซเบอร์ของพลเรือน

การใช้งานระบบไซเบอร์ของพลเรือนเริ่มต้นตั้งแต่ยุคที่คอมพิวเตอร์ถูกนำมาใช้งาน โดยเฉพาะอย่างยิ่งเมื่อการติดต่อสื่อสารผ่านช่องทางอินเทอร์เน็ตถูกนำมาใช้เป็นสื่อกลางในการติดต่อ ทำให้การใช้งานคอมพิวเตอร์เป็นเครื่องมือในการติดต่อสื่อสารมาจนถึงยุคปัจจุบัน[231] การใช้งานคอมพิวเตอร์เพื่อการสื่อสารในยุคแรกเป็นไปเพียงเพื่อการเข้าถึงข้อมูล ส่งต่อข้อมูล และการทำงานที่เกี่ยวข้องกับการสั่งการระบบปฏิบัติการของคอมพิวเตอร์ แต่ด้วยความนิยมในการวิจัยและพัฒนาของนักวิทยาศาสตร์คอมพิวเตอร์ทำให้มีความพยายามในการขยายขีดความสามารถในการทำงานของคอมพิวเตอร์ให้มีลักษณะและรูปแบบที่หลากหลายมากขึ้น ทำให้จากเดิมที่เครื่องคอมพิวเตอร์อาจทำงานได้เพียงหน้าที่ของพิมพ์ดีดเปลี่ยนมาเป็นการทำงานในลักษณะของโทรศัพท์ เครื่องเล่นวิดีโอ กล้องถ่ายรูป เครื่องส่งจดหมาย ฯลฯ ได้

นอกจากการทำงานของคอมพิวเตอร์ที่หลากหลายมากขึ้นแล้ว รูปแบบการเชื่อมต่อการทำงานของคอมพิวเตอร์ในปัจจุบันยังก้าวหน้าไปในระดับไร้ข้อจำกัด เช่น การเชื่อมต่อคอมพิวเตอร์กับกล้องถ่ายรูป การเชื่อมต่อคอมพิวเตอร์กับกล้องวงจรปิด การเชื่อมต่อคอมพิวเตอร์กับโทรศัพท์เคลื่อนที่ การเชื่อมต่อคอมพิวเตอร์กับเครื่องจักรโรงงานอุตสาหกรรม การเชื่อมต่อคอมพิวเตอร์กับรถยนต์ ฯลฯ

การเปลี่ยนแปลงรูปแบบคอมพิวเตอร์ก็เปลี่ยนแปลงไปหลากหลาย ด้วยลักษณะการทำงานขั้นพื้นฐานของคอมพิวเตอร์ที่ประกอบด้วยระบบบันทึกข้อมูล ระบบจัดเก็บข้อมูล ระบบประมวลผลข้อมูล ระบบการแสดงผลข้อมูล และระบบการเชื่อมต่ออุปกรณ์อื่น ทำให้จากเดิมอุปกรณ์ที่เรียกว่าคอมพิวเตอร์หมายถึงสิ่งที่มีแป้นพิมพ์ มีจอแสดงผลและมีหน่วยประมวลผลข้อมูลซึ่งต้องตั้งทำงานกับโต๊ะ เปลี่ยนมาเป็นอุปกรณ์ที่ขนาดเล็กลงแต่สามารถทำงานได้แบบเดียวกับคอมพิวเตอร์รูปแบบเช่นว่า ได้แก่ เครื่องแทปเล็ต และโทรศัพท์เคลื่อนที่ เป็นต้น

ขณะที่อุปกรณ์เชื่อมต่อการทำงานของคอมพิวเตอร์ในรูปแบบอื่นหลายชนิดก็มักจะมีการทำงานของหน่วยประมวลผลทางอิเล็กทรอนิกส์ แต่ไม่ได้ทำหน้าที่สมบูรณ์เช่นอุปกรณ์ในรูปแบบคอมพิวเตอร์ เช่น กล้องวงจรปิดมีระบบประมวลผล ระบบจัดเก็บข้อมูลและระบบรับ-ส่งข้อมูล แต่ไม่

---

[231] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

มีระบบแสดงผล รถยนต์อัจฉริยะมีระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบการรับ-ส่งข้อมูล และระบบแสดงผล แต่ไม่ได้ทำหน้าที่หลากหลายแบบเดียวกับเครื่องคอมพิวเตอร์ แทปเล็ต และโทรศัพท์เคลื่อนที่ เป็นต้น ลักษณะการทำงานรูปแบบไซเบอร์ในอุปกรณ์ที่กล่าวมานี้ จะมีความเกี่ยวข้องกับการปฏิบัติการทางไซเบอร์ซึ่งอาจนำไปสู่การปฏิบัติภารกิจการจารกรรมและการโจมตีทางไซเบอร์ได้

(3) การใช้งานปฏิบัติการทางไซเบอร์เพื่อวัตถุประสงค์ร้าย

การใช้ปฏิบัติทางไซเบอร์เพื่อวัตถุประสงค์ร้ายนั้นพัฒนามาจากแนวคิดในการสร้างโปรแกรมเพื่อกู้คืนข้อมูลคอมพิวเตอร์ในช่วง ค.ศ.1990 การใช้งานระบบไซเบอร์ในลักษณะดังกล่าวเป็นที่รู้จักอย่างกว้างขวางในปี ค.ศ.2017 ในรูปแบบของโปรแกรมเรียกค่าไถ่ (Ransomware) ที่ชื่อว่า WannaCry[232] การเตรียมการใช้ระบบไซเบอร์เพื่อปฏิบัติการทางทหารนั้นเกิดขึ้นในปฏิบัติต่อต้านการโจมตีทางอากาศโดยองค์กรป้องกันแอตแลนติกเหนือที่ประเทศเซอร์เบียในทศวรรษ ค.ศ.2000 แต่ก็มีการล้มเลิกไปเนื่องจากคาดว่าอาจส่งผลกระทบต่อพลเรือน โดยการปฏิบัติการทางไซเบอร์ทางทหารปรากฏขึ้นจริงในปี ค.ศ.2007 จากการที่กองกำลังอิสราเอลใช้การโจมตีทางไซเบอร์เพื่อขัดขวางระบบป้องกันภัยทางอากาศของประเทศซีเรียและเป็นการสนับสนุนให้ปฏิบัติการโจมตีทางอากาศของกองทัพอิสราเอลสามารถกระทำได้สะดวกขึ้น[233] ในการใช้งานระบบไซเบอร์ของพลเรือนอาจเป็นไปทั้งเพื่อประโยชน์ในการสื่อสารและการสันทนาการ แต่ในทำนองกลับกันการใช้งานระบบไซเบอร์ก็อาจเป็นไปเพื่อวัตถุประสงค์ร้ายในการสร้างความเสียหายต่อบุคคลอื่นได้และการใช้งานระบบไซเบอร์ในลักษณะการก่อความเสียหายนี้จะเป็นลักษณะเดียวกับการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีทางทหาร

การใช้งานมัลแวร์คอมพิวเตอร์เพื่อวัตถุประสงค์ร้ายเริ่มตั้งแต่ยุคเริ่มต้นการใช้คอมพิวเตอร์จนถึงปัจจุบันโดยเป็นความพยายามในการพิสูจน์ให้เห็นว่าชุดคำสั่งหรือโปรแกรมทางคอมพิวเตอร์นั้นมีพฤติกรรมที่คล้ายสิ่งมีชีวิตได้คือการผลิตตัวเองขึ้นมาใหม่หรือการทำซ้ำตัวเอง การ

---

[232] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

[233] Ibid.

เคลื่อนที่ผ่านพื้นที่ทางไซเบอร์ได้ด้วยตัวเองเป็นต้น พัฒนาการดังกล่าวถูกเปลี่ยนวัตถุประสงค์การใช้งานจากการเลียนแบบสิ่งมีชีวิตให้เป็นโปรแกรมประสงค์ร้ายหรือมัลแวร์

มัลแวร์ (Malware) เป็นคำที่เกิดขึ้นในช่วงปี ค.ศ.2000 เนื่องจากมีการสร้างโปรแกรมประสงค์ร้ายมากขึ้น นักวิทยาศาสตร์คอมพิวเตอร์จึงใช้คำเรียกโปรแกรมประสงค์ร้ายใหม่ไปใช้คำว่า “Malware” หรือ malicious software ซึ่งรวมโปรแกรมทุกอย่างที่อาจส่งผลเสียหายต่อการใช้งานคอมพิวเตอร์ให้เป็น malware อันประกอบด้วย ไวรัส (virus) หนอน (worm) สปายแวร์ (spyware) ดปรแกรมเรียกค่าไถ่ (ransomware) โทรจัน (trojan) ฯลฯ ลักษณะการทำงานของ Malware แต่ละชนิดมีความแตกต่างกันดังต่อไปนี้[234]

1. ไวรัสคอมพิวเตอร์เป็นโปรแกรมคอมพิวเตอร์ที่สามารถทำซ้ำตัวเองได้แบบเดียวกับที่สิ่งมีชีวิตสามารถขยายพันธุ์ได้ นอกจากนั้นผลที่เกิดขึ้นจากการที่คอมพิวเตอร์ติดไวรัสยังคล้ายกับลักษณะที่มนุษย์ติดเชื้อไวรัส[235] กล่าวคือเมื่อคอมพิวเตอร์ติดเชื้อไวรัส อุปกรณ์คอมพิวเตอร์อาจร้อนขึ้น ทำงานได้ช้าลง หน่วยความจำเต็ม เกิดการส่งข้อมูลไปยังที่ต่างๆ โดยที่ไม่มีการสั่งการจากมนุษย์ ข้อมูลในเครื่องคอมพิวเตอร์หาย มีการย้ายข้อมูลหรือทำซ้ำข้อมูลไปยังอุปกรณ์อื่น จนถึงการทำให้เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ นอกจากนั้นไวรัสยังสามารถขยายพันธุ์ไปตามช่องทางต่างๆ ในเครือข่ายคอมพิวเตอร์ได้

ไวรัสคอมพิวเตอร์เป็นแนวคิดที่เกิดภายหลังจากการผลิตเครื่อง ENIAC ในปี ค.ศ. 1946 โดยเริ่มต้นในปี ค.ศ.1949 John Von Neumann นักคณิตศาสตร์ชาวอเมริกันได้เสนอทฤษฎี Theory of Self-Reproducing Automata[236] ซึ่งอธิบายว่าโปรแกรมคอมพิวเตอร์สามารถทำซ้ำตัวเองได้ แต่ในระยะแรกนั้นทฤษฎีของ Neumann ยังไม่ได้มีการสร้างโปรแกรมคอมพิวเตอร์ที่สามารถทำซ้ำตัวเองได้จริง จนกระทั่งปี ค.ศ.1966 บทความของ Neumann ได้รับการตีพิมพ์ และ Bob Thomas นักเขียนโปรแกรมคอมพิวเตอร์ชาวอเมริกัน ได้นำทฤษฎีของ Neumann มาสร้าง

---

[234] Elizabeth Piper, “Cyber Attack Hits 200,000 in at Least 150 Countries: Europol.” Reuters, May 14, 2017, [online] accessed February 16, 2022. Available from: https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX,

[235] John Von Neumann, Theory of Self-Reproducing Automata, (Urbana and London: University of Illinois Press, 1966), p. 76.

[236] Ibid.

โปรแกรมชื่อ Creeper สำเร็จในปี ค.ศ.1971[237] Creeper สร้างขึ้นมาเพื่อจำลองการทำซ้ำของโปรแกรมคอมพิวเตอร์ และเพื่อทำให้คนอื่นๆ ได้ทราบความสำเร็จของงานทดลอง เขาจึงเขียนประโยคว่า “I’m the creeper, catch me if you can.” ติดไปในโปรแกรมให้มีการแสดงข้อความนี้ที่คอมพิวเตอร์เป้าหมายหากโปรแกรมมีการทำซ้ำเกิดขึ้นที่คอมพิวเตอร์เครื่องใด นอกจากนั้นเขายังปล่อย Creeper เข้าไปในคอมพิวเตอร์เมนเฟรม DECPDP-10 ซึ่งปฏิบัติการบนระบบ Tenex เพื่อแสดงให้เห็นว่าไม่ว่า Creeper จะอยู่ในอุปกรณ์ใดที่มีลักษณะการทำงานแบบเดียวกับคอมพิวเตอร์ Creeper ก็สามารถทำซ้ำตัวเองได้เสมอ

การเกิดขึ้นของไวรัสนำไปสู่การพัฒนาโปรแกรมต่อต้านไวรัส (Anti-virus) ในช่วงเวลาเดียวกัน โดยผู้คิดค้นโปรแกรมต่อต้านไวรัสคือ Raymond Tomlinson นักเขียนโปรแกรมคอมพิวเตอร์ชาวอเมริกัน Tomlinson พบไวรัส Creeper บนคอมพิวเตอร์เมนเฟรม เขาจึงสร้างโปรแกรม Reverse Creeper ขึ้นมา โดยตั้งชื่อว่า Reaper ซึ่ง Reaper จะทำหน้าที่ค้นหา Creeper ที่ถูกทำซ้ำขึ้นทุกตัวรวมถึงตัวต้นฉบับด้วยแล้วทำการลบ Creeper ทั้งหมดทิ้งไป[238]

การคิดค้นไวรัสเกิดขึ้นเพราะเริ่มมีการพัฒนาระบบอินเทอร์เน็ตเพื่อการใช้งาน โดยการพัฒนาอินเทอร์เน็ตในช่วงแรกเกิดขึ้นจากโครงการ ARPANET (Advance Research Projects Agency Network) ของกระทรวงกลาโหมสหรัฐอเมริกา โดยโครงการ ARPANET ให้การสนับสนุนให้หน่วยงานการศึกษาในประเทศสหรัฐอเมริกาทำการวิจัยและทดลองการส่งข้อมูลผ่านระบบ Protocol ของคอมพิวเตอร์ เมื่อมีระบบการทำงานแบบเชื่อมต่อเครือข่ายคอมพิวเตอร์ได้จึงมีคนพยายามนำ Creeper เข้าสู่ระบบ ARPANET และ Creeper สามารถเดินทางผ่านโมเด็มไปยังคอมพิวเตอร์เครื่องอื่นได้ และด้วยความที่คอมพิวเตอร์ในอดีตมีความจุน้อยในระดับ kilobyte จึงทำให้การทำซ้ำตัวเองของไวรัสจำนวนมากมีผลทำให้คอมพิวเตอร์เมนเฟรมทำงานช้าลง แม้ไวรัสหนึ่งตัวจะมีขนาดเพียงระดับ byte ก็ตาม[239]

ใน ค.ศ.1962 มีการสร้างเกมส์ที่หน่วยงาน Bell Lab ชื่อเกมส์ Darwin ซึ่งมีรูปแบบคล้ายไวรัส โดยการเขียนโปรแกรมขึ้นมาสองโปรแกรมในคอมพิวเตอร์ กำหนดให้โปรแกรมหนึ่งค้นหา

---

[237] Imran Alam, “First Computer Virus-Creeper,” Linked in, February 4, 2022, [online] Accessed January 10, 2023. Available from: https://www.linkedin.com/pulse/first-computer-virus-creeper-imran-alam

[238] Pandora FMS Team, “History of Computer Viruses: Creeper and Reaper,” Pandora FMS, October 10, 2018, [online] accessed December 18, 2020. Available from: https://pandorafms. com /blog/ creeper-and-reaper/

[239] Ibid.

อีกโปรแกรมหนึ่งที่มีสภาพแวดล้อมเหมือนกัน เข้าไปเกาะโปรแกรมดังกล่าวแล้วลบโปรแกรมนั้นทิ้ง ซึ่งไวรัสยุคต่อมาเป็นการนำ Darwin กับ Creeper มาผสมกัน[240]

ใน ค.ศ.1974 มีการค้นพบโปรแกรม Rabbit ในคอมพิวเตอร์เมนเฟรม ซึ่งสามารถทำสำเนาได้รวดเร็วทำให้ ส่วนจัดเก็บข้อมูล (Storage) เต็ม และทำงานต่อไม่ได้ โปรแกรม Rabbit เป็นพัฒนาการอีกขั้นหนึ่งที่โปรแกรมต่อต้านไวรัสไม่สามารถกำจัดได้ง่าย[241]

ขณะที่ใน ค.ศ.1982 มีการพบไวรัส Elk Cloner[242] ซึ่งเป็นไวรัสที่ปรากฏในระบบปฏิบัติการ Apple DOS 3.3 บนเครื่อง apple 2 โปรแกรม Elk Cloner สามารถทำสำเนาตัวเองได้ใน Boot sector ขณะที่ระบบปฏิบัติการ (Operating System: OS) ยังไม่ทำงาน สร้างความตื่นตระหนกในวงการคอมพิวเตอร์ในขณะนั้นจนถึงขั้นที่หลายคนเชื่อว่าไวรัส Elk Cloner เป็นนวัตกรรมของมนุษย์ต่างดาว เพราะ Elk Cloner ทำให้ภาพในจอคอมพิเตอร์กลับหัว และมีตัวหนังสือวิ่งโดยปรากฏข้อความว่า “The Program with a Personality. It will get on all your disks. It will infiltrate your chips. Yes, It’s Cloner! It will stick to you like glue. It will modify ram too. Send in the Cloner.” ปรากฏว่ามีการจับกุมตัวผู้สร้าง Elk Cloner ได้ โดยผู้ต้องหาเป็นนักเรียนอายุ 15 ปี ชื่อว่า Richard Skrenta

ใน ค.ศ.1983 Len Edelman เป็นผู้ใช้คำว่า “ไวรัส” เป็นคนแรกโดยอ้างอิงจากพฤติกรรมการทำสำเนาตัวเองของโปรแกรมซึ่งไม่ได้รับการยอมรับจากเครื่องเป้าหมาย อย่างไรก็ดีในปีเดียวกันนี้มีการจัดงาน Information Security Conference ครั้งที่ 7 โดยบุคคลผู้จัดงานนี้ขึ้นมาคือ Fred Cohen[243] ซึ่ง Cohen ได้ประกาศให้ทุกคนรับรู้ว่าโปรแกรมที่สามารถทำสำเนาตัวเองได้และสามารถติดต่อไปยังเครื่องคอมพิวเตอร์อื่นๆ ได้ ให้เรียกว่า “ไวรัสคอมพิวเตอร์” ทำให้ Fred

---

[240] Gerald A. Edgar, "Darwin: A survival game for programmers." Computer Language, Vol.4 (4) (April 1987): 79-86.

[241] Matt Burgess, “The Bad Rabbit malware was disguised as a Flash update,” Wired, October 27, 2017, [online] accessed January 19, 2020. Available from: https://www.wired.co.uk /article/bad-rabbit-ransomware-flash-explained

[242] Scott Levy and Jedidiah R. Crandall, “The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus,” arXiv:2007.15759, June 20, 2020, [online] accessed January 19, 2022. Available from: https://arxiv.org/abs/2007.15759,

[243] Macus J. Ranum, “Fred Cohen on strategic security: ‘Start with the assumptions,” TechTarget, February 2018, [online] accessed January 19, 2020. Available from: https://www. techtarget. com/searchsecurity/opinion/Fred-Cohen-on-strategic-security-Start-with-the-assumptions,

Cohen ได้รับการยกย่องว่าเป็น “บิดาแห่งวงการไวรัส” นอกจากนั้น Cohen ยังได้ใช้เครื่องคอมพิวเตอร์ Wag 11/750 สาธิตวิธีการติดไวรัสของเครื่องคอมพิวเตอร์ เพื่อให้คนเห็นภาพการติดไวรัสของไฟล์ หรือโปรแกรมต่างๆ ด้วย

ใน ค.ศ.1986 ชายชาวปากีสถานอายุ 19 ปี ชื่อ Basit Farooq ได้ร่วมกับ Amjad Farooq พี่ชาย สร้างไวรัสที่ชื่อว่า Brain[244] มีเป้าหมายในการทำลายเครื่อง IBM PC และ IBM Compatible ทั้งหมด ซึ่งแท้จริงนั้น Brain เป็นโปรแกรมที่สร้างขึ้นมาเพื่อการตรวจจับโปรแกรมละเมิดลิขสิทธิ์และคุ้มครอง Software ที่ถูกกฎหมายในปากีสถาน แต่ปรากฏว่ามีผู้นำ Sort code โปรแกรมไปดัดแปลงเป็นไวรัส

ไวรัสที่ร้ายแรงที่สุดที่ปรากฏขึ้นมาใน ค.ศ.1989 ไวรัสดังกล่าวชื่อว่า Stone[245] การทำงานของ Stone คือการฝังตัวใน Master boot record และจะมีการสั่งการให้คอมพิวเตอร์ reboot ตัวเองหลายๆ ครั้ง พร้อมขึ้นประโยคว่า “Your computer is now stoned” เป็นไวรัสที่แพร่กระจายมากที่สุดชนิดหนึ่งและส่งผลกระทบต่อผู้ใช้งานอินเทอร์เน็ตมากที่สุด

ต่อมาใน ค.ศ.1990 มีไวรัสกลุ่มหนึ่งที่สามารถแตกสายพันธุ์ได้มากกว่า 50 สายพันธุ์ มีลักษณะการทำงานเหมือนกัน แต่เมื่อมีการทำสำเนาจะมีการสร้างชื่อใหม่ขึ้นมาไม่ซ้ำกัน ไวรัสกลุ่มนี้เรียกชื่อว่า “Jerusalem Family” ซึ่งเชื่อว่าต้นกำเนิดมาจากมหาวิทยาลัยเยรูซาเล็มในประเทศอิสราเอล Jerusalem Family เป็นไวรัสที่โด่งดังมากในช่วงเวลาหนึ่ง[246]

ขณะที่มีผู้พยายามพัฒนาไวรัสที่มีความสามารถในการทำลายสูงขึ้น โดยใน ค.ศ. 1991 ที่ประเทศออสเตรเลียมีการพบไวรัส Michelangelo[247] ซึ่งในขณะนั้นไวรัสดังกล่าวยังไม่มีชื่อว่า Michelangelo ลักษณะการติดเชื้อไวรัสนี้จะอยู่ในระบบปฏิบัติการ DOS แต่ไม่แสดงผลกระทบต่อคอมพิวเตอร์ ต่อมาในวันที่ 6 มีนาคม ค.ศ.1992 ซึ่งเป็นวันคล้ายวันเกิดของ Michelangelo ศิลปิน

---

[244] Harold Joseph Highland, “The Brain Virus: Fact and Fantasy,” Computers and Security, Vol. 7, (1988): 367-370.

[245] Nitesh Kumar Dixit, Lokesh Mishra, Mahendra Singh Charan and Bhabesh Kumar Dey, “The New Age of Computer Virus and Their Detection,” International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, (May 2012): 81.

[246] Margaret Rouse, “What does Jerusalem Virus Mean?” Techopedia, May 31, 2012, [online] accessed January 19, 2020. Available from: https://www.techopedia. com/definition /27875/jerusalem-virus

[247] Jonathan Yenkin, “Company Tracks Down Michelangelo Computer Virus,” AP news, January 29, 1992, [online] accessed January 19, 2020. Available from: https://apnews.com/article/1b3d0b1803e743a0898f2c1dedd73f69

ชื่อดัง ไวรัสดังกล่าวก็ปฏิบัติการลบ 100 sector แรกของ Hard disc ซึ่งติดเชื้อ โดยพบผู้ถูกโจมตีด้วยไวรัสชนิดนี้สูงถึงราว 20,000 ราย การลบข้อมูล 100 sector แรกของHard Disk นี้มีผลให้หัวอ่าน Hard Disk ไม่สามารถทำงานได้ หรือหมายความว่า Hard Disk นั้นเสียนั่นเอง ถือว่าเป็นไวรัสตัวแรกที่สามารถทำลาย Hardware ได้[248]

ขณะที่ใน ค.ศ.1995 มีไวรัสที่สามารถแทรกตัวมากับไฟล์ Microsoft words ได้ โดยอาศัยช่องโหว่ติดมากับ Macro ของโปรแกรม Microsoft Words (ส่วนติดตั้งเพื่อกำหนดคุณสมบัติพิเศษของ Microsoft Words) ไวรัสนี้ชื่อว่า Concept ถือเป็นไวรัสตัวแรกที่กระจายสู่โลกภายนอกผ่านทางอินเทอร์เน็ต เนื่องจากในช่วงเวลาดังกล่าวมีการใช้อินเทอร์เน็ตเป็นที่แพร่หลายแล้ว เครื่องคอมพิวเตอร์ที่ติดไวรัส Concept จะแสดงข้อความว่า “That’s enough to prove my point” ดังนั้นหากผู้ใช้งานคอมพิวเตอร์ไม่ทราบความหมายของข้อความดังกล่าวหรือไม่สังเกตก็จะไม่รู้เลยว่าเครื่องคอมพิวเตอร์ของตนติดเชื้อไวรัสแล้ว [249]

การพัฒนาไวรัส Concept นี้เป็นรูปแบบในรุ่นที่ 2 ของไวรัสคอมพิวเตอร์ โดยรุ่นที่ 1 ไวรัสจะอยู่ในรูปแบบของโปรแกรมเดี่ยวในสกุล “.exe” ซึ่งจะทำงานในเครื่องคอมพิวเตอร์โดยการทำซ้ำตัวเองดังที่กล่าวมา แต่ไวรัสในรุ่นที่ 2 ไม่ใช่โปรแกรมเดี่ยวในสกุล “.exe” แต่เป็นไฟล์โปรแกรม “.exe” ที่แทรกอยู่ในไฟล์อื่น ทำให้การตรวจจับไวรัสในช่วงเวลานั้นทำได้ยากขึ้นกว่าช่วงที่ผ่านมา ต่อมาในภายหลังวิธีการแทรกไฟล์ประสงค์ร้ายในไฟล์อื่นที่เป็นโปรแกรมปกติ ถูกเรียกว่า “Trojan” โดยเทียบเคียงกับกรณีม้า Trojan[250] ซึ่งชาวเมืองทรอยเข้าใจว่าเป็นของปลอดภัยและนำเข้ามาเก็บไว้ในเมือง แต่ในม้า Trojan ดังกล่าวมีทหารเมืองสปาร์ต้าซ่อนอยู่และออกมาทำลายประชาชนเมืองทรอยในเวลาที่ทุกคนนอนหลับ

ไวรัสที่สร้างขึ้นมาเพื่อวัตถุประสงค์ในการทำลายข้อมูลคอมพิวเตอร์มีการพัฒนาอย่างต่อเนื่อง ใน ค.ศ.1998 พบไวรัส CIH/Chernobyl[251] ซึ่งมีอำนาจทำลายล้างมากและยังสามารถ

---

[248] Jonathan Yenkin, “Company Tracks Down Michelangelo Computer Virus,”

[249] Ibid.

[250] Roger A. Grimes, “9 types of malware and how to recognize them,” CSO, November 17, 2020, [online] accessed January 10, 2022. Available from: https://www.csoonline. com/article /2615925/security-your-quick-guide-to-malware-types.html

[251] Katie Terrell Hanna, “Chernobyl Virus,” TechTarget, December 2021, [online] accessed January 19, 2022. Available from: https://www.techtarget.com/searchsecurity /definition/Chernobyl-virus

ทำงานตามเวลาที่กำหนดได้ โดยทุกวันที่ 26 ไวรัสจะทำการลบข้อมูลคอมพิวเตอร์ที่ติดเชื้อทั้งหมด ลบข้อมูลการ boot ทั้งหมด ทำให้คอมพิวเตอร์ไม่สามารถทำการ boot ได้ นอกจากนั้นยัง flash bios ทำให้ mainboard ไม่สามารถทำงานได้ ความเสียหายอาจถึงระดับที่ทำให้ bios เสีย ซึ่งจะต้องเปลี่ยน mainboard ของคอมพิวเตอร์ใหม่จึงจะทำให้คอมพิวเตอร์ทำงานได้อีกครั้ง

2. หนอน (Worm) เกิดขึ้นใน ค.ศ.1999 มีลักษณะการทำงานที่แตกต่างจากไวรัส กล่าวคือการติดไวรัสจะต้องมีการดาวน์โหลดไฟล์หรือโปรแกรมคอมพิวเตอร์ที่มีเชื้อไวรัสเข้ามายังคอมพิวเตอร์ก่อน คอมพิวเตอร์จึงจะติดเชื้อไวรัสได้ แต่มัลแวร์ที่พบใหม่นี้สามารถเดินทางในระบบอินเทอร์เน็ตได้ด้วยตัวเอง และสามารถเข้าไปในคอมพิวเตอร์แบบเดียวกับวิธีการของไวรัสได้

เมื่อหนอน (worm) เข้าไปในเครื่องคอมพิวเตอร์ได้หนอน (worm) จะทำสำเนาตัวเองในเครื่องคอมพิวเตอร์แล้วเกาะกับ mail client หากผู้ใช้งานคอมพิวเตอร์ส่งอีเมลไปหาผู้อื่น หนอน (worm) จะติดไปกับอีเมลและเดินทางไปอยู่ในเครื่องคอมพิวเตอร์ปลายทางที่ถูกใช้ในการเปิดอีเมล โดยหนอน (worm) ตัวเดิมและสำเนายังอยู่ในเครื่องแรกที่ติดเชื้อด้วย พฤติกรรมของ หนอน (worm) จึงมีลักษณะเหมือนหนอนที่สามารถคลานไปยังที่ต่างๆ และไปออกไข่ในทรัพยากรทางไซเบอร์ต่างๆ ได้ จากพฤติกรรมดังกล่าวจึงมีผู้ให้ชื่อว่า “worm” หนอน (worm) เองไม่ได้สร้างผลร้ายแรงต่อการทำลายเครื่องคอมพิวเตอร์แต่สร้างความรำคาญให้กับผู้ใช้งานเช่นการทำให้เครื่องคอมพิวเตอร์ช้าลง

3. Trojan เป็นโปรแกรมที่พัฒนาก่อนหน้า ค.ศ. 2000 เล็กน้อย มัลแวร์ชนิดนี้จะการซ่อนตัวเองเข้ามาในเครื่องคอมพิวเตอร์พร้อมกับไฟล์หรือโปรแกรมดังที่ได้กล่าวมาแล้ว มัลแวร์ที่อยู่ใน Trojan อาจเป็นไวรัส หนอนหรือโปรแกรมอื่นๆ ก็ได้ เมื่อมัลแวร์สามารถเข้าไปยังคอมพิวเตอร์เครื่องใดได้ ก็จะปฏิบัติการตามที่ผู้เขียนโปรแกรมมัลแวร์นั้นสั่งการต่อไป รูปแบบการทำงานของ Trojan มักปรากฏเป็นการขโมยข้อมูลจากเครื่องคอมพิวเตอร์แล้วส่งไปที่อื่น ข้อมูลดังกล่าวอาจได้แก่ การขโมยรหัสผ่านอีเมล รหัสผ่านเฟซบุค ขโมยหมายเลขและรหัสบัตรเครดิต ฯลฯ แล้วทำการส่งข้อมูลดังกล่าวกลับไปหาผู้สั่งการ นอกจากนั้นยังอาจเป็นการควบคุมเครื่องคอมพิวเตอร์ที่ Trojan อาศัยอยู่นั้นให้กลายเป็น Zombie ได้[252]

[252] Roger A. Grimes, “9 types of malware and how to recognize them,” CSO, November 17, 2020.

4. Spyware เกิดขึ้นหลัง ค.ศ. 2000 โดย Spyware เป็น Software ที่เข้ามาในเครื่องแล้วทำหน้าที่นำโฆษณามาแสดงเมื่อมีการใช้งานเครื่องคอมพิวเตอร์ Spyware สามารถติดมาได้ทั้งกับอีเมลและติดจากการเข้าสู่เว็บไซต์ ต่อมาเกิด adware ทำหน้าที่เหมือน spyware แต่ adware แตกต่างจาก spyware ตรงที่ adware จะฝังตัวเองในเครื่องคอมพิวเตอร์ เมื่อเราเปิด browser ที่เชื่อมต่อกับอินเทอร์เน็ตจะมีการแสดงโฆษณาแทนหน้า browser[253] โดยปกติจะเป็นโฆษณาเว็บไซต์การพนันและเว็บไซต์ลามกอนาจาร ในปี ค.ศ.2005 บริษัท Sony พบโปรแกรม rootkit ซึ่งมักจะเข้าไปอยู่ในระดับลึกของระบบการประมวลผลคอมพิวเตอร์ rootkit จะทำหน้าที่เปิดช่องให้ spyware และ adware เข้ามาในเครื่องคอมพิวเตอร์ การทำงานของโปรแกรมมัลแวร์เหล่านี้โดยปกติโปรแกรม anti-virus จะไม่สามารถสแกนเจอได้ ต้องใช้โปรแกรมที่ทำหน้าที่เฉพาะทางแก้ไขและการกำจัดมัลแวร์ดังกล่าวโปรแกรม anti-virus จะต้องมีชื่อไฟล์ที่กำหนดไว้ตรงกับชื่อมัลแวร์นั้นๆ ด้วย เช่น rootkit 32 rootkit 64 ฯลฯ มิเช่นนั้นจะไม่สามารถกำจัดมัลแวร์นั้นได้เลย

ต่อมา ค.ศ. 2008 ปรากฏการใช้งาน botnet[254] ซึ่งมีลักษณะคล้าย หนอน (worm) แต่มีการพัฒนามากขึ้นคือ botnet จะจำลองเครื่องคอมพิวเตอร์ให้เป็น zombie โดยคอมพิวเตอร์ที่ถูก botnet ควบคุมจะทำหน้าที่เป็น Host ในการส่งตัว botnet ออกไปยังอุปกรณ์อื่น botnet จึงทำหน้าที่เป็นเครื่องมือของหนอน (worm) โดยมีเงื่อนไขว่าคอมพิวเตอร์จะต้องถูกเปิดการใช้งานไว้และเชื่อมต่ออินเทอร์เน็ตตลอดเวลา botnet มักจะทำงานช่วงกลางคืน ทำให้การรับ-ส่งข้อมูลทางอินเทอร์เน็ตของคอมพิวเตอร์ host มีอัตราการทำงานสูงในเวลากลางคืน โดย botnet จะใช้เครื่องคอมพิวเตอร์ส่งเมลไปยังที่อยู่ต่างๆ ที่มีในอีเมลของเครื่อง host ทั้งหมด และกระจายตัวเองต่อไปยังเครื่องอื่นๆ

โดยปกติการกำจัด Spyware ต้องใช้โปรแกรมเฉพาะชื่อ Malwarebytes ซึ่งสามารถทำการค้นหา spyware adware และ rootkit ได้ นอกจากนั้นจะต้องใช้โปรแกรม Registry Editor เข้าไปเจาะ Registry ของเครื่องคอมพิวเตอร์ ทำการสแกน port ต่างๆ เพื่อค้นหา spyware แล้วนำออก และทำการป้องกันการเข้ามาของ spyware อีกครั้ง[255]

---

[253] Roger A. Grimes, “9 types of malware and how to recognize them,”

[254] Josh Fruhlinger, “What is a botnet? When infected devices attack,” CSO, April 5, 2022, [online] accessed February 16, 2023. Available from: https://www .csoonline.com/article /3240364/what-is-a-botnet.html

[255] Ibid.

(4) การใช้งานระบบไซเบอร์ทางการทหาร

จากลักษณะการทำงานของระบบไซเบอร์มีลักษณะดังที่กล่าวมาทำให้ปฏิบัติการทางไซเบอร์เพื่อก่อให้เกิดความเสียหายถูกมองว่ามีลักษณะเหมือนการใช้อาวุธ เพราะปฏิบัติการทางไซเบอร์ก่อให้เกิดได้ทั้งความเสียหายต่อข้อมูลและอุปกรณ์ที่เกี่ยวข้อง รวมถึงผลต่อเนื่องที่อาจเกิดขึ้นจากอุปกรณ์ต่อพ่วงอื่นๆ เช่น ระบบอาวุธที่สั่งงานผ่านเครือข่ายไซเบอร์ ปฏิบัติการทางไซเบอร์จึงเป็นปัจจัยในการขัดกันทางอาวุธได้ หากปฏิบัติการดังกล่าวเกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ

ในขณะที่การใช้ปฏิบัติการทางไซเบอร์เป็นวิธีการเพื่อเข้าถึงข้อมูลความลับ การเปลี่ยนแปลงข้อมูล การสร้างข่าวลวงเพื่อให้เกิดความเข้าใจผิด ฯลฯ ปฏิบัติการทางไซเบอร์ดังกล่าวจึงเป็นเพียงการทำให้ได้มาซึ่งความได้เปรียบทางการทหารแต่มิได้เป็นอาวุธเพื่อการทำลายเป้าหมายโดยตรง กรณีนี้ระบบไซเบอร์ย่อมเป็นเพียงวิธีในการขัดกันทางอาวุธ (Method) และในความเป็นจริงนั้นระบบไซเบอร์อาจถูกใช้ในสองลักษณะคือทั้งใช้เป็นอาวุธและเป็นวิธีการ โดยการใช้งานระบบไซเบอร์เพื่อวัตถุประสงค์ในการก่อความเสียหายถูกเรียกว่า “การก่อวินาศกรรมทางไซเบอร์ “(Cyber sabotage) และการใช้งานระบบไซเบอร์ที่มิได้มีวัตถุประสงค์ในการทำลายแต่มีวัตถุประสงค์ในปฏิบัติการทางข้อมูลข่าวสารถูกเรียกว่า “การจารกรรมทางไซเบอร์” (Cyber espionage)[256] นิยามทั้งสองนี้เป็นการจำแนกโดยนักวิชาการด้านไซเบอร์ที่ต้องการแบ่งลักษณะของปฏิบัติการโจมตีทางไซเบอร์ (Cyber Attack) ปฏิบัติการโจมตีทางไซเบอร์นี้เป็นที่เข้าใจของคนทั่วไปว่าหมายถึง “สงครามไซเบอร์” (Cyber warfare) ซึ่งคำว่าสงครามทางไซเบอร์เป็นนิยามของสงครามในพื้นที่ทางไซเบอร์ โดยมีลักษณะของการนำเอาคำว่าสงครามหรือการต่อสู้ทางทหารเชิงกายภาพไปรวมเข้ากับการโจมตีในพื้นที่การทำงานของคอมพิวเตอร์และสัญญาณคลื่นแม่เหล็กไฟฟ้า

การก่อวินาศกรรมทางไซเบอร์ หรือการใช้ปฏิบัติการทางไซเบอร์เพื่อวัตถุประสงค์ในการทำลายนี้ย่อมหมายรวมถึงการปล่อยไวรัสทางคอมพิวเตอร์ และการใช้ระบบไซเบอร์เพื่อการโจมตีในลักษณะของ DDoS (Distributed Denial of Service)[257] ฯลฯ เพื่อทำลายเครือข่ายการทำงานของคอมพิวเตอร์เป้าหมาย การกระทำลักษณะดังกล่าวอาจนำไปสู่ความเสียหายทางกายภาพต่อ

---

[256] Cordula Droege, “Get off my cloud: Cyber warfare, International Humanitarian Law and the protection of civilians,” International Review of the Red Cross, Volume 94 Number 886, (2012): 533-578.

[257] William Boothby, “Some legal challenges posed by remote attack,” International Humanitarian Law and the protection of civilians,” International Review of the Red Cross, Volume 94 Number 886, (2012): 580.

คอมพิวเตอร์ ความเสียหายต่อระบบการทำงานของคอมพิวเตอร์ การทำลายระบบเครือข่ายและอุปกรณ์ต่อพ่วงอื่นๆ ที่เชื่อมโยงกับการทำงานของคอมพิวเตอร์ด้วย

ขณะที่การจารกรรมทางไซเบอร์นั้น หมายความถึงปฏิบัติการที่ไม่ได้มีเป้าหมายในการทำลายโดยตรง เป็นเพียงการทำให้ได้มาซึ่งข้อมูลสำคัญของฝ่ายตรงข้าม รวมถึงการสร้างข้อมูลข่าวสารลวงเพื่อประโยชน์ของฝ่ายตนเอง ฯลฯ การจารกรรมทางไซเบอร์จึงเป็นวิธีการที่สามารถนำมาใช้ร่วมกับการขัดกันทางอาวุธเพื่อสร้างความได้เปรียบในการทำสงครามได้

2.4.1.2 ปัญญาประดิษฐ์กับระบบอาวุธอิสระ (Autonomous Weapon Systems)

นิยามของคำว่า Autonomous Weapon Systems ไม่มีการให้ความหมายอย่างเป็นทางการแต่ในเว็บไซต์ของคณะกรรมการกาชาดระหว่างประเทศ ประเทศไทยในชื่อ “อาวุธสังหารอัตโนมัติ”[258] “อาวุธที่สามารถกำหนดเป้าหมายด้วยตัวเองโดยไม่มีมนุษย์ควบคุม”[259] ฯลฯ ในการศึกษาวิจัยนี้จะใช้คำว่า “ระบบอาวุธอิสระ” ซึ่งหมายความว่าอาวุธดังกล่าวสามารถตัดสินใจอิสระได้ด้วยตัวเอง (Autonomous)

เอกสารทางการของคณะกรรมการกาชาดระหว่างประเทศได้นิยามความหมายของคำว่า “Autonomous Weapon Systems” ว่าหมายถึง “Autonomous Weapon Systems select and apply force to targets without human intervention”[260] ซึ่งมีใจความสำคัญคือ ระบบอาวุธที่เลือกเป้าหมายได้และปฏิบัติการต่อเป้าหมายได้โดยไม่ต้องอาศัยการควบคุมของมนุษย์ หรือระบบอาวุธที่สามารถทำงานได้ด้วยการตัดสินใจเองเช่นเดียวกับมนุษย์ที่สามารถตัดสินใจปฏิบัติหน้าที่ได้นั่นเอง

---

[258] Richard Lennane, “New types of weapons need new forms of governance,” Humanitarian Law and Policy, June 28, 2018, [online] accessed June 10, 2021. Available from: https://blogs.icrc.org/law-and-policy/2018/06/28/weapons-governance-new-types-weapons-need-new-forms-governance/

[259] Ibid.

[260] International Committee of the Red Cross, “ICRC position on autonomous weapon systems,” ICRC Article, (May 12, 2021): 2, [online] Accessed: June 10, 2021. Available from: https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

งานศึกษาทางวิชาการหลายชิ้นเสนอการแบ่งอาวุธทำงานเองเป็น 2 ประเภท คือ อาวุธอัตโนมัติหรือ Automatic Weapons และ อาวุธทำงานอิสระหรือ Autonomous Weapons “Autonomous” ความหมายกว้างกว่าคำว่า “อัตโนมัติ” ในขณะที่ “Automatic” ย่อมหมายถึงการทำงานตามเงื่อนไขใดเงื่อนไขหนึ่งทันทีจึงถูกแปลว่า “อัตโนมัติ” หรือระบบการทำงานด้วยตัวเองโดยไม่ต้องมีการคิด (think) ซึ่งเป็นหนึ่งในลักษณะของความเป็นอิสระ แต่คำว่า “อิสระ” (หรือคิดด้วยตัวเอง, Autonomous) ควรหมายความถึงการรวมกันของระบบอัตโนมัติหลายรูปแบบ[261] ดังนั้นผู้วิจัยจึงเลือกใช้คำว่า “อิสระ” ซึ่งหมายถึงการทำงานโดยการคิดและตัดสินใจด้วยตัวเองโดยปราศจากการแทรกแซงจากมนุษย์ แทนคำว่า “Autonomous” เพื่อไม่ก่อให้เกิดความทับซ้อนกับคำว่า “อัตโนมัติ” ซึ่งหมายถึง “Automatic” ตามที่เข้าใจกันโดยทั่วไปอยู่แล้ว

เพื่อให้เกิดความเข้าใจความหมายของคำว่า “อัตโนมัติ” กับคำว่า “อิสระ” จึงขอยกตัวอย่างดังต่อไปนี้

ตัวอย่างการทำงานแบบอัตโนมัติ (Automatic) เช่น ประตูซึ่งสามารถทำการเปิดได้เมื่อมีวัตถุหรือคนเข้าใกล้ในระยะที่กำหนด และสามารถปิดได้เองภายใน 5 วินาทีเมื่อไม่มีสิ่งกีดขวาง ถือว่าเป็นระบบอัตโนมัติเนื่องจากประตูไม่ต้องคิดหรือประมวลผลใดๆ เป็นเพียงการทำงานตามเงื่อนไขที่ผู้ออกแบบกำหนดไว้เท่านั้น

ทุ่นระเบิดสังหารบุคคลสามารถทำงานได้เมื่อมีคนเหยียบหรือมีคนเดินผ่านระบบเซ็นเซอร์ถือเป็นการทำงานระบบอัตโนมัติเป็นไปตามเงื่อนไขการทำงานของอุปกรณ์ เพียงแต่การเหยียบวัตถุระเบิดอาจผ่านกลไกที่ไม่ซับซ้อนเท่ากับระบบเซ็นเซอร์เท่านั้น

ระบบป้องกันภัยภาคพื้นดินซึ่งมีการติดตั้งปืนทำงานร่วมกับระบบเซ็นเซอร์แบบอินฟราเรดซึ่งจะทำการยิงเมื่อมีผู้เข้าเขตที่กำหนดเอาไว้ถือว่าเป็นระบบอัตโนมัติเนื่องจากไม่ต้องอาศัยการคิดหรือประมวลผลใดๆ เป็นเพียงการทำงานตามเงื่อนไขที่กำหนดเอาไว้เท่านั้น

---

[261] Martin Hagström, Characteristics of autonomous weapon systems’, in Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert meeting, Versoix, Switzerland, 15–16 March 2016. (Geneva: International Committee of the Red Cross, 2016): 23. [online] accessed June 20, 2021. Available from: https://icrcndresourcecentre.org/wp-content/uploads/2017/11/4283_002_Autonomus-Weapon-Systems_WEB.pdf

ตัวอย่างการทำงานแบบอิสระ (Autonomous) เช่นหุ่นยนต์ดูดฝุ่นสามารถทำการดูดฝุ่นได้โดยที่มนุษย์ไม่ต้องกำหนดว่าจะเริ่มต้นดูดฝุ่นจากที่ใดไปที่ใด ห้องมีขนาดเท่าไร มีผนังส่วนใดของห้อง ดูดฝุ่นอย่างไรจึงจะครอบคลุมทุกพื้นที่ในห้อง เมื่อพลังงานหมดหุ่นยนต์จะต้องทำอย่างไร หากหุ่นยนต์ดูดฝุ่นสามารถทำภารกิจได้สมบูรณ์คือดูดฝุ่นได้ทั้งห้องด้วยตัวเองเช่นนี้ถือว่าเป็นระบบที่หุ่นยนต์สามารถตัดสินใจได้อิสระ[262]

ระบบอาวุธที่ใช้ยิงโจมตีเป้าหมายได้ด้วยระบบนำวิถีซึ่งมนุษย์ไม่ต้องอาศัยความแม่นยำของมนุษย์เองในการใช้งาน เพียงระบุเป้าหมายที่ต้องการและอาวุธนั้นทำการเข้าหาเป้าหมายในตำแหน่งที่เป้าหมายอยู่โดยการคำนวณตำแหน่งจากทางภูมิศาสตร์ คลื่นความร้อนหรือใช้สัญญาณเรดาร์ด้วยระบบอาวุธนั้นเองโดยที่มนุษย์ไม่ต้องควบคุมอีกเช่นนี้ถือว่าเป็นระบบอิสระ[263]

ปัญหาประการหนึ่งคือระดับการทำงานของระบบอาวุธอิสระคือควรจำแนกการทำงานในหลายลักษณะหรือไม่ เนื่องจากระดับการทำงานของระบบอาวุธอิสระมีความแตกต่างกัน เช่น อาวุธบางลักษณะเป็นการทำงานแบบ Highly automated คือทำงานตามเงื่อนไขแต่มีเงื่อนไขหลายอย่างประกอบรวมกันอย่างซับซ้อน ขณะที่ บางระบบเป็นแบบบ semi-autonomous คือมนุษย์ควบคุมบางส่วนและระบบอาวุธทำงานด้วยตัวเองบางส่วน กับระบบอิสระแบบสมบูรณ์ fully-autonomous หมายถึงระบบอาวุธที่ทำงานได้ด้วยตัวเองโดยที่มนุษย์ไม่เกี่ยวข้องกับการทำงานของระบบอาวุธเลย (นอกจากการเปิดระบบปฏิบัติการ)

ปัญหานี้ค่อนข้างมีความคลุมเครืออยู่พอสมควร และผู้เชี่ยวชาญทางด้านอาวุธหลายคนเสนอว่าควรแยกระดับการทำงานของระบบอาวุธ เพราะจะมีความสัมพันธ์กับเรื่องความรับผิดชอบของมนุษย์ผู้ใช้งานระบบอาวุธนั้น และแนวทางการใช้งานระหว่างมนุษย์กับเครื่องจักร (Human-machine Interaction) ว่าอยู่ในระดับใดยังถือเป็นเรื่องสำคัญในมิติของกฎหมาย เพราะข้อจำกัดการใช้งานทั้งด้านพื้นที่และเวลาที่สัมพันธ์กับการสั่งการของมนุษย์เป็นเรื่องสำคัญ รวมถึงมาตรการตรวจสอบว่าเป้าหมายการโจมตีนั้นชอบด้วยกฎหมายหรือไม่ก็เป็นเรื่องสำคัญจึงเป็นหน้าที่ของมนุษย์

---

[262] European Commission, A definition of AI: Main capabilities and scientific disciplines, European Commission's High-Level Expert Group on Artificial Intelligence, Brussels, December 18, 2018, p. 3. [online] accessed February 20, 2022. Available from: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

[263] Ibid.

ผู้ควบคุม[264] กรณีที่มนุษย์ไม่มีส่วนเกี่ยวข้องกับการทำงานของอาวุธในการตัดสินใจต่อเป้าหมายเท่าไร ความเป็นอิสระของระบบอาวุธก็จะยิ่งมีมากขึ้นจนอาจถึงระดับอิสระโดยสมบูรณ์แบบ ปัญหาทางกฎหมายก็ย่อมจะเปลี่ยนแปลงไปตามข้อเท็จจริงในการใช้งานระบบอาวุธแต่ละระดับด้วย[265] เช่น หากอาวุธทำงานโดยเกี่ยวข้องกับการควบคุมโดยมนุษย์อยู่บ้าง โดยเฉพาะอย่างยิ่งในการสั่งทำลายเป้าหมายมนุษย์ผู้สั่งการอาจคำนึงถึงความเหมาะสมในการตัดสินใจขั้นสุดท้ายได้ การปรับใช้หลักความได้สัดส่วนในการโจมตีหรือการปรับใช้หลักความระมัดระวังล่วงหน้าก่อนการโจมตีย่อมสามารถทำได้ และอาจนำไปสู่การตัดสินใจยกเลิกการปฏิบัติการได้เมื่อเห็นว่าไม่สมควร ในขณะที่ระบบอาวุธทำงานอิสระโดยการคิด-วิเคราะห์ด้วยระบบอาวุธเองเมื่อต้องเผชิญกับบริบทสภาพแวดล้อมที่ไม่แน่นอนเกี่ยวกับความเหมาะสมในการทำลายโอกาสในการยุติภารกิจเป็นไปได้ค่อนข้างยากเพราะเงื่อนไขการทำงานของการประมวลผลแบบคอมพิวเตอร์มีข้อจำกัดที่แตกต่างจากมนุษย์ เมื่อมีการประเมินว่าสิ่งใดเป็นภัยคุกคามก็จะทำลายทันที หากมนุษย์ไม่สามารถยุติการทำงานในขั้นสุดท้ายได้ โอกาสที่ปฏิบัติการดังกล่าวจะเป็นการละเมิดต่อหลักความได้สัดส่วนในการโจมตีก็มีโอกาสเกิดมากขึ้น เป็นต้น

การทำงานของระบบอาวุธอิสระเกี่ยวข้องกับระบบการทำงานของปัญญาประดิษฐ์อย่างมาก เพราะปัจจัยสำคัญประการหนึ่งที่ระบบอิสระแตกต่างจากระบบอัตโนมัติคือระบบอิสระจะต้องคิดได้ ระบบอาวุธอิสระจึงทำงานได้ด้วยตัวเองอย่างเหมาะสมเท่าที่ระบบอาวุธสามารถทำได้เพื่อการทำลายเป้าหมาย เช่น หุ่นยนต์สังหารทำงานด้วยตัวเองเพื่อในการค้นหาศัตรูหรือข้าศึก (เป็นไปตามที่ระบบปัญญาประดิษฐ์มีข้อมูลและการประมวลผลได้ จากการออกแบบของมนุษย์) ระบบการประมวลผลของปัญญาประดิษฐ์ในหุ่นยนต์จะทำการแยกแยะพลเรือนออกจากพลรบ โดยข้อมูลที่หุ่นยนต์มีบันทึกไว้ เช่น พิจารณาจาก เครื่องแบบ การถืออาวุธ หรือสัญลักษณ์ ฯลฯ การทำงานของระบบอาวุธอิสระจึงต้องมีการประมวลผลแบบอัลกอริทึ่มหรือการทำงานโดยการประมวลผลทางคอมพิวเตอร์ผ่านสมการทางคณิตศาสตร์บนเงื่อนไขที่ซับซ้อนเพื่อให้ได้คำตอบที่ดีที่สุด

---

[264] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 10. [online] Accessed: August 2, 2019. Available from: https://icrcndresourcecentre.org/wp-content/uploads/2017/11/4283_002_Autonomus-Weapon-Systems_WEB.pdf

[265] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, p. 10.

สำหรับการปฏิบัติการ อย่างไรก็ดีการทำงานซับซ้อนของระบบอาวุธอิสระไม่ได้หมายความว่าจะต้องเป็นการทำงานในระดับปัญญาประดิษฐ์แบบสมบูรณ์เสมอไป

ตัวอย่างของการทำงานในระบบป้องกันภัยทางอากาศ Iron Dome ก็จะต้องมีการทำงานด้วยการประมวลโดยการส่งสัญญาณเรดาร์ตรวจภัยคุกคามจากจรวดหรือขีปนาวุธเข้ามาในดินแดนอิสราเอล ในระยะที่สามารถโต้ตอบได้อย่างปลอดภัย โดยระบบประมวลผลแล้วว่าเป็นภัยคุกคามที่ทำลายได้[266] ระยะที่จรวดต่อต้านสามารถเข้าถึงคือระยะใด ระยะที่ปลอดภัยอยู่ตำแหน่งใด เมื่อใดคือเวลาที่เหมาะสมในการยิงจรวดต่อต้าน การทำงานเช่นว่านี้เป็นลักษณะการทำงานประกอบร่วมกันหลายส่วนทั้งระบบค้นหาตำแหน่งเป้าหมายด้วยเรดาร์ การประมวลผลด้วยคอมพิวเตอร์ซึ่งมีโปรแกรมการประมวลผลแบบอัลกอริทึ่มที่ซับซ้อน ความซับซ้อนนี้ย่อมมากกว่าการทำงานของทุ่นระเบิดสังหารบุคคลหรือทุ่นระเบิดทำลายรถถัง

ข้อพิจารณาประการต่อมาคือระบบอาวุธอิสระนั้นย่อมหมายถึงทั้งระบบอาวุธที่เป็นวัตถุ เช่น จรวดต่อต้านจรวดหรือขีปนาวุธ หุ่นยนต์สังหาร อากาศยานไร้คนขับเพื่อการโจมตี ฯลฯ และการทำงานของชุดคำสั่งและการประมวลผลของซอฟท์แวร์ที่ไม่มีรูปร่างทางกายภาพ คำสั่งหรือโปรแกรมการทำงานของคอมพิวเตอร์ ระบบประมวลผล การสื่อสารผ่านเครือข่ายดิจิทัลและการใช้สัญญาณ GPS ผ่านระบบดาวเทียมเพื่อการสั่งการอาวุธ ฯลฯ เช่นหากเรายอมรับว่าการโจมตีทางไซเบอร์เทียบเท่ากับการใช้อาวุธได้ มัลแวร์ที่ใช้เป็นเครื่องมือในการโจมตีก็ย่อมถือเป็นอาวุธอิสระได้ โดยการนำโทรจันซึ่งซ่อน worm เอาไว้เข้าสู่ระบบเครือข่ายอินเทอร์เน็ต (เว็บไซต์) โดย worm ซึ่งซ่อนตัวอยู่นั้นถูกสั่งการเอาไว้ให้เข้าไปควบคุมเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ใดๆ ที่ทำงานได้เช่นเดียวกับคอมพิวเตอร์และอยู่ในเครือข่ายคอมพิวเตอร์ทางการทหารของฝ่ายศัตรู เมื่อถึงกำหนดตามเงื่อนไขที่ผู้สั่งการกำหนดเอาไว้ worm นั้นจะสั่งการให้คอมพิวเตอร์ทุกเครื่องที่ถูกควบคุมยุติการทำงานพร้อมกัน กรณีเช่นนี้ก็อาจถือว่าเป็นการทำงานของระบบอาวุธอิสระได้

[266] Göktuğ Sönmez and Gökhan Batu, “Iron Dome Air Defense System: Basic Characteristics, Limitations, Local and Regional Implications,” Policy Brief 169, Center for Middle Eastern Studies, 2021, p.11. [online] Accessed May 9, 2023. Available from: https://orsam.org.tr/d_hbanaliz/iron-dome-air-defense-system-basic-characteristics-limitations-local-and -regional-implications.pdf

ความเข้าใจเรื่องระบบอาวุธอิสระในปัจจุบันของคนทั่วไปมักให้ความสนใจกับหุ่นยนต์ทางการทหาร ไม่ว่าจะเป็นหุ่นยนต์สังหาร หุ่นยนต์ตรวจการ หุ่นยนต์เก็บกู้ระบิด หรือแม้กระทั่งหุ่นยนต์ให้ความช่วยเหลือทางมนุษยธรรม แต่ก่อนหน้าการมาถึงของหุ่นยนต์นั้นมีพัฒนาการของระบบอาวุธบางชนิดที่มีลักษณะกึ่งอัตโนมัติ จนถึงอัตโนมัติ เช่น ระบบอาวุธเพื่อการป้องกันภัยทางอากาศ และระบบการทำงานของอาวุธนำวิถี ฯลฯ ระบบอาวุธดังกล่าวจะทำให้เราเข้าใจการทำงานของระบบอาวุธอิสระในปัจจุบันมากขึ้นว่าความอิสระของอาวุธคืออะไร พัฒนาการในปัจจุบันเป็นอย่างไร และจะก่อให้เกิดผลทางกฎหมายที่เปลี่ยนแปลงไปอย่างไรด้วย

ระบบอาวุธในยุคดั้งเดิมได้แก่ ระบบอาวุธเพื่อการป้องกันภัยทางอากาศ ด้วย จรวด ขีปนาวุธ ปืนใหญ่ และปืนครกหรือระบบ C-RAM (Counter Rocket, Artillery and Mortar; C-RAM) ระบบอาวุธเหล่านี้มีการใช้งานมาตั้งแต่ ค.ศ.1960[267] โดยวัตถุประสงค์ทั้งการทำลายภาคพื้นดินและการทำลายภาคอากาศ ส่วนที่เกี่ยวข้องกับพัฒนาการของระบบอาวุธอิสระในปัจจุบันคือการทำลายภาคอากาศ โดยเฉพาะอย่างยิ่งกับปฏิบัติการป้องกันภัยทางอากาศ ซึ่งกองทัพของหลายประเทศต่างมีความพยายามในการพัฒนาเทคโนโลยีของตนเองเพื่อความมั่งคงทางน่านฟ้าในสงครามยุคปัจจุบัน ระบบอาวุธเพื่อการป้องกันภัยทางอากาศที่สามารถปฏิบัติภารกิจได้สำเร็จมักอยู่ในรูปแบบของอาวุธนำวิถี โดยการสั่งการของผู้ยิงให้อาวุธนั้นเข้าโจมตีเป้าหมายทางอากาศอย่างแม่นยำ

ระบบการทำงานของระบบป้องกันภัยทางอากาศ C-RAM ในระยะเริ่มต้นของพัฒนาการนั้นไม่ใช่ระบบอัตโนมัติ แต่มีมนุษย์เกี่ยวข้องในฐานะผู้ควบคุมและทำการเลือกเป้าหมายก่อนตัดสินใจโจมตี ในขณะที่ปัจจุบันมีการพัฒนาระบบ C-RAM ให้สามารถยิงเป้าหมายคุกคามโดยอัตโนมัติตามกำหนดเงื่อนไข เวลาและเป้าหมายได้[268] ทำให้การต่อต้านสามารถกระทำต่อหลายเป้าหมายในเวลาเดียวกันได้

ระบบ C-RAM เป็นระบบอาวุธต่อต้านแบบพื้นฐานซึ่งเกี่ยวกับระบบนำวิถี ผู้วิจัยจึงขออธิบายพัฒนาการของระบบอาวุธนำวิถีซึ่งเป็นแนวทางในการพัฒนาระบบอาวุธอิสระในปัจจุบันดังนี้

ระบบอาวุธนำวิถีในรูปแบบจรวดยุคแรกที่โลกได้รู้จักคือจรวด V2 หรือที่รู้จักในชื่อ V-Weapons (Vergeltungswaffen) ของกองทัพเยอร์มันในสงครามโลกครั้งที่ 2 จรวด V2 เป็นจรวดนำวิถีระยะไกลเพื่อการตอบโต้ทางยุทธวิธี (Long-range artillery weapons) อาวุธชนิดนี้พัฒนาขึ้น

---

[267] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 29.

[268] Ibid., p. 12.

มาเพื่อเป็นระบบอาวุธต่อต้านการโจมตี (Retaliatory Weapons or Reprisal Weapons) จากฝ่ายศัตรู โดยโครงการพัฒนาระบบอาวุธตอบโต้ระยะไกลนี้มีการวิจัยและพัฒนาจรวดนำวิถีระยะไกลระบบเจ็ทแบบ V1[269] และจรวดนำวิถีระยะไกลระบบเชื้อเพลิงเหลวแบบ V2 (ซึ่งต่อมาในภายหลังมักเรียกทั้งระบบ V1 และ V2 เป็นแบบ V2 ทั้งหมด) และปืนใหญ่ต่อต้านการโจมตี แบบ V3[270]

ระบบอาวุธ V-Weapons ของเยอรมันนี้มีวัตถุประสงค์สำคัญเพื่อการตอบโต้การโจมตีของกองทัพสหราชอาณาจักรในช่วงสงครามโลกครั้งที่ 2 ในขณะที่กองทัพสหราชอาณาจักรก็มีการพัฒนาระบบเรดาร์เพื่อป้องกันภัยทางอากาศมาก่อนหน้านั้น หลังจากที่กองทัพเยอรมันได้มีการใช้อาวุธนี้ต่อต้านการโจมตีของกองทัพสหราชอาณาจักรแล้ว กองทัพเยอรมันก็ได้ใช้ระบบอาวุธ V-Weapons โจมตีหลายประเทศในยุโรป เช่น เบลเยี่ยมและฝรั่งเศส ซึ่งมีการประมาณการณ์ว่ามีผู้เสียชีวิตจากการใช้ระบบอาวุธ V-Weapons นี้ประมาณ 18,000 คน และส่วนใหญ่เป็นพลเรือน[271]

ระบบอาวุธจรวด V2 ซึ่งเป็นระบบจรวดนำวิถี (Guided Missile or Guided Rocket) ในยุคแรกเริ่ม ในช่วงสงครามโลกครั้งที่ 2 นี้ มีองค์ประกอบการทำงานของอาวุธ 5 ประการที่สำคัญ คือ 1. การกำหนดเป้าหมาย 2. ระบบการนำทาง 3. ระบบการบินของจรวด 4. ระบบเครื่องยนต์ขับเคลื่อน และ 5. ระบบหัวรบ[272]

ระบบอาวุธนำวิถีซึ่งปรากฏในระบบการป้องกันภัยทางการทหารมีความแตกต่างกันตามเทคโนโลยีของแต่แต่ละประเทศ อย่างไรก็ดีอาจแบ่งเป็นหมวดหมู่ได้ ดังนี้

1) ขีปนาวุธและจรวดต่อต้านการโจมตี (Missile and Rocket Defense Weapons)

ระบบป้องกันภัยรูปแบบนี้มีระยะทำลายพิสัยใกล้ นิยมติดตั้งในเรือและบนบก โดยปกติใช้งานระบบ C-RAM ซึ่งมีความเที่ยงตรง แม่นยำ และตอบสนองได้ฉับไวต่อการป้องกันการโจมตี ระบบต่อต้านการโจมตีนี้จะประกอบด้วยส่วนการทำงานแบบอิสระ (Autonomous) สามารถค้นหา ตรวจสอบ และคัดเลือกเป้าหมายด้วยตัวเองไม่ต้องใช้มนุษย์ควบคุม ระบบขีปนาวุธเพื่อการป้องกันภัย

---

[269] Kenneth P. Werrell, The Evolution of the Cruise Missile, (Alabama: Air University Press, 1985), p. 41-42.

[270] Basil Collier, The Battle of the V-Weapons. (Morley, The Elm field Press, 1976), p. 138.

[271] Michael J. Neufeld, The Rocket and the Reich: Peenemunde and the Coming of the Ballistic Missile Era. (New York: The Free Press, 1995), pp. 137, 237.

[272] V. Phaninder Reddy, Rocket and Missiles, Lecture Notes, (Telangana: Institute of Aeronautical Engineering, 2000): pp. 7-12.

ทางอากาศใช้ข้อมูลแบบเดียวกับข้อมูลการบินพลเรือนเพื่อการวิเคราะห์และประมวลผล นอกจากนั้นยังมีการติดตั้งระบบทำลายตัวเองไว้หากการตัดสินใจผิดพลาดและก่อให้เกิดความเสียหายต่อพลเรือน (Self-destructing Round) เพื่อไม่ให้ความเสียหายเกิดขึ้นกับพลเรือนในขอบเขตที่กว้างขวางจนเกินไป โดยระบบขีปนาวุธเพื่อการป้องกันที่มีชื่อเสียง คือระบบ Iron Dome ของกองทัพอิสราเอลและ Terminal High Altitude Area Defense System (THAAD) ของกองทัพสหรัฐอเมริกา[273]

Iron Dome เป็นระบบป้องกันภัยทางอากาศของกองทัพอิสราเอลซึ่งสามารถทำการป้องกันการโจมตีได้หลายเป้าหมายในเวลาเดียวกัน ผลิตโดยบริษัท Rafael Advance Defense System เป็นการทำงานร่วมกันของระบบ Dual-Mission Counter Rocket Artillery, and Mortar (C-RAM) และระบบ Very Short Range Air Defense (V-SHORAD) system[274] การป้องกันภัยทางอากาศของ Iron Dome เป็นไปโดยอัตโนมัติเมื่อมีการตรวจพบการโจมตีด้วยขีปนาวุธ จรวด ปืนใหญ่หรือเครื่องยิงลูกระเบิดซึ่งเคลื่อนที่เข้ามาในดินแดนอิสราเอล โดยเรดาร์ของระบบ Iron Dome จะตรวจตราการโจมตี การติดตั้งเรดาร์นี้จะมีอยู่รอบชายแดนอิสราเอล เรดาร์จะมีการรายงานไปยังระบบควบคุมและทำการประเมินจุดตกของขีปนาวุธซึ่งเป็นภัยคุกคาม ในขณะที่ระบบประมวลผลจะสั่งการแท่นยิงขีปนาวุธต่อต้านการโจมตี เพื่อทำลายภัยคุกคามทางอากาศดังกล่าว ระยะทำการของขีปนาวุธของระบบ Iron Dome จะอยู่ในระยะ 4-70 กิโลเมตร และการทำลายขีปนาวุธโจมตีจะกระทำนอกเขตอยู่อาศัยของพลเมืองเท่านั้น[275]

ในอนาคตจะมีการพัฒนาระบบ Iron Dome ให้สามารถทำการได้ในระยะไกล โดยมีความพยายามเพิ่มวิถีทำการให้มากขึ้นถึง 70-250 กิโลเมตร[276]

การเปิดตัวระบบ Iron Dome ของกองทัพอิสราเอลเริ่มต้นใน ค.ศ. 2011 แต่การใช้งานจริงเกิดขึ้นใน ค.ศ. 2012 เพื่อต่อต้านการโจมตีของกลุ่มฮามาส ในปฏิบัติการดังกล่าวมีการรายงานว่าระบบ Iron Dome สามารถทำลายภัยคุกคามทางอากาศในฉนวนกาซาได้ถึง 85% (ทั้งนี้ไม่รวมขีปนาวุธที่ยิงมาจากที่อื่น ซึ่งรวมแล้วมีขีปนาวุธโจมตีอิสราเอลกว่า 1,500 ลูก) ความเสียหายที่เกิดขึ้นกับ

---

[273] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 10.

[274] Rafael Advanced Defense Systems LTD., (n.d.) Iron dome; Dual- mission counter rocket, artillery and mortar (C-RAM) and very short-range air defense (V-SHORAD) system, [online] Accessed: May 20, 2021, Available from: https://web.archive.org/web/20120710092155/ http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/0/1190.pdf

[275] Jeremy M. Sharp, U.S. foreign aid to Israel, (Washington, DC: Congress Research Service, 2015), p. 9.

[276] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 32.

พลเรือนมีเพียงการเสียชีวิต 4 ราย ในขณะที่ต่อมาอิสราเอลได้พัฒนาความจุแบตเตอร์รี่ของระบบยิงขีปนาวุธของ Iron Dome ให้มีมากขึ้น

ในความขัดแย้งของอิสราเอลและกลุ่มฮามาสใน ค.ศ. 2014 มีรายงานว่าระบบ Iron Dome นั้นมีความแม่นยำมากขึ้นถึงประมาณร้อยละ 90[277] แม้อาจมีความผิดพลาดในการจำแนกอากาศยานพันธมิตรและภัยคุกคามบ้างก็ตาม แต่ความผิดพลาดของระบบ Iron Dome ก็เป็นสัดส่วนค่อนข้างน้อย เมื่อเทียบกับประสิทธิภาพในการป้องกันภัย[278]

ระบบ Terminal High-Altitude Area Defense System (THAAD) ซึ่งเดิมคือ Theater High Altitude Area Defense ของกองทัพสหรัฐอเมริกา เป็นระบบป้องกันภัยทางอากาศที่มีการใช้งานมาตั้งแต่ ค.ศ. 2008 ใช้เพื่อการป้องกันการโจมตีระยะใกล้จากขีปนาวุธ รวมถึงระบบอาวุธอิสระอื่นๆ โดยการทำงานของเรดาร์เพื่อค้นหาและติดตามการเคลื่อนที่ของขีปนาวุธที่เป็นภัยคุกคามมีการคำนวณวิถีการเคลื่อนที่และทำลายเป้าหมายด้วยระบบขีปนาวุธป้องกัน แม้กข THAAD มีความคล้ายคลึงกับระบบ Iron Dome แต่ประเทศสหรัฐอเมริกาทำการพัฒนาเทคโนโลยีขึ้นมาด้วยตัวเองหลังสงครามอ่าวเปอร์เซียใน ค.ศ. 1991[279] THAAD จะใช้ขีปนาวุธที่ไม่ติดตั้งหัวรบเพื่อการทำลายขีปนาวุธโจมตีเพื่อลดความเสียหายที่อาจเกิดขึ้นจากแรงระเบิด หน่วยงาน Missile Defense Agency (MDA) มีบทบาทสำคัญในการวิจัยและพัฒนา ต่อมาใน ค.ศ. 2014 สหรัฐอเมริกามีร่วมมือกับอิสราเอลในการแลกเปลี่ยนเทคโนโลยีระหว่างกัน ทำให้สหรัฐอเมริกาได้นำองค์ความรู้ของระบบ Iron Dome มาใช้เพื่อการพัฒนาระบบขีปนาวุธเพื่อการป้องกันของตนเองต่อไป[280]

การทำงานของระบบป้องกันภัยทางอากาศมีการใช้เรดาร์เพื่อค้นหาเป้าหมายซึ่งเป็นช่องทางการสื่อสารเดียวกับสัญญาณดาวเทียมที่พลเรือนใช้ ระบบดังกล่าวคือ GPS การใช้งานระบบป้องกันภัยทางอากาศจึงมีส่วนหนึ่งที่เกี่ยวข้องกับระบบสื่อสารผ่านดาวเทียมในอวกาศเพื่อการใช้งานของอาวุธภาคพื้นดิน[281] จึงน่าจะเป็นประเด็นที่จะต้องพิจารณาต่อไปว่าจะแยกระหว่างการใช้งานดาวเทียมเพื่อประโยชน์ของพลเรือนและประโยชน์ทางการทหารอย่างไร

---

[277] Jeremy M. Sharp, U.S. foreign aid to Israel, (2015), p. 9.

[278] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, pp. 31-32.

[279] Ibid.

[280] Jeremy M. Sharp, U.S. foreign aid to Israel, (2015), p. 9.

[281] Dale Stephens, "The international legal implications of military space operations: Examining the interplay between international humanitarian law and the outer space legal regime," International Law Studies, vol. 94, (2018): 77.

ประโยชน์ของระบบป้องกัยภัยทางอากาศคือสร้างความปลอดภัยแก่พลเรือนและมีความแม่นยำในการทำลายเป้าหมาย นักเทคโนโลยีด้านอาวุธหลายคนเชื่อว่าในอนาคตระบบป้องกันภัยทางอากาศจะมีขนาดเล็กลงและมีการใช้อย่างแพร่หลายมากขึ้นจนถึงอาจมีการใช้ในระบบอวกาศ[282] อย่างไรก็ดี การพัฒนาอาวุธให้ทำงานได้อย่างมีประสิทธิภาพสูงในขอบเขตพื้นที่กว้างขวางนี้อาจนำมาซึ่งปัญหาระหว่างผู้ควบคุมระบบอาวุธดังกล่าวกับการทำงานของระบบอาวุธอิสระที่อาจข้อผิดพลาดขึ้นในสภาพแวดล้อมหรือสถานการณ์ที่เกินความคาดหมายได้[283] นักวิชาการด้านอาวุธจึงค่อนข้างเห็นในทิศทางเดียวกันว่าปฏิบัติการของระบบอาวุธนั้นจะต้องเปิดโอกาสให้มนุษย์สามารถเข้าแทรกแซง ด้วยการสั่งหยุดหรือชะลอการปฏิบัติการเพื่อประเมินความเสียหายที่อาจเกิดแก่พลเรือนได้ด้วย[284]

ผลการใช้งานระบบอาวุธ C-RAM จากสถิติที่ 11 ปีที่ผ่านมา มีการใช้ระบบ C-RAM ในปฏิบัติการทางทหารค่อนข้างน้อยและไม่เคยพบรายงานความเสียหายแก่พลเรือนจากการใช้งานระบบ C-RAM เลย[285]

2) ระบบอาวุธเชิงรุกเพื่อป้องกันยานพาหนะสงครามจากการถูกโจมตีด้วย ขีปนาวุธจรวด และเครื่องยิงลูกระเบิด และระบบอาวุธป้องกันสถานที่ หรือพรมแดนจากการโจมตีของบุคคล (Vehicle “active-protection” Weapons and anti-personnel “sentry” Weapons) เช่น ระบบ Trophy (ASRPRO-A) active protection system ซึ่งติดตั้งในรถถังและยานพาหนะในการรบ เพื่อการป้องกันภัยคุกคาม ระบบอาวุธดังกล่าวปรากฏการใช้งานไม่นานนี้ในราว 5 ปีที่ผ่านมา เป็นที่นิยมใช้งานในกองทัพหลายประเทศ ระบบอาวุธนี้จะทำงานควบคู่ไปกับระบบเรดาร์ตรวจจับการเคลื่อนที่ของจรวดหรือลูกระเบิดที่จะเข้ามาทำลายยานพาหนะ โดยจะมีการคำนวณทิศทางและระยะการทำลาย ก่อนจะมีการยิงกระสุนเหล็กอัตโนมัติเพื่อทำลายภัยคุกคามดังกล่าว[286]

นอกจากระบบการป้องกันยานพาหนะแล้ว ยังมีระบบอาวุธป้องกันการโจมตีของบุคคลหรือ anti-personnel “sentry” Weapons หรือ Sentry Tech หรือระบบอาวุธยิงอัตโนมัติติดตั้งบนฐานยิง ทำงานร่วมกับใช้ระบบการตรวจจับการเคลื่อนไหวด้วยคอมพิวเตอร์ เพื่อจำแนกเป้าหมายที่เป็นมนุษย์ อย่างไรก็ดี ในการทำงานของระบบอาวุธนี้จะมีผู้ควบคุมว่าเป้าหมายซึ่งเป็นมนุษย์รายใดนั้นอยู่ใน

---

[282] Wolff Heintschel von Heinegg, “Neutrality and outer space,” International Law Studies, vol. 93, (2017): 528

[283] William Boothby, “Space weapons and the law,” International Law Studies, vol. 93, (2017): 208.

[284] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p. 48.

[285] Ibid., p. 11.

[286] Ibid., p. 48.

ข่ายที่จะถูกโจมตีได้หรือไม่ โดยจะต้องมีผู้ควบคุมเป็นผู้เลือกและพิจารณาความเหมาะสมในการทำลายเป้าหมายด้วย อย่างไรก็ดี ระบบอาวุธป้องกันการโจมตีของบุคคลที่สามารถทำการคัดเลือกเป้าหมายด้วยระบบประมวลผลของตนเองก็มีอยู่เช่นกัน แต่มิใช่การทำงานแบบอิสระเต็มรูปแบบ เพราะก่อนการทำลายเป้าหมาย จะมีการกำหนดให้คำสั่งการไปอยู่ที่ผู้ควบคุมซึ่งเป็นมนุษย์ ซึ่งเป็นผู้ตัดสินในใจการโจมตีเป้าหมายในลำดับสุดท้าย[287]

C,hในปัจจุบันยังไม่มีรายงานเรื่องความเสียหายแก่พลเรือนจากการใช้งาน The Trophy แต่น่าพิจารณาว่าหากระบบอาวุธนี้ถูกติดตั้งในอากาศยานไร้คนขับในขณะที่การสื่อสารระหว่างผู้ควบคุมและระบบอาวุธล้มเหลว ปฏิบัติการของระบบอาวุธอิสระนี้จะยังคงชอบด้วยกฎหมายหรือไม่ ประเด็นนี้ผู้เชี่ยวชาญอธิบายว่าควรถือว่าเป็นความรับผิดชอบของผู้สั่งการ (Commander)[288] โดยจะต้องยุติการปฏิบัติการทุกกรณี หากมีการใช้ระบบอาวุธดังกล่าวต่อไป แม้จะเกิดความล้มเหลวในการสื่อสารต้องถือว่าผู้สั่งการมีความรับผิดชอบต่อความเสียหายที่จะเกิดขึ้นแก่พลเรือนด้วย[289]

การทำงานของระบบ Sentry Tech โดยปกตินั้นจะมีการควบคุมทางไกลโดยมนุษย์เป็นสำคัญ ระบบอาวุธ Sentry Tech ที่มีการใช้งานในประเทศเกาหลีใต้คือ SGR A-1 ซึ่งมีการควบคุมโดยมนุษย์ในปฏิบัติการ เริ่มมีการใช้งานมาตั้งแต่ปี ค.ศ. 2010 เป็นระบบป้องกันภัยภาคพื้นดินที่กองทัพเกาหลีใต้ติดตั้งไว้ในเขตปลอดทหารตลอดแนวพรมแดนเกาหลีใต้และเกาหลีเหนือเพื่อทำหน้าที่แทนทหาร ระบบเซ็นเซอร์อัตโนมัติของระบบจะทำการตรวจจับการเคลื่อนไหวบริเวณพรมแดน มีรัศมีในการตรวจตราราว 3 กิโลเมตร ทำงานร่วมกับปืนกล 5.5 มิลลิเมตรและเครื่องยิงลูกระเบิดขนาด 40 มิลลิเมตรติดตั้งอยู่เพื่อการใช้งาน ในการปฏิบัติหน้าที่นั้นจะประกอบด้วยการทำงานของอาวุธร่วมกับการสั่งการทางไกลของทหารผู้ควบคุม เมื่อระบบตรวจจับเป้าหมายภัยคุกคามได้ ทหารผู้ควบคุมจึงดำเนินการต่อหากสิ่งที่ตรวจพบเป็นมนุษย์ผู้ควบคุมสามารถแจ้งเตือนหรือสอบถามเป้าหมายมนุษย์ดังกล่าวก่อนได้ ปัจจุบันระบบ SGR A-1 เป็นระบบตรวจตราอัตโนมัติที่ใช้งานประกอบกับการสั่งการยิงโดยมนุษย์และยังสามารถสั่งการให้ระบบตัดสินใจอัตโนมัติในการยิงเป้าหมายด้วยตนเองได้[290]

---

[287] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, p. 48.

[288] Jens David Ohlin, "The Combatant's Stance: Autonomous Weapons on the Battlefield," International Law Studies, vol. 92, (2016): 29.

[289] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, p. 11.

[290] Ugo Pagallo, The Laws of Robots: Crimes, Contracts and Torts. (New York: Springer, 2013), p. xi.

3) ระเบิดคลัสเตอร์แบบมีเซ็นเซอร์ค้นหาเป้าหมาย ขีปนาวุธค้นหาเป้าหมาย และโดรนโจมตีเป้าหมายแบบทำลายตัวเอง (Sensor-fused Munitions, Missiles and Loitering Munitions) เป็นระบบอาวุธอิสระตามโปรแกรมที่ผู้โปรแกรมบันทึกเอาไว้ เพื่อการค้นหาและทำลายเป้าหมายตามที่กำหนด บางครั้งมีการติดตั้งระบบเซ็นเซอร์ เรดาร์และระบบประมวลผลในระบบอาวุธ เพื่อค้นหาเป้าหมายตามโปรแกรมที่ตั้งไว้และสามารถโจมตีเป้าหมายตามระบบประมวลผลได้[291]

โดรนโจมตีเป้าหมาย (Loitering Munitions) ที่นิยมใช้ในกองทัพอเมริกา[292]โดยทั่วไปแตกต่างจากโดรนโจมตีอิสระเล็กน้อย โดยโดรนอิสระสามารถค้นหา คัดเลือกและทำลายเป้าหมายและสามารถเข้าสู่พื้นที่และเวลาตามที่กำหนดได้ด้วย ทั้งนี้การทำงานของโดรนจะเป็นการประมวลผลร่วมกันระหว่างโปรแกรมที่กำหนดไว้และระบบเซ็นเซอร์เช่นเดียวกับระเบิดคลัสเตอร์แบบมีเซ็นเซอร์ค้นหาเป้าหมาย ขีปนาวุธค้นหาเป้าหมาย[293]

การจำแนกความความแตกต่างของระบบอาวุธ Sensor-fused munitions, missiles and loitering munitions ว่าเป็นอิสระเพียงใดนั้น อาจมีหลากหลายรูปแบบโดยจากการจัดแบ่งของผู้เชี่ยวชาญด้านอาวุธเห็นว่าอาจแบ่งได้เป็นลักษณะต่าง ๆ ดังนี้ 1) การเคลื่อนที่แบบอิสระ (Self-mobility) โดยการเคลื่อนที่ด้วยระบบนำทางของตัวเอง 2) ระบบนำทางอิสระ (Self-direction) หรือความสามารถในการแยกแยะและคัดเลือกเป้าหมายได้อิสระ 3) ระบบการตัดสินใจอิสระ (Self-determination) หรือความสามารถในการโจมตีและเปลี่ยนแปลงการทำงานได้โดยอิสระ โดยการกำหนดภาระกิจ และเป้าหมายได้ด้วยตนเอง

ระบบอาวุธอยู่ในการพัฒนาปัจจุบัน คือขีปนาวุธระยะไกลแบบ Long-Range Anti-Ship Missile (LRASM) เป็นระบบอาวุธเพื่อต่อต้านเรือ โดยสามารถเคลื่อนที่และนำทางได้แบบอิสระด้วยวิธีการยิงระยะไกลผ่านชั้นอวกาศและทำงานร่วมกับระบบเซ็นเซอร์[294]

ในขณะที่ผู้เชี่ยวชาญบางฝ่ายมองว่าการใช้งานอากาศยานไร้คนขับโดยปกตินั้นมักมีมนุษย์เกี่ยวข้องในระดับการทำงาน (Human in the Loop) เพื่อคัดเลือกและโจมตีเป้าหมาย ปัจจุบันมีการใช้

---

[291] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p.33.

[292] Ugo Pagallo, The Laws of Robots: Crimes, Contracts and Torts, p. xi.

[293] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Expert Meeting Report, March 15-16, 2016, p.33.

[294] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, p. 48 and p. 12.

งาน Tactical Advanced Recce Strike (TARES) หรือระบบการทำงานของโดรนสังหารซึ่งเดินทางได้ไกล 200 กิโลเมตร บินได้นาน 4 ชั่วโมง สามารถติดหัวรบที่หนักได้ถึง 20 กิโลกรัมและระบบโดรนสังหารป้องกันการโจมตีบุคคล Hero 30 ซึ่งเดินทางได้ไกล 40 กิโลเมตร ในเวลา 30 นาทีต่อการเดินทาง 1 ครั้ง และติดหัวรบที่หนักได้ถึงครึ่งกิโลกรัม[295]

จรวดทำลายใต้น้ำและจรวดบรรจุแคปซูลทำลายใต้น้ำ หรือ Torpedoes and encapsulated torpedo mines ได้แก่ จรวด Sea Hake Heavyweight torpedo ซึ่งมีระบบโซนาร์ในการตรวจจับเป้าหมายก่อนการโจมตี ระบบอาวุธทำงานร่วมกับผู้ปฏิบัติการที่เป็นมนุษย์ผ่านสายเคเบิล ผู้ปฏิบัติการจึงสามารถสั่งยกเลิกการโจมตีได้ ขณะที่ MU 90 lightweight Torpedo เป็นอาวุธที่สามารถค้นหาเป้าหมายด้วยระบบเซ็นเซอร์ มีวัตถุประสงค์เพื่อโจมตีเรือดำน้ำตามระดับความลึกที่โปรแกรมไว้ เช่นเดียวกับ SHKVL rocket-propelled torpedo

นอกจากนั้นยังมีระบบ Mark 60 CAPTOR encapsulated torpedo ซึ่งเป็นระบบอาวุธที่ทิ้งไว้ในท้องทะเลโดยระบบอาวุธจะทำหน้าที่ตรวจจับเรือดำน้ำตามโปรแกรมที่ตั้งไว้ เมื่อตรวจพบเป้าหมายจะมีการยิงจรวจออกมาโจมตีเรือดำน้ำเป้าหมายเช่นเดียวกับ PMK-1/2 ซึ่งเป็น Self-propelled sea mines รูปแบบหนึ่ง[296]

ระบบการป้องกันการโจมตีรูปแบบที่กล่าวมานี้มีความคาบเกี่ยวกันระหว่างการใช้เพื่อการป้องกันและการใช้เพื่อการทำลายกล่าวคือเทคโนโลยีจรวดทำลายใต้น้ำเป็นอุปกรณ์ที่ติดตั้งไว้เพื่อการป้องกันประเทศของรัฐชายฝั่งจากการโจมตีของเรือรบศัตรูจึงมีไว้เพื่อการป้องกันประเทศแต่ในขณะเดียวกันเทคโนโลยีนี้ก็สามารถทำการโจมตีเรือรบหรือเรือดำน้ำเพื่อป้องกันการเดินทางเข้าสู่ดินแดนของรัฐชายฝั่งทั้งที่ฝ่ายตรงข้ามอาจไม่ได้ทำการโจมตีก่อน ซึ่งย่อมก่อให้เกิดข้อพิจารณาทางกฎหมายต่อความรับผิดของรัฐในกรณีที่ต่างกันด้วย[297] นอกเหนือจากนั้นยังมีประเด็นที่หลายคนตั้งข้อสังเกตเรื่องความแม่นยำในการจำแนกเป้าหมายของระบบอาวุธดังกล่าวด้วยว่าระบบอาวุธนั้นจะแยกแยะเรือรบทางการทหารกับเรือพาณิชย์ของเอกชนได้อย่างแม่นยำเพียงใด

---

[295] Ibid.

[296] International Committee of the Red Cross, Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, p. 14.

[297] Hitoshi Nasu and David Letts, "The Legal Characterization of Lethal Autonomous Maritime Systems: Warship, Torpedo, or Naval Mine?" International Law Studies. Stockton Center of International Law, U.S. Naval War College, Vol. 96 (2020): 90.

การทำความเข้าใจระบบนำวิถีว่ามีความเกี่ยวข้องกับเทคโนโลยีที่พลเรือนใช้งานอย่างไรนั้นเป็นเรื่องจำเป็นต่อการพิจารณาความสัมพันธ์ระหว่างการใช้งานอาวุธอิสระ ซึ่งอาจอธิบายได้ดังนี้[298]

ในยุคแรกที่มีการใช้ระบบจรวดนำวิถีนั้น ระบบนำทางจะอาศัยระบบการแผ่คลื่นรังสีเพื่อตรวจจับเป้าหมาย เช่น คลื่นอินฟาเรด เลเซอร์ หรือคลื่นวิทยุ ฯลฯ ระบบอาวุธนี้อาจเข้าสู่เป้าหมายโดยตรวจวัดจากคลื่นความร้อนที่ออกมาจากระบบเครื่องยนต์ของเป้าหมายหรือการตรวจจับจากสัญญาณวิทยุสั่งการหรือระบบเรดาร์สั่งการของฝ่ายศัตรู โดยทั่วไประบบการสั่งการแบบนำวิถีมีสองรูปแบบใหญ่ๆ คือ

1) การนำทางแบบการยิงครั้งเดียว (Fire-and-forget) อาจกระทำโดยการตรวจจับเป้าหมายของระบบจรวดเอง หรือการช่วยเหลือจากระบบเรดาร์ หรือระบบเลเซอร์กำหนดเป้าหมายของฝ่ายสนับสนุน ระบบการนำทางแบบยิงครั้งเดียวนี้เมื่อมีการสั่งการยิงจรวดแล้วจะไม่สามารถดำเนินการเปลี่ยนแปลงปฏิบัติการใดๆ ได้จนกว่าจรวดจะทำลายเป้าหมาย[299]

2) ระบบการนำทางแบบเห็นภาพ (TV Guidance) เป็นระบบนำทางโดยมีมนุษย์หรือคอมพิวเตอร์ประมวลผลเป็นส่วนหนึ่งในปฏิบัติการ โดยการมองเป้าหมายผ่านทางกล้องตรวจจับ ซึ่งอาจเป็นกล้องอินฟาเรดที่ติดอยู่กับจรวด (เดิมนั้นระบบนำทางแบบนี้ใช้นกพิราบประกอบการนำทางการยิงจรวด แต่ต่อมาภายหลังมีการใช้กล้องอินฟาเรดติดระบบอาวุธแทน)[300]

ในภายหลังมีการนำหลายระบบประกอบรวมกันเพื่อทำให้ระบบการนำวิถีเกิดความแม่นยำเที่ยงตรงยิ่งขึ้น

ระบบการกำหนดเป้าหมาย (Targeting Systems) มีหลายรูปแบบ ได้แก่ ระบบ INS (Inertial Navigation System) ซึ่งใช้ระบบการประมวลผลด้วยการตรวจจับการเคลื่อนไหวประกอบด้วยการทำงานของไจโรสโคป และคอมพิวเตอร์ประมวลผลการเคลื่อนที่[301] ระบบ TERCOM (Terrain Contour Matching) อาศัยการประมวลผลจากข้อมูลแผนที่ประกอบร่วมกับข้อมูลการ

---

[298] George M. Siouris, Missile Guidance and Control Systems, (New York: Springer, 2014), p. 99.

[299] John Harris, Nathan Slegers, "Performance of Fire-and-Forget Anti-Tank Missile with a Damaged Wing," Faculty Publications - Biomedical, Mechanical, and Civil Engineering. Vol. 7. (2009): 1-2. [online] accessed June 15, 2022. Available from: https://digitalcommons.georgefox.edu/mece_fac/7

[300] George M. Siouris, Missile Guidance and Control Systems, p. 646.

[301] Ibid., p. 583.

เคลื่อนที่ของเป้าหมายที่มีการบันทึกเอาไว้ในอดีต[302]ระบบการนำทางด้วยดาวเทียม (Satellite Guidance)[303] ซึ่งระบบกำหนดเป้าหมายทั้งหมดจะช่วยให้ทราบตำแหน่งปัจจุบันของเป้าหมายการโจมตี และจะทำงานร่วมกับระบบการคำนวณการเดินทางของจรวด ระบบการกำหนดเป้าหมายอาจดำเนินการผ่านการสั่งการของมนุษย์ผ่านการสั่งการระยะไกล หรือการทำงานโดยอัตโนมัติ ซึ่งในปัจจุบันการทำงานของระบบกำหนดเป้าหมายมีการพัฒนาไปถึงขั้นการเรียนรู้เป้าหมายโดยระบบอาวุธเองด้วยระบบอินฟาเรด[304]

ระบบการบินของอาวุธ (Flight System)[305]ระบบการบินของอาวุธประกอบด้วยส่วนสำคัญด้วยระบบขับเคลื่อน และระบบอากาศพลศาสตร์ (ครีบ ปีก และหางหลัง ฯลฯ) ระบบการบินของจรวดนี้จะต้องทำงานร่วมกับการประมวลผลของระบบนำทางและระบบกำหนดเป้าหมายเสมอเพื่อให้เกิดความแม่นยำในการโจมตีเป้าหมาย

ระบบเครื่องยนต์ของอาวุธ (Engine System)[306]โดยปกติระบบขับเคลื่อนขีปนาวุธหรือจรวดมักเป็นระบบเจ็ทหรือเทอร์โบเจ็ท โดยอาจใช้เชื้อเพลิงแบบของแข็งเช่นดินระเบิดเป็นตัวขับเคลื่อนหรือการใช้ของเหลวเช่นน้ำมันหรือแก๊สเป็นตัวขับเคลื่อนระบบก็ได้ ขณะที่จรวดบางประเภทมีการใช้ทั้งสองระบบรวมกัน นอกจากนั้น ยังมีระบบหัวรบของจรวดซึ่งมักเป็นวัตถุระเบิดที่มีอานุภาพในการทำลายล้าง เช่น ระเบิดแบบกลุ่ม ระเบิดไฟ นิวเคลียร์ อาวุธเคมี อาวุธชีวภาพ ฯลฯ[307]

ระบบนำวิถีทั่วไปจะประกอบด้วยระบบหลักสำคัญ 2 ประการคือ ระบบการค้นหาและระบุเป้าหมาย และระบบอาวุธยิงเป้าหมาย โดยการค้นหาและระบุเป้าหมายนั้นมักใช้วิธีการทำงานของระบบเรดาร์ หรือระบบการตรวจจับจากคลื่นความร้อน (Infrared) ส่วนระบบอาวุธยิงเป้าหมายจะทำงานโดยระบบอาวุธนำวิถีซึ่งอาจมีระบบเรดาร์ติดอยู่ที่อาวุธหรือไม่แล้วแต่ลักษณะของเทคโนโลยีและการใช้งานแต่ละรูปแบบ

---

[302] Ibid., p. 551.

[303] Ibid., p. 644.

[304] Ibid.

[305] Ibid., p. 332.

[306] Ibid., p. 521.

[307] George M. Siouris, Missile Guidance and Control Systems, p. 4.

ส่วนสำคัญของระบบนำวิถีคือเรดาร์ (RADAR) เป็นคำที่ย่อจากคำว่า Radio Detection and Ranging ซึ่งหมายถึง ระบบการตรวจจับวัตถุด้วยคลื่นแม่เหล็กไฟฟ้า หลักการทำงานสำคัญของระบบเรดาร์คือการส่งสัญญาณคลื่นแม่เหล็กไฟฟ้าจากอุปกรณ์ส่งสัญญาณออกไปกระทบวัตถุเป้าหมายก่อนที่คลื่นแม่เหล็กไฟฟ้านั้นจะสะท้อนส่งกลับมายังอุปกรณ์รับสัญญาณ (เสาอากาศหรือเสาสัญญาณ) และมีการประมวลผลผ่านสมการอีกลำดับหนึ่ง ก่อนแสดงค่าตำแหน่งของเป้าหมายในจอแสดงผลเพื่อนำไปใช้ประโยชน์ต่อไป การทำงานของระบบเรดาร์นี้จะสามารถบอกข้อมูลได้ทั้งระยะ มุมและข้อมูลการเคลื่อนที่ของวัตถุเป้าหมาย (ความเร็วและตำแหน่ง)[308]

ระบบการทำงานของเรดาร์ถูกใช้งานเพื่อทั้งวัตถุประสงค์ทางพลเรือนและวัตถุประสงค์ทางการทหารทหารมาเป็นระยะเวลายาวนาน การใช้งานเรดาร์เพื่อประโยชน์ของพลเรือน ได้แก่ การใช้งานเรดาร์ในระบบการจราจรทางอากาศ การใช้เรดาร์เพื่อนำทางอากาศยาน การใช้เรดาร์เพื่อการสำรวจสภาพอากาศ ฯลฯ ขณะที่ทางทหารมีการนำเรดาร์มาใช้งานเพื่อการป้องกันภัยทางอากาศ ระบบนำวิถีของอาวุธ การสำรวจห้วงอวกาศ ฯลฯ[309]

ระบบการค้นหาและระบุเป้าหมายแบบเรดาร์นี้มีการพัฒนาตั้งแต่ก่อนยุคสงครามโลกครั้งที่ 2 ในหลายประเทศเป็นการลับ เพื่อวัตถุประสงค์ในการพัฒนาระบบป้องกันภัยทางอากาศของประเทศตนเอง ทั้งนี้เนื่องจากในทศวรรษ ค.ศ.1880 Heinrich Hertz นักวิทยาศาสตร์ชาวเยอรมันได้เสนอทฤษฎีการสะท้อนกลับของคลื่นแม่เหล็กไฟฟ้าต่อวัตถุที่เป็นโลหะ[310] ทำให้มีความพยายามของนักวิทยาศาสตร์ในหลายประเทศพยายามนำเอาทฤษฎีนี้ไปพัฒนาต่อยอดเพื่อใช้ประโยชน์

ในต้นศตวรรษที่ 20 Christian Hulsmeyer นักฟิสิกส์ชาวเยอรมันได้นำเอาทฤษฎีของ Hertz มาพัฒนาสร้างเป็นอุปกรณ์ป้องกันเรือชนกันกรณีที่มีหมอกในทะเล ในช่วงเวลาเดียวกันที่ประเทศอังกฤษก็มีการพัฒนาการใช้งานคลื่นแม่เหล็กไฟฟ้า โดยสร้างระบบที่ชื่อว่า chain home

---

[308] Niraj Prasad Bhatta and M. Geetha Priya, “RADAR and its Applications,” IJCTA, Vol. 10, No.3, (2017): 1-9.

[309] Ibid., pp. 1-9.

[310] Patricia Spieth Ramsay, “Heinrich Hertz, the Father of Frequency,” The Neurodiagnostic Journal, Vol. 53, No.1,(2013): 3-26, DOI: 10.1080/21646821.2013.11079882. p.10.

เพื่อใช้ในการตรวจจับวัตถุ ระบบ chain home เป็นการค้นหาและระบุเป้าหมายทางอากาศโดยการเทียบเคียงกับระยะห่างระหว่างเสาอากาศ โดยเสาแต่ละต้นจะส่งคลื่นและรับสัญญาณสะท้อนกลับ[311]

การทำงานของระบบ chain home ดังกล่าวเป็นผลมาจากการศึกษาวิจัยของ Robert Watson Watt นักวิทยาศาสตร์ชาวอังกฤษผู้เสนองานวิจัยการสะท้อนกลับของคลื่นสัญญาณให้กับรัฐบาลอังกฤษ และมีการทดลองใช้เครื่องบิน บินผ่านเสาส่งสัญญาณเพื่อวิเคราะห์การเคลื่อนที่และตำแหน่ง ปรากฏว่าการทดลองดังกล่าวประสบความสำเร็จ ต่อมาใน ค.ศ.1935 รัฐบาลอังกฤษจึงอนุมัติงบประมาณสร้างเสาสัญญาณ chain home ขึ้นมา 5 สถานี และมีการขยายสถานีอีกหลายสถานีในเวลาต่อมา[312]

หลักการทำงานของเสาสัญญาณคือการสร้างการเหนี่ยวนำระหว่างคลื่นแม่เหล็กและคลื่นไฟฟ้าซึ่งมีความเร็วเท่ากับความเร็วแสง และการสร้างขนาดของคลื่นแม่เหล็กไฟฟ้าเพื่อตรวจจับวัตถุจะต้องไม่ใหญ่ไปกว่าขนาดของวัตถุเป้าหมาย ปกตินิยมใช้ขนาดคลื่น 3 ช่วง คือ ช่วงที่ 1 ขนาด 0.5-20 GHz ช่วงที่ 2 ขนาด 35-40 GHz ช่วงที่ 3 ขนาด 94 GHz แต่นิยมใช้ช่วงที่ 1 มากที่สุดเพราะสามารถส่งสัญญาณได้ไกลที่สุด ในยุคต่อมาคลื่นแม่เหล็กไฟฟ้าเป็นประโยชน์อย่างมากต่ออุปกรณ์ที่เราใช้ในชีวิตประจำวันเช่น คลื่น AM FM สัญญาณโทรศัพท์มือถือ สัญญาณวิทยุสื่อสาร คลื่นโทรทัศน์ รวมถึงรังสีเอกซ์ ฯลฯ

ระบบ chain home นี้สามารถตรวจจับได้ทั้งตำแหน่งและทิศทางของวัตถุ แต่กระนั้นก็ตามการใช้คลื่นแม่เหล็กไฟฟ้าที่ใกล้เคียงกับเรดาร์ในปัจจุบันก็ยังไม่สำเร็จจนกระทั่งมีการคิดค้นและสร้างสรรค์อุปกรณ์ที่ชื่อว่า “Cavity Magnetron”[313] ซึ่งเป็นอุปกรณ์กำเนิดคลื่นไมโครเวฟด้วยพลังงานไฟฟ้าขึ้นมาได้ จึงทำให้เกิดอุปกรณ์ส่งสัญญาณคลื่นแม่เหล็กไฟฟ้าในยุคเริ่มต้นก่อนกลายเป็นระบบเรดาร์ในปัจจุบัน

---

[311] Justin Roger Lynch, “The Chain Home Early Warning Radar System A Case Study in Defense Innovation,” JFQ 95, (4th Quarter 2019): 100-103. [online] Accessed: July 15, 2022. Available from: https://ndupress.ndu.edu/Portals/68/ Documents/jfq/jfq-95/jfq-95_100-103_Lynch.pdf,

[312] Ibid., p. 101.

[313] Henry A. H. Boot and John T. Randall, “Historical Notes on the Cavity Magnetron,” IEEE Transactions on Electron Devices, Vol. 23 No.7, (July 1976): 724-729.

นอกจากอุปกรณ์ส่งสัญญาณแล้วอุปกรณ์สำคัญในการรับสัญญาณที่ส่งกลับมาเพื่อประมวลผลในทำงานของเรดาร์ในยุคเริ่มต้นคือ Oscilloscope[314] เป็นเครื่องมืออ่านสัญญาณสะท้อนกลับ เพื่อคำนวณหาระยะของเป้าหมายและคำนวณหาทิศทางเป้าหมายทำโดยวิเคราะห์ความสัมพันธ์ระหว่างมุมเสาอากาศและตัวเป้าหมาย

ใน ค.ศ.1934 สหราชอาณาจักรและสหรัฐอเมริกาได้มีความร่วมมือในการพัฒนาเรดาร์เพื่อการป้องกันการโจมตีทางอากาศ เป็นที่มาของการสร้างคำว่า “Radio Detection and Ranging” ซึ่งใช้คำย่อว่า “RADAR”[315] ขึ้นมาในช่วงเวลาดังกล่าว โดยหน่วยงานที่มีบทบาทสำคัญในการพัฒนาระบบเรดาร์คือ Signal Corp ของสหรัฐอเมริกา เหตุที่เกิดความร่วมมือดังกล่าวขึ้นเป็นเพราะความหวาดกลัวภัยคุกคามทางอากาศจากทั้งอากาศยาน จรวดและขีปนาวุธที่มีการพัฒนาในช่วงเวลาดังกล่าว โดยรัฐบาลสหราชอาณาจักรเชื่อว่าประเทศของตนเสี่ยงต่อภัยคุกคามดังกล่าวในระดับสูง[316]

การส่งสัญญาณคลื่นแม่เหล็กไฟฟ้าในระบบเรดาร์นี้มีการทำงาน 2 แบบ คือ แบบที่ 1 แบบต่อเนื่อง (Continuous wave)[317] ที่นิยมใช้กับระบบนำวิถี แบบที่ 2 เป็นการส่งสัญญาณเป็นช่วงๆ และมีจังหวะการรอคลื่นสะท้อนกลับ (Pulse) ซึ่งปรากฏทั้งระบบ High PRF (High Reputation Frequency) และ Low PRF (Low Reputation Frequency) ซึ่งจะเป็นประโยชน์แตกต่างกัน โดย High PRF เป็นคลื่นความถี่สูง (ส่งสัญญาณถี่กว่าปกติ) นิยมใช้เพื่อตรวจหาเป้าหมายแบบละเอียดในระยะใกล้ ในขณะที่ Low PRF มีประโยชน์ในการตรวจจับเป้าหมายระยะไกลโดยไม่ต้องการความละเอียดของเป้าหมาย[318]

ระบบการทำงานของเรดาร์ ประกอบด้วย แหล่งกำเนิดสัญญาณคลื่นแม่เหล็กไฟฟ้าที่อยู่ในระบบเรดาร์เรียกว่า Transmitter ซึ่งในยุคแรกใช้อุปกรณ์ชื่อว่า Cavity Magnetron เป็นตัวกำเนิดสัญญาณ ต่อมาจึงมีการพัฒนาเป็นระบบ Klystron เนื่องจากแหล่งกำเนิดสัญญาณทั้งสองประเภทมีขนาดค่อนข้างใหญ่ทำให้ยุคต่อมามีการพัฒนาเป็นระบบ Travelling Wave Tube ซึ่งมีขนาดเล็กลงมา รวมถึงระบบ Solid State Transmitter[319] เสาสัญญาณ (Radar Antenna) ซึ่งจะอยู่ในรูปแบบ

---

[314] Rich Markley, Oscilloscope Basics, (Bangkok: Rohde & Schwarz, 2015) pp. 5-31.

[315] Merrill I. Skolnik, Introduction to RADAR Systems, Second edition, (Singapore: McGraw-Hill Book Co., 1981), p.9.

[316] Ibid.

[317] George M. Siouris, Missile Guidance and Control Systems, p. 420.

[318] Merrill I. Skolnik, Introduction to RADAR Systems, p. 29.

[319] Hamish Meikle, Modern Radar Systems, (London: Artech House, 2008) p. 7-9.

ของเสาหรือจานรับ-ส่งสัญญาณคลื่น ทำหน้าที่บังคับทิศทางของคลื่นที่ส่งออกและเพิ่มกำลังส่งให้กับคลื่น นอกจากนี้เสาสัญญาณยังทำหน้าที่บีบคลื่นให้กว้างหรือแคบได้ตามการออกแบบ ความกว้างและแคบของคลื่นมีผลต่อการตรวจจับเป้าหมาย ยิ่งคลื่นมีมุมแคบเท่าไรก็จะยิ่งทำให้การตรวจจับเป้าหมายมีความละเอียดมากขึ้นเท่านั้น[320]

เสาสัญญาณจะรับคลื่นจาก Transmitter โดยคลื่นความถี่ต่ำจะส่งผ่านสายสัญญาณไปยังเสา ส่วนคลื่นความถี่สูงจะส่งผ่านอุปกรณ์ Wave guide นอกจากนั้นเสาสัญญาณจะทำการรับคลื่นที่ส่งกลับมาและส่งต่อไปยังตัวรับสัญญาณ (Receiver) โดยเสาสัญญาณมี 2 ประเภทคือ Reflector Antenna และ Array Antenna เสาสัญญาณแบบ Reflector Antenna[321] จะมีตัวสะท้อนสัญญาณทั้งแบบทึบและแบบโปร่งที่มีรูปแบบโค้งทรงเดียวกับลักษณะของคลื่นที่มีการรับ-ส่ง ที่หน้าแผ่นสะท้อนจะมีตัวส่งสัญญาณที่ชื่อว่า Feed Horn ทำหน้าที่ส่งสัญญาณไปกระทบกับแผ่นสะท้อนก่อนส่งคลื่นออกไปยังทิศทางที่ต้องการ เรดาร์แบบนี้วัดเป้าหมายได้เฉพาะทิศทางและระยะ แต่วัดความความสูงไม่ได้ จึงมีการพัฒนาอุปกรณ์ในภายหลังที่ชื่อว่า Stack beam เพื่อวัดความสูงของเป้าหมาย

Reflector Antenna ที่ต้องการลดขนาดลงจะมีการออกแบบตัวสะท้อนคลื่นเป็น 2 ชั้น โดยตัวสะท้อนแผ่นที่ 1 จะต้องมีช่องว่างให้คลื่นทะลุผ่านไปยังชั้นที่ 2 ได้ เรียกระบบนี้ว่า Twisted Cassegrain ระบบนี้จะช่วยลดระยะระหว่าง Feed Horn และแผ่นสะท้อน เรดาร์ชนิดนี้นิยมใช้ในระบบเครื่องบินขับไล่และเรือรบเนื่องจากสามารถส่งสัญญาณออกไปตรงๆ ได้

Array Antenna คือการนำเสาอากาศมาเรียงต่อกันเป็นชุดเพื่อรวมสัญญาณให้เดินทางไปยังทิศทางที่ต้องการ[322] รูปแบบของ Array Antenna มีค่อนข้างหลากหลาย ตั้งแต่ Yaggi Array Antenna, Linear Array Antenna, Planar Array Antenna, Phase Array Antenna ฯลฯ

Phase Array Antenna[323] เป็นระบบที่สามารถปรับรูปแบบของคลื่นได้หลากหลาย เนื่องจากมีอุปกรณ์ Phase Shifter จึงมีการพัฒนาเป็น 3 รูปแบบย่อยคือ Conventional Array, Lens Array และ Reflector Array ระบบ Phase Array Antenna ทำงานโดย Active Electronically Scan Array ซึ่งเป็นการนำเอาแหล่งกำเนิดคลื่นแบบ Solid State ขนาดเล็กมาเรียง

---

[320] Ibid.

[321] Ibid., p. 110.

[322] Hamish Meikle, Modern Radar Systems, p. 168.

[323] Ibid., p. 492.

ต่อกันในจำนวนมากแต่ละชิ้นจะมีตัวปรับสัญญาณของตัวเองจึงทำงานได้อิสระและสามารถทำงานร่วมกับระบบควบคุมขั้นสูงได้จึงเป็นที่นิยมใช้ในระบบเรดาร์ยุคปัจจุบัน

นอกจากองค์ประกอบของเสาสัญญาณแล้วรูปแบบการค้นหาเป้าหมายของเสาสัญญาณยังเป็นเรื่องสำคัญเพราะจะทำให้การทำงานของระบบเรดาร์สมบูรณ์ขึ้นมี 2 วิธีการที่ใช้กันในปัจจุบันคือ รูปแบบที่ 1 การหมุนเสาสัญญาณที่เรียกว่าระบบ Mechanically Scan และรูปแบบที่ 2 การเปลี่ยนระดับคลื่น (Shift phase) เรียกว่าระบบ Electronically Scan รูปแบบการเคลื่อนที่ของเสามีดังนี้

รูปแบบที่ 1 Circular Scan การหมุนเสาสัญญาณเสาจะหมุนรอบตัวเอง 360 องศาไปเรื่อยๆ ใช้ในการค้นหาเป้าหมายที่ครอบคลุมทุกทิศทาง การหมุนเร็วหรือช้าขึ้นอยู่กับว่าจะทำการตรวจจับเป้าหมายชนิดใด เสาสัญญาณที่หมุนไวใช้ในการตรวจจับเป้าหมายระยะใกล้และเคลื่อนที่ไวส่วนเสาสัญญาณที่หมุนช้าใช้ในการตรวจจับเป้าหมายระยะไกลเพื่อให้ได้สัญญาณสะท้อนกลับที่ชัดเจน[324]

รูปแบบที่ 2 Sector Scan เป็นการตรวจจับเป้าหมายทิศทางเดียว เสาสัญญาณจึงขยับเฉพาะทิศทางด้านเดียว ซึ่งช่วยลดระยะเวลาการสะท้อนกลับ โดยมากใช้เพื่อตรวจการป้องกันภัยทางอากาศ[325]

รูปแบบที่ 3 Raster Scan คล้ายกับการทำงานของ Sector Scan แต่ใช้ในระบบเครื่องบินขับไล่ เหมาะกับการตรวจจับเป้าหมายในระดับความสูงที่ต่างกัน[326]

รูปแบบที่ 4 Electronically Scan เป็นระบบเปลี่ยนทิศทางของคลื่นด้วยระบบ phase shifter จึงไม่ต้องมีการขยับอุปกรณ์ แต่สามารถทำงานได้แบบเดียวกับ Sector Scan และ Raster Scan นอกจากนั้นยังสามารถทำการรับ-ส่งสัญญาณแบบสุ่มได้ด้วย เพื่อป้องกันการวิเคราะห์คลื่นของฝ่ายศัตรู[327]

ระบบการระบุเป้าหมายประกอบด้วยระบบการระบุเป้าหมายเดี่ยว (Single Target Tracking)[328] เป็นการติดตามเป้าหมายเดียวและจะไม่ตรวจจับเป้าหมายอื่นซึ่งเหมาะสำหรับการโจมตี

---

[324] Ibid.

[325] Ibid., p. 492.

[326] Hamish Meikle, Modern Radar Systems, p. 492.

[327] Ibid.

[328] Merrill I. Skolnik, Introduction to RADAR Systems, p. 33.

เป้าหมายเฉพาะ รูปแบบ Track-While-Scan เป็นการทำงานผสมกันของการตรวจจับเป้าหมายเดียวและหลายเป้าหมายไปพร้อมกัน สามารถระบุเป้าหมายเฉพาะได้และยังระบุเป้าหมายอื่นไปพร้อมกันได้ ต้องใช้อุปกรณ์ดิจิทัลขั้นสูงในการบันทึกและประมวลผลสามารถระบุได้ทั้ง ทิศทาง ระยะ ความสูง และความเร็วของเป้าหมาย ปัจจุบันระบบ Track-While-Scan สามารถค้นหาเป้าหมายได้พร้อมกันถึง 10 เป้าหมายและสามารถสั่งการทำลายเป้าหมายได้พร้อมกัน 4 เป้าหมาย

ลักษณะการทำงานของสัญญาณที่แยกแยะเป้าหมายเคลื่อนที่และเป้าหมายไม่เคลื่อนที่อยู่บนพื้นฐานของหลักการ Doppler filter[329] คือการกรองสัญญาณคลื่นสะท้อนกลับ หากคลื่นสะท้อนกลับมีความถี่สูงหมายความว่าเป้าหมายนั้นเป็นเป้าหมายเคลื่อนที่ได้ ในขณะที่หากคลื่นสะท้อนกลับมีความถี่ต่ำหมายความว่าเป้าหมายดังกล่าวเป็นเป้าหมายไม่เคลื่อนที่ซึ่งอาจหมายความว่าเป็นสถานที่ ระบบเรดาร์จึงสามารถแยกแยะเป้าหมายต่างๆ ได้ ประเภทของเรดาร์ทางทหารอาจแบ่งได้ดังนี้[330]

1) เรดาร์แจ้งเตือนล่วงหน้า (Early warning radar) เป็นเรดาร์ตรวจจับระยะไกลที่สุดมีระยะทำการประมาณ 270 ไมล์ทะเล หรือ 500 กิโลเมตร มักสร้างเป็นสถานีรับ-ส่งสัญญาณขนาดใหญ่และใช้เป็นเครือข่ายป้องกันภัยทางอากาศของประเทศ เรดาร์แบบนี้นิยมใช้สัญญาณระดับ 0.5-3 GHz ซึ่งเป็นคลื่นความถี่ต่ำแต่สามารถส่งสัญญาณไปได้ไกลมีการหมุนเสาสัญญาณช้ามากประมาณมากกว่า 10 วินาทีต่อรอบ นอกจากนั้นเรดาร์ชนิดนี้ยังนิยมติดตั้งในเรือรบและอากาศยาน เช่น เรือรบ USS Lake Erie (CG-70) ซึ่งติดตั้งระบบเรดาร์ Spy-I ของบริษัท Lockheed Martin หรือเครื่องบิน E-3 Sentry: AWACs

2) เรดาร์เฝ้าตรวจ (Surveillance Radar)[331] เป็นเรดาร์ที่ใช้ตรวจการระยะไกลแต่มีระยะทำการสั้นกว่าเรดาร์แจ้งเตือนล่วงหน้านิยมใช้กับการตรวจจับเป้าหมายผิวน้ำมีการหมุนเสาสัญญาณ 5-10 วินาทีต่อ 1 รอบ

3) Target Acquisition Radar นิยมใช้ในหน่วยต่อสู้อากาศยานเพื่อตรวจจับเป้าหมายที่เข้ามาในดินแดนมีการหมุนไวมากทุก 1-2 วินาทีโดยระยะตรวจจับเป้าหมายจะสัมพันธ์กับระยะยิงไกลสุดของระบบอาวุธนั้นๆ

---

[329] Ibid., p. 117.

[330] John N. Briggs, Target Detection by Marine Radar, (London: The Institution of Electrical Engineers, 2004), pp. 39-40.

[331] Hamish Meikle, Modern Radar Systems, p. 615.

4) Fire Control Radar[332] เป็นเรดาร์ควบคุมระบบการยิงอาวุธมีหน้าที่ติดตามเป้าหมายและให้ข้อมูลกับระบบอาวุธโดยเฉพาะอย่างยิ่งระบบอาวุธนำวิถีในรูปแบบต่างๆ เรดาร์ชนิดนี้มักมีความละเอียดสูงและมีระยะการตรวจจับที่เหมาะสมต่อระยะยิง

5) Synthetic Aperture Radar[333] เป็นเรดาร์ซึ่งใช้สร้างภาพจำลองภูมิประเทศแบบคร่าวๆ สามารถจำแนกวัตถุที่เป็นโลหะและวัตถุที่เคลื่อนไหวได้ดี เป็นเรดาร์คลื่นสั้นความถี่สูงให้ภาพค่อนข้างละเอียดแต่ไม่เท่าภาพถ่าย

6) Air Intercept Radar or Multi-mode Fighter Radar หรือเรดาร์เครื่องบินขับไล่เดิมนั้นใช้ร่วมกับระบบยิงจรวดแบบอากาศสู่อากาศจากเครื่องบินขับไล่และมีการควบคุมการทำงานของเรดาร์ด้วยเจ้าหน้าที่อีกคนที่ไม่ใช่นักบินเช่นในเครื่องบิน F14 แต่ในปัจจุบันเครื่องบินสามารถประมวลผลได้เองทำให้เครื่องบินขับไลในปัจจุบันสามารถปฏิบัติภารกิจได้ทั้งการต่อสู้ทางอากาศ การโจมตีภาคพื้นและการลาดตระเวน เรดาร์ที่ติดตั้งในเครื่องบินขับไล่นั้นมักติดตั้งที่บริเวณส่วนหัวของเครื่องบินเรดาร์จึงต้องมีขนาดเล็ก

7) Missile Seeker Radar หรือเรดาร์ในจรวดนำวิถีนิยมใช้กับจรวดต่อต้านเรือผิวน้ำและจรวดนำวิถีแบบอากาศสู่อากาศเป็นเรดาร์ขนาดเล็กที่ติดตั้งบริเวณหัวจรวด มักตรวจจับเป้าหมายได้ในระยะใกล้[334] การต่อต้านระบบเรดาร์ทำได้ด้วยการลวง การรบกวนสัญญาณ กองทัพใดที่สามารถครอบครองพื้นที่ย่านความถี่ที่หลากหลายกว่าก็สามารถเลือกใช้ย่านความถี่ในการโจมตีได้มากกว่าทำให้ได้เปรียบในการทำสงคราม[335]

ระบบนำวิถีทำให้การใช้งานจรวดทำลายเป้าหมายสามารถทำได้ไกลขึ้น แม่นยำขึ้น ช่วยลดผลกระทบความเสียหายข้างเคียงที่อาจเกิดขึ้นกับพลเรือนได้ ทำให้เครื่องบินรบในปัจจุบันเช่นเครื่องบินรบ F15 ที่บรรจุจรวดทำลายเป้าหมาย 6 ลูกแบบนำวิถี สามารถทำลายเป้าหมายได้ 6 เป้าหมายอย่างแม่นยำ ระบบนำวิถีในปัจจุบันประกอบด้วยรูปแบบดังต่อไปนี้

---

[332] Ibid., p. 489.

[333] Ibid., p. 176.

[334] Rajatendu Das, “Advances in Active Radar Seeker Technology,” Defence Science Journal, Vol.55. No.3, (July 2005): 329. [online] accessed May 10, 2022. Available from: https://core.ac.uk/download/pdf/333720359.pdf,

[335] Ibid.

1) GOT – Go-onto-target (ระบบนำวิถีโดยการเข้าหาตัวเป้าหมายโดยตรง) ระบบ GOT จะทำงานได้ต่อเมื่อมีการตรวจพบวัตถุเป้าหมายก่อน และระบบนำวิถีจะพาจรวดทำลายเคลื่อนที่เข้าหาเป้าหมายดังกล่าว การนำวิถีรูปแบบนี้จะมีระบบตรวจจับเป้าหมายและติดตามตำแหน่งเป้าหมายตลอดเวลา สามารถทำการคำนวณเส้นทางการเข้าสู่เป้าหมายได้ตลอดเวลา ซึ่งระบบนำวิถีนี้อาจติดตั้งที่จรวดทำลายเป้าหมายหรือที่อุปกรณ์หรือแท่นยิงของผู้สั่งยิงก็ได้ ระบบนำวิถีแบบนี้ใช้ได้กับทั้งระบบอาวุธที่ยิงจากอากาศสู่อากาศ อากาศสู่พื้นดินและพื้นดินสู่อากาศ[336]

1.1) Remote control guidance[337] คือระบบการควบคุมจรวดทำลายเป้าหมายโดยผู้ควบคุมระยะไกล มนุษย์จึงเข้ามาเกี่ยวข้องกับระบบนำวิถีโดยการควบคุมการเดินทางของจรวด ผู้ควบคุมการยิงอาจอยู่ภาคพื้นดิน เรือ หรืออากาศยานก็ได้ การควบคุมอาจทำได้โดยการส่งสัญญาณผ่านคลื่นวิทยุหรือการส่งสัญญาณผ่านสาย ระบบอาวุธชนิดนี้จะไม่มีอุปกรณ์อิเล็กทรอนิกส์ที่ซับซ้อนติดตั้งที่จรวดเลย เพราะจะไม่มีการนำทางในตัวจรวดอีกแล้ว ทำให้มีพื้นที่มากขึ้นในการบรรจุหัวรบหรือบรรจุเชื้อเพลิง ทำให้จรวดเดินทางได้ไกลขึ้นหรือมีอำนาจทำลายมากขึ้น ในขณะที่ต้นทุนการผลิตไม่สูงจนเกินไป

รูปแบบของการยิงแบบ Remote Control เช่น จรวด Troll Missile ซึ่งเป็นจรวดนำวิถีติดตั้งในรถถังใช้ในการทำลายรถถังฝ่ายตรงข้าม จะเป็นการสั่งยิงจรวดผ่านสายสัญญาณ

ระบบ Remote Control Guidance ประกอบด้วยการทำงานระบบย่อยๆ 2 ระบบคือ Command Guidance[338] (ระบบนำวิถีแบบใช้สัญญาณควบคุม) ระบบนี้ผู้ควบคุมลูกจรวดจะทำการควบคุมจรวดตลอดเวลาที่จรวดพุ่งเข้าสู่เป้าหมาย ผู้ควบคุมจะทำหน้าที่ควบคุมทิศทางทั้งหมดของจรวดจนกว่าจะปฏิบัติการทำลายเป้าหมายสำเร็จผู้ควบคุมจะต้องติดตามเป้าหมายตลอดเวลาเพื่อให้รู้ตำแหน่ง ทิศทาง ความเร็วของเป้าหมายโดยทำงานร่วมกับเรดาร์และระบบ Command Guidance แบ่งเป็นระบบย่อย ตามการติดตามเป้าหมายและการบังคับลูกจรวด ได้แก่ Manual command to

---

[336] Research and Technology Organization, Technologies for Future Precision Strike Missile Systems, RTO Lecture series 221 bis, North Atlantic Treaty Organization, RTO-EN-018 AC/323 (SCI-087 bis) TP/37, (2000). pp. 5-2, 5-3. [online] accessed June 12, 2022. Available from: https://www.sto.nato.int/publications/STO%20Educational%20Notes/RTO-EN-013/EN-013-$$ALL.PDF,

[337] George M. Siouris, Missile Guidance and Control Systems, p. 615.

[338] George M. Siouris, Missile Guidance and Control Systems, p.163.

line of sight (MCLOS)[339] คือ การติดตามเป้าหมาย และการบังคับลูกจรวดทำโดยมนุษย์ Semi-Manual command to line of sight (SMCLOS) คือ การติดตามเป้าหมายทำโดยจรวด แต่การบังคับทิศทางจรวดทำโดยมนุษย์[340] Semi-Automatic command to line of sight (SACLOS) คือ การติดตามเป้าหมายทำโดยมนุษย์ แต่การบังคับทิศทางจรวดเป็นไปโดยอัตโนมัติ[341] และ Automatic command to line of sight (ACLOS) คือ การติดตามเป้าหมายและการบังคับจรวดเป็นไปโดยอัตโนมัติ[342]

การทำงานระบบ Command Guidance ประกอบด้วย เรดาร์ควบคุมการยิงจะทำหน้าที่ติดตามเป้าหมายและปรับปรุงข้อมูลตลอดเวลาก่อนจะส่งข้อมูลต่อไปยังระบบยิงจรวดและมีการยิงจรวดออกไปจากแท่นยิงขณะที่จรวดถูกยิงออกไปจะยังคงมีการสื่อสารระหว่างจรวดและส่วนประมวลผลที่แท่นยิงเพื่อควบคุมทิศทางในการไปสู่เป้าหมายโดยส่วนควบคุมจะต้องคำนวณและส่งข้อมูลไปยังจรวดเพื่อให้จรวดเดินทางไปด้วยความเร็วและทิศทางที่เหมาะสมกับเป้าหมายจนกว่าจรวดจะทำลายเป้าหมายสำเร็จ การควบคุมแบบนี้จึงต้องมีทั้งการติดตามเป้าหมาย การควบคุมทิศทางของจรวดและการส่งสัญญาณควบคุม

ตัวอย่างจรวดรูปแบบนี้เช่นจรวด S-75 (SA-2) เป็นจรวดดั้งเดิมในยุค 1960 มีการนำมาใช้ในการยิงเครื่องบินสอดแนม U-2 ของกองทัพสหรัฐอเมริกาในสถานการณ์ Cuba crisis โดยจรวด S-75 ใช้เรดาร์แบบ Fansong มีแท่นยิง 6 แท่นยิง เรดาร์หนึ่งตัวยิงได้เพียงครั้งละ 1 เป้าหมาย

---

[339] Ibid., pp.164-165.

[340] Muhammad Hanifudin Al Fadli, Dadang Gunawan, Romie Oktovianus Bura, and Larasmoyo Nugroho, “Design and Implementation of Anti-Tank Guided Missile (ATGM) Control System Using Semi-Automatic Command Line of Sight (SACLOS) Method Based on Digital Image Processing,” Jurnal Pertahanan, Vol. 7 No. 2 (2021): 218. [online] Accessed: January 20, 2022. Available from: https://www.academia.edu/59048238/Design_and_Implementation_of_Anti_Tank_Guided_Missile_Atgm_Control_System_Using_Semi_Automatic_Command_Line_of_Sight_Saclos_Method_Based_on_Digital_Image_Processing

[341] Ibid.

[342] Muhammad Hanifudin Al Fadli, Dadang Gunawan, Romie Oktovianus Bura, and Larasmoyo Nugroho, “Design and Implementation of Anti-Tank Guided Missile (ATGM) Control System Using Semi-Automatic Command Line of Sight (SACLOS) Method Based on Digital Image Processing,”: 218.

ขณะที่การยิงอาวุธแบบ Beam Riding[343] (ระบบนำวิถีแบบใช้คลื่นส่งสัญญาณ) เป็นระบบที่จรวดจะเดินทางตามลำคลื่นที่ส่องไปยังเป้าหมายโดยมีทั้งคลื่นเลเซอร์และคลื่นเรดาร์ จรวดจะมีระบบเซ็นเซอร์รับคลื่นอยู่ที่ท้ายของจรวดและมีอุปกรณ์คำนวณและบังคับทิศทางติดตั้งในจรวด การทำงานของระบบประกอบด้วยอุปกรณ์ควบคุมการยิงส่งคลื่นไปยังเป้าหมาย (การส่งคลื่นจะต้องกระทำตลอดเวลาปฏิบัติการณ์) หลังจากนั้นจรวดจะถูกยิงออกจากแท่นยิงและระบบประมวลผลในจรวดจะทำการวัดค่าตลอดเวลาว่าจรวดยังเดินทางอยู่ในคลื่นหรือไม่ ลูกจรวดจึงเดินทางในคลื่นตลอดเวลา

เดิมนั้นการส่งสัญญาณด้วยเรดาร์จะมีค่าความแม่นยำต่ำเพราะคลื่นช่วงปลายจะกว้างมาก ต่างจากคลื่นเลเซอร์ที่ปลายลำคลื่นไม่กว้างมากความแม่นยำจึงสูงกว่าจรวดในยุคที่ยิงผ่านเรดาร์ ได้แก่ RIM-8 Talos ปัจจุบันปลดประจำการแล้ว[344] ปัจจุบันจรวดที่ใช้การยิงด้วยเลเซอร์ ได้แก่ จรวด RBS-70 ซึ่งมีระยะทำการ 5 กิโลเมตร ผู้ยิงจะมี Optical ติดตามเป้าหมาย ใช้การควบคุมด้วยมือโดยมองผ่านกล้องตลอดเวลา สัญญาณเลเซอร์จะออกจากแท่นยิงไปยังเป้าหมาย ผู้ยิงจะต้องส่งเลเซอร์ไปที่เป้าหมายตลอดเวลาเพื่อให้จรวดเดินทางตามแสงเลเซอร์[345]

1.2) Homing guidance เป็นระบบการนำทางของจรวดทำลายเป้าหมายโดยการคำนวณเกิดขึ้นในอุปกรณ์ที่ติดตั้งในจรวดเอง ทำให้จรวดสามารถทำงานได้ด้วยตัวเอง โดยปกติจรวดสามารถทำลายเป้าหมายที่ไม่ไกลมากมักจะเป็นจรวดขนาดเล็กตั้งแต่ 10-30 เซนติเมตรแต่จะมีระบบประมวลผลทางคอมพิวเตอร์ติดตั้งอยู่ภายในเพื่อการควบคุมจรวด[346] ระบบ Homing Guidance แบ่งเป็นระบบย่อย 2 ระบบ คือ Semi-active homing และ Passive homing[347]

Semi-active homing ระบบอาวุธจะมองเห็นเป้าหมายจากสัญญาณสะท้อนที่มาจากผู้ทำการยิง จรวดจึงมีเพียงระบบรับสัญญาณเท่านั้น โดยคลื่นที่ผู้ยิงจรวดใช้จะต้องส่องไปที่เป้าหมาย

---

[343] George M. Siouris, Missile Guidance and Control Systems, p. 164.

[344] Ibid.

[345] Elizabeth Kirkham and Nneka Okechukwu, Controlling the Transfer of Man-Portable Air Defence Systems: A guide to Best Practice, (London: Saferworld, 2010), part 3, p. 6. [online] Accessed May 10, 2022. Available from: https://www.files.ethz.ch/isn/126449/MANPADS%20with%20footnotes%20REV.pdf, accessed May 10, 2022.

[346] Rafael Yanushevsky, Modern Missile Guidance, (London: CRC Press, 2008), p. 115.

[347] Ibid., p. 199.

ตลอดเวลาทำให้มีข้อดีคือจรวดเบาลงเพราะอุปกรณ์น้อย ราคาถูกแต่ข้อเสียคือผู้ยิงจรวดจะต้องบอกทิศทางตลอดเวลา[348]

การทำงานระบบ Semi-active homing ผู้ยิงจะต้องยิงสัญญาณ Illumination radar ไปยังเป้าหมายและติดตามเป้าหมายจนกว่าจรวดจะเดินทางถึงเป้าหมาย ในช่วงแรกที่ยิงจรวดออกไประบบนำวิถีจะยังไม่ทำงานเมื่อถึงระยะกลางจรวดจะต้องทำงานร่วมกับระบบนำวิถีอื่นๆ เมื่อจรวดเดินทางเข้าใกล้เป้าหมายในระยะ 10 ไมล์ทะเลหรือประมาณ 18 กิโลเมตร จรวดจะเริ่มทำงานตามระบบนำวิถีโดยภาครับสัญญาณที่ติดตั้งบนจรวดจะเริ่มทำการเพื่อทำการรับสัญญาณจาก Illumination radar แล้วประมวลผลเพื่อเดินทางเข้าสู่เป้าหมาย

ตัวอย่าง จรวดที่ใช้ระบบ Semi-active homing ได้แก่ R-27R/ER หรือ AA-11A/C จะมีส่วนหลังของ guidance action จะมีระบบคำนวณทิศทางและระบบนำวิถี[349]

Passive homing ระบบอาวุธจะมีเพียงภาครับสัญญาณเช่นเดียวกับระบบ Semi-active homing แต่จะใช้การรับสัญญาณที่เกิดจากการแพร่คลื่นของเป้าหมายเอง โดยปกติมักเป็นคลื่นความร้อน (IR Homing guidance) จากเครื่องยนต์ของเป้าหมาย หรือการติดตามเรดาร์ที่มักใช้ในระบบจรวดต่อต้านเรดาร์ (Passive Radar Homing, Anti-Radiation missile) จรวดแบบ Passive เรียกอีกแบบหนึ่งว่าแบบ fire and forget คือการเดินทางติดตามคลื่นตลอดเวลา ตราบเท่าที่มีการแพร่คลื่นของเป้าหมาย จรวดก็สามารถติดตามไปได้ ระบบติดตามในจรวดเรียกว่า Seeker[350]

ข้อดีคือหลังจากที่ยิงจรวดออกไปผู้ยิงไม่ต้องควบคุมอีกแล้ว เพราะจรวดจะติดตามเป้าหมายเอง แต่ก็มีข้อเสียที่ระบบนำวิถีแบบนี้จะมีระยะทำการสั้น และมีขอบเขตจำกัดในการทำงานขึ้นอยู่กับระยะที่ตรวจพบความร้อนและสภาพอากาศในขณะนั้น ตัวอย่างของจรวดเช่น AIM-9X side wider จะมี Seeker ลักษณะคล้ายกล้องดิจิทัลซึ่งทำให้จรวดมองเห็นภาพเป้าหมายเหมือนภาพจริง และสามารถติดตามเป้าหมายได้จากรังสีอินฟาเรดที่แผ่ออกมาจากเป้าหมาย ในขณะที่ระบบจรวดแบบเก่า AIM-9M จะมองเห็นเพียงจุดความร้อน และต้องใช้เทคนิคพิเศษประกอบการทำงานด้วย

---

[348] Ibid., p. 200.

[349] "R-27 (AA-10 Alamo) Guided Medium Range Air-To-Air Missile" Airforce Technology, December 9, 2020. [online] Accessed June 10, 2022. Available from: https://www.airforce-technology.com/projects/r-27-aa-10-alamo-guided-medium-range-air-missile/

[350] "R-27 (AA-10 Alamo) Guided Medium Range Air-To-Air Missile,"

3) Active homing[351] ระบบนี้จรวดจะมีทั้งภาคส่งสัญญาณและภาครับสัญญาณอยู่ในตัวจรวดเองมักเป็นแบบเรดาร์ เนื่องจากระบบนี้จรวดจะทำงานได้ด้วยตัวเองจึงไม่ต้องพึ่งพาการส่งสัญญาณจากผู้ยิง (Fire and forget) ระบบนี้ผู้ยิงสามารถใช้เรดาร์โหมด Track-while-scan ได้[352] ซึ่งสามารถทำการยิงเป้าหมายหลายเป้าหมายพร้อมกันได้และไม่ต้องระบุเป้าหมายเดียวตลอดเวลาทำให้ลดความเสี่ยงจากการถูกโจมตีด้วย ARM และสามารถต่อต้านสัญญาณรบกวนได้ โดยใช้เทคนิค Home-on jam[353] หรือการเปลี่ยนระบบการติดตามจากที่ติดตามจากสัญญาณเรดาร์เป็นการติดตามจากสัญญาณรบกวนที่ถูกส่งออกมาจากเป้าหมาย อย่างไรก็ดีทางเทคนิคระบบการรบกวนสัญญาณก็จะทำให้การโจมตีของจรวดไม่สามารถทำงานได้แม่นยำเช่นกัน ข้อเสียคือระบบนำวิถีแบบนี้มีราคาที่แพงมาก

ระบบการทำงาน Active homing เช่น จรวดสามารถติดตามเป้าหมายได้ 6 เป้าหมายพร้อมกัน และสามารถสั่งยิงได้พร้อมกัน โดยจรวดแต่ละลูกจะเดินทางไปตำแหน่งที่เป้าหมายอยู่ (Missile Link) ซึ่งจะแยกการทำงานแต่ละลูก โดยระบบนี้จะทำการเมื่อจรวดเข้าสู่เป้าหมายในระยะกลาง ดังนั้นก่อนหน้าที่จะเข้าสู่ระยะกลาง ผู้สั่งการยิงจะต้องควบคุมจรวด เมื่อถึงระยะที่กำหนด จรวดจะทำงานด้วยระบบเรดาร์ของตัวเองจนเข้าทำลายเป้าหมายสำเร็จ (จรวดส่งสัญญาณจากตัวเองไปกระทบเป้าหมายแล้วรับสัญญาณมาประมวลผลเพื่อเข้าสู่เป้าหมายได้เอง) ในระยะที่จรวดสามารถปฏิบัติการเองได้ ผู้สั่งการยิงสามารถหยุดระบบเรดาร์ของตนเองในการติดตามเป้าหมายเพื่อทำการหลบหนีได้ (Fire and forget) เช่น จรวด AIM-120 AMRAAM (US) เป็นจรวดที่นิยมของกองทัพอเมริกา ในขณะที่กองทัพรัสเซียก็จะมี R-77, RVV-AE (หรือชื่อ AA-12 ของ NATO)[354]

นอกจากนี้ยังมีระบบที่อยู่ระหว่าง Command Guidance และ Semi-active Homing คือ ระบบ Track-via-Missile ซึ่งเป็นการผสมทั้งสองระบบเข้าด้วยกันเนื่องจากระบบ Command Guidance ในจรวด SAM มีข้อจำกัดคือเป้าหมายในระยะไกลที่ลำคลื่นส่องชี้เป้าหมายกว้างออกทำให้ความแม่นยำในการทำลายเป้าหมายลดลง ซึ่งแนวทางในการแก้ไขปัญหาทำโดยเพิ่มขนาดจรวดให้

---

[351] Rafael Yanushevsky, Modern Missile Guidance, p. 197.

[352] James Constant, Fundamentals of Strategic Weapons: Offense and Defense Systems, (Amsterdam: Martinus Nijhoff Publishers, 1981), p.193.

[353] Chi-Hao Cheng and James Tsui, An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques. (London: River Publishers, 2021), p. 47.

[354] Rafael Yanushevsky, Modern Missile Guidance, p. 197.

ใหญ่ขึ้น เพิ่มอำนาจทำลายมากขึ้นโดยไม่ต้องกระทบเป้าหมายโดยตรงแต่อาศัยแรงระเบิดลายเป้าหมาย จรวดก็จะหนักมากซึ่งข้อจำกัดนี้แก้ไขโดยระบบ SARH[355]

อย่างไรก็ดี SARH ก็มีข้อจำกัดเมื่อนำมาใช้งานกับจรวด SAM เนื่องจากจรวด SAM รุ่นเก่าใช้เทคโนโลยี Conical Scanning ซึ่งจะมีจานรับสัญญาณหมุนตลอดเวลาใช้ Illumination Radar ส่งสัญญาณแบบต่อเนื่อง (Continuous wave) ระบบนี้จะมีปัญหาเมื่อพบการรบกวนสัญญาณ (ECM) และจรวดจะไม่แม่นยำเท่าจรวดที่ยิงแบบ Pulse Radar จากแท่นยิง[356]

ระบบ TVM จะทำงานได้ในระยะไกลและมีความแม่นยำมากกว่าระบบ Command guidance ระบบการทำงานจะเป็นการส่งสัญญาณจากจรวดมาที่ภาคพื้นดินเพื่อมีการเปรียบเทียบค่าเป้าหมายตลอดเวลา ทำให้จรวดสามารถต่อต้านระบบรบกวนได้ดีขึ้น

TVM ทำงานโดยเรดาร์ติดตามเป้าหมายเพื่อให้ทราบระยะห่าง ความสูง ทิศทางและความเร็วโดยระบบ SAM สมัยใหม่ที่ติดตั้งใน Patriot หรือ S-400 ก็สามารถติดตามได้หลายเป้าหมาย (track-while-scan) ได้ด้วย เมื่อเรดาร์ตรวจพบว่าเป้าหมายเข้ามาในระยะยิงแท่นยิงจะประมวลผลและสั่งการจรวดยิงออกไป ในระยะแรกแท่นยิงจะสื่อสารให้จรวดเดินทางไปตามทิศทางที่เป้าหมายเคลื่อนที่ผ่าน data link โดยระบบนำวิถีจะยังไม่ทำงานเป็นรูปแบบเดียวกันกับระบบ Command guidance แต่เมื่อจรวดเดินทางถึงระยะที่สามารถได้ จรวดจะเปิด Seeker เพื่อทำงาน ทำให้การทำงานคล้ายระบบ Semi-active radar homing เมื่อจรวดได้รับสัญญาณสะท้อนกลับจะส่งข้อมูลกลับไปยังผู้ทำการยิง ซึ่งผู้ทำการยิงก็จะประเมินผลจากค่าที่ได้รับจากจรวดอีกครั้ง แล้วเปรียบเทียบกับค่าที่ผู้ยิงใช้เรดาร์ติดตามด้วยตัวเอง ทำให้รู้ค่าความคลาดเคลื่อนและรู้ว่ามีการรบกวนสัญญาณเกิดขึ้นหรือไม่ และผู้ยิงจะทำการแก้ไขค่าให้ถูกต้องและส่งข้อมูลดังกล่าวกลับไปที่ data link อีกครั้งหนึ่ง เพื่อให้จรวดทราบว่าตัวเองจะเดินทางไปทิศทางใด โดยจรวดแต่ละลูกจะมีระบบคำนวณเส้นทางของตัวเอง ทำให้ระบบนำวิถีแบบนี้มีความซับซ้อนสูง ระบบนำวิถีแบบ CVM ปรากฏในจรวด S-400 ของกองทัพรัสเซียและจรวด PAC-2 Patriot ของกองทัพสหรัฐอเมริกา (แต่ใน PAC-3 จะใช้ระบบ Active homing แล้ว)[357]

---

[355] George M. Siouris, Missile Guidance and Control Systems, p. 164.

[356] Ibid.

[357] Rafael Yanushevsky, Modern Missile Guidance, p. 197.

2) GOLIS – go onto location in space[358] (ระบบนำวิถีโดยการเข้าพื้นที่ที่เป้าหมายอยู่)

เป็นระบบที่จรวดเดินทางไปยังพื้นที่ที่เป้าหมายตั้งอยู่เป็นระบบนำวิถีแรกๆ ที่มนุษย์สร้างขึ้นมา ไม่มีการนำวิถีสู่เป้าหมายเฉพาะเจาะจงแต่ระบบอาวุธจะทำได้เพียงเคลื่อนที่ไปยังเป้าหมายที่กำหนดเอาไว้ ระบบนี้จึงมีความแม่นยำต่ำไม่สามารถติดตามเป้าหมายเคลื่อนที่ได้ ใช้ได้กับเป้าหมายนิ่งและการโจมตีอาวุธที่มีอานุภาพทำลายล้างสูง GOLIS สามารถทำงานได้แม้ไม่ทราบว่าวัตถุเป้าหมายคือสิ่งใดแต่ระบบนำวิถีจะพาอาวุธไปสู่พื้นที่ที่เป้าหมายอยู่ ระบบนำวิถีแบบนี้จะใช้งานกับภารกิจที่ไม่ต้องการความแม่นยำมากนั้นเช่น การนำวิถีช่วงกลาง (Mid-course) ที่ต้องการให้จรวดเข้าไปในพื้นเป้าหมายแบบคร่าวๆ ก่อนเปิดระบบนำวิถีเต็มรูปแบบเมื่อถึงระยะทำการ GOLIS มีระบบย่อยๆ ได้แก่

2.1) Inertial Guidance System (INS) ระบบนำวิถีด้วยแรงเฉื่อยของจรวดเองวัดค่าว่ากำลังเดินทางไปทางไหน[359] การวัดค่าความเฉื่อยทำได้โดยอุปกรณ์ Gyroscope และจะมีการประมวลผลกับระบบภายในจรวดเพื่อบอกว่าจรวดเดินทางไปทิศทางไหน ด้วยความเร็วเท่าไร เดิม Gyroscope มีขนาดใหญ่มากจึงติดตั้งไม่ได้ในจรวดขนาดเล็กแต่ปัจจุบันมีการพัฒนามาใช้ Laser Gyroscope และ Fiber-optic Gyroscope

ระบบ INS จะมีความคลาดเคลื่อนเมื่อใช้งานไปในระยะหนึ่ง เนื่องจากเป็นการประมวลผลในระบบของตัวเอง ยิ่งจรวดเดินทางไกลเท่าไรความคลาดเคลื่อนก็อาจเกิดขึ้นได้มากเท่านั้น ปัจจุบันจึงมีการใช้งาน INS ร่วมกับระบบ GPS ทำให้เกิดความแม่นยำสูงขึ้นและมีความคลาดเคลื่อนลดลง (ระดับเป็นเมตร)

2.2) Astro-Inertial guidance System ระบบนำวิถีด้วยแรงเฉื่อยและแสงดวงดาว เป็นระบบที่รวมระบบ INS มารวมกับระบบนำวิถีแบบแสงดาว (Celestial Navigation) หรือในอีกชื่อ

---

[358] Gulick, J. F., and J. S. Miller, Missile Guidance: Interferometer Homing Using Body Fixed Antennas. Technical Memorandum TG1331 (TSC-W36-37), (Maryland: Johns Hopkins University Applied Physics Laboratory, 1982), p.101.

[359] Paul Zarchan, Tactical and Strategic Missile Guidance (6th ed.). (Reston, VA: American Institute of Aeronautics and Astronautics, 2012), p. 12.

หนึ่งว่า Stellar-Inertial Navigation เป็นระบบนำวิถีที่นิยมใช้กับเรือดำน้ำ (Submarine Launch Ballistic Missile: SLBM)[360]

Astro-Inertial guidance System ถูกพัฒน่าขึ้นเพื่อใช้กับ Ballistic Missile แบบยิงข้ามทวีป ที่จะต้องยิงขีปนาวุธออกไปนอกชั้นบรรยากาศก่อนที่ขีปนาวุธจะตกกลับมาสู่เป้าหมายในพื้นโลก ระบบการนำวิถีแบบปกติจึงไม่สามารถใช้ได้[361]

ปกติขีปนาวุธจากพื้นดินสู่พื้นดินโดยทั่วไปอาจใช้ระบบนำวิถีแบบ INS ก็เพียงพอแต่เรือดำน้ำนั้นมีการเคลื่อนที่ใต้น้ำกลางทะเลตลอดเวลาจึงเป็นการยากที่จะกำหนดค่าเป้าหมายที่ชัดเจนก่อนการยิง การวัดค่าตำแหน่งด้วยแสงของดวงดาวจะเป็นประโยชน์ต่อการคำนวณความคลาดเคลื่อนของ INS ซึ่งจรวดต้องเดินทางด้วยความเร็วสูงและเดินทางออกไปนอกชั้นบรรยากาศโลก[362]

กองทัพสหรัฐอเมริกาได้เคยมีการทดลองใช้ขีปนาวุธ Trident ซึ่งมีระบบการทำงานร่วมกันระหว่าง GPS และ INS แต่กลับปรากฏผลว่าอาจไม่สามารถใช้ได้ในปฏิบัติการจริง

ระบบ Astro-Inertial guidance System ถูกติดตั้งในเครื่องบินรบเช่นกัน ตัวอย่างของเครื่องบินที่มีการติดตั้งอาวุธระบบนำวิถีนี้ได้แก่ SR-71 Blackbird ของกองทัพสหรัฐอเมริกา นอกจากนั้น ในเครื่องบิน B-2 ของกองทัพสหรัฐอเมริกายังมีการติดตั้งระบบ Astro-Inertial guidance System ไว้เพื่อเป็นระบบสำรองในกรณีที่ระบบ GPS ไม่สามารถทำงานได้

2.3) Terrain Contour Matching (TERCOM)[363] ระบบนำวิถีด้วยการเปรียบเทียบสภาพภูมิประเทศกับข้อมูลที่จรวดมีอยู่ นิยมใช้งานในระบบจรวดร่อน (Cruise Missile) ส่วนประกอบสำคัญของระบบนำวิถีแบบนี้คือเรดาร์วัดความสูง แผนที่ภูมิประเทศแบบดิจิทัลที่จะบันทึกในหน่วยความจำของจรวด และระบบคอมพิวเตอร์ควบคุมและประมวลผล จรวดร่อนที่ทำงานโดยองค์ประกอบพื้นฐานทั้งสามประการที่กล่าวมาสามารถเดินทางในเพดานบินต่ำได้โดยปราศจากการควบคุมโดยมนุษย์

---

[360] Paul Zarchan, Tactical and Strategic Missile Guidance, p. 12.

[361] Ibid.

[362] Ibid.

[363] Ibid.

การทำงานของระบบ Terrain Contour Matching คือการที่จรวดเดินทางไปในอากาศและจะมีการบันทึกค่าความสูงของตัวเองจากระดับพื้นที่ซึ่งจรวดเดินทางผ่าน และระบบ Matching จะนำเอาค่าความสูงนั้นมาเปรียบเทียบกับค่าความสูงในแผนที่ดิจิทัลซึ่งบันทึกไว้ในหน่วยความจำของจรวด และจะมีการประมวลผลค่าความสูงนี้เพื่อให้จรวดเดินทางไปตามทิศทางที่มีการกำหนดไว้เพื่อเข้าสู่พื้นที่เป้าหมาย การเคลื่อนที่โดยการเปรียบเทียบค่าความสูงของเรดาร์กับแผนที่ดิจิทัลในหน่วยความจำแบบ Terrain Contour Matching มีจุดเด่นคือระบบจรวดนำวิถีรูปแบบนี้จะเคลื่อนที่ผ่านภูมิประเทศที่เป็นภูเขา ซอกเขา หรือหุบเขาต่างๆ ได้ดี โดยไม่ต้องบินในเพดานบินที่สูงและสามารถลัดเลาะไปตามซอกเขาได้ก่อนเข้าสู่พื้นที่เป้าหมาย[364] อย่างไรก็ดีระบบ Terrain Contour Matching ก็มีจุดอ่อนที่การเปรียบเทียบความสูงจากเรดาร์ของจรวดกับแผนที่ดิจิทัลมีความละเอียดน้อย จึงนำมาสู่การพัฒนาระบบใหม่ที่ชื่อว่า Digital Scene Matching Area Correlator: DSMAC ระบบนี้ทำงานบนพื้นฐานของ TERCOM แต่มีการเพิ่มกล้องดิจิทัลที่ตัวจรวดเพื่อให้มีการบันทึกภาพจริงของภูมิประเทศและนำข้อมูลมาเปรียบเทียบกับภาพแผนที่ดิจิทัลในระบบประมวลผลของจรวด ทำให้ได้ข้อมูลที่ละเอียดมากกว่าการเปรียบเทียบด้วยความสูงเพียงประการเดียว นอกจากนั้น DSMAC สามารถใช้งานร่วมกับระบบ INS และ GPS เพื่อให้เกิดการระบุพิกัดที่แม่นยำได้มากขึ้น ในปัจจุบันระบบนำวิถีแบบ TERCOM นี้มีการทำงานร่วมกับปัญญาประดิษฐ์ที่ใช้ในการประมวลผลการเลือกเส้นทางที่เหมาะสมในการเข้าหาเป้าหมายด้วย การประมวลผลด้วยปัญญาประดิษฐ์นี้จะมีการใช้ข้อมูลความสูงจากระบบ TERCOM เปรียบเทียบกับภาพถ่ายดาวเทียมของภูมิประเทศเพื่อคำนวณเส้นทางที่เหมาะสมในการเข้าหาเป้าหมาย[365]

ระบบนำวิถีแบบ TERCOM มีการใช้งานครั้งแรกกับจรวดนำวิถี Tomahawk (Tomahawk Land Attack Missile: TLAM) ในสงครามอ่าวเปอร์เซียครั้งที่ 1 ใน ค.ศ.1991[366]

ระบบการทำงานของ TERCOM ในจรวด Tomahawk จะต้องมีการบันทึกภาพถ่ายดาวเทียมของภูมิประเทศเป้าหมายทั้งหมดก่อนแปลงเป็นภาพภูมิประเทศแบบดิจิทัลเพื่อให้จรวดสามารถ

---

[364] Paul Zarchan, Tactical and Strategic Missile Guidance, p. 12.

[365] Ibid.

[366] Ibid.

เปรียบเทียบค่าความสูงที่อยู่ในแผนที่กับค่าความสูงที่จรวดวัดได้ในทุกๆ วินาทีตลอดการเดินทาง ทำให้จรวดรู้เส้นทางเข้าสู่เป้าหมายที่ถูกต้องสามารถลัดเลาะตามเส้นทางต่างๆ ได้ในเพดานบินต่ำ[367]

ในการทำงานของระบบนำวิถีทั้งในการโจมตีและการป้องกันภัยทางอากาศนั้นมีการพัฒนามากขึ้นในปัจจุบันโดยมีการนำเอาการประมวลผลแบบอัลกอริทึ่มและลักษณะการทำงานของปัญญาประดิษฐ์มาเกี่ยวข้องมากขึ้น จึงต้องมีการพิจารณาความเกี่ยวข้องของปัญญาประดิษฐ์ การประมวลผลแบบอัลกอริทึ่มและการทำงานของระบบอาวุธดังนี้

การทำงานของปัญญาประดิษฐ์หรือ Artificial Intelligence; AI ทำหน้าที่เป็น “สมองเทียม” ให้กับคอมพิวเตอร์หรือหน่วยประมวลผลของคอมพิวเตอร์อยู่ในรูปแบบโปรแกรมคอมพิวเตอร์ที่สร้างขึ้นมาเพื่อให้คิด เรียนรู้ วิเคราะห์ แยกแยะ จำแนก ประมวลผลไปจนถึงระดับการตัดสินใจด้วยตัวเองได้และเป็นส่วนสำคัญในระบบอาวุธอิสระ[368]

อย่างไรก็ดีมีการให้นิยามปัญญาประดิษฐ์ที่ค่อนข้างหลากหลายขึ้นอยู่กับมุมมองของผู้ที่เกี่ยวข้องในแต่ละศาสตร์ เช่น วิทยาศาสตร์คอมพิวเตอร์อาจมองว่าปัญญาประดิษฐ์มีความหมายเฉพาะที่แตกต่างจากการบริหารการตลาด ในขณะที่บางครั้งในศาสตร์เดียวกันก็อาจมีความเข้าใจที่แตกต่างกันก็ได้ โดยทางการตลาดอาจตั้งชื่อปัญญาประดิษฐ์ตามสิ่งที่คาดว่าจะก่อให้เกิดผลทางการตลาด คำว่าปัญญาประดิษฐ์จึงเกิดขึ้นในนวัตกรรมหลายเรื่องซึ่งจะส่งผลให้ผู้บริโภคตัดสินใจซื้อสินค้าหรือบริการนั้น ในขณะที่วิทยาศาสตร์คอมพิวเตอร์อาจนิยามปัญญาประดิษฐ์ถึงสิ่งที่มีความซับซ้อนในการประมวลผล เช่น เครื่องคิดเลขสามารถประมวลผลได้ แต่ก็ไม่มีใครเรียกว่าปัญญาประดิษฐ์ ในขณะที่โปรแกรมประมวลผลทางการตลาดอาจมีการวิเคราะห์ข้อมูลที่ซับซ้อนกว่าสามารถแสดงผลความสัมพันธ์ต่างๆ ที่ดีกว่า จะเรียกว่าปัญญาประดิษฐ์ได้หรือไม่ หรือกรณีประตูเลื่อนอัตโนมัติเราไม่เรียกว่าปัญญาประดิษฐ์แต่ถ้าประตูจำหน้าคนได้จะเป็นปัญญาประดิษฐ์ได้หรือไม่

---

[367] Paul Zarchan, Tactical and Strategic Missile Guidance, p. 12.

[368] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,” SN Computer Science, Vol. 2. (2021): 425. [online] accessed July 20, 2022. Available from: https://www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview,

แล้วหากประตูสามารถสื่อสารกับคนเพื่อให้ระบุตัวตนก่อนเข้าจะเป็นปัญญาประดิษฐ์หรือไม่[369] เป็นต้น

ระบบที่น่าจะเรียกว่าเป็นปัญญาประดิษฐ์ควรจะหมายถึงการรู้จัก (recognize) ไม่ใช่การจดจำ (memorize) เช่น ระบบการพิสูจน์ด้วย Password ต้องใส่รหัสที่ถูกต้องจึงจะเข้าสู่ระบบได้ เครื่องคอมพิวเตอร์จึงทำเพียงการ Memorize ในขณะที่การจดจำลายนิ้วมือเพื่อการเข้าสู่ระบบไม่สามารถกำหนดตำแหน่งลายนิ้วมือที่เที่ยงตรงเสมอได้ โปรแกรมคอมพิวเตอร์จึงต้องจดจำลายนิ้วมือในตำแหน่งต่างๆ เพื่อนำมาใช้ในการประมวลผล โดยจะต้องมีการเปรียบเทียบกับชุดข้อมูลลายนิ้วมือที่มีอยู่ และจะต้องมีเกณฑ์การเปรียบเทียบว่าความน่าเชื่อมั่นมีมากน้อยเพียงใดเพื่อยืนยันตัวตนที่ตรงกับข้อมูลที่มีอยู่ การจดจำแบบนี้เรียกว่า recognition เป็นลักษณะของการรู้จัก การรู้จักเป็นกลไกสำคัญของ Machine Learning ซึ่งจะทำให้เครื่องจักรทำงานได้[370]

ระบบปัญญาประดิษฐ์ซึ่งเป็นที่ยอมรับในยุคแรกคือเกมส์คอมพิวเตอร์ เพราะเกมส์มีสาระสำคัญอยู่ที่การแข่งขันและการแข่งขันนั้นหากไม่ทำระหว่างผู้เล่นที่เป็นคนด้วยกันก็จะต้องเป็นการแข่งขันระหว่างคนกับ Bot หรือโปรแกรมเกมส์นั้น Bot หรือโปรแกรมเกมส์จึงต้องมีความสามารถในการคิดและรู้จักการแก้ไขปัญหาเฉพาะหน้าเมื่อต้องแข่งขันกับมนุษย์

อย่างไรก็ดีแม้ Bot เกมส์จะเป็นที่มาของปัญญาประดิษฐ์แต่หากพิจารณารายละเอียดของเกมส์แต่ละชนิดอาจพบว่าไม่ถูกต้องเสมอไปที่จะกล่าวเช่นนั้น เนื่องจากในการเขียนโปรแกรมคอมพิวเตอร์จะต้องมีการสร้างเงื่อนไข If, Then, Else, Else if เป็นพื้นฐาน เช่น หากเซ็นเซอร์พบวัตถุเข้าใกล้ในระยะ 3 เมตร ให้ประตูเปิด เมื่อผ่านไป 5 วินาทีให้ปิดประตู หรือหากเซ็นเซอร์ตรวจพบสิ่งขีดขวางการปิดประตูก็ให้ทำการเปิดอีกครั้ง เป็นต้น การทำงานของโปรแกรมคอมพิวเตอร์พื้นฐานนี้จึงไม่มีการวิเคราะห์ที่ซับซ้อนแบบที่ปัญญาประดิษฐ์ควรจะเป็น ในกรณีเกมส์คอมพิวเตอร์บางเกมส์ก็ทำงานในรูปแบบการทำตามกฎที่ผู้เขียนโปรแกรมกำหนดเอาไว้ ไม่ต้องมีการใช้สติปัญญาเพื่อคิดทำงานในสถานการณ์ที่หลากหลายมากกว่าที่ผู้เขียนโปรแกรมกำหนดไว้ ระบบการทำงานตามเงื่อนไขนี้เป็นลักษณะการทำงานทั่วไปแบบอัตโนมัติ (Automation) เพื่อให้เครื่องจักรทำงานแทนคนเท่านั้น

[369] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,” p. 425.

[370] Ibid., p. 426-427.

การที่เราต้องโปรแกรมให้ระบบรู้ทุกเรื่องที่เราต้องการและทำงานตามที่เราสั่งเท่านั้นไม่น่าจะเรียกว่าระบบปัญญาประดิษฐ์[371]

เป้าหมายสำคัญของการสร้างปัญญาประดิษฐ์ไม่ใช่การทำอะไร เมื่อไร แต่หมายถึงการบรรลุเป้าหมายอะไร สิ่งสำคัญไม่ใช่วิธีการแต่เป็นผลลัพธ์ ปัญญาประดิษฐ์จึงต้องรู้จักวิธีการที่ดีที่สุดและเลือกวิธีการที่ดีที่สุดเพื่อปฏิบัติภารกิจด้วยตัวเอง[372] การจะทำให้ปัญญาประดิษฐ์ทำงานสำเร็จได้จำต้องอาศัยการทำงานของอัลกอริทึมซึ่งจะเป็นขั้นตอนที่ปัญญาประดิษฐ์ใช้เพื่อการวิเคราะห์ อนุมานข้อมูลเพื่อนำไปสู่ผลลัพธ์และสร้างทางเลือกสู่เป้าหมาย การทำงานของปัญญาประดิษฐ์ที่ประสบผลสำเร็จจึงหมายถึงปัญญาประดิษฐ์จะต้องทำงานด้วยความซับซ้อนพบทางเลือกที่ไม่จำกัด ทางเลือกที่ดีที่สุดไม่แน่นอนขึ้นอยู่กับสถานการณ์และสภาพแวดล้อมที่อาจเปลี่ยนแปลงตลอดเวลา เช่น เกมส์หมากล้อมซึ่งมีทางเลือกมากมายในการเดินหมาก การเขียนโปรแกรมคอมพิวเตอร์เกมส์หมากล้อมจึงอาศัยการทำงานตามเงื่อนไขแต่เพียงอย่างเดียวไม่ได้ แต่ต้องอาศัยการเรียนรู้ของโปรแกรม ทั้งการเรียนจากการลองผิดลองถูกแล้วจดจำ และการสร้างสถานการณ์จำลอง (Simulating) เพื่อสร้างปัญหา สร้างทางเลือกและค้นหาวิธีการที่ดีที่สุดด้วยตัวเองโดยไม่ต้องมีการเรียนรู้และจดจำผ่านสถานการณ์จริง[373]

ในแอพลิเคชั่นที่ไม่ซับซ้อนมากเช่นระบบการให้คำแนะนำ การวินิจฉัย การประมาณค่า อาจมีการสร้างโมเดลจากข้อมูลจำนวนมากแล้วทำการวิเคราะห์ข้อมูลที่มีเพื่อการตัดสินใจแต่ไม่ได้มีการเรียนรู้อะไรใหม่จึงไม่เป็นระบบปัญญาประดิษฐ์[374] ปัญญาประดิษฐ์ในความหมายทั่วไปอาจหมายถึงความสามารถของคอมพิวเตอร์ทางระบบดิจิทัลหรือความสามารถของหุ่นยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์ในการปฏิบัติภารกิจซึ่งโดยทั่วไปจะต้องใช้สติปัญญา[375]

ขณะที่ OECD มีการให้คำจำกัดความว่าปัญญาประดิษฐ์คือระบบที่ใช้เครื่องจักรที่สามารถทำการคาดการณ์หรือตัดสินใจที่มีอิทธิพลต่อสภาพแวดล้อมจริงหรือเสมือนตามชุดของวัตถุประสงค์ที่กำหนดไว้โดยมนุษย์โดยใช้เครื่องและ/หรือมนุษย์ในการนำเข้าวัตถุดิบหรือข้อมูล (input) เพื่อ (1)

---

[371] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,” SN Computer Science, Vol. 2. (2021): 425-427.

[372] Ibid., p. 428.

[373] Ibid.

[374] Ibid., p. 425.

[375] Ibid.

รับรู้สภาพแวดล้อมจริงและ/หรือเสมือน (2) สกัดและตกผลึกการรับรู้ดังกล่าวเป็นแบบจำลองต่างๆ ผ่านการวิเคราะห์ในลักษณะอัตโนมัติ (3) ใช้การอนุมานหรือการคาดคะเนตามหลักเหตุผลด้วยแบบจำลอง (Model Inference) เพื่อกำหนดตัวเลือกสำหรับข้อมูลหรือการกระทำโดยระบบปัญญาประดิษฐ์รูปแบบต่างๆ จะได้รับการออกแบบให้ทำงานด้วยระดับความเป็นอิสระที่แตกต่างกัน [376]

ปัญญาประดิษฐ์มีส่วนย่อยที่เกี่ยวข้อง ได้แก่ Big Data ซึ่งเป็นระบบจัดเก็บข้อมูลก่อนนำไปทำการวิเคราะห์ Machine Learning หรือการเรียนรู้ของโปรแกรมคอมพิวเตอร์เพื่อจัดเก็บข้อมูลและเพื่อประมวลผล Robot เป็น Hardware ที่ทำงานโดยอาศัยการประมวลผลจากซอฟท์แวร์ Image Processing การประมวลผลสัญญาณภาพให้คอมพิวเตอร์มองเห็นได้ด้วยตัวเองและเก็บข้อมูลภาพดังกล่าวเพื่อประมวลผล Signal Processing หรือการประมวลผลสัญญาณ[377] เช่น การประเมินคลื่นไฟฟ้าหัวใจ คลื่นสมองเพื่อพิจารณารูปแบบสัญญาณต่างๆ เป็นต้น

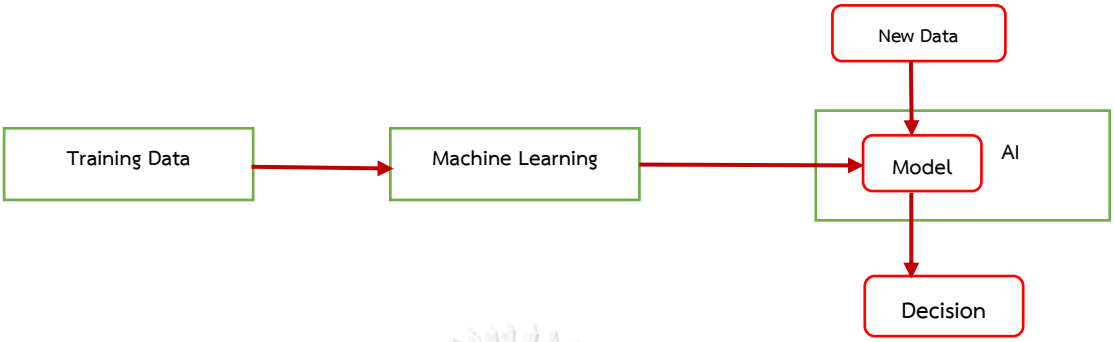
ขณะที่ส่วนประกอบสำคัญในการทำงานของปัญญาประดิษฐ์คืออัลกอริทึ่ม อัลกอริทึ่มเป็นขั้นตอนวิธี รายละเอียดการวิเคราะห์ด้วยการประมวลผลของคอมพิวเตอร์ เช่น หากเราอยากรู้ว่าวันนี้มีโอกาสที่ฝนจะตกมากเพียงใด เราก็ต้องมีข้อมูลที่แน่นอนจำนวนมากของโอกาสที่ฝนตกและโอกาสที่ฝนไม่ตกรวมตลอดถึงเงื่อนไขต่างๆ ที่เกี่ยวข้องกับสถานการณ์ฝนตกและสามารถคำนวณความน่าจะเป็นโดยการจำแนกข้อมูลเหล่านั้นเพื่อนำไปสู่คำตอบที่ดีที่สุดได้โดยจะต้องมีการวิเคราะห์และการอนุมานที่สอดคล้องกับแอพพลิเคชั่นที่เราต้องการใช้งานด้วย

---

[376] OECD, “Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO),” OECD Economy Digital Papers, No. 291, (November 2019): 7. Accessed: January 15, 2023. Available from: https://www.oecd-ilibrary.org/docserver/d62f618a-en.pdf?expires=1679043632&id=id&accname=guest&checksum=AB4 8031E1C037FAD29746BB78DC284D9, และ พีรพัฒ โชคสุวัฒนสกุลและคณะ, *Thailand Artificial Intelligence Guidelines* 0.1: แนวปฏิบัติเกี่ยวกับมาตรฐานการใช้ปัญญาประดิษฐ์ (กรุงเทพ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2565). หน้า 32. [online] accessed 15 มกราคม 2566. Available from: https://www.law.chula.ac.th/wp-content/uploads/2023/03/TAIG-20230222.pdf

[377] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

กลไกในทำงานของปัญญาประดิษฐ์อาจแสดงได้เป็นรูปแบบดังต่อไปนี้



ภาพการทำงานของปัญญาประดิษฐ์

การสร้างโมเดลอาจเขียนครั้งเดียวเพื่อรวบรวมข้อมูลมาใช้ในการวิเคราะห์และประมวลผล หรืออาจมีการแก้ไขหลายครั้งเพื่อแก้ไขการทำงานของปัญญาประดิษฐ์ก็ได้ โมเดลถือว่าเป็นสิ่งที่ทำให้เกิดการวิเคราะห์และการตัดสินใจ

การใช้โมเดลมีผลเป็นอย่างมากในการประมวลผลและตัดสินใจที่รวดเร็วขึ้น เพราะไม่ต้องนำข้อมูลจำนวนมากมาวิเคราะห์แต่สามารถเลือกโมเดลที่เหมาะสมมาใช้ในการตัดสินใจได้เอง

ปัญญาประดิษฐ์เป็นสิ่งที่กล่าวถึงมากขึ้นในยุคปัจจุบันเพราะปัจจัยอย่างน้อย 3 ประการ คือ

1) ประสิทธิภาพในการประมวลผลดีขึ้นจากการที่ปัจจุบันอุปกรณ์อิเล็กทรอนิกส์ที่สามารถประมวลผลซับซ้อนได้มีมากขึ้น เช่น โทรศัพท์มือถือสามารถทำการประมวลผลได้หลายแอพลิเคชั่นที่ซับซ้อนขึ้น[378]

2) Big Data หรือการจัดเก็บข้อมูลมีพื้นที่มหาศาล[379] เช่น การโฆษณาร้านค้าในปัจจุบันในระบบออนไลน์ผู้ให้บริการสามารถค้นหาข้อมูลความต้องการของลูกค้าแต่ละรายจากสถิติการค้นหา wish list และพฤติกรรมของลูกค้า เพื่อนำเสนอสินค้าสู่ลูกค้าโดยตรงได้ ในอนาคตเชื่อว่าปัญญาประดิษฐ์จะสามารถนำมาติดตั้งในชั้นขายของปกติได้ด้วย

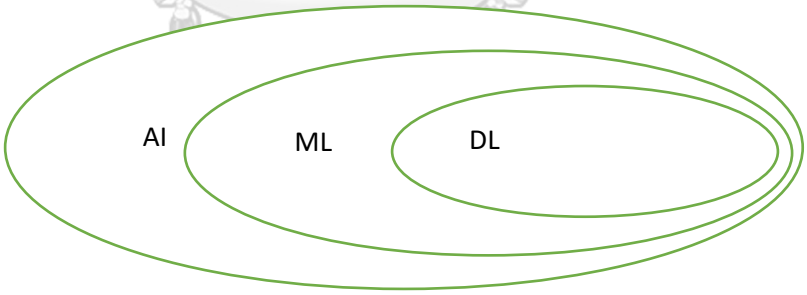
[378] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

[379] Ibid.

3) Deep Learning ข้อมูลในระบบอินเทอร์เน็ตสามารถจัดเก็บข้อมูลเชิงพฤติกรรมของบุคคลได้ และสามารถนำข้อมูลเหล่านี้ไปสอนปัญญาประดิษฐ์ได้ ปัจจุบันไปถึง Unstructured data ซึ่งเก็บจากเซ็นเซอร์ แผนที่ ฯลฯ ทำให้ปัญญาประดิษฐ์มีความสามารถเก็บข้อมูลที่หลากหลายได้มากขึ้น[380]

ปัญญาประดิษฐ์ที่สามารถนำมาใช้งานได้จริงในปัจจุบันคือระบบ Autonomous car และ Object Detection โดยสร้างเป็น Autonomous Drone เพื่อล่า Rogue Drone คือโดรนต่อต้านโดรนบุกรุก

การทำงานของปัญญาประดิษฐ์นั้นมีการทำงานของ Artificial Neural Network (เป็นส่วนหนึ่งของระบบ Machine Learning) ปัญญาประดิษฐ์ที่ไม่มี Machine Learning ก็จะไม่สามารถทำงานได้ ในขณะที่ Machine Learning ที่ไม่ได้ถูกใช้งานในปัญญาประดิษฐ์ก็ไม่มีประโยชน์ในการทำงาน ส่วน Deep Learning เป็นส่วนย่อยของ Machine Learning โดย Deep Learning ใช้ระบบ Neural Network ในการเรียนรู้ ซึ่งอาจแสดงความสัมพันธ์ระหว่างปัญญาประดิษฐ์กับ Machine Learning และ Deep Learning ได้ดังนี้



ภาพความสัมพันธ์ระหว่างปัญญาประดิษฐ์กับ Machine Learning และ Deep Learning

Artificial Neural Network เป็นการจำลองเอาระบบเส้นประสาทในสมองมนุษย์มาอยู่ในระบบการทำงานของโปรแกรมคอมพิวเตอร์เพื่อให้คอมพิวเตอร์มีความสามารถในการเรียนรู้ได้แบบ

[380] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

เดียวกับสมองมนุษย์ โดยมีองค์ประกอบการทำงาน 4 ส่วน คือ 1) input & output 2) weight 3) Bias 4) Activation Function

input & output หรือการนำเข้าข้อมูลเพื่อนำไปประมวลในหน่วย function ก่อนเสนอผลลัพธ์ Weight เป็นเงื่อนไขพิจารณาว่า input ตัวไหนสำคัญหรือไม่ input ไหนมีค่าน้ำหนักที่เหมาะสมในการประมวลผล Bias จะอยู่ในการทำงานของ Function ในการประมวลผล ทำให้มีการนำปัจจัยอื่นมาสร้างความยืดหยุ่นให้ข้อมูลมากขึ้น Activation Function ทำให้โมเดลการประมวลผลสามารถทำได้ทั้งในเชิง Linear และ Non-linear[381]

Artificial Neural Network คือการนำเอา Artificial Neuron มาต่อกันเยอะๆ ทำให้เกิดการประมวลผลที่ซับซ้อนขึ้น การทำงานของ Artificial Neuron มีหลายรูปแบบ เช่น XOR Problem คือการคำนวณ input 2 ชุดข้อมูลเพื่อนำไปสู่การคาดการณ์ (Predict) ผลลัพธ์[382] เช่น

Input	Input	Output
0	0	0
0	1	1
1	0	1
1	1	0

ภาพที่ 2.3 ลักษณะการคาดการณ์ผลลัพธ์ในโปรแกรมปัญญาประดิษฐ์

การเรียนรู้ของ Neural Network ทำได้โดยการสุ่มค่า weight และค่า bias ให้ได้มากที่สุด และการนำเอาข้อมูลที่อัพเดทแล้วมาวนใช้ใหม่ใน network[383]

ประเภทของ Deep Learning - หลักการทำงานของระบบ Deep Learning คือการเรียงลำดับข้อมูลเพื่อทำการคาดการณ์ในลำดับต่อไป ในระดับพื้นฐานที่สุดจะอาศัยการทำงานแบบ Time Series จึงสามารถแบ่งการทำงานของ Deep Learning ได้ดังนี้

[381] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

[382] Ibid.

[383] Ibid.

1) Feed Forward Neural Network ทำงานโดยการรับ input ไปประมวลผลก่อนแสดง output ในแนวระนาบ (Linear) ข้อเสียคือระบบนี้ไม่มีความยืดหยุ่น ทำการ predict โดยอาศัยเงื่อนไขที่กำหนดอย่างตายตัวเท่านั้น[384] เช่น

2) Recurrent Neural Network เป็นระบบการคาดการณ์ที่ไม่ใช่ระบบทางตรง มีการนำเอา output กลับมาใช้เป็น input เพื่อการพยากรณ์หลายชั้น โดยใช้ระบบ Time Series Data ในการทำงาน ซึ่งหมายถึงข้อมูลจะมีการจัดเรียงเป็นลำดับ เช่น ช้าง กิน อ้อย คำทั้งสามถูกเรียงตามลำดับไวยากรณ์ทำให้ระบบสามารถคาดการณ์ลำดับคำได้ (มีการกำหนดเงื่อนไขเอาไว้ก่อนล่วงหน้า) หากมีการพิมพ์คำว่าอ้อย ช้าง กิน ระบบก็จะทำการจัดเรียงคำใหม่ให้ถูกต้อง เพราะลำดับคำไม่ถูกต้องตามโปรแกรมที่บันทึกไว้[385] เป็นต้น

ลักษณะการทำงานดังกล่าวเกิดจากการนำเอา input ข้อมูลเดิมไปแสดงเป็น output และมีการนำเอาoutput ย้อนกลับมาเป็น input อีกรอบเพื่อแสดงผล จึงเรียกว่า “Recurrent” เพื่อการคาดการสถานการณ์ล่วงหน้า (Predict)

ข้อจำกัดของ RNN คือหากมีข้อมูล input 2-3 ชุดหลังซ้ำกันจะทำให้รูปแบบการคาดการณ์มีความคลาดเคลื่อนมากขึ้น เพราะอัลกอริทึ่มไม่สามารถคำนวณได้ว่าข้อมูลที่จะเกิดขึ้นลำดับต่อไปจะเป็นข้อมูลชุดใหม่หรือข้อมูลชุดเดิม ทำให้ RNN ไม่สามารถเรียนรู้ความสัมพันธ์ระยะยาวได้จึงก่อให้เกิดการพัฒนาระบบ LSTM หรือ Long Short Term Memory

3) Long-Short Term Memory มีโครงสร้างการทำงานที่เหมือนกับ RNN แต่เพิ่มเติมหน่วยความจำเพิ่มเติมเข้าไป จากที่ใช้เพียง input เดิมเพื่อไปแสดงผลเป็น output ก็มีการนำ memory มาประมวลผลร่วมด้วยทำให้ข้อมูลที่นำมาใช้ประมวลผลมีความละเอียดมากขึ้น LSTM เรียนรู้ความสัมพันธ์ในระยะยาวได้ นอกจากนั้น LSTM ยังมีความสามารถในการลบข้อมูลที่ไม่จำเป็นในการตัดสินใจ เพิ่มข้อมูลใหม่ที่เห็นว่าจำเป็นและเวลาไหนที่จะนำข้อมูลส่วนไหนในหน่วยความจำไปใช้ประโยชน์เพื่อการแสดงผล[386]

---

[384] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

[385] Ibid.

[386] Ibid., p, 426.

4) Convolutional Neural Network เป็นระบบ Deep Learning ที่สร้างขึ้นมาเพื่อแก้ไขปัญหา input ที่เป็น Image data เป็นระบบที่ซับซ้อนขึ้นกว่า ANN ปกติ เนื่องจากรูปภาพ 2 มิติเป็นข้อมูลที่ระบบทั้งสามประการแรกนำข้อมูลเข้าไปไม่ได้ ใช้รูปแบบ Convolution ที่เป็นการเลียนแบบการมองเห็นของมนุษย์[387]

ระบบ Convolutional Neural Network ใช้ระบบ Convolution Operation ในการทำงาน ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอนคือ 1) Input image 2) Feature Detector, Filter, Kernel 3) Feature map

1) ขั้นตอนการ Input - Convolutional Neural Network จะจำลองความสามารถในการมองเห็นแบบเดียวกับตามนุษย์ หมายความว่าระบบ โดยมองภาพที่ปรากฏต่อหน้าจากการรับรู้ขนาด (ที่ไม่ใช่การชัง ตวง วัด) รูปแบบ ฯลฯ สิ่งเหล่านี้ในทางวิทยาการคอมพิวเตอร์เรียกว่า Feature เช่น การที่เราเห็นคนดีใจเราจะสังเกตจากการแสดงออกด้วยการยิ้มหรือการหัวเราะ หากเรานำภาพการยิ้มหรือหัวเราะของคนไปสแกนเพื่อสร้าง input ให้โปรแกรมคอมพิวเตอร์ ระบบ CNN ก็จะทำการบันทึกลักษณะสิ่งที่เรียกว่าความดีใจนี้เอาไว้ในหน่วยความจำ[388]

2) กระบวนการ Feature Detector, Filter หรือ Kernel[389]เป็นกระบวนการทำงานของโปรแกรมคอมพิวเตอร์ที่ทำการแปลงข้อมูล input ซึ่งเป็นรูปภาพให้กลายเป็นชุดตัวเลขทางคณิตศาสตร์ในระบบเลขฐาน 2 ภาพถูกเก็บไว้จึงเป็นเพียงข้อมูลตัวเลข 0 และ 1 ตามตำแหน่งต่างๆ ที่โปรแกรมคอมพิวเตอร์กำหนดเอาไว้เป็นค่าสำหรับการประมวลผลภาพที่บันทึกไว้ และทุกครั้งที่มีการนำภาพ input เข้าสู่ระบบโปรแกรม ก็จะมีการเทียบว่าภาพใหม่ตรงกับภาพเดิมหรือไม่ หรือเป็นภาพที่ไม่เคยเห็นมาก่อน และผู้สั่งการข้อมูลกำหนดให้โปรแกรมรับรู้ว่าเป็นภาพอะไร กระบวนการทำงานลักษณะนี้เรียกว่า Feature Detector

3) Feature map คือภาพที่โปรแกรมบันทึกเอาไว้เป็นชุดข้อมูลตัวเลข โดยจัดเอาไว้เป็นภาพต้นแบบสำหรับการเปรียบเทียบกับภาพที่จะเห็นต่อไปในอนาคต หากภาพที่โปรแกรมเห็นในอนาคต

---

[387] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 425.

[388] Ibid., p. 426.

[389] Ibid., p. 424.

เป็นภาพที่ตรงกับชุดข้อมูลที่โปรแกรมบันทึกเอาไว้ โปรแกรมก็จะสามารถแสดงผลได้ทันทีว่าภาพนั้นคือภาพอะไร[390]

ระบบ Machine Learning มี 3 รูปแบบคร่าวๆ ได้แก่

1) Supervised Machine Learning[391] คือการเรียนรู้ผ่านข้อมูลที่ผู้โปรแกรมข้อมูลทำการใส่ทั้ง input และ output ที่ชัดเจน เพื่อให้โปรแกรมเรียนรู้ข้อมูลก่อนการประมวลผล การทำงานของ Supervise Machine Learning มีระบบย่อยคือ การทำงานแบบ Regression เป็นการคาดการณ์ปริมาณที่เป็นลักษณะการชั่ง ตวง วัด เช่น ส่วนสูง น้ำหนัก เงินเดือน ฯลฯ และการทำงานแบบ Classification คือการแยกแยะว่าสิ่งที่ machine รับรู้นั้นเป็น คน สัตว์ สิ่งของ หรือเป็นอีเมลสแปมหรือไม่ เป็นต้น

2) Unsupervised Machine Learning[392] เป็นการเรียนรู้ที่ผู้โปรแกรมไม่ได้กำหนดค่า input ให้โปรแกรมแต่ไม่มีการกำหนดค่า output ที่ชัดเจน โปรแกรมจะไม่รู้ว่าต้องหาอะไรเป็นการหาคำตอบที่ไม่รู้จากการประมวลผล การทำงานของ UNL แบ่งเป็น 2 ส่วนย่อยคือ Clustering การจัดหมวดหมู่ของข้อมูลเพื่อให้ในการประมวลผล เช่น การจัดกลุ่มเป้าหมายลูกค้าเพื่อการโฆษณา และ Association คือการสร้างกฎเพื่อจัดการข้อมูล เช่นกำหนดเงื่อนไขโดยอาศัยพฤติกรรมผู้บริโภคที่มักซื้อขนมพร้อมน้ำอัดลม โปรแกรมก็จะคำนวณที่ตั้งของชั้นขนมที่ใกล้น้ำอัดลม คนที่ชอบดูภาพยนตร์ลักษณะเดียวกัน เป็นต้น

3) Reinforcement Machine Learning[393] จะมีลักษณะการเรียนรู้คล้ายคนที่สุด ด้วยการตั้งเงื่อนไข 3 ประการ คือ Goal Action และ Reward วิธีเรียนรู้แบบนี้จะไม่มีรูปแบบตายตัวแต่มีเงื่อนไขเพียงการบอกเป้าหมายให้ Machine รู้ Machine ดำเนินการตามเป้าหมายที่กำหนด หากได้ผลลัพธ์ที่ดีที่สุดมนุษย์จะให้รางวัล หากได้ผลลัพธ์ไม่ดีก็จะลงโทษ เช่นการสั่งให้รถยนต์เคลื่อนที่ไปข้างหน้า 10 เมตร รถยนต์จะเคลื่อนที่ไปตามเป้าหมายที่สั่ง โดยเราไม่ต้องบอกว่าต้องทำอะไรก่อนหลัง ทำอย่างไร ให้รถยนต์เรียนรู้ด้วยตัวเองผ่านการทำถูกผิดจนได้วิธีการที่เหมาะสมที่สุด

---

[390] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 429.

[391] Ibid., p. 421.

[392] Ibid.

[393] Ibid., p. 424.

ปัญญาประดิษฐ์มีแนวโน้มเก่งขึ้นแต่ไม่ทั้งหมด[394] เช่น ทางการแพทย์ ยังต้องพึ่งการวินิจฉัยของหมอประกอบด้วย การใช้งานปัญญาประดิษฐ์มักสั่งได้เป็นภารกิจ (Task) ไม่ใช่สั่งทั้งหมด คนทำงานในบางอาชีพ ไม่ได้มีแค่ภารกิจเดียวแต่มีหลายภารกิจปัญญาประดิษฐ์ทำได้ไม่หมด เช่น ครูไม่ได้สอนแค่หนังสือ แต่ต้องให้คำแนะนำ เขียนผลงาน ให้กำลังใจ ฯลฯ เช่นนี้ ปัญญาประดิษฐ์ทำไม่ได้ ปัญญาประดิษฐ์โรงงานอุตสาหกรรมเป็นปัญญาประดิษฐ์ที่นิยมเพราะทำงานได้จริง แต่ราคาสูง แรงงานมนุษย์จึงยังเป็นเรื่องจำเป็นอยู่ในกรณีที่ไม่สามารถซื้อปัญญาประดิษฐ์มาใช้ได้

ขณะที่ปัญญาประดิษฐ์ในเชิงจริยศาสตร์ (ทางปรัชญา) ยังไม่มีทิศทางที่ถูกเสียทีเดียว เพราะยังจำกัดความได้ยากว่าปัญญาประดิษฐ์เรียนรู้จากอดีตหรือสิ่งที่มนุษย์ใส่เข้าไป เพราะบางครั้งปัญญาประดิษฐ์ก็เรียนจากอดีต เช่น การใช้ปัญญาประดิษฐ์ทำงานตัดสินคดี แม้จะทำได้ก็จริงแต่เป็นการเรียนรู้จากคดีก่อนๆ รวมถึงอคติที่อยู่ในคำพิพากษาด้วย ปัญญาประดิษฐ์ที่เรียนรู้พฤติกรรมของคนจากอินเทอร์เน็ตก็จะเรียนรู้สิ่งที่เป็นอคติของคนด้วย เช่น คนเคยหาข่าวการเมืองซีกแบบหนึ่ง ปัญญาประดิษฐ์ก็จะหาข้อมูลแบบนั้นมาให้มากๆ ซึ่งอาจเป็นเพียงความสนใจของเราในยุคหนึ่งก็ได้แต่ไม่ใช่เรื่องที่เราให้ความสนใจเป็นหลักตลอดเวลา

หรือการให้ปัญญาประดิษฐ์ตัดสินว่าหากเจอคนหนึ่งคนกับคนห้าคนบนถนนปัญญาประดิษฐ์จะเลือกชนใครเป็นสิ่งที่มนุษย์ไม่ทำจึงเกิดปัญหาว่าความรับผิดชอบเป็นของใคร เช่นนี้รถไร้คนขับก็จะไม่สามารถพัฒนาได้จนเป็น Autonomous ยังคงให้คนต้องควบคุมอยู่บ้าง หรือประเทศไทยคนขับรถไม่มีระเบียบโอกาสชนกันมีสูงคนยังต้องมีส่วนในการบังคับด้วย

ปัญญาประดิษฐ์เกี่ยวข้องกับกับการใช้งานระบบอาวุธอิสระ โดยเฉพาะอย่างยิ่งในระบบป้องกันภัยทางอากาศประเทศอิสราเอล เช่น Iron Dome ซึ่งเป็นที่รู้จักกันดีและ Iron Beam ซึ่งเป็นระบบป้องกันภัยทางอากาศรูปแบบใหม่ Iron Beam เป็นระบบป้องกันภัยทางอากาศของประเทศอิสราเอลโดยการยิงเป้าหมายด้วยเลเซอร์ การโจมตีสามารถกระทำได้ทั้งการยิงโดรน ปืนครก จรวด และจรวดนำวิถีต่อต้านรถถัง ระบบอาวุธนี้มีการทดลองเป็นที่สำเร็จแล้ว ระบบ Iron Beam ถูกพัฒนาขึ้นเพื่อเสริมการทำงานของระบบต่อต้านภัยทางอากาศ Iron Dome กองทัพอิสราเอลอ้างว่า

[394] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,”: 432.

ระบบ Iron Beam มีต้นทุนการยิงต่อครั้งประมาณ 3.5 เหรียญดอลล่าร์สหรัฐอเมริกาเท่านั้น เทคโนโลยี Iron Beam เป็นเทคโนโลยีแรกที่ใช้เลเซอร์ยิง UAV ได้[395]

การพัฒนา Iron Beam เกิดขึ้นเนื่องจากอิสราเอลต้องเผชิญกับการถูกโจมตีโดยกลุ่มฮามาส ซึ่งมีการยิงจรวดนำวิถีกว่า 4,000 ลูกโจมตีอิสราเอล นอกจากนั้น ยังเป็นการส่งสารถึงอิหร่าน โดยอิสราเอลมองว่าอิหร่านคือประเทศที่เป็นภัยคุกคามต่อตะวันออกกลาง ด้วยเหตุที่อิหร่านให้การสนับสนุนกลุ่มฮูติในประเทศเยเมน โดยกลุ่มฮูติใช้ UAV และจรวดนำวิถี โจมตีชาติพันธมิตรซาอุดิอาระเบีย

ระบบการป้องกันภัยทางอากาศของอิสราเอลเริ่มมีการใช้งานมาตั้งแต่ช่วงปี ค.ศ.2006 และพัฒนามาจนเกิด Iron Dome จนกระทั่งปี ค.ศ.2019 อิสราเอลจึงสามารถพัฒนาระบบป้องกันภัยทางอากาศด้วยเลเซอร์สำเร็จ ซึ่งช่วยลดค่าใช้จ่ายให้กับระบบ Iron Dome

การทดสอบระบบ Iron Beam สามารถยิงต่อต้านโดรนได้สำเร็จในปี ค.ศ.2021 นอกจากนั้น ระบบ Iron Beam ยังสามารถต่อต้านอาวุธไม่นำวิถี กระสุนวิถีโค้ง และจรวดนำวิถีต่อต้านรถถังได้

อิสราเอลมีระบบป้องกันภัยทางอากาศหลายชั้น ได้แก่ ระบบป้องกันภัยทางอากาศระยะใกล้ (Short range missiles) ที่รู้จักอย่างแพร่หลายคือระบบ Iron Dome ระบบป้องกันภัยทางอากาศระยะกลาง (Mid-long range missiles) คือระบบ David's Sling และระบบป้องกันภัยทางอากาศระยะไกล (Ballistic missile threat) คือระบบ Arrow 2 และ Arrow 3

นอกจาก Iron Beam แล้วอิสราเอลยังมีการใช้งานระบบ Iron Dome ซึ่งเป็นระบบป้องกันภัยทางอากาศที่ใช้ต่อต้านระบบจรวดนำวิถีและจรวดนำวิถีร่อน ในขณะที่ระบบ David's Sling ใช้ป้องกันจรวดนำวิถีร่อนและขีปนาวุธบางชนิด ส่วนระบบ Arrow ใช้ในการป้องกันขีปนาวุธ โดยในปัจจุบันอิสราเอลมีความพยายามในการพัฒนาระบบ Arrow 4 เพื่อป้องกันระบบอาวุธ Hyper Sonic

จากการประเมินของกองทัพอิสราเอลมีข้อมูลน่าเชื่อว่าการโจมตีแบบเต็มรูปแบบด้วยอาวุธทางอากาศนั้นอาจทำให้ระบบ Iron Dome ต้องยิงจรวดต่อต้านถึง 30,000 ลูกพร้อมกัน ซึ่งจะมีต้นทุนสูงหลายล้านเหรียญ การพัฒนาเทคโนโลยีเลเซอร์ขึ้นมาสนับสนุนจึงทำให้ระบบป้องกันภัยทาง

---

[395] Sakshi Tiwari, "Making History- Israel becomes the first country to successfully shoot down drones with Iron Beam Laser Interceptors," The Eurasian Times, April 15, 2022. [online] Accessed: August 30, 2022. Available from: https://eurasiantimes.com/israel-successfully-shoot-down-drones-with-laser-interceptor/

อากาศมีทางเบือกที่มากขึ้น อย่างไรก็ดี ระบบป้องกันภัยทางอากาศด้วยเลเซอร์ก็มีข้อจำกัดในการทำงานภายใต้สภาพอากาศที่เลวร้าย การใช้เลเซอร์เป็นระบบเสริมในการป้องกันภัยจึงมีความเหมาะสมกว่าการใช้งานเป็นระบบหลัก

นอกจากระบบป้องกันภัยทางอากาศของประเทศอิสราเอลแล้ว ประเทศสหรัฐอเมริกาก็มีระบบป้องกันภัยทางอากาศ Patriot (MIM-104) ซึ่งเป็นระบบป้องกันภัยทางอากาศระบบพื้นสู่อากาศ ใช้ในการป้องกันการโจมตีจากขีปนาวุธและอากาศยาน ระบบ Patriot Patriot ถูกนำมาใช้ประจำการในการรบตั้งแต่ทศวรรษที่ 1980 และมีการปรับปรุงระดับความสามารถอยู่หลายครั้ง (Patriot Advanced Capability: PAC) มีการพัฒนาตั้งแต่ PAC 1- PAC 3[396]

ระบบป้องกันภัยทางอากาศแบบ Patriot เริ่มต้นในปี 1966 โดยรัฐมนตรีว่าการกระทรวงกลาโหมของสหรัฐอเมริกา Robert McNamara มีการอนุมัติโครงการ Surface-to-air Missile Defense: SAM-D โดยบริษัท Raytheon ทำหน้าที่เป็นผู้พัฒนาโครงการ มีเทคโนโลยียุคเริ่มต้นที่นำมาพัฒนาต่อยอดคือระบบป้องกันภัยทางอากาศ Nike-Zeus ซึ่งมีประจำการอยู่แต่เดิม แต่ด้วยข้อจำกัดหลายประการ Nike-Zeus จึงไม่ถูกนำมาใช้งานจริงเลย หลังจากพัฒนาอยู่ 4 ปี ในปี ค.ศ.1970 ก็พัฒนาระบบ Track-via-Missile สำเร็จ โดยเป็นการพัฒนาทั้งอุปกรณ์ และโปรแกรมคอมพิวเตอร์ และมีการทดลองกับการบินหลายครั้ง ต่อมาในปี ค.ศ.1972 มีการพัฒนาระบบให้สมบูรณ์ขึ้นทั้งระบบเรดาร์ และโปรแกรมคอมพิวเตอร์ และชิ้นส่วนระบบนำวิถีขั้นสูง พร้อมไปกับการพัฒนาระบบสนับสนุนภาคพื้นดิน[397]

การออกแบบระบบป้องกันภัยทางอากาศนี้มีความซับซ้อนค่อนข้างสูง จึงต้องมีการทดสอบอยู่หลายครั้งว่าจะสามารถใช้งานได้จริง ก่อนอนุมัติให้มีการพัฒนาต่อไป จนกระทั่ง ค.ศ.1974 จึงเริ่มมีการทดลองระบบ SAM-D โดยมีการทดสอบทั้งระบบควบคุมจรวด โครงสร้างทางอากาศพลศาสตร์

[396] Andreas Parsch, “Raytheon MIM-104 Patriot.” Directory of U.S. Military Rockets and Missiles. (2002), http://www.designation-systems.net/dusrm/m-104.html, accessed June 12, 2022.

[397] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.” Center for a New American Security, January 2017, pp. 6-7. [online] Accessed: June 12, 2022. Available from: http://www.jstor.org/stable/resrep06103

และการติดตามเป้าหมายจากสถานีควบคุมภาคพื้นดิน ต่อมาใน ค.ศ.1975 การทดสอบระบบ SAM-D ก็สำเร็จโดยการทดสอบยิงโดรน จึงถือเป็นความสำเร็จของระบบ Sam-D[398]

ค.ศ.1976 โครงการ SAM-D เปลี่ยนชื่อเป็น Patriot และเร่งการพัฒนาและผลิต จากเป้าหมายเดิม ค.ศ.1983 มาเป็น ค.ศ.1980 โดยตัดขั้นตอนบางประการออกไป ทำให้การผลิต Patriot เริ่มต้นใน ค.ศ.1980 โดยเริ่มจากชุดยิง 5 ชุด และจรวด 155 นัด การพัฒนาครั้งนี้เกิดปัญหาระหว่างการทดสอบทำให้สายการผลิตต้องหยุดชะงักเพื่อแก้ไขปัญหาที่เกิดขึ้นก่อน หลังการแก้ไขครั้งที่ 3 และมีการเขียนคู่มือประกอบการใช้งาน ระบบก็สามารถใช้งานได้ดี การทดสอบในครั้งที่ 3 นี้พบว่าจรวดสามารถทำลายเป้าหมายได้ถึงร้อยละ 50 หลังจากทดสอบสำเร็จจึงมีการเร่งการผลิตเต็มรูปแบบ เพื่อนำไปประจำการในยุโรป[399]

กองทัพบกสหรัฐนำระบบ Patriot เข้าประจำการครั้งแรกในปี ค.ศ.1984 โดยใช้ชื่อว่า MIM-104A Patriot เดิมทีนั้นตามหลักนิยมของกองทัพสหรัฐอเมริกาใช้ระบบป้องกันภัยทางอากาศเพื่อการต่อต้านขีปนาวุธ แต่ใน Training and Doctrine Command (กองบัญชาการการฝึกและหลักนิยมกองทัพบกสหรัฐ) ได้ตัดความสามารถในการทำลายนี้ออกไป MIM-104A จึงเหลือเพียงภารกิจหลักในการทำลายอากาศยานเท่านั้น เนื่องจากมีความกังวลเรื่องงบประมาณและข้อจำกัดทางเทคนิค แต่ในปี ค.ศ.1985 เมื่อการผลิตมีประสิทธิภาพมากขึ้นและมีการเปลี่ยนผู้บริหารใหม่ของโครงการ Patriot จึงมีการเพิ่มขีดความสามารถในการทำลายขีปนาวุธได้ด้วย ซึ่งเดิมนั้นเน้นไปที่การทำลายขีปนาวุธทางยุทธวิธี SS-21 (OTR-21 Tochka Tactical Ballistic Missile) การพัฒนาเพิ่มเติมนี้ได้รับความเห็นชอบจากกระทรวงกลาโหมและมีการอนุมัติการพัฒนาโครงการต่อไปอีก 5 ปี[400]

ในยุคแรกโครงการพัฒนาระบบป้องกันภัยทางอากาศเพื่อต่อต้านขีปนาวุธใช้ชื่อว่า Patriot Anti-Tactical Missile Capability: PAC-1 (ซึ่งต่อมาจะเปลี่ยนเป็นชื่อ Patriot Advanced Capability) โดยมีการเปลี่ยน Software เพื่อปรับการทำงานของระบบเรดาร์เพื่อให้รองรับต่อการตรวจจับการเคลื่อนที่ของขีปนาวุธ ทั้งนี้ในจรวดเองก็จะต้องมีการเปลี่ยนหัวรบและตัวจุดชนวนใหม่เพื่อให้รองรับต่อเป้าหมายที่มีความเร็วสูง ทำให้มีงบประมาณเพิ่มขึ้น จำเป็นที่จะต้องหาพันธมิตรในการร่วมพัฒนา โดยสหรัฐอเมริกาได้ขอความร่วมมือจากประเทศเยอรมันให้การสนับสนุนการพัฒนา

---

[398] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 6-7.

[399] Ibid.

[400] Ibid.

ระบบ PAC-1 นี้ และเยอรมันได้ให้ความช่วยเหลือทางการเงินถึงร้อยละ 40 ของงบประมาณโครงการทั้งหมด แต่ด้วยความเร่งรีบในการผลิต ทำให้หัวรบใหม่ยังไม่มีการผลิตจริง แต่ยังคงใช้หัวรบแบบเดิม[401]

Phase แรกของการผลิตจึงเป็นการปรับปรุง Software ระบบนำวิถีและการควบคุมจรวดเท่านั้น การปรับปรุงนี้ทำให้จรวดเดินทางได้สูงขึ้นเพื่อไปปะทะกับขีปนาวุธ นอกจากนั้นระบบเรดาร์ยังถูกนำมาใช้เพื่อให้จรวดสามารถค้นหาเป้าหมายที่เพดานบินสูงได้ ในปี ค.ศ.1986 มีการพัฒนาระบบสำเร็จและทดลองใช้งานต่อต้านจรวดแบบ Lance Missile ซึ่งคล้ายกับจรวด SS-21 ของสหภาพโซเวียต[402]

Phase 2 เป็นการปรับปรุงทั้งหัวรบ ระบบจุดชนวน รวมถึงโปรแกรมและระบบอัลกอริทึ่มในระบบนำวิถีใหม่ ทำให้หัวรบใหม่มีน้ำหนักถึง 200 ปอนด์ บรรจุดินระเบิดแรงสูงน้ำหนัก 100 ปอนด์ ซึ่งมีส่วนประกอบของสะเก็ดระเบิดเหล็กกล้าเพื่อวัตถุประสงค์ในการทำลายเปลือกของขีปนาวุธเป้าหมาย และมีตัวจุดชนวนแบบเฉียดระเบิดที่จะวัดค่าระยะห่างจากเป้าหมาย ด้วย Pulse Doppler Radar นอกจากนี้ยังมีการเพิ่มความสามารถให้เรดาร์ควบคุมการยิงเพื่อตัดการรบกวนสัญญาณจากพื้นดินและการต่อต้านการรบกวนสัญญาณเรดาร์ระยะไกลหรือ Stance of jammer นอกจากนี้ยังมีการเพิ่มความคงทนให้มากขึ้น โครงการระยะนี้ดำเนินการในช่วงปี ค.ศ.1986-1989 โดยสายการผลิตหลังปี ค.ศ.1989 จะเป็นการผลิตในรูปแบบของ PAC-2 ทั้งหมด[403]

ในวันที่ 2 สิงหาคม ค.ศ.1990 ประธานาธิบดี Saddam Hussain ผู้นำประเทศอิรักได้เปิดฉากโจมตีประเทศคูเวต ซึ่งขณะนั้นจรวด PAC-2 ยังอยู่ในระหว่างการเริ่มต้นผลิตได้เพียง 5 เดือน จึงมีจรวดเพียง 3 ลูกที่ใช้เพื่อการทดสอบของกองทัพสหรัฐอเมริกา ยังไม่มีการทดสอบใช้งานในสถานการณ์จริงเลย อีกทั้งการออกแบบ PAC-1 และ PAC-2 ถูกออกแบบมาเพื่อการต่อต้านขีปนาวุธ SS-21 และ SS-23 ของสหภาพโซเวียต ขณะที่อิรักใช้งานขีปนาวุธ SCUD ซึ่งเป็นขีปนาวุธรุ่นเก่าที่สหภาพโซเวียตขายให้ประเทศโลกที่ 3 แต่อิรักได้ทำการปรับปรุงระบบจรวดใหม่ ทำให้ SCUD เป็น

[401] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 6-7.

[402] Ibid.

[403] Ibid.

ขีปนาวุธที่มีความเร็วสูงกว่า SS-21 และ SS-23 (ประมาณ 5,200-5,900 ฟุตต่อวินาที) โดย SCUD มีความเร็วสูงถึงประมาณ 7,200 ฟุตต่อวินาที[404]

กระทรวงกลาโหมสหรัฐอเมริกาจึงต้องมีการประชุมเพื่อพัฒนาระบบต่อต้านขีปนาวุธ SCUD โดยการนำเทคโนโลยี PAC-1 มาพัฒนาให้เป็น PAC-2 และจะต้องเร่งการผลิตให้ทันต่อการปฏิบัติการ ในเดือนมกราคม ค.ศ.1991 โรงงาน Raytheon จึงต้องทำงานโดยไม่หยุดพัก และวิศวกรต้องทำงานวันละ 18 ชั่งโมงเพื่อให้ Pac-2 พร้อมใช้งาน โดยในเดือนมกราคม ค.ศ.1991 มีจรวด PAC-2 ประจำการในกองทัพมากถึง 400 ลูก[405]

ในวันที่ 17 มกราคม ค.ศ.1991 กองทัพสหรัฐได้เริ่มต้นปฏิบัติการโจมตีอิรักร่วมกับกองทัพพันธมิตร ทำให้อิรักตอบโต้ด้วยการยิงขีปนาวุธ SCUD จึงเป็นครั้งแรกที่ PAC-2 ได้ใช้งานต่อต้านการโจมตีของ SCUD โดยไม่เคยมีการทดสอบในสถานการณ์จริงมาก่อนและมีการเก็บรวบรวมข้อมูลการทำงานเพื่อพัฒนาระบบต่อไป โดยในปฏิบัติการแรก มีการยิง Patriot รวมทั้งสิ้น 159 นัด มีการใช้งานสำเร็จในพื้นที่ประเทศซาอุดิอาระเบียถึงร้อยละ 70 สำเร็จในอิสราเอลร้อยละ 40 ซึ่งเป็นการปกป้องพลเรือนได้หลายร้อยคนและเป็นแนวทางต่อไปในการพัฒนาขีปนาวุธเพื่อการป้องกันภัยทางอากาศ[406]

ใน ค.ศ.1983 มีความพยายามในการพัฒนาระบบ hit-to-kill หรือการทำลายเป้าหมายด้วยการชน และมีการทดสอบสำเร็จใน ค.ศ.1987 ทำให้กองทัพสหรัฐอเมริกาตั้งโครงการใหม่ชื่อว่า Extended Range Intercept Technology โดยมีการออกแบบระบบสำเร็จใน ค.ศ.1989 และมีการทดสอบการบินสำเร็จใน ค.ศ.1994 ซึ่งต่อมาได้มีการพัฒนาเป็นโครงการจรวด PAC-3 ซึ่งเป็นจรวดแบบใหม่ของกองทัพบกสหรัฐ โดยเป็นการพัฒนาระบบเครือข่ายใหม่ทั้งหมด เปลี่ยนมาใช้เครือข่าย Link 16 และสามารถแบ่งปันเป้าหมายได้กับ platform ต่างๆ ในระบบ นอกจากนั้นอุปกรณ์ในการติดตามเป้าหมาย Travelling Wave Tube (TWT) ยังสามารถสร้างคลื่นแบบใหม่ ทำให้สามารถติดตามเป้าหมายได้ดีขึ้นกว่าเดิม[407]

---

[404] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 6-7.

[405] Ibid.

[406] Ibid.

[407] Ibid.

จรวด PAC-3 มาพร้อมกับจรวดแบบใหม่คือ MIM-104F ที่พัฒนาขึ้นมาเพื่อการทำลายเป้าหมายขีปนาวุธโดยเฉพาะและจรวด PAC-3 นี้จะมีขนาดเล็กลงทำให้เครื่องยิงจรวด PAC-2 เดิมสามารถบรรจุจรวด PAC-3 ได้ถึง 4 นัด และมี Seeker แบบ Active Radar Homing ซึ่งมีคลื่นความถี่สูง Ka-Band ขนาดความถี่คลื่น 26.5-40 GHz ทำให้จรวดสามารถเดินทางเข้าหาเป้าหมายได้เองในช่วงความถี่ปลาย แต่ระยะยิงจรวด PAC-3 จะลดลงเหลือ 20-40 กิโลเมตร ระยะสูงที่สุดที่จรวดเดินทางไปทำลายเป้าหมายได้คือ 65,000 ฟุต จรวดนี้จะทำลายเป้าหมายโดยการพุ่งชนโดยตรง ทำให้ไม่ต้องใช้ตัวจุดชนวนแบบเฉียดระเบิด โดยหัวรบยังคงบรรจุดินระเบิดแรงสูงเอาไว้เล็กน้อยเพื่อเพิ่มโอกาสในการทำลายที่สูงขึ้น โดยจรวดจะระเบิดเมื่อทำลายเป้าหมาย[408]

PAC-3 เป็นระบบที่ไม่เหมาะกับการทำลายเป้าหมายอากาศยาน ในปฏิบัติการจริงเพื่อการเข้าปะทะจึงมีการใช้ทั้ง PAC-2 และ PAC-3 ใช้งานร่วมกันในกองทัพเพื่อทำลายเป้าหมายทั้งอากาศยานและขีปนาวุธ

ส่วนประกอบในการทำงานของระบบ Patriot ประกอบด้วย 1) ส่วนควบคุมการยิง ประกอบด้วยสถานีควบคุม เรดาร์ ชุดสายอากาศในการสื่อสารและเครื่องกำเนิดไฟฟ้า และ2) ส่วนแท่นยิง - อุปกรณ์ทั้งหมดจะติดตั้งบนรถบรรทุกหรือรถพ่วงลากจูง ซึ่งจะต้องสามารถเตรียมความพร้อมก่อนการใช้งานได้ภายในเวลา 1 ชั่วโมง

หัวใจสำคัญของระบบ Patriot คือระบบเรดาร์ควบคุมการยิง ใช้ทั้งค้นหาเป้าหมายและกำหนดเป้าหมายในการยิง ปกติใช้ระบบ AM/MPQ-53 กับจรวด PAC-1 และ PAC-2 ส่วนระบบ AM/MPQ-65 ได้รับการพัฒนาขึ้นมาเพื่อใช้กับจรวด PAC-3 โดยระบบเรดาร์นี้ใช้เทคโนโลยีแบบ Passive Electronically Scanned Array และมีตัวสร้างคลื่น (Travelling Wave Tube) จำนวน 2 ชุด ทำให้เรดาร์สามารถค้นหาเป้าหมายและติดตามเป้าหมายไปได้พร้อมกัน ในขณะที่เสาอากาศแบบ Phase Array มีส่วนประกอบของ Phase shifter มากถึง 5,000 ชิ้น ทำหน้าที่ทั้งการค้นหาและติดตามเป้าหมาย การพิสูจน์ฝ่าย การส่องเป้าหมายในระบบ active homing และ TVM ส่วน TVM link และการกำจัดค่าสัญญาณรบกวน (Sidelobe) เทคโนโลยี Phase Array ทำให้ลำคลื่นมีความแคบ สามารถตรวจจับเป้าหมายได้แม่นยำ สามารถตรวจจับเป้าหมายขนาดเล็ก หรือที่มีค่า RCS ต่ำได้ อีกทั้งกำลังส่งสูงและการสลับค่าความถี่สามารถทำได้กว้าง ทำให้สามารถต่อต้านการรบกวนได้

[408] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 6-7.

ดี[409]ปัจจุบันระบบเรดาร์ที่อยู่ระหว่างการพัฒนาเพื่อนำมาใช้คือ AM/MPQ-65A แบบ Active Electronically Scanned Array

สถานีควบคุมและสั่งการยิงของระบบ Patriot ใช้ AM/MSQ-104 Engagement Control Station (ECS) เป็นห้องควบคุมขนาดเล็กติดตั้งบนรถบรรทุก ทำหน้าที่เป็นศูนย์กลางสั่งการของกองร้อย มีระบบควบคุมการยิง ระบบ Terminal ของ DATA link และอุปกรณ์สื่อสาร ในห้องสั่งการนี้มีการออกแบบระบบควบคุมความดันและปรับอากาศเพื่อป้องกันรังสีนิวเคลียร์ อาวุธเคมีและอาวุธชีวภาพ รวมถึงระบบอาวุธ EMP ห้องสั่งการยิงนี้สามารถสั่งแท่นยิงได้ทั้งแบบสายไฟเบอร์ออฟติกและสัญญาณวิทยุแบบเข้ารหัส[410]

เสาอากาศย่านคลื่น UHF จะตั้งอยู่สูงเพื่อการรับสัญญาณที่ดีขึ้นและเชื่อมต่อข้อมูลกับหน่วยยิงอื่น โดย ECS จะเชื่อมต่อการสื่อสารแบบ UHF กับกลุ่มของเสาอากาศ Antenna mast group แบบ OE-349 เพื่อส่งสัญญาณไปหาเครือข่ายข้างเคียง ทำให้สามารถสื่อสารระหว่างกองร้อย Patriot ในเครือข่ายเดียวกันได้ เรียกว่า Patriot Data Information Link (PADIL) และยังสามารถเชื่อมต่อไปยังข้อมูลคำสั่งจากหน่วยเหนือกองบังคับการกองพัน Patriot ได้[411]

เครื่องกำเนิดไฟฟ้า ใช้แบบ EPP-3 (Electric Power Plant) เป็นเครื่องกำเนิดไฟฟ้าจากเครื่องยนต์ดีเซลเพื่อให้พลังงานกับ ECS และระบบเรดาร์ สามารถสร้างกำลังไฟได้ 115 kW 3 Phase 400Hz เครื่องกำเนิดไฟฟ้ามีเชื้อเพลิง 100 แกลลอน สามารถผลิตกระแสฟ้าได้ 8 ชั่วโมงติดต่อกัน[412]

แท่นยิง - แท่นยิง Patriot จะมี 3 แบบหลักๆ คือ M901 Launch, M902 Launch และ M903 Launch ทั้งสามแบบสามารถทำงานผ่านสายสัญญาณไฟเบอร์ออฟติก และการทำงานไร้สาย แท่นยิงนี้ติดตั้งบนรถบรรทุกหรือรถลากจูงที่มีการติดตั้งขาปรับระดับ สามารถวางกำลังในพื้นที่ลาดเอียง 10 องศาได้ โดยมีเครื่องกำเนิดไฟฟ้าในตัว[413]

[409] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 8.

[410] Ibid.

[411] Ibid.

[412] Ibid.

[413] Ibid.

แท่นยิง M901 จะรองรับจรวด PAC-2 ได้ 4 นัด ในขณะที่ M902 รองรับจรวด PAC-3 ได้ 16 นัด ส่วน M903 มีการปรับแต่งเพื่อให้รองรับได้ทั้งจรวด PAC-2 PAC-3 รวมถึงจรวดรุ่นใหม่เช่น MSC และ SkyCeptor[414]

ลูกจรวด (Missile) - จรวดที่ใช้งานใน Patriot มี 2 ประเภท คือ 1) PAC-2 ได้แก่ MIM-104C (PAV-2), MIM-104D (PAC-2/GEM) , MIM-104E (PAC-2/GEM+) ใช้เพื่อต่อต้านเป้าหมายอากาศยานหรืออากาศยานไร้คนขับ มีขีดความสามารถต่อต้านขีปนาวุธบางประเภทได้ การระเบิดของจรวดจะมีสะเก็ด จุดระเบิดด้วยชนวนเฉียดระเบิด มีระบบนำวิถีด้วย TVM ที่พัฒนามาจาก semi-active homing system โดยเรดาร์จะส่งคลื่นสะท้อน illumination ออกไปยังเป้าหมาย โดยสัญญาณจะท้อนจะถูกส่งมาที่ส่วนหัวของจรวด และจรวดจะทำการส่งสัญญาณกลับมาที่สถานีอีกครั้ง เพื่อการคำนวณค่าความคลาดเคลื่อน ก่อนจะมีการคำนวณผลและส่งข้อมูลกลับไปยังจรวดอีกครั้ง การส่งสัญญาณที่ซับซ้อนนี้ต้องการการสื่อสารที่ดีและปลอดภัย จรวด PAC-2 มีความยาว 5.2 เมตร เส้นผ่านศูนย์กลาง 410 มิลลิเมตร น้ำหนัก 2,000 ปอนด์ หรือ 900 กิโลกรัม เฉพาะส่วนหัวรบหนัก 200 ปอนด์ จรวด PAC-2 ในทศวรรษ 1990 มีการพัฒนาระบบเป็น PAC-2 GEM (Guidance Enhanced Missile) มีการปรับปรุงตัวจุดชนวน และ seeker แบบสัญญาณรบกวนต่ำ ต่อมามีการพัฒนาเป็น PAC-2 GEM-T เพื่อใช้ในการยิงเป้าหมาย Ballistic Missile และ PAC-2 GEM-C เพื่อใช้ยิงเป้าหมาย Cruise Missile[415]

2) PAC-3 มีขนาดความยาวเท่า PAC-2 แต่มีเส้นผ่านศูนย์กลาง 225 มิลลิเมตร มีการเปลี่ยนระบบนำวิถีเป็น Active Radar Homing ทำให้การหวังผลตอนปลายในการทำลายเป้าหมายมีสูงขึ้น หัวรบมีดินระเบิดแรงสูงขนาดเล็ก จรวดมีน้ำหนักรวม 300 กิโลกรัม[416]

ในภายหลัง PAC-3 มีการปรับปรุงเป็น PAC-3 MSE (Missile Segment Enhancement) จึงเรียกชื่อ PAC-3 รุ่นก่อนเป็น PAC-3 CRI (Cost Reduction Initiative) จรวด PAC-3 MSE มีขนาดกว้างขึ้น โดยมีเส้นผ่านศูนย์กลาง 300 มิลลิเมตร มีชุด Booster แบบใหม่ และมีการปรับปรุง

---

[414] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 8.

[415] Ibid.

[416] Ibid.

Software ให้สามารถต่อต้านขีปนาวุธพิสัยกลางได้ โดยตั้งแต่ ค.ศ.2017 จะมีการผลิตเฉพาะจรวด PAC-3 MSE เท่านั้น[417]

ระยะยิง - PAC-2 สามารถยิงอากาศยานได้ไกลถึง 150 กิโลเมตร ส่วน PAC-3 ใช้ต่อต้านขีปนาวุธที่ระยะ 20 กิโลเมตร ในความสูง 65,000 ฟุต แต่ PAC-3 MSE สามารถใช้ยิงต่อต่านขีปนาวุธได้ไกลถึง 35 กิโลเมตร ที่ความสูง 112,000 ฟุต[418]

การประกอบกำลัง (Organization) จะมีการจัดสัดส่วนเป็น กองบังคับการกองร้อย หมวดควบคุมการยิง หมวดแท่นยิง และหมวดสนับสนุน[419] ในหมวดควบคุมการยิงจะประกอบด้วย กองบังคับการหมวดและหมู่ควบคุมการยิง โดยในหมู่ควบคุมการยิงจะประกอบด้วยสถานีควบ คุมการยิง ECS ส่วนเรดาร์ เสาอากาศแบบ OE-349 และเครื่องกำเนิดไฟฟ้า นอกจากนี้หมวดควบคุมการยิงยังมีระบบป้องกันภัยทางอากาศระยะประชิดด้วย MANPADS ทำการคุ้มกันระยะใกล้

หมวดแท่นยิงจะประกอบด้วย กองบังคับการหมวด กับ 4 หมู่แท่นยิง โดยแต่ละหมู่แท่นยิงจะมีแท่นยิง 2 ชุด ทำให้ 1 กองร้อยจะมีแท่นยิงได้สูงสุด 8 แท่นยิง แต่ทางปฏิบัติจะลดจำนวนลงเพื่อความคล่องตัวในการปฏิบัติการ

กองพันป้องกันภัยทางอากาศแบบ Patriot จะประกอบด้วยกองร้อย Patriot 4-6 กองร้อย โดยมี 1 กองบังคับการกองพันร่วม ทำงานร่วมกับกองบัญชาการกองร้อย กองร้อยจะถูกวางกำลังในหลายทิศทางเพื่อการระวังภัยทางอากาศรอบทิศทาง และเชื่อมระบบการสื่อสารด้วย PADIL ทุกส่วนปฏิบัติการจะมีข้อมูลที่ตรงกันตลอดเวลา

Patriot เริ่มประจำการในกองทัพตั้งแต่ ค.ศ.1984 และใช้งานจริงใน ค.ศ.1991 แต่ยังมีข้อสงสัยในทางทฤษฎีว่าจรวด SCUD ถูกทำลายจริงหรือถูกผลักไปในทิศทางอื่น เนื่องจากยังไม่เคยมีการใช้ระบบจรวดนำวิถีเพื่อการป้องกันภัยทางอากาศมาก่อน[420]

---

[417] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System.”: 8.

[418] Ibid.

[419] Ibid.

[420] Andreas Parsch, “Raytheon MIM-104 Patriot,” Directory of U.S. Military Rockets and Missiles. (2002), [online] Accessed: June 12, 2022. Available from: http://www.designation-systems.net/dusrm/m-104.html

ในปี ค.ศ.2003 ปฏิบัติการ Iraq is freedom มีการใช้จรวด PAC-2 GEM และ PAC-3 โดยมีแท่นยิงกว่า 40 ชุดในพื้นที่การรบ ใน ค.ศ.2005 มีรายงานว่ามีการยิงขีปนาวุธที่เป็นภัยคุกคามจำนวน 9 ครั้ง และมีการต่อต้านสำเร็จ 8 ครั้ง ไม่พบความเสียหายข้างเคียงและการเสียหายของกำลังพลเลย นอกจากนี้ใน ค.ศ.2014 ยังมีรายงานความสำเร็จของการใช้งานในประเทศอิสราเอลเพื่อปฏิบัติการต่อต้านอากาศยานไร้คนขับของฮามาส และอากาศยานของซีเรีย[421] และยังมีรายงานความสำเร็จในการใช้งานที่ประเทศซาอุดีอาระเบียและสหรัฐอาหรับเอมิเรตในการต่อต้านขีปนาวุธจากกบฏฮูติ ปัจจุบันมีผู้ใช้งานระบบ Patriot ทั้งสิ้น 17 ประเทศ โดยโปแลนด์จะเป็นประเทศที่ 18 รวมถึงยูเครนที่น่าเชื่อว่าจะได้รับการช่วยเหลือจากสหรัฐในการป้องกันสาธารณูปโภคและความปลอดภัยของพลเรือนแต่ยังมีความเสี่ยงเนื่องจากระบบอาวุธนี้จะต้องตกเป็นเป้าหมายลำดับต้นในการโจมตีของกองทัพรัสเซีย[422]

ระบบ Patriot เป็นระบบป้องกันภัยทางอากาศหลักของสหรัฐอเมริกา NATO และพันธมิตรของสหรัฐอเมริกาในภูมิภาคต่างๆ มีประโยชน์ในการป้องกันสถานที่สำคัญ เขตที่อยู่ของพลเมือง และฐานทัพหลักทางทหาร จากการโจมตีด้วยขีปนาวุธยุทธวิธีและขีปนาวุธพิสัยใกล้ คาดการณ์ว่าระบบนี้น่าจะประจำการไปถึงปี 2040[423]

หุ่นยนต์สังหารอิสระ - การใช้งานหุ่นยนต์ในทางการทหารในปัจจุบันอยู่ในรูปแบบของหุ่นยนต์ทหารคุ้มกัน (Sentry Robot) ได้รับการพัฒนาและมีการใช้งานจริงในประเทศเกาหลีใต้และอิสราเอล โดยในปี ค.ศ.2006 บริษัทซัมซุงเทควินของเกาหลีใต้ได้วิจัยและพัฒนาหุ่นยนต์เพื่อใช้งานในเขตปลอดทหาร และมีการเปิดตัวหุ่นยนต์ดังกล่าวในชื่อ SGR A-1 ในปี ค.ศ.2010 หุ่นยนต์ทหารคุ้มกัน SGR A-1 ได้ถูกนำมาติดตั้งในเขตปลอดทหารตลอดแนวพรมแดนเกาหลีใต้และเกาหลีเหนือเพื่อทำหน้าที่แทนทหารในเขตดังกล่าว ระบบเซ็นเซอร์อัตโนมัติของหุ่นยนต์จะทำการตรวจจับการเคลื่อนไหวบริเวณพรมแดน โดยมีรัศมีในการตรวจตราราว 2 ไมล์ และมีปืนกลขนาด 5.5 มิลลิเมตร และเครื่องยิงลูกระเบิดขนาด 40 มิลลิเมตรติดตั้งอยู่เพื่อการใช้งาน เมื่อหุ่นยนต์ตรวจพบการเคลื่อนไหวจะมีการส่งสัญญาณกลับไปที่ศูนย์บัญชาการ และทหารผู้ควบคุมการทำงานหุ่นยนต์ที่ศูนย์

---

[421] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System,”: 6-7.

[422] Natasha Bertrand and Oren Liebermann, “US assessing potential damage of Patriot missile defense system following Russian attack near Kyiv,” CNN. May 16, 2023. [online] Accessed: May 17, 2023. Available from: https://edition.cnn. com/ 2023/05/16/politics/patriot-missile-damage-ukraine/index.html

[423] John K. Hawley, “PATRIOT WARS: Automation and the Patriot Air and Missile Defense System,”: 6-7.

บัญชาการสามารถสื่อสารกับบุคคลที่หุ่นยนต์ตรวจพบได้เพื่อตัดสินใจดำเนินการต่อไป ปัจจุบันหุ่นยนต์ SGR A-1 เป็นระบบตรวจตราอัตโนมัติที่ใช้งานประกอบกับการสั่งการยิงโดยมนุษย์และยังสามารถสั่งการให้หุ่นยนต์ตัดสินใจอัตโนมัติในการยิงเป้าหมายได้ด้วยตนเองอีกด้วย[424]

ในขณะที่การใช้งานหุ่นยนต์ทหารคุ้มกันในประเทศอิสราเอลนั้น เป็นการติดตั้งหุ่นยนต์ทหารคุ้มกันในเขตพรมแดนกาซา ซึ่งหุ่นยนต์ทหารคุ้มกันจะทำหน้าที่ในการตรวจตราและรายงานผลกลับไปที่ศูนย์บัญชาการ ซึ่งจะมีทหาร (มนุษย์) เป็นผู้ประเมินข้อมูลและตัดสินใจว่าควรจะมีการสั่งยิงเป้าหมายดังกล่าวหรือไม่ ในขณะปัจจุบัน หุ่นยนต์ทหารคุ้มกันยังอยู่ภายใต้การควบคุมของมนุษย์ แต่ประเด็นที่จะต้องคิดต่อไปคือหากหุ่นยนต์สามารถทำงานได้ด้วยตนเองโดยอิสระแบบสมบูรณ์ จะมีประเด็นทางกฎหมายที่ต้องพิจารณาเพิ่มเติมหรือไม่ เนื่องจากการพัฒนาระบบตัดสินใจด้วยตนเองของหุ่นยนต์ได้เกิดขึ้นในปัจจุบันแล้ว[425]

เทคโนโลยีอาวุธที่ตัดสินใจได้ด้วยตนเองนั้นค่อนข้างเป็นนิยายทางวิทยาศาสตร์พอสมควร เพราะเป็นการสร้างอาวุธที่มีประสิทธิภาพขั้นสูงกว่าที่เคยมีมาในอดีต ถือเป็นการปฏิวัติการสงครามในยุคใหม่ เพราะโดยทั่วไปมนุษย์จะมีส่วนในการตัดสินใจเมื่อต้องใช้อาวุธในการทำลายเป้าหมาย ในขณะที่ระบบอาวุธที่ตัดสินใจได้ด้วยตนเองนั้นสามารถมีอิสระในการตัดสินใจเพื่อทำลายเป้าหมายได้โดยปราศจากการตัดสินใจของมนุษย์ ซึ่งเทคโนโลยีเหล่านี้มีการพัฒนาในปัจจุบันและมีผู้เชี่ยวชาญหลายท่านให้ความเห็นว่าอาจมีระบบอาวุธตัดสินใจได้ด้วยตนเองแบบสมบูรณ์เกิดขึ้นมาแล้ว เนื่องจากนักวิทยาศาสตร์ทางด้านคอมพิวเตอร์สามารถเขียนโปรแกรมอัลกอริทึมให้จักรกลเกิดกระบวนการเรียนรู้ได้สำเร็จแล้ว หุ่นยนต์ในปัจจุบันจึงสามารถแสดงออกตามอย่างที่มนุษย์สามารถทำได้ นอกจากนั้นระบบการโปรแกรมข้อมูลทางคอมพิวเตอร์ในปัจจุบันยังสามารถสร้างระบบการวิเคราะห์ที่ซับซ้อนแก่หุ่นยนต์ในการจดจำและพัฒนาพฤติกรรมจากประสบการณ์ที่พบเห็นได้อีกด้วย เช่น ระบบการควบคุมยานพาหนะอัตโนมัติในปัจจุบัน แม้ว่าระบบหุ่นยนต์ตัดสินใจอัตโนมัติจะยังไม่เกิดขึ้นในเชิงพาณิชย์ก็ตาม[426]

ในกองทัพเรือสหรัฐอเมริกามีการใช้ระบบอัตโนมัติที่ทำงานโดยระบบตรวจจับเป้าหมายโดยให้คลื่นแม่เหล็กไฟฟ้ามาหลายปีแล้ว เช่น ระบบอาวุธแบบ Phalanx และระบบอื่นๆ ในลักษณะเดียวกัน ซึ่งเป็นระบบอาวุธทำงานอัตโนมัติที่ติดตั้งบนเรือรบ โดยเครื่องยิงอาวุธแบบ Phalanx เป็นเครื่องยิงอาวุธ

---

[424] Cecilia Anderson, Killer Robot-Autonomous Weapons and Their Compliance with IHL, p.25.

[425] Ibid., p.25.

[426] Hitoshi Nasu and Robert McLaughlin (eds), New Technologies and the Law of Armed Conflict, p. 215-216.

ต่อต้านขีปนาวุธโดยมีระบบตรวจจับเป้าหมายอัตโนมัติ และสามารถตอบโต้ต่อเป้าหมายได้ทันทีด้วยตัวเอง ระบบดังกล่าวอาจไม่ใช่เทคโนโลยใหม่เสียทีเดียว เพราะก่อนหน้านั้นได้มีการใช้งานระบบขีปนาวุธป้องกันในรูปแบบของ ขีปนาวุธ Patriot ของสหรัฐอเมริกา และระบบอาวุธอิสราเอลที่ชื่อว่า Iron Dome มานานหลายปีแล้ว และระบบอาวุธที่ค่อนข้างตัดสินใจอิสระได้ด้วยตนเองในปัจจุบันคือเฮลิคอปเตอร์ K-Max ของกองทัพสหรัฐอเมริกาซึ่งติดตั้งโปรแกรมเส้นทางการบินอิสระด้วยตนเอง ในการขนส่งสิ่งของไปยังกองกำลังที่ปฏิบัติการณ์ในอัฟกานิสถาน เช่นเดียวกันกับเครื่องบินรบ X-47B ซึ่งติดตั้งระบบการบินขึ้นและการลงจอดแบบอัตโนมัติ[427] อย่างไรก็ดีระบบอัตโนมัติที่ติดตั้งในอากาศยานเหล่านี้ยังไม่มีการติดตั้งระบบการตัดสินใจโจมตีด้วยตนเอง แต่หน่วยงานเช่น British Royal Air Force และ US Defense Advanced Research Projects Agency (DARPA) ยังคงพัฒนาระบบอาวุธตัดสินใจได้ด้วยตนเองต่อไป[428]

อิสราเอลได้ทำการทดสอบระบบป้องกันประเทศทางเลือกอื่นนอกเหนือจากระบบ Iron Dome ซึ่งเป็นระบบป้องกันขีปนาวุธระยะใกล้ โดยระบบดังกล่าวคือระบบ Iron Beam เป็นเลเซอร์ป้องกันขีปนาวุธระยะใกล้แบบจำกัดเป้าหมาย ซึ่งมีการทดลองมาหลายครั้งจนกระทั่งประสบผลสำเร็จ[429]

ระบบป้องกันประเทศดังกล่าวเป็นผลมาจากความร่วมมือของ กองทัพอิสราเอล (IDF: Israel Defense Forces) กับกองทัพสหรัฐอเมริกา ซึ่งเริ่มมาตั้งแต่สงครามอ่าวเปอร์เซีย

การพัฒนาระบบเลเซอร์เพื่อการป้องกัน ทำโดยบริษัท Israel Advance Defense System โดยตัวต้นแบบสร้างเสร็จเมื่อปี 2009 ใช้ชื่อว่า Iron Beam High-Energy Laser (HEL) เปิดตัวครั้งแรกในงานสิงคโปร์แอร์โชว์ ในปี 2014 มีระบบการทำงานแบบ dual multi-kilowatt solid-state lasers สามารถทำงานร่วมกับระบบเรดาร์และพาหนะเคลื่อนที่ไกล มีระยะทำลายเป้าหมายประมาณ 7 กิโลเมตร โดยสามารถทำลายขีปนาวุธ โดรน และกระสุนปืนใหญ่ ภายใน 4 วินาที หลังจากที่ระบบเซ็นเซอร์ตรวจจับเป้าหมายได้

---

[427] Hitoshi Nasu and Robert McLaughlin (eds), New Technologies and the Law of Armed Conflict, pp. 216-217.

[428] Ibid., p. 217.

[429] Mark Episkopos, "Forget the Iron Dome: This Israel Laser is Changing Air Defense," The National Interest, July 15, 2021, [online] Accessed: April 19, 2022. Available from: https://nationalinterest.org/blog/reboot/forget-iron-dome-israeli-laser-changing-air-defense-189704

เหตุที่มีการศึกษาระบบทางเลือกในการป้องกันประเทศดังกล่าวเนื่องจาก ระบบ Iron Dome มีต้นทุนสูง และไม่ทนทาน เมื่อเปรียบเทียบระบบ Iron Dome กับนะบบ Iron Beam แล้ว Iron Beam มีต้นทุนเพียง 2,000 เหรียญสหรัฐอเมริกาต่อการยิง 1 ครั้ง ในขณะที่ Iron Dome มีต้นทุนถึง 100,000-150,000 เหรียญสหรัฐ ต่อการยิง 1 ครั้ง อย่างไรก็ดี โครงการนำ Iron Beam มาใช้ยังคงไม่เกิดขึ้น เพราะรัฐบาลอิสราเอลเองก็มีประเด็นความขัดแย้งทางการเมืองภายในเกี่ยวกับงบประมาณในการป้องกันประเทศ

2.4.1.3 อุปกรณ์บังคับวิทยุกับอากาศยานไร้คนขับ

ระบบพาหนะไร้คนขับ (Unmanned Vehicle System) เป็นการนำเอาระบบการควบคุมพาหนะระยะไกลมาใช้ร่วมกับปฏิบัติการทางทหาร โดยระบบพาหนะไร้คนขับนี้หมายรวมถึงพาหนะไร้คนขับทางบก พาหนะไร้คนขับทางน้ำ และพาหนะไร้คนขับทางอากาศ (อากาศยานไร้คนขับ) ทั้งนี้ในการศึกษาวิจัยนี้อาจไม่ได้ให้ความสำคัญกับระบบพาหนะไร้คนขับทางบกและพาหนะไร้คนขับทางน้ำเท่ากับระบบอากาศยานไร้คนขับ ด้วยเหตุผลว่าระบบพาหนะไร้คนขับทุกระบบนั้นมีระบบการทำงานพื้นฐานที่คล้ายกัน แต่ระบบอากาศยานไร้คนขับมีลักษณะการทำงานบางประการที่แตกต่างจากพาหนะไร้คนขับระบบอื่นอย่างมีนัยสำคัญ อันได้แก่

1) ระบบอากาศยานไร้คนขับมีระยะทำการที่สร้างความได้เปรียบในการต่อสู้มากกว่าระบบพาหนะไร้คนขับชนิดอื่น เนื่องจากเป็นการใช้พื้นที่ทางอากาศจึงสะดวกในการเดินทางผ่านพื้นที่ต่างๆ จึงทำให้สามารถเข้าถึงเป้าหมายได้เร็ว และสามารถโจมตีเป้าหมายเฉพาะเจาะจงได้อย่างแม่นยำ ระบบอากาศยานไร้คนขับจึงเป็นที่นิยมอย่างแพร่หลายในปัจจุบันสำหรับปฏิบัติการทางทหารของกองทัพและกลุ่มกองกำลังต่างๆ

2) ระบบอากาศยานไร้คนขับมีลักษณะการทำงานที่หลากหลาย ยืดหยุ่น และสามารถพัฒนาได้อย่างกว้างขวาง เนื่องจากระบบอากาศยานไร้คนขับเป็นการเดินทางในพื้นที่ทางอากาศสามารถเดินทางไปตำแหน่งต่างๆ ได้สะดวกจึงเหมาะกับการใช้งานเพื่อการลาดตระเวน การตรวจตรา การค้นหาเป้าหมาย การระบุเป้าหมายการโจมตี รวมถึงการโจมตีเป้าหมาย โดยอาจทำหนึ่งหรือหลายภารกิจได้ในปฏิบัติการเดียว นอกจากนั้น การพัฒนาระบบอากาศยานไร้คนขับยังมีต่อเนื่องและหลากหลายตามภารกิจที่แตกต่างของอากาศยานไร้คนขับด้วย เช่น อากาศยานไร้คนขับเพื่อการจารกรรมสามารถพัฒนาให้มีขนาดเล็กลงได้ อากาศยานไร้คนขับเพื่อการโจมตีสามารถติดตั้งระบบนำ

วิถีและอาวุธยิงแบบนำวิถีได้ นอกจากนั้นยังปรากฏหลายกรณีว่ามีการประยุกต์ใช้อากาศยานไร้คนขับเชิงพาณิชย์เพื่อปฏิบัติการโจมตีทางทหารด้วย อากาศยานไร้คนขับจึงเป็นระบบพาหนะที่สร้างประเด็นข้อพิจารณาทางกฎหมายค่อนข้างมาก

ระบบอากาศยานไร้คนขับอาจแบ่งเป็นประเภทต่างๆ ตามภารกิจได้ดังนี้

(1) อากาศยานไร้คนขับซึ่งสามารถค้นหาและทำลายเป้าหมายได้อัตโนมัติ อากาศยานไร้คนขับที่สามารถปฏิบัติภารกิจค้นหาเป้าหมายและสามารถทำลายเป้าหมายได้อย่างอิสระนั้นยังอยู่ในระหว่างการพัฒนา[430] ทั้งนี้ไม่พบรายงานการใช้งานระบบกาศยานไร้คนขับโจมตีอิสระเต็มรูปแบบแต่อย่างใดแม้มีการอ้างจากกองทัพรัสเซียว่ามีการใช้อากาศยาน KUB-BLA ซึ่งเป็นอากาศยานระบบปัญญาประดิษฐ์ที่สามารถค้นหาและโจมตีเป้าหมายรวมถึงสามารถทำการหลบหนีการติดตามได้ก็ตาม

โดยปกตินั้นอากาศยานไร้คนขับส่วนใหญ่อาศัยคลื่นวิทยุในการส่งและรับสัญญาณควบคุมของผู้ปฏิบัติงาน ส่งภาพวิดีโอ และใช้ระบบนำทางผ่าน GPS รวมถึงการใช้เทคนิคเทียบเคียงพื้นที่ทางภูมิศาสตร์ด้วยกลุ่มดาวบริวารอื่นๆ อากาศยานไร้คนขับชนิดปฏิบัติภารกิจด้วยตัวเองเต็มรูปแบบนั้นยังไม่พบรายงานว่ามีการใช้ในสถานการณ์ใด ดังนั้นการต่อต้านอากาศยานไร้คนขับนั้นอาจกระทำได้โดยเทคนิคการรบกวนคลื่นสัญญาณวิทยุ ซึ่งทำได้ 2 วิธีการ คือ 1) การครอบครองคลื่นวิทยุด้วยปฏิบัติการทางไซเบอร์และ 2) การรบกวนคลื่นสัญญาณวิทยุ ทั้งสองวิธีการนี้มีข้อดีและข้อเสียแตกต่างกัน แต่อาจใช้งานทั้งสองวิธีการนี้เสริมกันในยุทธวิธีต่อต้านภัยคุกคามขั้นสูงได้[431]

ปัจจุบันหน่วยงานที่พัฒนาระบบอากาศยานไร้คนขับโจมตีอิสระมีค่อนข้างหลากหลาย เช่น หน่วยงาน US Defense Advanced Research Projects Agency หรือ DARPA[432] ซึ่งพัฒนาระบบ Semi-Autonomous หรือกึ่งอิสระ ได้แก่ US Air Force's RQ1 และ MQ1 Predators ซึ่งยังคงอาศัยการควบคุมและการตัดสินใจจากมนุษย์ ในขณะที่ระบบการทำลาย

---

[430] Cecilia Anderson, Killer Robot-Autonomous Weapons and Their Compliance with IHL, p.26.

[431] Defence Review Asia Staff, "What is the best drone defeat technique?" Defence Review Asia, March 21, 2023, [online] Accessed: March 22, 2023. Available from: https://defencereviewasia.com/what-is-the-best-drone-defeat-technique/

[432] Ugo Pagallo, The Law of Robot: Crimes, Contracts and Torts, p. ix.

เป้าหมายโดยอัตโนมัติปรากฏอยู่ในการใช้งานเครื่องยิงจรวดต่อต้านเรือรบที่ชื่อว่า Phalanx CIWS ของกองทัพเรือสหรัฐอเมริกา[433]

ขณะที่บริษัทในเครือ Zala Aero ของประเทศรัสเซียมีการพัฒนาอากาศยานไร้คนขับโจมตีอิสระ KUB-BLA ซึ่งอ้างว่าสามารถบินด้วยความเร็ว 130 กิโลเมตรต่อชั่วโมง มีระยะเวลาทำการบิน 30 นาที ระยะทำการไกล 40 กิโลเมตร บรรทุกวัตถุระเบิดได้ 3 กิโลกรัม โดยอาวุธยิงที่ติดตั้งในอากาศยานไร้คนขับ KUB-BLA นี้สามารถติดตั้งระบบนำวิถีและหัวรบได้

(2) ระบบพาหนะไร้คนขับซึ่งใช้ในการลาดตระเวนและค้นหาเป้าหมาย การใช้อากาศยานไร้คนขับชนิดลาดตระเวนและค้นหาเป้าหมายเริ่มปรากฏเป็นรูปธรรมหลังเหตุการณ์ 11 กันยายน พ.ศ.2544 (ค.ศ.2001) โดยเป็นการใช้อากาศยานไร้คนขับของกองทัพสหรัฐอเมริกาเพื่อต่อต้านการก่อการร้ายของกลุ่มอัลเคด้า (Al Qaeda) ในประเทศอัฟกานิสถาน[434] ปฏิบัติการทางทหารด้วยการใช้อากาศยานไร้คนขับของกองทัพสหรัฐอเมริกานั้นเริ่มต้นเพื่อการค้นหาบุคคลเป้าหมายซึ่งเป็นผู้นำกลุ่มก่อการร้ายนายโอซามา บิน ลาเดน (Osama bin Laden) เริ่มมีการขยายพื้นที่ในการปฏิบัติการจากประเทศอัฟกานิสถานเป็นพื้นที่ประเทศอื่นๆ ในช่วงเวลาต่อมา โดยพบปฏิบัติการใช้อากาศยานไร้คนขับในประเทศต่างๆ ถึง 6 ประเทศ ได้แก่ อัฟกานิสถาน อิรัก ปากีสถาน เยเมน โซมาเลีย และลิเบีย[435] รัฐบาลสหรัฐอเมริกาอ้างว่าการใช้งานอากาศยานไร้คนขับของกองทัพสหรัฐอเมริกาดังกล่าวเป็นไปเพื่อเหตุผลของการป้องกันตัว แต่ในความเป็นจริงแล้วลักษณะของปฏิบัติการนั้นมีความใกล้เคียงกับลักษณะของการคุกคามต่อสันติภาพตามข้อ 2 (4) ของกฎบัติสหประชาชาติ[436] เนื่องจากเป็นการใช้อากาศยานไร้คนขับในปฏิบัติการทางทหารเพื่อวัตถุประสงค์ในการโจมตีเป้าหมายในดินแดนของประเทศอื่นเป็นสำคัญ

ในปัจจุบันนั้นกองทัพสหรัฐอเมริกายังคงมีการใช้อากาศยานไร้คนขับเพื่อการสอดแนมในปฏิบัติการหลายแห่ง เช่น อากาศยานไร้คนขับเพื่อการสอดแนม MQ-9 (Reaper) ซึ่งล่าสุดได้

---

[433] Ugo Pagallo, The Law of Robot: Crimes, Contracts and Torts, p.3.

[434] Craig Martin, "Target Killing, Self-Defense, and the Jus ad Bellum Regime," in Claire Finkelstein, Jens David Ohlin, Andrew Altman (eds.), Targeted Killings: Law & Morality in an Asymmetrical World, (Oxford: Oxford University Press, 2012), p. 223.

[435] Ibid., p. 223.

[436] Ibid., p. 224.

ถูกเครื่องบินขับไล่ของกองทัพรัสเซียสกัดการปฏิบัติการจนอากาศยานไร้คนขับดังกล่าวตกลงในทะเลดำ[437] ฯลฯ

(3) การควบคุมอาวุธระยะไกล (Remote control weapons) การควบคุมอาวุธระยะไกลปรากฏพัฒนาการในการขัดกันทางอาวุธระหว่างยูเครนและรัสเซีย โดยยูเครนได้มีการพัฒนาแอพลิเคชั่นสำหรับคอมพิวเตอร์ แทปเล็ต และโทรศัพท์มือถือ สำหรับกองทัพในการสั่งยิงปืนใหญ่และจรวดต่อสู้กองทัพรัสเซีย แอพลิเคชั่นนี้เป็นที่นิยมในกองทัพทหารยูเครนมากขึ้นในปัจจุบัน การสั่งการทางไกลนี้สามารถทำงานร่วมกับสัญญาณดาวเทียมและข้อมูลกรองเกี่ยวกับภาพถ่ายทางอากาศ มีการประมวลผลผ่านอัลกอริทึ่มแบบเรียลไทม์เพื่อการยิงเป้าหมายเฉพาะเจาะจงอย่างแม่นยำ การใช้แอพลิเคชั่นในรูปแบบนี้เป็นที่นิยมเนื่องจากสามารถอัพเดทข้อมูลได้รวดเร็ว มีต้นทุนที่ต่ำ และมีประสิทธิภาพดี[438]

ตัวอย่างการใช้งานอากาศยานไร้คนขับในปฏิบัติการทางทหารในสถานการณ์ความขัดแย้งได้แก่ กรณีดังต่อไปนี้

การใช้อากาศยานไร้คนขับของกองทัพสหรัฐอเมริกาในปฏิบัติการต่อต้านการก่อการร้ายในประเทศเยเมนและปากีสถาน[439]

วันที่ 23 มีนาคม พ.ศ.2558 สำนักข่าวอิสระ The Bureau of Investigative Journalism รายงานข่าวว่ารัฐบาลสหรัฐอเมริกาส่งอากาศยานไร้คนขับ (โดรน) จำนวน 90 ถึง 109 ลำ เพื่อปฏิบัติการโจมตีในประเทศเยเมน โดยมีการสังหารบุคคลไปประมาณ 431-639 คน ในจำนวนนี้มีพลเรือนอยู่ประมาณ 65-96 คน และคาดว่ามีเด็กเสียชีวิตประมาณ 8 คน ส่วนกรณีการปฏิบัติการของอากาศยานไร้คนขับของรัฐบาลสหรัฐอเมริกาในประเทศปากีสถานนั้นมีรายงานว่ามีการใช้อากาศยานไร้คนขับประมาณ 363 ลำ มีการสังหารบุคคล

---

[437] Oren Liebermann, Jennifer Hansler, Haley Britzky, and Natasha Bertrand, "Russian fighter jet forces down US drone over Black Sea," CNN online, March 15, 2023, [online] Accessed: March 20, 2023. Available from: https://edition.cnn.com/2023/03/14/politics/us-drone-russian-jet-black-sea/index.html

[438] Katie Bo Lillis and Oren Liebermann, "How Ukraine became a testbed for Western weapons and battlefield innovation," CNN, January 16, 2023, [online] Accessed: February 20,2023. Available from: https://edition.cnn.com/2023/01/15/politics/ukraine-russia-war-weapons-lab/index.html

[439] Jeffrey Bachman, " The New York Times and Washington Post: Misleading the public about US drone strikes," Journalism Studies, Vol. 18, No.4, (2017): 470-494.

ประมาณ 2,445-3,945 คน ในจำนวนนี้ประกอบด้วยพลเรือนเสียชีวิตประมาณ 421-960 คน และมีการประมาณการว่าพลเรือนที่เสียชีวิตดังกล่าวเป็นเด็กประมาณ 172-207 คน[440]

อย่างไรก็ดี ปรากฏว่าหน่วยงานของรัฐบาลสหรัฐอเมริกาหลายหน่วยงานออกมาแถลงข่าวในลักษณะที่แตกต่างออกไป ได้แก่ สำนักข่าวกรองแห่งสหรัฐอเมริกา (CIA) ออกมาแถลงข่าวว่าจำนวนผู้เสียชีวิตจากปฏิบัติการอากาศยานไร้คนขับของรัฐบาลสหรัฐอเมริกามีจำนวนเพียงหลักหน่วย[441] ขณะที่ประธานาธิบดีในขณะนั้นคือนายบารัค โอบามาได้แถลงว่าปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับของสหรัฐอเมริกาเป็นไปอย่างเข้มงวดและแม่นยำจึงเกิดผลกระทบต่อพลเรือนในสัดส่วนที่ต่ำ[442] และรองประธานวุฒิสภา Dianne Feinstein ได้กล่าวอ้างข้อมูลในลักษณะเดียวกันว่าจำนวนผู้เสียชีวิตจากการโจมตีด้วยอากาศยานไร้คนขับของรัฐบาลสหรัฐอเมริกามีจำนวนเพียงหลักหน่วยเท่านั้น[443] นอกจากนั้นยังมีหน่วยงานของรัฐบาลอเมริกาหลายหน่วยงาน เช่น ที่ปรึกษาทางด้านกฎหมายของประธานาธิบดีและที่ปรึกษากระทรวงกลาโหมของสหรัฐอเมริกาต่างกล่าวอ้างในลักษณะเดียวกันว่าในปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับของกองทัพสหรัฐอเมริกานั้นเป็นไปโดยชอบด้วยกฎหมายสอดคล้องต่อกฎหมายว่าด้วยการขัดกันทางอาวุธและกฎหมายมนุษยธรรมระหว่างประเทศ เช่นอนุสัญญาเจนีวา ค.ศ.1949 กฎหมายจารีตประเพณีระหว่างประเทศรวมถึงสอดคล้องต่อหลักการขั้นพื้นฐานอื่นๆ ด้วย เช่นหลักการแยกแยะ หลักความได้สัดส่วน รวมตลอดถึงการทำตามบรรทัดฐานการทำสงครามที่เกิดขึ้นมาในอดีต[444]

---

[440] Jeffrey Bachman, “The New York Times and Washington Post: Misleading the public about US drone strikes,”: 472.

[441] Scott Shane and Salman Masood, “Drone Strike in Pakistan Kills Haqqani Commander,” The New York Times, October 14, 2011, [online] Accessed: April 10, 2021. Available from: https://www.nytimes.com/2011/10/14/world/asia/drone-attack-in-pakistan-kills-a-haqqani-leader.html

[442] Mark Landler, “Civilian Deaths Due to Drones are not Many, Obama Says,” The New York Times, January 30, 2012. [online] Accessed: April 10, 2022. Available from: https://www.nytimes.com/2012/01/31/world/middleeast/civilian-deaths-due-to-drones-are-few-obama-says.html

[443] Lee Ferran, “Intel Chair: Civilian Drone Casualties in ‘Single-Digits’ Year-to-Year,” ABC News, February 7, 2013. [online] Accessed: April 10, 2022. Available from: http://abcnews.go.com/blogs/headlines/2013/02/intel-chair-civilian-dronecasualties-in-single-digits-year-to-year/.

[444] Jeffrey Bachman, “ The New York Times and Washington Post: Misleading the public about US drone strikes,”: 490.

Amnesty International ให้ข้อมูลในทำนองกลับกันกับสิ่งที่รัฐบาลสหรัฐอเมริกากล่าวอ้าง โดย Amnesty International รายงานว่าปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับของรัฐบาลสหรัฐอเมริกาในประเทศปากีสถานนั้นก่อให้เกิดความเสียหายแก่ชีวิตบุคคลโดยผิดกฎหมายและอาจเข้าข่ายการกระทำที่เป็นอาชญากรรมสงคราม[445] นอกจากนั้น องค์กร Human Rights Watch ยังกล่าวอ้างว่าจากการสืบสวนมีอากาศยานไร้คนขับจำนวนหนึ่งซึ่งปฏิบัติภารกิจในประเทศเยเมนปรากฏว่ามีการกระทำการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศโดยมีการสังหารพลเรือนและเป็นการใช้อาวุธโดยไม่เลือกปฏิบัติ[446]

สำนักข่าวต่างๆ รายงานความเสียหายที่เกิดขึ้นจากการใช้อากาศยานไร้คนขับของกองทัพสหรัฐอเมริกาแตกต่างออกไปจากข่าวของรัฐบาลสหรัฐอเมริกาและข้อมูลดังกล่าวก็ไม่ตรงกับรายงาน ของหน่วยงานภาคเอกชน เช่น Amnesty International และ Human Rights Watch ตัวอย่างข่าวที่ปรากฏได้แก่

วันที่ 17 พฤษภาคม พ.ศ.2552 สำนักข่าว The New York Times พาดหัวข่าวว่า “ทหาร 25 นาย เสียชีวิตจากปฏิบัติการโจมตีที่ปากีสถาน” โดยไม่มีการระบุถึงความเสียหายที่เกิดขึ้นต่อพลเรือน[447] ในขณะที่ The Bureau of Investigative Journalism ระบุว่ามีพลเรือนราว 9 คนเสียชีวิตจากปฏิบัติการดังกล่าวด้วย[448]

[445] Amnesty International, “‘Will I Be Next?’: US Drone Strikes in Pakistan,” (New York: Amnesty International, 2013), p.43. [online] Accessed: October 22, 2022. Available from: https://www.amnesty.org/en/documents/asa33/013/2013/ en/

[446] Human Rights Watch, Between a Drone and Al-Qaeda: The Civilian Cost of US Targeted Killings in Yemen, Human Rights Watch, 2013, pp.3-6. [online] Accessed: October 22, 2022. Available from: https://www.hrw.org/sites/default/ files/report_pdf/yemen1013web.pdf

[447] Pir Zubair Shah, Sabrina Tavernise, Mark Mazzetti. “Taliban Leader in Pakistan Is Reportedly Killed.” The New York Times, August 8, 2009. [online] Accessed: April 9, 2020. Available from: https://www.nytimes.com/2009/08/08/world /asia/08pstan.html

[448] Bureau of Investigative Journalism, “Obama 2009 Pakistan Strikes.” The Bureau of Investigative Journalism, August 10, 2011. [online] Accessed: April 9, 2020. Available from: http://www.thebureauinvestigates.com/2011/08/10 /obama2009-strikes/

ขณะที่วันที่ 1 กันยายน พ.ศ.2555 สำนักข่าว The New York Times พาดหัวข่าวว่า “เยเมน: โดรนสังหารกลุ่มบุคคลซึ่งคาดว่าเป็นทหาร”[449] รายงานข่าวระบุว่ามีผู้เสียชีวิตจากการโจมตีจำนวน 8 คน และเป็นทหารทั้งหมด แต่ The Bureau of Investigative Journalism รายงานว่ามีผู้เสียชีวิตจากปฏิบัติการดังกล่าว 12 คน โดยผู้เสียชีวิตทั้งหมดเป็นพลเรือน[450] ข้อมูลที่ปรากฏในข่าวของ The New York Times นั้นนำมาจาก The Associated Press ซึ่ง The New York Times ได้มีการพิจารณาเนื้อหาก่อนที่จะเผยแพร่ข้อมูลแล้ว จึงถือเป็นความรับผิดชอบของสำนักข่าว The New York Times

The Washington Post ได้พาดหัวข่าววันที่ 24 มิถุนายน พ.ศ.2552 ว่า “ปฏิบัติการโจมตีทางอากาศคร่าชีวิตกลุ่มผู้ก่อความไม่สงบหลายราย” โดยรายละเอียดตามข่าวระบุว่ากลุ่มเป้าหมายที่ถูกโจมตีมีจำนวน 52 คน[451] ในขณะที่ The Bureau of Investigative Journalism ทราบว่ามีผู้เสียชีวิตจากปฏิบัติการดังกล่าวประมาณ 60-83 คน ในจำนวนนี้มีการยืนยันว่าเป็นพลเรือนประมาณ 18 คน และปฏิบัติการดังกล่าวยังทำให้พลเรือนราว 50 คนเกือบเสียชีวิต[452]

ข้อมูลการปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับของประเทศสหรัฐอเมริกาก่อให้เกิดความสับสนค่อนข้างมากระหว่างการรายงานข่าวของรัฐบาล องค์กรเอกชน และสำนักข่าวต่างๆ โดยหน่วยงานของรัฐมักจะรายงานความเสียหายต่อพลเรือนในจำนวนน้อย ในขณะที่หน่วยงานเอกชนและสำนักข่าวต่างๆ รายงานความเสียหายต่อพลเรือนในจำนวน

[449] Associated Press, “Yemen: Drone Kills Suspected Militants, Officials Say. The New York Times, September 1, 2012. [online] Accessed: April 9, 2020. Available from: https://www.nytimes.com/2012/09/01/world/middleeast/drone-kills-suspected-militants-in-yemen-officials-say.html

[450] Bureau of Investigative Journalism, “Yemen: Reported US Covert Action 2012,” Bureau of Investigative Journalism, [online] Accessed: April 9, 2020. Available from: https://www.thebureauinvestigates.com/2012/05/08/yemen-reported-us-covert-action-2012/.

[451] Joby Warrick, “Airstrike Kills Dozens of Insurgents,” Washington Post, June 24, 2009. [online] Accessed: April 9, 2020. Available from: http://www.washingtonpost.com

[452] Bureau of Investigative Journalism, “Obama 2009 Pakistan Strikes.” The Bureau of Investigative Journalism, August 10, 2011.

ค่อนข้างมาก และการรายงานข่าวความเสียหายที่ค่อนข้างมากของสำนักข่าวต่างๆ สร้างความสงสัยต่อประชาชนค่อนข้างมาก

ในมุมมองของผู้สื่อข่าวในท้องที่ได้มีการรายงานว่าปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับนั้นมีผลกระทบต่อชีวิตพลเรือนค่อนข้างมาก เพราะในการโจมตีหลายครั้งนั้นผู้ถูกโจมตีไม่ทราบเลยว่าตนเองจะถูกยิงโดยอากาศยานไร้คนขับเมื่อใด บางครั้งก็มีการโจมตีระหว่างที่เป้าหมายทำละหมาดตอนเช้า บางครั้งเป็นการโจมตีระหว่างการเดินทางไปมัสยิด ในขณะที่บางครั้งการโจมตีเกิดขึ้นระหว่างที่เป้าหมายกำลังทำอาหารและอยู่กับครอบครัวในสวนหลังบ้าน[453] มุมมองของผู้สื่อข่าวในพื้นที่รายนี้สะท้อนให้เห็นถึงทัศนะของคนทั่วไปที่เห็นผลกระทบจากการใช้อากาศยานไร้คนขับเพื่อการโจมตีหลายประเด็น ได้แก่ ปฏิบัติการโจมตีระยะไกลก่อให้เกิดความได้เปรียบของผู้โจมตีเป็นอย่างมาก ในขณะที่ผู้ถูกโจมตีป้องกันตัวเองได้น้อยมากหรือแทบป้องกันตัวไม่ได้เลย ความเสียหายของผู้โจมตีอาจได้แก่การสูญเสียอากาศยานไร้คนขับ แต่ความสูญเสียของเป้าหมายคือชีวิตและร่างกาย การโจมตีด้วยอากาศยานไร้คนขับนั้นเป็นปฏิบัติการระยะไกลแต่มีความแม่นยำในการโจมตีเป้าหมายมาก หากผู้ควบคุมปฏิบัติการโจมตีระบุเป้าหมายตามข้อมูลที่ได้รับการยืนยันจากหน่วยงานบังคับบัญชามา แต่ข้อมูลดังกล่าวเป็นข้อมูลที่ผิดพลาด เช่น เป้าหมายดังกล่าวไม่ใช่กลุ่มผู้ก่อความไม่สงบหรือเป็นเพียงพลเรือนธรรมดา การโจมตีด้วยอากาศยานไร้คนขับซึ่งสามารถสั่งการได้รวดเร็วนี้ย่อมนำมาซึ่งความเสียหายแก่บุคคลที่ได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศได้ หรือแม้แต่กรณีที่ผู้ปฏิบัติการโจมตีเห็นเป้าหมายผ่านกล้องซึ่งติดตั้งในอากาศยานไร้คนขับ และจะต้องตัดสินใจโจมตีแต่การตัดสินใจดังกล่าวผิดพลาด เพราะเป้าหมายไม่ใช่ทหารหรือผู้ก่อการร้ายจริง ความเสียหายย่อมเกิดขึ้นได้ง่ายกว่าการโจมตีด้วยบุคคลปกติ นอกจากนั้น การโจมตีระยะไกลยังส่งผลต่อความรู้สึกของคนทั่วไปว่าจะมีผลให้ผู้ควบคุมปฏิบัติการตัดสินใจตามหลักศีลธรรมลดลง โดยมีทัศนะว่าการโจมตีระยะไกลตัดสินใจได้ง่าย แม้ว่าการกระทำดังกล่าวจะทำให้คนเสียชีวิต แต่ผู้ปฏิบัติการจะรู้สึกถึงความรับผิดชอบน้อยลงเพราะไม่ได้เป็นปฏิบัติการโดยตรงของมนุษย์ในสนามรบ (เทียบกับความรู้สึกของผู้ใช้งานแพลตฟอร์มสื่อสังคมออนไลน์ ที่มักจะมีการแสดงออกในเชิงรุนแรง หยาบคาย หรือ

[453] James DeShaw Rae, "Remote Killing and the Ethics of Drone Warfare," in James DeShaw Rae (eds), Analyzing the Drone Debates: Targeted Killing, Remote Warfare, and Military Technology, (New York: Palgrave Pivot, 2014). pp.79-97. [online] Accessed: April 9, 2020. Available from: https://doi.org/10.1057/9781137381576_4,

การสร้างข้อความเท็จ เพราะผู้ใช้งานสื่อสังคมออนไลน์มักรู้สึกว่าโลกออนไลน์เป็นโลกเสมือนตนอยู่ห่างไกลจากผู้รับสารจึงสามารถทำอะไรก็ได้และไม่ต้องรับผิดชอบจากสิ่งที่กระทำดังกล่าว)

กรณีการใช้อากาศยานไร้คนขับในการขัดกันทางอาวุธกรณีความขัดแย้งระหว่างประเทศรัสเซียและประเทศยูเครน

ความขัดแย้งทางการเมืองระหว่างประเทศรัสเซียและประเทศยูเครนซึ่งมีมาอย่างยาวนานได้ปะทุขึ้นจนเป็นเหตุการขัดกันทางอาวุธ เนื่องจากกรณีที่ประเทศยูเครนต้องการเข้าเป็นสมาชิกขององค์กรสนธิสัญญาเพื่อการป้องกันแอตแลนติกเหนือ (NATO) ซึ่งขัดกับความประสงค์ของผู้นำประเทศรัสเซียที่ต้องการให้ประเทศยูเครนเป็นกลาง จนเมื่อวันที่ 24 กุมภาพันธ์ พ.ศ.2562 ประธานาธิบดีของรัสเซีย นายวลาดิเมียร์ ปูตินได้แถลงการณ์ผ่านโทรทัศน์ว่าตนอนุมัติปฏิบัติการพิเศษของกองกำลังทหารในการบุกเข้าไปยังพื้นที่ดอนบาสก์ของยูเครน[454] และมีข้อเรียกร้องให้ทหารยูเครนวางอาวุธและกลับบ้าน

ประเทศยูเครนเองได้ทำการต่อต้านการบุกของกองทัพรัสเซีย โดยใช้กองกำลังทหารของตนเอง หน่วยอาสาสมัครที่รัฐบาลขอความช่วยเหลือจากประชาชน พร้อมกันนี้กองกำลังยูเครนได้รับการสนับสนุนทางด้านยุทโธปกรณ์จากประเทศในยุโรปหลายประเทศ โดยหนึ่งในเทคโนโลยีที่ทำให้กองทัพยูเครนได้เปรียบกองทัพรัสเซียอย่างมากคืออากาศยานไร้คนขับสังหาร Bayraktar TB-2 ซึ่งมีการปล่อยภาพเคลื่อนไหวการใช้อากาศยานไร้คนขับของกองทัพยูเครนเพื่อทำลายรถบรรทุกขีปนาวุธของกองทัพรัสเซีย ในวันที่ 27 กุมภาพันธ์ พ.ศ. 2565 ซึ่งนับเป็นภาพการโจมตีกองทัพรัสเซียด้วยอากาศยานไร้คนขับภาพแรกที่ปรากฏในความขัดแย้งครั้งนี้ หลังจากนั้นได้มีการใช้อากาศยานไร้คนขับ Bayraktar TB-2 ในปฏิบัติการทางทหารของกองทัพยูเครนอีกหลายครั้ง โดยในวันที่ 2 พฤษภาคม พ.ศ.2565 กองทัพ

[454] "ความขัดแย้งระหว่างรัสเซีย-ยูเครน 2 เมื่อต่างฝ่ายยืนยันที่จะสู้เพื่อปกป้องประเทศ," (25 กุมภาพันธ์ 2565). https://themomentum.co/report-russia-ukraine-fight-2/.

ยูเครนได้ใช้อากาศยานไร้คนขับ Bayraktar TB-2 โจมตีเรือเร็วโจมตีชายฝั่งของกองทัพรัสเซีย บริเวณใกล้เคียงกับเกาะ Zmiilinyi ซึ่งอยู่ห่างจากโอเดสซาไป 70 ไมล์ทะเล[455]

อากาศยานไร้คนขับ Bayraktar TB-2 เป็นอากาศยานไร้คนขับทางยุทธวิธีแบบติดอาวุธขนาดกลาง และปฏิบัติการรบในระดับความสูงปานกลาง พัฒนาและผลิตโดยบริษัท Baykar Savunma ในประเทศตุรกี โดย Bayraktar TB-2 เป็นอากาศยานไร้คนขับโจมตีซึ่งมีความแม่นยำสูง และมีระบบการทำงานที่ซับซ้อน คือการทำงานร่วมกันระหว่างเทคโนโลยีอากาศยานไร้คนขับ ระบบยิงขีปนาวุธ มีการควบคุมผ่านสถานีภาคพื้นดินซึ่งจะทำการสนับสนุนข้อมูลการบินและการรับภาพระยะไกลที่ส่งมาจากกล้องติดอากาศยาน โดยสถานีปฏิบัติการนี้จะเป็นสถานีเคลื่อนที่ซึ่งติดตั้งกับรถบรรทุกทางการทหาร มีผู้ควบคุม 3 คน คือ นักบิน ทหารสื่อสาร และฝ่ายบัญชาการภารกิจ

โครงสร้างหลักของ Bayraktar TB-2 ผลิตจากคาร์บอนไฟเบอร์ เคฟล่าร์ และวัสดุสังเคราะห์แบบผสม มีการติดตั้งระบบกล้องบันทึกภาพพร้อมระบบอินฟาเรดความละเอียดสูง สามารถบันทึกได้ทั้งภาพนิ่งและภาพเคลื่อนไหว และระบบเลเซอร์เพื่อค้นหาและระบุเป้าหมาย ขับเคลื่อนด้วยเครื่องยนต์เบนซินขนาด 75 กิโลวัตต์ ให้กำลัง 100 แรงม้าเพื่อหนุนใบพัด ติดตั้งขีปนาวุธ 4 ลูก ซึ่งทำงานด้วยระบบนำวิถีด้วยเลเซอร์ (MAM-L laser-guided bombs) และระบบขีปนาวุธต่อต้านรถถัง OMTAS Anti-tank Missiles[456]

Bayraktar TB-2 มีภารกิจหลักแบบ ISR คือ การสอดแนม การเฝ้าระวังและการลาดตระเวน (Intelligence, Surveillance and Reconnaissance) มีอายุการใช้งานประมาณ 400,000 ชั่วโมง การปฏิบัติภารกิจแต่ละครั้งสามารถอยู่ในอากาศได้นาน 27 ชั่วโมง 3 นาที ที่ระดับความสูง 25,030 ฟุต หรือ 7,629 เมตร

Bayraktar TB-2 ไม่ได้มีไว้เพื่อใช้งานเฉพาะกองทัพยูเครนเท่านั้น เพราะบริษัท Baykar Savunma ได้ผลิต Bayraktar TB-2 และส่งมอบให้กับกองทัพหลายประเทศด้วยกัน ได้แก่ กองทัพตุรกี กองทัพกาตาร์ กองทัพอาเซอร์ไบจาน กองทัพเติร์กเมนิสถาน และกองทัพ

---

[455] อาคม รวมสุวรรณ, “ส่องโดรนพิฆาต Bayraktar TB-2 จนเรือเร็วตรวจฝั่งรัสเซียดิ่งทะเลดำสองลำซ้อน,” ไทยรัฐออนไลน์, วันที่ 4 พฤษภาคม พ.ศ.2565. [online] สืบค้นเมื่อวันที 10 พฤษภาคม พ.ศ.2565 จากเว็บไซต์ https://www.thairath.co.th/news/auto/news/2383455

[456] เรื่องเดียวกัน.

โปแลนด์ นอกจากนี้ Bayraktar TB-2 ยังได้รับความนิยมในการสั่งซื้อไปประจำการในกองทัพต่างๆ อีกหลายประเทศ ด้วยเหตุที่ราคาถูกกว่าอากาศยานไร้คนขับที่มีเทคโนโลยีสูงของประเทศสหรัฐอเมริกา เช่น Predator, Reaper หรืออากาศยานไร้คนขับของอิสราเอล Israeli Heron นอกเหนือจาก Bayraktar แล้ว ยูเครนยังได้รับการสนับสนุนอากาศยานไร้คนขับ Switchblade จากกองทัพสหรัฐอเมริกาด้วย[457]

ขณะที่ปรากฏรายงานข่าวว่ากองทัพรัสเซียได้นำอากาศยานไร้คนขับ KUB-BLA ที่มีระบบปัญญาประดิษฐ์ติดตั้งในระบบอากาศยาน ทำให้สามารถปฏิบัติภารกิจได้หลากหลาย ทั้งการโจมตี การค้นหาเป้าหมาย และการหลบหนีการตรวจจับ แม้จะไม่มีข้อมูลที่ชัดเจนเกี่ยวกับระยะเวลาที่มีการเริ่มต้นใช้งานอากาศยานไร้คนขับดังกล่าว โดยมีเพียงหลักฐานที่พบในประเทศยูเครนคือซากอากาศยานไร้คนขับ KUB-BLA ที่ตกในบางพื้นที่ของยูเครน[458]

อากาศยานไร้คนขับแบบ KUB-BLA ผลิตโดยบริษัท ZALA Aero group ซึ่งเป็นบริษัทพัฒนาและผลิตอาวุธเทคโนโลยีสูงของประเทศรัสเซีย มีการเปิดตัวอากาศยานไร้คนขับ KUB-BLA ครั้งแรกในงานแสดงเทคโนโลยีทางการบินของรัสเซียเมื่อปี ค.ศ.2019[459]

KUB-BLA สามารถทำความเร็วได้สูงสุด 130 กิโลเมตรต่อชั่วโมง ทำการบินได้นาน 30 นาที บรรทุกวัตถุระเบิดได้ 3 กิโลกรัม บริษัทผู้ผลิตอ้างว่า KUB-BLA มีระบบการค้นหาคัดเลือกและทำลายเป้าหมายด้วยตัวเอง สามารถหลบหลีกการตรวจจับจากฝ่ายตรงข้ามได้ นอกจากนี้แล้ว KUB-BLA ยังสามารถปฏิบัติภารกิจต่อต้านอากาศยานไร้คนขับ และการวิเคราะห์ภาพภูมิประเทศเชิงลึกได้[460] ผู้เชี่ยวชาญทางด้านเทคโนโลยีอากาศยานบางคนแสดงความเห็นว่า KUB-BLA เป็นตัวอย่างหนึ่งของ Killer Robot ในรูปแบบของอากาศยานไร้คนขับ ในขณะที่นักวิชาการเช่น Michael Horowitz ผู้เชี่ยวชาญทางด้านเทคโนโลยีทางทหารแห่งมหาวิทยาลัยเพนซิลวาเนียมีความเห็นว่า แม้บริษัทผู้ผลิตอากาศยานไร้คนขับ

---

457 อาคม รวมสุวรรณ, “ส่องโดรนพิฆาต Bayraktar TB-2 จนเรือเร็วตรวจฝั่งรัสเซียดิ่งทะเลดำสองลำซ้อน,”

458 “รัสเซียส่งโดรนพลีชีพ KUB-BLA ติดตั้งปัญญาประดิษฐ์ AI เข้าไปปฏิบัติการในยูเครน” TNN online, 21 มีนาคม 2565, [online] สืบค้นเมื่อวันที่ 16 มกราคม พ.ศ.2566 จากเว็บไซต์ https://www.tnnthailand.com/news/tech/108526/?fbclid=IwAR2fvcQgDFRHRHZQhoP3yLvHeJk5kHa6gXX25okHSNFUugI3LWo s6TMAKE

459 เรื่องเดียวกัน.

460 “รัสเซียส่งโดรนพลีชีพ KUB-BLA ติดตั้งปัญญาประดิษฐ์ AI เข้าไปปฏิบัติการในยูเครน”

KUB-BLA จะอ้างว่ามีเทคโนโลยีปัญญาประดิษฐ์ติดตั้งกับอุปกรณ์ดังกล่าว แต่การทำงานแบบอิสระเต็มรูปแบบ (fully-autonomous) ยังไม่เกิดขึ้นจริง ในปฏิบัติการบินของอากาศยานไร้คนขับโดยปกติยังต้องมีการสั่งการควบคุมด้วยมนุษย์อยู่ ทั้งการควบคุมทิศทางการบินและการคัดเลือกเป้าหมาย ข้อวิตกกังวลเรื่องการเป็นหุ่นยนต์สังหารแบบอิสระนั้นน่าจะเกินความเป็นจริงมากไป[461]

ZALA Aero group มีบทบาทสำคัญในการผลิตอากาศยานไร้คนขับเพื่อการพาณิชย์ อากาศยานไร้คนขับเพื่อการทหาร และอุปกรณ์ที่เกี่ยวกับปฏิบัติการของอากาศยานไร้คนขับ เช่น ระบบกล้องตรวจหาเป้าหมายและกล้องตรวจตราบนอากาศยานไร้คนขับ ระบบคอมพิวเตอร์ควบคุมอากาศยานไร้คนขับ ซอฟท์แวร์ระบบปฏิบัติการสำหรับอากาศยานไร้คนขับ สถานีความคุมอากาศยานไร้คนขับแบบเคลื่อนที่ และรวมถึงระบบต่อต้านอากาศยานไร้คนขับชนิดรบกวนสัญญาณสื่อสาร (Gun Drone Jammer)[462]

นอกจากการใช้อากาศยานไร้คนขับ KUB-BLA ของกองทัพรัสเซียแล้วยังพบว่ารัสเซียมีการใช้อากาศยานเชิงพาณิชย์ Mugin-5 ของบริษัท Mugin Limited ประเทศจีน มาดัดแปลงทำอากาศยานไร้คนขับเพื่อการโจมตีด้วย โดยสำนักข่าว CNN รายงานว่าทหารยูเครนทำการยิงอากาศยานไร้คนขับของรัสเซีย ซึ่งทราบจากการตรวจพิสูจน์ว่าเป็นอากาศยาน Mugin-5 ผลิตจากประเทศจีน อากาศยานดังกล่าวเป็นที่รู้จักในสังคมออนไลน์ในชื่อ Alibaba Drone มีราคาขายในประเทศจีนอยู่ที่ 15,000 เหรียญดอลลาร์สหรัฐอเมริกา[463] เหตุการณ์ทำลายอากาศยานไร้คนขับดังกล่าวเกิดขึ้นเวลา 02.00 นาฬิกาของวันเสาร์ที่ 11 มีนาคม พ.ศ.2566 โดยหน่วยความมั่นคงยูเครน (SBU) ได้ทำการแจ้งเตือนหน่วยทหารในภาคตะวันออกของยูเครนว่าตรวจพบอากาศยานไร้คนขับจะผ่านบริเวณดังกล่าว หน่วยทหารในพื้นที่จึงทำการตรวจตราและพบว่าอากาศยานดังกล่าวบินผ่านพื้นที่ในระดับต่ำทำให้สามารถตอบโต้ได้ด้วยการใช้อาวุธปืนยิง เมื่ออากาศยานตกลงสู่พื้นดินจึงมีการเข้าไปตรวจสอบและพบว่าอากาศยานดังกล่าวมีการบรรทุกวัตถุระเบิดน้ำหนักประมาณ 20 กิโลกรัม

---

[461] Will Knight, “Russia’s Killer Drone in Ukraine Raises Fears About AI in Warfare,” Wired, March 17, 2022, [online] Accessed: April 16, 2023. Available from: https://www.wired.com /story/ai-drones-russia-ukraine/

[462] Ibid.

[463] Rebecca Wright, Ivan Watson, Olha Konovalova, and Tom Booth, “Chinese-made drone, retrofitted and weaponized, downed in eastern Ukraine,” CNN online, March 16, 2023. [online] Accessed: March 18, 2023. Available from: https://edition.cnn.com /2023/03/16/europe/china-made-drone-downed-eastern-ukraine-hnk-intl/index.html

มาด้วย โดยนักวิชาการผู้เชี่ยวชาญด้านอาวุธจาก Staffordshire University นาย N.R. Jenzen-Jones ให้ความเห็นว่าการนำอากาศยานไร้คนขับเชิงพาณิชย์มาใช้ในสงครามนั้นเกิดขึ้นกับทั้งฝ่ายยูเครนและรัสเซีย[464] แม้อากาศยานไร้คนขับดังกล่าวจะไม่ได้เป็นเทคโนโลยีที่มีความซับซ้อนในเชิงการทำงาน แต่การใช้งานอากาศยานเชิงพาณิชย์ติดตั้งอาวุธดังกล่าวชี้ใช้เห็นปัญหาของการนำสิ่งของที่พลเรือนใช้งานมาเป็นประโยชน์ทางการทหารอย่างชัดเจน

ประเด็นที่มีการกล่าวถึงในงานวิชาการด้านกฎหมายระหว่างประเทศนอกเหนือจากกฎหมายมนุษยธรรมระหว่างประเทศคือการใช้อากาศยานไร้คนขับในปฏิบัติการนอกการขัดกันทางอาวุธเพื่อการกำหนดเป้าหมายสังหาร (Target Killing) เป้าหมายการสังหารที่กล่าวถึงนี้หมายถึงการวิสามัญฆาตกรรม (Extra-judicial Killing) โดยอ้างอิงจาก UN Special Rapporteur on Extrajudicial Killing, Study on Targeted Killing ซึ่งผู้เชี่ยวชาญของสหประชาชาติอธิบายว่าการวิสามัญฆาตกรรมหมายถึงการที่เจ้าหน้าที่ของรัฐได้กระทำการสังหารบุคคลที่มิได้อยู่ในการควบคุมของตนโดยการปฏิบัติการดังกล่าวจะต้องกระทำอยู่ภายใต้การพิจารณาความจำเป็นโดยชอบด้วยกฎหมาย[465]

นิยามดังกล่าวมีประเด็นปัญหาเกิดขึ้นว่า กรณีการใช้งานอากาศยานไร้คนขับในการปฏิบัติการทางทหารนอกสงครามเพื่อการต่อสู้โดยก่อให้เกิดผลกระทบสืบเนื่องจากการโจมตีซึ่งมิได้เกิดจากเจตนาของผู้ปฏิบัติการรวมถึงกรณีการปฏิบัติการโจมตีเพื่อการป้องกันจะถือว่าอยู่ในขอบเขตความชอบด้วยกฎหมายในการวิสามัญฆาตกรรมหรือการกำหนดเป้าหมายสังหารหรือไม่[466]

เหตุที่มีการพิจารณาประเด็นดังกล่าวนั้นเนื่องจากมีการใช้อากาศยานไร้คนขับเพื่อปฏิบัติการต่อต้านการก่อการร้ายซึ่งมิได้อยู่ในสนามรบ โดยลักษณะการใช้งานอากาศยานไร้คนขับ

---

[464] Rebecca Wright, Ivan Watson, Olha Konovalova, and Tom Booth, “Chinese-made drone, retrofitted and weaponized, downed in eastern Ukraine,”

[465] United Nations, UN Special Rapporteur on Extrajudicial Killing, Study on Targeted Killing, UN doc. A/HRC/14/24/Add.6 (28 May 2010)

[466] Christine Gray, “The Limits of Force” (Volume 376), in Collected Courses of the Hague Academy of International Law. (2015) p.123. [online] Accessed: September 22, 2022. Available from: https://referenceworks.brillonline.com/entries/the-hague-academy-collected-courses/*A9789004297685_02?lang=de

เพื่อการต่อต้านการก่อการร้ายนี้เกิดขึ้นอยู่บ่อยครั้ง และมีประเทศที่สนับสนุนหลักการนี้ได้แก่ประเทศสหรัฐอเมริกาและประเทศอิสราเอล[467]

2.4.1.4 การสื่อสารผ่านดาวเทียมกับเทคโนโลยีอาวุธทางอวกาศ

เทคโนโลยีทางอวกาศที่กล่าวถึงนี้หมายถึงเทคโนโลยีระบบการกำหนดพิกัดบนพื้นโลก (Global Positioning System: GPS)[468] ซึ่งในปัจจุบันการใช้งานระบบ GPS นี้อยู่ในลักษณะการใช้งานร่วมกันของพลเรือนและพลรบ (Dual-use character) โดยในทางการทหารนั้น ระบบ GPS จะเป็นประโยชน์อย่างมากต่อการระบุพิกัดเพื่อการโจมตี ระบบ GPS จึงไม่ใช่อาวุธในตัวเองแต่เป็นวิธีการที่นำมาประกอบกับการใช้อาวุธเพื่อความได้เปรียบในการขัดกันทางอาวุธ ซึ่งย่อมตกอยู่ภายใต้กฎหมายมนุษยธรรมระหว่างประเทศอย่างหลีกเลี่ยงไม่ได้

ปัญหาทางกฎหมายที่น่าจะเกิดขึ้นคือการแบ่งแยกเป้าหมายว่าระบบการส่งสัญญาณแบบใดที่จะถือว่าเป็นไปเพื่อประโยชน์ทางการทหารซึ่งตกเป็นเป้าหมายของการโจมตีได้ ลักษณะปัญหาในการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศต่อเรื่องเทคโนโลยีทางอวกาศจึงแทบจะมีความคล้ายคลึงกับปัญหาของการใช้งานระบบไซเบอร์ อย่างไรก็ดีหากใช้เกณฑ์การพิจารณาว่าระบบเทคโนโลยี GPS ใดเป็นไปเพื่อประโยชน์ทางการทหารมากกว่า และจะตกเป็นเป้าหมายในการโจมตีได้ก็ย่อมทำได้ ผลประการที่จะต้องตามมาคือความเสียหายต่อทรัพย์สินหรือการสื่อสารของพลเรือนที่จะต้องเกิดขึ้น หากทรัพย์สินหรือการสื่อสารของพลเรือนนั้นไปมีความเกี่ยวข้องกับเป้าหมายทางการทหารอย่างไม่สามารถแยกจากกันได้ชัดเจน

Duncan Blake นักวิชาการทางด้านกฎหมายมนุษยธรรมระหว่างประเทศแห่งศูนย์วิจัยกฎหมายทหาร ของมหาวิทยาลัยนิวเซาท์เวลส์ ประเทศออสเตรเลีย ระบุว่าอาวุธทางอวกาศมีการใช้งานและพัฒนาใน 5 รูปแบบ คือ

1) ระบบอาวุธที่อาศัยการทำงานของดาวเทียมในการระบุตำแหน่ง (Space-Enabled Weapons) เช่น ระบบดาวเทียมเพื่อนำทางภาคพื้นดิน (Global Navigation Satellite Systems: GNSS or GLONASS ซึ่งพัฒนาโดยประเทศรัสเซีย หรือระบบกำหนดตำแหน่งบนพื้นโลก

---

[467] Christine Gray, “The Limits of Force”, p. 124.

[468] Duncan Blake, “Military Strategic Use of Outer Space,” in Hitoshi Nasu and Robert McLaughlin (editors), New Technologies and the Law of Armed Conflict. (The Hague: T.M.C. Asser Press, 2014), p. 105.

(Global Positioning System: GPS) ซึ่งพัฒนาโดยประเทศสหรัฐอเมริกา ซึ่งการทำงานทั้งสองระบบสามารถปรับใช้ได้กับการคำนวณระยะทางเพื่อการยิงจรวด และการกำหนดตำแหน่งเพื่อการโจมตี[469] โดยใช้ประกอบกับการลาดตระเวนและระบุเป้าหมายของอากาศยานไร้คนขับหรือโดรนได้

2) ระบบอาวุธที่ใช้งานในชั้นอวกาศ (Weapons “in” Space) เช่น เครื่องยิงจรวดหรือกระสุนต่อต้านอวกาศยานที่ใช้งานได้ในชั้นอวกาศ ซึ่งมีความเป็นไปได้ที่อาวุธดังกล่าวอาจมีการใช้งานในอนาคตอันใกล้ แต่ในปัจจุบันยังคงอยู่ในขั้นของการวิจัยและพัฒนาเท่านั้น[470]

3) อาวุธที่ใช้งานเพื่อต่อสู้กับระบบอาวุธในชั้นอวกาศ (Weapons “to” Space) ได้แก่ อาวุธที่ไม่ต้องติดตั้งในชั้นอวกาศแต่สามารถใช้เพื่อทำลายเป้าหมายในชั้นอวกาศได้ อาวุธต่อต้านระบบดาวเทียม ซึ่งในปัจจุบันประเทศสหรัฐอเมริกาและประเทศรัสเซียได้มีการพัฒนาระบบอาวุธดังกล่าวแล้ว[471]

4) ระบบอาวุธที่ทำการจากภาคอวกาศสู่โลก (Weapons “from” Space) ระบบอาวุธชนิดนี้ยังไม่เกิดขึ้นจริงในปัจจุบัน แต่มีความเป็นไปได้ที่จะเกิดขึ้นจากพัฒนาการในการใช้คลื่นสัญญาณวิทยุหรือสัญญาณไฟฟ้าซึ่งยิงตรงจากระบบดาวเทียมเพื่อให้เกิดผลต่อการทำลายในพื้นโลกได้[472] ซึ่งหากมีการใช้งานระบบดาวเทียมดังกล่าวเพื่อการทหารได้ย่อมก่อให้เกิดข้อท้าทายต่อหลักกฎหมายในการควบคุมการใช้งานดาวเทียมไปอีกขั้นหนึ่ง

5) ระบบอาวุธที่ใช้งานผ่านอวกาศ (Weapons “through” Space) หรือระบบการยิงอาวุธระยะไกลจากชั้นบรรยากาศโลกสู่ชั้นอวกาศและกลับมาสู่ชั้นบรรยากาศโลกอีกครั้งหนึ่งเพื่อทำลายเป้าหมายระยะไกล เช่น การยิงขีปนาวุธระยะไกล โดยเฉพาะอย่างยิ่งขีปนาวุธที่สามารถยิงข้ามทวีปได้ ซึ่งจะเป็นประโยชน์อย่างมากในการโจมตี[473] ทั้งนี้ การทำงานของอาวุธดังกล่าวยังคงต้องอาศัยการทำงานประกอบร่วมกับการระบุตำแหน่งด้วยดาวเทียม ปัจจุบันประเทศสหรัฐอเมริกาและรัสเซียได้มีการพัฒนาระบบอาวุธดังกล่าวเพื่อนำไปสู่การใช้งานจริงทางการทหาร

[469] Duncan Blake, “Military Strategic Use of Outer Space,”:. 105.

[470] Ibid., pp. 108-109.

[471] Ibid., pp. 109-110.

[472] Ibid., p. 110.

[473] Ibid., p. 111.

นอกจากการใช้สัญญาณดาวเทียมเพื่อการระบุตำแหน่งบนพื้นโลกแล้วยังพบการใช้ภาพถ่ายดาวเทียมเพื่อการระบุตำแหน่งที่ตั้งของฝ่ายศัตรูทางการทหารด้วย โดยในช่วงเดือนมีนาคม พ.ศ.2566 รัฐบาลยูเครนได้ใช้ภาพถ่ายทางอากาศเพื่อค้นหาตำแหน่งที่ตั้งของกองทัพรัสเซียในบริเวณดินแดนประเทศยูเครน ภาพจากดาวเทียมกว่าร้อยภาพทำให้ได้ว่าใน 4 พื้นที่ของประเทศยูเครนมีกองกำลังทหารของรัสเซียอยู่ในพื้นที่ได้แก่ 1) พื้นที่ชายฝั่งตะวันตกของไครเมีย 2) หมู่บ้าน Rivnopil ทางเหนือของเมืองMariupol 3) บริเวณทางหลวงหมายเลข E105 ทางตะวันตกของเมือง Tokmak และ 4) เมือง Tokmak การตรวจพบที่ตั้งของกองทัพรัสเซียในพื้นที่ดังกล่าวทำให้รัฐบาลยูเครนสามารถย้ายพลเรือนออกจากบางพื้นที่เพื่อความปลอดภัยได้ โดยเฉพาะอย่างยิ่งการย้ายพลเรือนออกจากเมือง Tokmak และเปลี่ยนพื้นที่ดังกล่าวให้เป็นแนวรบระหว่างกองกำลังยูเครนและรัสเซีย[474]

2.4.1.5 เทคโนโลยีนาโนและเทคโนโลยีลดการตรวจจับ

เทคโนโลยีนาโนถือเป็นความก้าวหน้าทางวิทยาศาสตร์ที่ส่งผลสำคัญต่อการดำเนินชีวิตของมนุษย์ในปัจจุบัน โดยเทคโนโลยีระดับอะตอมหรือโมเลกุลขนาด 1-100 นาโนเมตรนี้ถูกพัฒนาขึ้นมาโดยไม่มีวัตถุประสงค์เพื่อสร้างอันตรายแก่มนุษย์ และปรากฏว่ามีการนำไปใช้ในทางทหารด้วยเพื่อเพิ่มประสิทธิภาพการใช้งานของอาวุธ[475]

เทคโนโลยีนาโนที่มีการนำมาใช้อย่างเป็นรูปธรรมในทางการทหารคือเทคโนโลยี Stealth ซึ่งใช้กับอากาศยานเพื่อลดโอกาสในการถูกตรวจจับโดยระบบเรดาร์ อินฟาเรดและรังสีอื่นๆ ในปัจจุบันเทคโนโลยีนาโนเริ่มเปลี่ยนแปลงไปจากการใช้เพื่อระบบอากาศยานมาสู่การสร้างสู่เครื่องแบบทหารลายพรางที่สามารถดูกซับแสงตกกระทบได้ทำให้ยากแก่การมองเห็น แม้ว่าการใช้เครื่องแบบทหารลายพรางจะเป็นที่ยอมรับในกฎเกณฑ์การทำสงครามแต่หากเครื่องแบบทหารกลายเป็นสิ่งที่ทำให้ทหารหลุดพ้นจากการตรวจจับด้วยเครื่องมือทั้งหลายรวมถึงการมองเห็นได้ยากด้วยตาเปล่า ก็เป็นที่น่าคิดว่าจะส่งผลอย่างไรต่อกฎเกณฑ์ในการทำสงครามหรือไม่ เพราะหลักเกณฑ์กรุงเฮก ค.ศ.1907

[474] Daniele Palombo and Erwan Rivault, “Ukraine war: Satellite images reveal Russian defences before major assault,” BBC News, (May 22, 2023) Accessed June 2, 2023. Available from: https://www.bbc.com/news/world-europe-65615184

[475] Hitoshi Nasu and Robert McLaughlin, (eds), New Technologies and the Law of Armed Conflict, p.145.

ข้อ 1 ระบุว่าทหารจะต้องสวมเครื่องแบบและสัญลักษณ์เฉพาะซึ่งมองเห็นได้ในระยะไกล และจะต้องถืออาวุธโดยเปิดเผย เช่นเดียวกับข้อ 4 A (2) ของอนุสัญญาเจนีวาฉบับที่ 3[476]

ยิ่งไปกว่านั้นการพัฒนาระบบพรางอาวุธเพื่อไม่ให้ถูกตรวจจับได้ยังได้รับการพัฒนาด้วย โดยการเคลือบสารคาร์บอน (Carbon nanotube coating) ที่ทำให้อาวุธนั้นมีสีที่กลมกลืนกับภูมิประเทศรอบข้างจนยากที่จะเห็นได้ นอกจากนี้ยังมีพัฒนาการระดับที่สูงขึ้นไปในชื่อ “metamaterials” ซึ่งเป็นการจัดเรียงโครงสร้างของโลหะรูปแบบใหม่ในระดับนาโน ทำให้โลหะมีลักษณะเป็น “Metaflex” คือพรางตัวจากการมองเห็นในระยะไกลได้[477]

ประเด็นเรื่องการสวมเครื่องแบบที่แยกออกจากพลเรือนของทหารและการถืออาวุธโดยเปิดเผยนั้นเป็นหลักการแยกแยะขั้นพื้นฐานในกฎหมายมนุษยธรรมระหว่างประเทศเพื่อแยกผู้ไม่มีส่วนเกี่ยวข้องกับปฏิบัติการทางทหารออกจากการสู้รบ จึงมีข้อพิจารณาว่าทหารที่สวมเครื่องแบบอำพรางตนเองจนถึงขั้นล่องหนได้นั้นจะถือเป็นการละเมิดหลักเกณฑ์ในการขัดกันทางอาวุธนี้หรือไม่ จริงอยู่ที่เครื่องแบบเป็นการแยกแยะระหว่างพลเรือนและพลรบ หากทหารสวมเครื่องแบบที่มองไม่เห็นย่อมไม่ได้ทำให้ทหารนั้นกลายเป็นพลเรือนไป แต่อาจมีผลทำให้ทหารคนนั้นไม่อยู่ในการสู้รบเลย เช่นนี้จะถือว่าขัดต่อหลักกฎหมายว่าด้วยการขัดกันทางอาวุธหรือไม่ การถืออาวุธล่องหนก็เช่นกันจะถือว่าขัดต่อหลักกฎหมายการขัดกันทางอาวุธหรือไม่เพราะไม่ การมองไม่เห็นอาวุธที่ถือจะทำให้เข้าใจผิดว่าทหารคนดังกล่าวได้รับความคุ้มครองตามกฎหมายหรือไม่

การใช้อาวุธล่องหนและเครื่องแบบทหารล่องหนนั้นยังอาจก่อให้เกิดปัญหาต่อหลักความระมัดระวังในการโจมตีด้วย โดยหากมีการสวมเครื่องแบบทหารล่องหน หรือถืออาวุธล่องหนในเขตพื้นที่ที่มีพลเรือนอยู่ย่อมก่อให้เกิดปัญหาต่อการคุ้มครองพลเรือนตามหลักความระมัดระวังในการโจมตี เพราะการประเมินความเสียหายที่จะเกิดแก่พลรบและพลเรือนจะทำได้ยากขึ้น จึงเป็นหน้าที่ของกองทัพและรัฐในการพิจารณาความเหมาะสมของการใช้เครื่องแบบและอาวุธในลักษณะดังกล่าว

เทคโนโลยีที่มีการกล่าวถึงในปัจจุบันที่มีการใช้อยู่คือเทคโนโลยี Stealth หรือเทคโนโลยีที่ลดโอกาสที่ศัตรูจะมองเห็นโดยการใช้วัสดุที่ตรวจจับไม่ได้จากรังสี คลื่นความร้อน หรือเรดาร์ ทั้งนี้รวมตลอดถึงการใช้เครื่องหมายพรางตา (camouflage) ด้วย[478] โดยประเด็นที่มีข้อถกเถียงว่าในอนาคต

---

[476] Hitoshi Nasu and Robert McLaughlin, (eds), New Technologies and the Law of Armed Conflict, p. 153.

[477] Ibid., p. 152-154.

[478] Ibid., p. 152.

จะเกิดขึ้นคือ การใช้เครื่องแบบทหารที่พรางตาจนเกือบจะล่องหนได้ และอาวุธที่ถูกพรางจนล่องหนได้ (Cloaked weapons)[479] โดยการใช้เทคโนโลยีพรางตาดังกล่าวย่อมส่งผลต่อการแบ่งแยกเป้าหมายในการโจมตี ประเด็นนี้หากพิจารณาให้ถี่ถ้วนย่อมพบได้ว่าหลักการแบ่งแยกพลเรือนออกจากพลรบด้วยลักษณะของการสวมเครื่องแบบ ถืออาวุธเปิดเผย และทำการรบตามประเพณีการทำสงครามนั้น มีไว้เพื่อคุ้มครองไม่ให้พลเรือนตกเป็นเป้าหมายของการโจมตีเท่านั้น ไม่มีหลักเกณฑ์ใดห้ามพลรบสวมเครื่องแบบพรางตา ดังสังเกตได้จากเครื่องแบบทหารในปัจจุบันที่ก็เป็นเครื่องแบบลายพรางแทบทั้งสิ้น เพราะการทำให้กองทัพของตนเองได้เปรียบจากการไม่ถูกโจมตีนั้นไม่ใช่ข้อห้ามตามหลักกฎหมายว่าด้วยการขัดกันทางอาวุธ เว้นเสียแต่กรณีที่พลรบสวมเครื่องแต่งกายพลเรือนเพื่อรบย่อมถือเป็นการกระทำที่ขัดต่อกฎหมายเกี่ยวกับการขัดกันทางอาวุธ รวมตลอดถึงพลรบที่ไม่สวมเครื่องแบบย่อมถือเป็นการไม่ปฏิบัติตามหลักเกณฑ์ของกฎหมายมนุษยธรรมระหว่างประเทศ ความคุ้มครองตามแบบพลรบดังเช่นกรณีการตกเป็นเชลยเมื่อถูกฝ่ายตรงข้ามจับตัวไปย่อมไม่เกิดขึ้น ส่วนพลรบปกติที่สวมเครื่องแบบพรางตาหรือแม้แต่ล่องหนได้ หากถูกจับได้ย่อมถือเป็นเชลยศึกตามอนุสัญญาเจนีวา เทคโนโลยีนาโนในเรื่องเครื่องแบบจึงไม่น่าจะเป็นปัญหาในเรื่องการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

ส่วนปัญหาในเรื่องการใช้อาวุธพรางนั้นน่าจะเป็นประเด็นในทางกฎหมายที่น่าพิจารณามากกว่า กล่าวคือหากอาวุธประจำกายที่ทหารถืออยู่ไม่สามารถมองเห็นได้ด้วยตาเปล่า ทหารฝ่ายตรงข้ามย่อมไม่สามารถตัดสินใจได้ว่าจะโจมตีได้หรือไม่

เทคโนโลยี Stealth - มีการพัฒนาและนำมาใช้งานกับทั้งเรือผิวน้ำ อากาศยาน และยานพาหนะทางบกเช่นรถถัง Stealth เป็นเทคโนโลยีช่วยลดการถูกตรวจจับ (Low Observable Technology) ไม่ว่าจะเป็นการตรวจพบด้วยสายตา เรดาร์ อินฟาเรด เสียง หรือระบบตรวจจับอื่นๆ เทคโนโลยี Stealth เป็นรูปแบบหนึ่งของ LOT เพื่อลดโอกาสในการถูกตรวจพบ[480]

อาจกล่าวได้ว่าเทคโนโลยีช่วยลดการถูกตรวจจับพัฒนามาจากแนวคิดในการซ่อนพรางตัว ในสงครามโลกครั้งที่ 1 กองทัพเยอรมันใช้วัสดุ Cellon (Cellulose Acetate) แทนผ้าใบในเครื่องบิน

---

[479] Hitoshi Nasu and Robert McLaughlin, (eds), New Technologies and the Law of Armed Conflict, p. 154.

[480] Arvind Gangoli Rao and Shripad P. Mahulikar, "Integrated review of stealth technology and its role in airpower". Aeronautical Journal. 106 (1066) (2002): 634-635. [online] accessed June 10, 2022, Available from: https://www.researchgate.net/publication/287536552_Integrated_review_of_stealth_technology_and_its_role_in_airpower

Linke-Hofmann R.I เพื่อลดการถูกมองเห็นด้วยสายตา แต่วัสดุดังกล่าวไม่ทนต่อสภาพอากาศและเสื่อมสภาพเร็ว ต่อมากองทัพอังกฤษได้พยายามพัฒนาเรือเหาะมาใช้แทนเครื่องบิน ซึ่งสามารถลดเสียงเครื่องยนต์ลงได้และใช้สีดำทาที่เรือเหาะเพื่อลดโอกาสมองเห็น

ภารกิจหลักของเรือเหาะเป็นไปเพื่อการสอดแนมแต่การปฏิบัติภารกิจดังกล่าวไม่คุ้มค่าต้นทุนการผลิตเรือเหาะเทคโนโลยีดังกล่าวจึงถูกล้มเลิกไป[481]

ในสงครามโลกครั้งที่ 2 เรือผิวน้ำของสัมพันธมิตรถูกโจมตีด้วยเรือดำน้ำของเยอรมันในยุทธการที่แอตแลนติก จึงเริ่มมีการพัฒนาระบบ Active Camouflage หรือ Diffused Lighting Camouflage โดยการใช้แสงส่องกระทบจุดต่างๆ บนตัวเรือให้ไม่สามารถมองเห็นรูปแบบเรือที่ชัดเจนได้ เพื่อลดการมองเห็นจากกล้องเรือดำน้ำ (Periscope) ขณะที่เรือดำน้ำ U-Boat U-480 เป็นเรือดำน้ำ Stealth รูปแบบแรกของเยอรมัน ที่มีการใช้แผ่นยางมาปิดที่ผิวเรือดำน้ำเพื่อป้องกันการสะท้อนของแสง และลดการสะท้อนกลับของคลื่นเสียงจากการตรวจจับด้วย Active Sonar และมีการทดลองใช้สีร่วมกับแผ่นยางที่ช่วยลดการตรวจจับของเรดาร์ ทำให้เมื่อเรือดำน้ำโผล่ขึ้นมาที่ผิวน้ำจะถูกตรวจจับจากเรดาร์เป็นเพียงเรือที่มีขนาด 1.5 เมตรเท่านั้น[482]

ในช่วงสงครามเย็น ปี ค.ศ.1958 CIA ต้องการลดค่าสะท้อนของสัญญาณเรด้ารในเครื่องบินลาดตระเวน Lockheed U-2 โดยมีการหุ้มฉนวนสายสัญญาณและแผงวงจรทุกชนิดบนเครื่องบิน นอกจากนั้นยังมีการใช้สีลดการสะท้อนกลับของเรดาร์ แต่ไม่ปรากฏความสำเร็จเพราะเทคโนโลยีดังกล่าวทำให้เครื่องบินแพงขึ้น หนักขึ้น ไม่คุ้มค่ากับปฏิบัติการที่มีประสิทธิภาพขึ้นเล็กน้อย[483]

ความพยายามของกองทัพสหรัฐอเมริกาในการพัฒนาเครื่องบินจารกรรมนำไปสู่การจ้างบริษัท Lockheed โดยทีมงาน Skunk Works หรือนามแฝงของ Lockheed Advanced Development Projects นำไปสู่การออกแบบเครื่องบิน A-12 ซึ่งสามารถบินได้เร็ว 3 เท่าของความเร็วเสียง และสามารถบินสูงได้ถึง 80,000 ฟุต เพื่อหลบเลี่ยงการถูกตรวจจับ มีการออกแบบ

---

[481] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, Master of Science in Electronic Warfare System Engineering, Naval Postgraduate School, Monterey California, March 2009, p. 31. [online] accessed June 20, 2022, Available from: https://core.ac.uk/download/pdf/36698589.pdf

[482] Ibid., p.31

[483] Ibid., p. 14.

ทั้งหมด 11 รุ่น ก่อนจะสำเร็จในรุ่น A-12 ซึ่งสมบูรณ์ทั้งรูปทรง แพนหางทรงเฉียง วัสดุผสมแทนโลหะ และสีที่ดูดซับสัญญาณเรดาร์[484]

A-12 เป็นต้นแบบของเครื่องบินลาดตระเวน SR-71 Blackbird ของกองทัพสหรัฐอเมริกา ในปี ค.ศ.1970 กองทัพสหรัฐอเมริกาก่อตั้งโครงการ Lockheed have blue เพื่อคิดค้นและพัฒนาเครื่องบินขับไล่ Stealth ซึ่งได้รับแนวคิดมาจาก Pyotr Yakovlevich Ufimtsev นักฟิสิกส์ชาวสหภาพโซเวียต ซึ่งคิดค้นเทคโนโลยีนี้ในปี ค.ศ.1962 และมีการตีพิมพ์หนังสือชื่อ “Method of Edge Waves in the Physical Theory of Diffraction” โดยได้มีการแปลเป็นภาษาอังกฤษในปี ค.ศ.1971 และมีการนำมาศึกษาและพัฒนาต่อในประเทศสหรัฐอเมริกา สิ่งที่ปรากฏในงานเขียนนี้คือการพัฒนาเทคโนโลยีเพื่อสร้างเครื่องบิน F-117 และเครื่องบิน B-2[485]

ทฤษฎีที่ Ufimtsev นำเสนอคือสมการลดค่า RCS (Radar Cross Section) แต่การทดสอบสมการลดค่า RCS จะต้องใช้ซุปเปอร์คอมพิวเตอร์ในการคำนวณ ซึ่งสหภาพโซเวียตไม่มีซุปเปอร์คอมพิวเตอร์จึงไม่สามารถพัฒนาสมการดังกล่าวให้กลายเป็นการออกแบบเครื่องบินได้ แต่สหรัฐอเมริกามีความสามารถดังกล่าวจึงก่อให้เกิดการพัฒนาสมการ RCS จนกระทั่งออกแบบเป็นเครื่องบินที่มีมุมลดการสะท้อนของเรดาร์ได้สำเร็จ และมีการนำมาผลิตเป็นเครื่องบิน Stealth เครื่องแรกของโลกในชื่อ F-117 Nighthawk ซึ่งต่อมาในภายหลังเทคโนโลยีการลดการสะท้อนของเรดาร์ก็ถูกนำมาใช้ในการผลิตเครื่องบินในรุ่นต่อๆ มา[486]

การลดขนาด RCS (Radar Cross Section) หรือค่าตัดขวางของเรดาร์ เป็นค่าที่เกิดจากการคำนวณเพื่อบอกถึงความสามารถในการสะท้อนกลับของสัญญาณเรดาร์ของวัตถุนั้นโดยอ้างอิงกับคลื่นความถี่ค่าหนึ่ง หากค่า RCS สูงแสดงว่าวัตถุนั้นสามารถสะท้อนเรดาร์ได้เป็นอย่างดี อย่างไรก็ดีค่า RCS ไม่ได้บอกขนาดพื้นที่หน้าตัดของวัสดุนั้น เช่น หากยิงเรดาร์ที่ขนาดสัญญาณ 10 GHz ไปกระทบโลหะที่มีขนาดหน้าตัด 1 ตารางเมตร ค่า RCS ที่คำนวณได้อาจเป็น 10,000 ตารางเมตร ดังนั้นการ

---

[484] Arvind Gangoli Rao and Shripad P. Mahulikar, "Integrated review of stealth technology and its role in airpower", pp. 634-635.

[485] Ibid., pp. 634-635.

[486] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, p. 71.

ลดค่า RCS ได้ย่อมหมายความว่าโอกาสในการถูกตรวจจับจากเรดาร์ย่อมลดลงไปได้ ไม่ว่าเครื่องบินจะมีขนาดเท่าไรก็ตาม[487]

เรดาร์ RADAR (Radio Detection and Ranging) เป็นอุปกรณ์ในการตรวจจับระยะทางและขนาดของวัตถุ เป็นเทคโนโลยีที่พัฒนาขึ้นมาสำเร็จครั้งแรกโดยประเทศอังกฤษ เป็นที่นิยมในการใช้งานระบบป้องกันภัยทางอากาศ เนื่องจากสามารถตรวจจับวัตถุเคลื่อนที่ทางอากาศที่ตามองไม่เห็นได้ นอกจากนั้นยังสามารถใช้เป็นเครื่องมือประกอบการทำงานของระบบอาวุธนำวิถีได้ด้วย ในขณะที่เทคโนโลยีต่อต้านการถูกตรวจจับด้วยเรดาร์ก็เกิดขึ้นมาในเวลาใกล้เคียงกัน[488] วิธีการที่นิยมใช้ในช่วงแรกๆ คือการใช้ ฟรอยด์อลูมิเนียมที่เรียกว่า Chaff เพื่อการลวงสัญญาณเรดาร์ หรือการใช้สัญญาณรบกวนสัญญาณเรดาร์ (Radar jamming)[489]

เครื่องบินที่ทำให้เทคโนโลยีลดการสะท้อนของเรดาร์ได้รับความนิยมเพิ่มมากขึ้นคือเครื่องบิน F-117 โดยปัจจัยหลักที่ทำให้การลดค่า RCS ได้ คือ รูปทรงและวัสดุที่ใช้ทำยานพาหนะ ในช่วงทศวรรษที่ 1960 เครื่องบินทิ้งระเบิด Avro Vulcan ของกองทัพอังกฤษเป็นเครื่องบินแรกๆ ที่ลดค่า RCS ได้โดยบังเอิญ โดยปรากฏว่าบางครั้งสัญญาณเรดาร์ตรวจจับเครื่องบินได้เล็กน้อยในขณะที่บางครั้งตรวจไม่พบเลย ในขณะที่เครื่องบินทิ้งระเบิดของกองทัพรัสเซีย Tupolev Tu-95 กลับเป็นเป้าในการถูกตรวจจับจากเรดาร์มากที่สุด เนื่องจากใบพัดทั้ง 4 ที่ปีกของเครื่องบินเป็นแหล่งสะท้อนเรดาร์ที่สำคัญ[490]

ในเทคโนโลยี Stealth มีปัจจัยสำคัญที่วัสดุซึ่งใช้ในการผลิตเครื่องบินเป็นจะต้องดูดซับหรือทำให้สัญญาณเรดาร์ทะลุผ่านไปได้ ปกติที่นิยมใช้กันคือการใช้วัสดุทรงสามเหลี่ยมภายในปีกเครื่องบินที่จะทำหน้าที่สะท้อนสัญญาณเรดาร์กลับไปกลับมาอย่างไม่เป็นระเบียบ ทำให้สัญญาณเรดาร์อ่อนกำลังลง นอกจากนั้นในบางกรณีก็จะเป็นการทำให้ปีกเครื่องบินทำมุมตั้งฉากกับสัญญาณเรดาร์หรือการให้ปีกเครื่องบินทำมุม Dihedral หรือ Trihedral โดยปกติเครื่องบินทั่วไป ใช้การทำมุมเช่นนี้ในแพนหางดิ่งและแพนหางระดับโดยจะต้องทำมุมให้เหมาะสม ในขณะที่เครื่องบิน F-117 จะมีการ

---

[487] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, p. 95.

[488] Ibid., p. 27.

[489] Ibid.

[490] Arvind Gangoli Rao and Shripad P. Mahulikar, "Integrated review of stealth technology and its role in airpower,": 635.

ออกแบบแพนหางที่ลดการสะท้อนของเรดาร์โยการทำมุมที่ดีที่สุด ในขณะที่เครื่องบิน B-2 จะทำการตัดแพนหางดิ่งออกไปเลย ซึ่งนอกจากจะลดค่า RCS ยังลดแรงต้านของอากาศ ทำให้พิสัยบินไกลขึ้นด้วย นอกจากนั้นเครื่องบิน Stealth จะต้องซ่อนเครื่องยนต์ไว้ในลำตัว ปีก หรือส่วนอื่นๆ ที่ต้องมีการออกแบบมาอย่างดี โดยจะต้องมีแผ่นกั้นของจุดหมุนทั้งหมดเพื่อไม่ให้ทำการสะท้อนกลับของสัญญาณเรดาร์ เครื่องบิน Stealth จะต้องไม่มีอาวุธ ถังเชื้อเพลิงหรือสิ่งใดๆ ยื่นออกมาจากตัวเครื่อง โดยจะต้องจัดเก็บไว้ในลำตัวให้หมด ช่องใดๆ ที่เปิดออกบริเวณลำตัวของเครื่องบินจะมีผลทำให้เครื่องบินลดประสิทธิภาพในการสะท้อนสัญญาณเรดาร์ลง[491]

เครื่องบิน F-22A Raptor ที่ขอบชายหน้าปีกและแพนหางระดับจะทำมุมเท่ากันและขนานกัน ขณะที่ช่องต่างๆ บนตัวเครื่องบิน เช่น ช่อง intake ช่องเติมน้ำมันกลางอากาศ ก็จะต้องออกแบบให้มีองศาเท่ากัน การออกแบบเครื่องบินในรูปแบบนี้จะทำให้สัญญาณเรดาร์กระจายออกไปยังทิศทางอื่นเพียงทิศทางเดียวแทนที่จะกระจายสัญญาณเรดาร์ออกไปรอบๆ แบบไร้ทิศทาง ขณะที่การออกแบบทรงขอบของเครื่องบินให้เป็นแบบหยักฟันปลา เช่น ส่วนท้ายของเครื่องยนต์ ส่วนเปิดปิดบริเวณลำตัวที่มีองศาที่เหมาะสม ก็จะช่วยลดการตรวจจับได้เช่นเดียวกัน ผลของการออกแบบดังกล่าวทำให้เครื่องบิน Stealth ไม่สามารถทำการบินได้อย่างมีเสถียรภาพ และการควบคุมโดยมนุษย์ทำได้ยาก จึงต้องใช้ระบบ fire by wired โดยให้คอมพิวเตอร์ทำการควบคุมเสถียรภาพของเครื่องบินตลอดเวลา เพื่อให้เครื่องบินเดินทางในอากาศตามที่นักบินควบคุมทิศทางได้[492]

นอกจากนั้นห้องโดยสารก็เป็นส่วนหนึ่งที่ต้องมีการออกแบบให้ลดการสะท้อนโดยกระจกครอบห้องนักบิน (Canopy) ก็จะต้องมีการเคลือบสาร vapor deposited gold หรือ indium tin oxide เพื่อลดค่าสัญญาณสะท้อนกลับและกระจายสัญญาณเรดาร์ไปทิศทางอื่นทั้งหมด เนื่องจากกระจกครอบห้องนักบินมีคุณสมบัติให้เรดาร์ผ่านทะลุได้ ทำให้ Console เก้าอี้นักบิน หมวกนักบินจะเป็นจุดสะท้อนสัญญาณเรดาร์ได้อย่างดี[493]

ส่วนสำคัญอีกประการหนึ่งคือ ในเครื่องบินรบทุกลำจะมีระบบเรดาร์ติดตั้งที่ส่วนหัวของเครื่องบิน หากระบบเรดาร์บนเครื่องบินทำมุมตั้งฉากกับสัญญาณเรดาร์ตรวจจับ ก็จะตกเป็นเป้าหมาย

---

[491] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, pp. 51-55.

[492] Ibid., pp. 78-82.

[493] Ibid., p. 47.

ได้ทันที เรดาร์ที่นิยมใช้ในเครื่องบินขับไล่จึงมักเป็นระบบ AESA; Active Electronically Scan Array ที่จะต้องไม่มีการหมุนเสาอากาศแบบ Mechanic และต้องให้เสาอากาศในระบบเรดาร์เครื่องบินทำมุมในทิศทางอื่น (ปกติทำมุมเชิดขึ้น) เพื่อไม่ให้เกิดการสะท้อนของเรดาร์ซึ่งจะทำให้ค่า RCS เพิ่มตามไปด้วย[494]

กรณีการใช้เทคโนโลยี Stealth กับเรือผิวน้ำ มักใช้เทคโนโลยีเดียวกับอากาศยาน แต่เนื่องด้วยเรือผิวน้ำมักมีขนาดใหญ่ และจะต้องสร้างจากโลหะเป็นหลักโดยใช้วัสดุทดแทนไม่ได้ จึงมักไม่ได้ช่วยลดค่า RCS ได้แบบเดียวกับอากาศยาน คงทำได้เพียงลดสัญญาณเรดาร์ให้เหลือน้อยลงกว่าเดิมเท่าที่จะทำได้ เรือผิวน้ำที่ใช้เทคโนโลยี Stealth เช่น เรือพิฆาตชั้น Arleigh Burke ของกองทัพสหรัฐอเมริกา หรือเรือ La Fayette ของกองทัพฝรั่งเศส[495]

เรือที่ใช้ระบบ Stealth เต็มรูปแบบได้แก่ USS Zumwalt (DDG-1000) และเรือ Independence-class littoral combat ship วัสดุที่ใช้ผลิตอากาศยานและเรือโดยปกติจะมีโลหะเป็นส่วนประกอบ การผลิตยานพาหนะด้วยเทคโนโลยี Stealth จึงต้องเหลือโลหะไว้เพียงเฉพาะส่วนที่สำคัญคือโครงสร้างหลัก เครื่องยนต์ และชิ้นส่วนที่ต้องการความทนทานสูง ส่วนวัสดุปิดผิวจะต้องเป็นคาร์บอนไฟเบอร์ซึ่งแข็งแรง มีความยืดหยุ่น น้ำหนักเบาและลดการสะท้อนสัญญาณเรดาร์ได้ดี เครื่องบินรบในปัจจุบันเช่น Euro fighter และ Saab JAS 39 Gripen ก็มีคาร์บอนไฟเบอร์เป็นส่วนประกอบหลัก[496]

สารเคลือบผิว (Radiation-Absorbent Materials: RAM) จะเป็นสีชนิดพิเศษที่ช่วยลดการสะท้อนของเรดาร์ ใช้เพื่อเคลือบผิวอากาศยาน มีหลักการทำงานคือสีที่เคลือบจะต้องเปลี่ยนสัญญาณแม่เหล็กไฟฟ้าของเรดาร์มาแปลงเป็นพลังงานความร้อน ก่อนจะยอมให้คลื่นที่เหลืออยู่ค่อนข้างน้อยสะท้อนกลับออกไป โดยปกติในปัจจุบันจะใช้ Composite dye electric และเส้นใยโลหะที่มี isotope ferrite[497] โดยข้อจำกัดของ Stealth ได้แก่

---

[494] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, p. 125.

[495] Ibid. p. 6.

[496] Ibid., p. 52.

[497] Ibid., p. 56.

1) เทคโนโลยี Stealth มักใช้ได้ดีกับคลื่นความถี่ปกติที่ 1-20 GHz แต่หากเป็นเรดาร์ความถี่ต่ำที่ 100-150 MHz สัญญาณคลื่นจะมีความกว้างกว่าขนาดอากาศยานทำให้แม้อากาศยานจะออกแบบด้วยเทคโนโลยี Stealth ก็ยังคงมีคลื่นสะท้อนกลับเช่นเดิม ทำให้ประเทศรัสเซียและจีนพัฒนาเรดาร์ความถี่ต่ำ เพื่อตรวจจับเครื่องบิน Stealth แต่เรดาร์ประเภทนี้จะต้องมีเสาอากาศขนาดใหญ่ ทำให้เป็นเป้าหมายในการโจมตีได้ง่าย โดยเฉพาะอย่างยิ่งจากการโจมตีด้วยจรวดนำวิถีแบบร่อน (Cruised Missile) นอกจากนี้ แม้สัญญาณเรดาร์ความถี่ต่ำจะตรวจพบเครื่องบิน Stealth ก็ตาม แต่การจะใช้จรวดนำวิถีเพื่อต่อต้านก็จะต้องใช้สัญญาณเรดาร์ความถี่สูงระดับ 10 GHz ซึ่งเทคโนโลยี Stealth สามารถรับมือได้เป็นอย่างดี ระบบจรวดนำวิถีจึงไม่สามารถทำลายเครื่องบิน Stealth ได้ง่ายนัก[498]

2) ค่า RCS ที่ลดลงของเครื่องบิน Stealth แตกต่างกันในแต่ละส่วนของเครื่อง เช่น ค่า RCS ที่ต่ำที่สุดจะอยู่ที่ด้านหน้าของเครื่องบิน แต่ส่วนอื่นจะมีค่า RCS ที่แตกต่างกันออกไปเช่นด้านบนหรือด้านล่างของเครื่อง ค่า RCS จะมีปริมาณที่มากไม่แตกต่างจากเครื่องบินทั่วไป เป็นจุดอ่อนที่ทำให้เครื่องบิน F-117 ของกองทัพสหรัฐอเมริกาถูกยิงตกในยูโกสลาเวียในปี ค.ศ.1999 เนื่องจากมีการบินซ้ำในตำแหน่งเดิม ทำให้ระบบป้องกันภัยทางอากาศสามารถวางแผนในการโจมตีต่อต้านได้[499]

ในทางทฤษฎีการค้นหาตำแหน่งของเครื่องบิน Stealth สามารถทำได้โดย Bistatic Radar หรือ Multi Static Radar ซึ่งใช้เรดาร์หลายตำแหน่งในการสะท้อนสัญญาณ หรือการมีเรดาร์ส่งสัญญาณและรับสัญญาณอยู่คนละตำแหน่งแต่เทคนิคนี้ยุ่งยากและซับซ้อนต้องใช้ผู้ปฏิบัติงานที่มีความเชี่ยวชาญสูง[500]

การลดสัญญาณ Infra-red - คลื่นความร้อน Infra-red จะถูกปล่อยออกมาจากวัตถุที่มีความร้อน เช่น อากาศยานจะมีความร้อนจากไอร้อนที่ออกจากเครื่องยนต์เจ็ท ท่อโลหะตอนท้าย ขอบและปีกของอากาศยานที่ปะทะกับอากาศในความเร็วสูง ความร้อนเหล่านี้อาจถูกตรวจจับได้ด้วยกล้องตรวจจับ Infra-red ซึ่งอยู่ไกลออกไปหลายสิบไมล์ อย่างไรก็ดี ตามหลักฟิสิกส์แล้วในชั้นบรรยากาศจะมีคาร์บอนไดออกไซด์และไอน้ำ ทำให้มีการดูดซับความร้อนลงไปได้ โอกาสในการถูกตรวจพบด้วย

---

[498] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, p. 95.

[499] Ibid., p. 20.

[500] Ibid., pp. 109-110.

กล้อง Infra-red ก็จะลดลงตามไป และการออกแบบอากาศยานก็จะต้องออกแบบให้อากาศเย็นไหลผ่านส่วนที่เกิดความร้อนได้ก่อนปล่อยออกตอนท้ายของเครื่องบิน เช่น เครื่องบิน B-2 นอกจากนั้นอาจมีการออกแบบให้ท่อความร้อนอยู่ด้านบนของอากาศยานเพื่อป้องกันการตรวจจับจากด้านล่าง เช่น F-117[501]

การลดการมองเห็นด้วยสายตา - การลดการมองเห็นด้วยสายตานั้น เดิมทีใช้สีลายพราง (Camouflage) ปัจจุบันยังเป็นที่นิยมในเครื่องบินที่ผลิตจากรัสเซีย โดยมากเป็นโทนสีน้ำตาลหรือโทนสีฟ้า แต่เครื่องบินของยุโรปและสหรัฐอเมริกา และจีนนิยมใช้โทนสีเทาด้วยเหตุว่ามีความกลมกลืนกับสีของเมฆในขณะที่เครื่องบิน Stealth ที่ปฏิบัติภารกิจกลางคืนนิยมใช้โทนสีดำด้าน[502]

ลายพรางที่นิยมในปัจจุบันคือลายพรางดิจิทัลที่นิยมใช้ในเครื่องแบบทหารและรถถัง ลายพรางแบบนี้ออกแบบมาเพื่อให้ผู้มองเห็นกะระยะวัตถุจากระยะไกลได้ยาก ในอากาศยานบางชนิดก็มีการนำเอาลายพรางดิจิทัลมาใช้เช่นกัน

การบินของเครื่องบิน Stealth ทุกครั้งมักจะเกิด Conrail หรือแนวเมฆสีขาวยาวที่เกิดขึ้นเมื่อเครื่องบิน บินที่เพดานบิน 25,000-40,000 ฟุต โดยเกิดจากไอน้ำซึ่งมาจากไอเสียของเครื่องบินทำปฏิกิริยาในอากาศจนเกิดเป็นแนวเมฆยาว ทำให้เครื่องบินสามารถถูกตรวจพบได้ง่ายด้วยสายตา ในเครื่องบินทิ่งระเบิด B-2 มีความพยายามจะติดตั้งถึงสารเคมีที่ปลายปีกเพื่อลดการเกิด Contrail แต่ต้องยกเลิกไป แล้วเปลี่ยนมาใช้ Censor ที่สามารถแจ้งเตือนนักบินเมื่อเกิด Contrail เพื่อให้นักบินทำการเปลี่ยนเพดานบินไปยังระดับความสูงที่ไม่ก่อให้เกิด Contrail[503]

การลดสัญญาณเสียง - ในยุคเริ่มแรกอากาศยานจะมีเสียงจากเครื่องยนต์และใบพัด แต่พัฒนาของเครื่องบินเจ็ท SR-71 ปัญหาดังกล่าวก็ลดลงไป เนื่องจากสามารถบินได้สูงมากจนทำให้คนที่อยู่ภาคพื้นดินไม่อาจได้ยินเสียงเครื่องบินได้[504]

กรณีของเฮลิคอปเตอร์จะมีเสียงที่เกิดจากช่องว่างของใบพัดที่มีขนาดเท่ากัน ทำให้เกิดการแทรกสอดของเสียง การออกแบบช่องว่างที่ไม่เท่ากันของใบพัดจะช่วยลดปัญหาเรื่องเสียงนี้ ขณะที่

---

[501] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, pp. 72-73.

[502] Ibid., p. 32.

[503] Ibid., p. 78.

[504] Ibid., p. 23.

เสียงเป็นปัญหาสำคัญของเรือดำน้ำ มีความพยายามลดสัญญาณ Acoustic ในเรือดำน้ำให้มากที่สุดด้วยเทคโนโลยีหลายประการ ทั้งการออกแบบใบพัดที่ก่อให้เกิดฟองอากาศน้อยเพื่อลดเสียง การออกแบบเครื่องยนต์และเตาปฏิกรณ์ที่เงียบ รวมถึงฉนวนยางปิดผิวเรือดำน้ำเพื่อลดสัญญาณสะท้อนจาก Active Sonar[505]

ยุทธวิธี (Tactic) - เครื่องบิน Stealth ไม่ใช่เครื่องบินล่องหนได้ และยังคงถูกตรวจจับจากเรดาร์ได้ในบางกรณี โดยเฉพาะอย่างยิ่งเมื่อบินเข้าใกล้เรดาร์ เรดาร์ทั่วไปจะตรวจจับเครื่องบิน Stealth ได้ในระยะใกล้มากๆ การใช้เครื่องบิน Stealth จึงต้องมีการวางแผนที่รัดกุมและละเอียดรอบคอบ โดยปกติ Stealth จะปฏิบัติบินผ่านช่องว่างหรือจุดอ่อนของระบบป้องกันภัยทางอากาศของข้าศึกเพื่อทำลายเป้าหมายสำคัญ เช่น กองบัญชาการ ระบบอาวุธต่อสู้อากาศยาน หรือเป้าหมายทางยุทธศาสตร์[506]

ปฏิบัติการของเครื่องบิน Stealth จะต้องมีการสนับสนุนโดยข้อมูลของหน่วยข่าวกรองที่ถูกต้องและแม่นยำ โดยเฉพาะข่าวกรองทางอิเล็กทรอนิกส์ (Electronic Intelligence) ซึ่งจะมีการอัพเดทที่ตั้ง การวางกำลัง เรดาร์และระบบป้องกันภัยทางอากาศของฝ่ายข้าศึกที่ถูกต้องและแม่นยำ และการเคลื่อนย้ายกำลังล่าสุดที่ถูกต้อง หากไม่มีการวางแผนการปฏิบัติการ เครื่องบิน Stealth ก็จะไม่ต่างจากเครื่องบินธรรมดาที่ไม่มีความคุ้มค่า[507]

เครื่องบิน B-2 หรือเครื่องบินขับไล่แบบ F-22 Raptor และ F-35 Lightning II ต่างใช้เทคโนโลยีลดการถูกตรวจพบในหลายรูปแบบ โดยเน้นการลดค่า RCS เนื่องจากระบบตรวจจับระยะไกลที่สำคัญคือเรดาร์[508]

ปัจจุบันหลายประเทศพยายามพัฒนาเครื่องบิน Stealth ของตัวเอง เช่น กองทัพรัสเซียพยายามพัฒนาเครื่องบิน Sukhoi Su-57 ในขณะที่จีนพยายามเร่งการผลิตเครื่องบิน Chengdu J-20 เข้าประจำการอย่างต่อเนื่อง และ J-37 ซึ่งอยู่ในการพัฒนา ขณะที่ญี่ปุ่น เกาหลีใต้และชาติในยุโรปมีความพยายามพัฒนาเครื่องบิน Stealth ของตนเองอยู่เช่นกัน อย่างไรก็ดีด้วยต้นทุนที่ค่อนข้างสูง

---

[505] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, p. 52.

[506] Ibid., p. 7.

[507] Ibid., p. 88.

[508] Ibid., p. 7.

เครื่องบิน Stealth ในยุคที่ 5 อาจไม่ใช่อากาศยานหลักในการต่อสู้ แต่จะเป็นการใช้เครื่องบิน Stealth ยุคที่ 4.5 ร่วมกับยุคที่ 5 เพื่อทดแทนจุดดีและจุดด้อยของแต่ละรุ่น[509]

2.4.2 ลักษณะความคลุมเครือของความสัมพันธ์ระหว่างผู้ใช้งานเทคโนโลยีกับผลของปฏิบัติการ

การใช้งานเทคโนโลยีหลายประการโดยเฉพาะอย่างยิ่งเทคโนโลยีไซเบอร์สร้างลักษณะของการพิสูจน์ตัวตนผู้กระทำกับปฏิบัติการที่เกิดขึ้นได้ยาก[510] เนื่องจากเป็นการปฏิบัติการระหว่างเครือข่ายด้วยเทคโนโลยีดิจิทัลซึ่งในบางกรณีไม่สามารถจำกัดขอบเขตพื้นที่การปฏิบัติการได้ ปัญหาที่ตามมาคือการตรวจสอบกลับไปที่ต้นทางของการสั่งการแม้จะกระทำได้ทางปฏิบัติแต่ก็จะต้องใช้เวลาในการตรวจสอบซึ่งในหลายกรณีแม้จะมีการตรวจสอบกลับไปจนถึงที่มาที่คาดว่าจะสัมพันธ์กับผู้สั่งปฏิบัติการมากที่สุดแต่ก็กลับพบการปฏิเสธความรับผิดชอบในปฏิบัติการที่เกิดขึ้น ซึ่งสถานการณ์ดังกล่าวมิได้ปรากฏแต่เพียงในปฏิบัติการทางไซเบอร์เท่านั้นแต่ในบางกรณียังรวมถึงการใช้งานอากาศยานไร้คนขับด้วย

2.4.2.1 ปัญหาการพิสูจน์ตัวตนของผู้ใช้งานระบบไซเบอร์

สถานการณ์การโจมตีระบบคัดแยกยูเรเนียมของโรงงานที่เมืองนาธานซ์ ประเทศอิหร่าน โดยมัลแวร์ Stuxnet ระหว่างปี ค.ศ.2009-2010 มีการตรวจสอบโดยผู้เชี่ยวชาญในประเทศอิหร่านและแถลงการณ์ว่าปฏิบัติการดังกล่าวมาจาก “ศัตรูตะวันตก” (Western enemies)[511] ซึ่งหมายความว่าปฏิบัติการดังกล่าวดำเนินการโดยฝ่ายสหรัฐอเมริกา

ปฏิบัติการ Stuxnet มีผลเป็นการรบกวนการทำงานของเครื่องคัดแยกยูเรเนี่ยม (Centrifuge) ของโรงงานถลุงยูเรเนี่ยม (Enrichment) ที่เมืองนาธานซ์ (Natanz) ประเทศอิหร่านซึ่ง

---

[509] Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, pp. 85-87.

[510] Timothe Lopez, L’adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 98.

[511] David Albright, Paul Brannan, and Christina Walrond, “Stuxnet Malware and Natanz: update of ISIS December 2010,” Institute for Science and International Security Report; (2011). p.4. [online] Accessed: September 22, 2022. Available from: https://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/

แม้จะยังไม่มีความเสียหายร้ายแรงที่เกิดขึ้นแต่ก็ทำให้การปฏิงานของเครื่องคัดแยกผิดปกติไปโดยใบพัดเครื่องอคัดแยกหมุนเร็วขึ้นอย่างมากในระยะเวลา 15 นาทีก่อนที่จะกลับคืนสู่ภาวะปกติ จากรายงานของ ISIS Stuxnet ระบุว่าขณะที่ใบพัดหมุนแรงที่สุดนั้นทำให้มอเตอร์ทำงานหนักมากเป็นผลให้ใบพัดเครื่องคัดแยกยูเรเนี่ยมเกิดความเสียหาย อย่างไรก็ดีรายงานนี้ระบุว่าการโจมตีดังกล่าวมิได้มีผลเพื่อทำลายเครื่องคัดแยกยูเรเนี่ยมอย่างถาวรเพียงแต่เป็นการรบกวนการทำงานเท่านั้น[512] ปฏิบัติการที่เกิดขึ้นดังกล่าวไม่พบว่ามีฝ่ายใดแสดงความรับผิดชอบต่อการกระทำและความเสียหายที่เกิดขึ้นแม้จะมีหลักฐานน่าเชื่อว่าสหรัฐอเมริกาจะเป็นต้นเหตุก็ตาม

ในกรณีการโจมตีทางไซเบอร์ประเทศจอร์เจียซึ่งเกิดขึ้นในสถานการณ์การขัดกันทางอาวุธในเดือนสิงหาคม ค.ศ.2008 ระหว่างกลุ่มเซาท์ออสเซเทีย (South Ossetia) กับรัฐบาลจอร์เจีย[513] ก็ปรากฏการโจมตีทางไซเบอร์ต่อเว็บไซต์ของรัฐบาลจอร์เจียด้วยปฏิบัติการปฏิเสธการเข้าถึงบริการทางอินเทอร์เน็ต (DDoS) ทำให้เว็ตไซต์รัฐบาลจอร์เจียไม่สามารถทำงานได้ 24 ชั่วโมง[514] นอกจากนั้นยังมีการโจมตีทางไซเบอร์พร้อมการโจมตีด้วยกองกำลังทหารเกิดขึ้นอีกครั้งในวันที่ 8 สิงหาคม ค.ศ.2008[515] ผลเสียหายจากการโจมตีทางไซเบอร์ดังกล่าวทำให้รัฐบาลจอร์เจียต้องใช้เวลาหลายวันในการแก้ไขให้เว็บไซต์ของรัฐบาลกลับมาใช้ได้เหมือนเดิม

จากเหตุการณีดังกล่าวแม้เจ้าหน้าที่รัฐบาลจอร์เจียจะได้ทำการสอบสวนและมีการกล่าวหารัฐบาลรัสเซียว่าอยู่เบื้องหลังการโจมตีทางไซเบอร์แต่รัฐบาลรัสเซียก็ปฏิเสธว่าการกระทำดังกล่าวไม่ใช่ปฏิบัติการของกองทัพรัสเซียแต่เป็นไปได้ว่าจะเป็นปฏิบัติการของพลเรือนรัสเซียซึ่งอาจปฏิบัติการในประเทศรัสเซียหรือที่สถานที่อื่น[516] ขณะที่ผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์ยืนยัน

---

[512] David Albright, Paul Brannan, and Christina Walrond, “Stuxnet Malware and Natanz: update of ISIS December 2010,” p. 4.

[513] Kadri Kaska Eneken Tikk, Liis Vihul, International Cyber Incidents: Legal Considerations, (Tallinn: Cooperative Cyber Defence Center of Excellence (CCD COE), 2010), p. 68. [online] accessed June 20,2022, Available from: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

[514] Williams C. Ashmore, “Impact of Alleged Russian Cyber Attacks,” Baltic Security and Defense Review, 11 (2009): 10.

[515] Ibid.

[516] John Markoff, “Before the Gunfire, Cyber Attacks,” The New York Times, August 12, 2008, [online] Accessed: September 22, 2022. Available from: https://www.nytimes.com/2008 /08/13/technology/13cyber.html,

ว่ากลุ่มปฏิบัติการโจมตีทางไซเบอร์ของรัสเซียนั้นรู้จักกันในชื่อกลุ่มเครือข่ายธุรกิจรัสเซีย (Russian Business Network) ซึ่งมีความเป็นไปได้สูงว่าจะเชื่อมโยงไปถึงรัฐบาลรัสเซีย[517]

การปฏิบัติการทางไซเบอร์ที่เกิดขึ้นในการขัดกันทางอาวุธดังกล่าวสะท้อนให้เห็นว่าแม้จะมีความพยายามในการตรวจสอบหาผู้กระทำการให้ได้เพียงใดก็จะพบกับปัญหาในการพิสูจน์ตัวตนของผู้กระทำการที่แท้จริงซึ่งหลายกรณีมักจะมีการปฏิเสธจากฝ่ายที่เชื่อว่าจะเป็นผู้กระทำการนั้น แม้ว่าการปฏิเสธดังกล่าวจะเป็นความจริงหรือไม่ก็ตามแต่ปัญหาที่น่าคิดคือกรณีที่ปฏิบัติการเหล่านี้เกิดขึ้นในขณะที่เกิดการขัดกันทางอาวุธการดำเนินการตอบโต้จะกระทำการได้อย่างไรและการตอบโต้เพียงใดจึงจะถือว่าเป็นไปโดยความได้สัดส่วนและตรงกับเป้าหมายที่แท้จริง

2.4.2.2 ปัญหาการพิสูจน์ตัวตนของผู้ใช้งานอากาศยานไร้คนขับ

กรณีการขัดกันทางอาวุธระหว่างรัสเซียและยูเครนปรากฏการใช้อากาศยานเชิงพาณิชย์ Mugin-5 ของบริษัท Mugin Limited ประเทศจีนโดยคาดว่าจะมาจากปฏิบัติการของกองทัพรัสเซีย มีการดัดแปลงอากาศยานไร้คนขับดังกล่าวด้วยการติดตั้งวัตถุระเบิดเข้าไปแต่ทหารยูเครนพบการบินเข้ามาของอากาศยานดังกล่าวจึงทำการยิงอากาศยานดังกล่าวตก ภายหลังจากการตรวจพิสูจน์พบว่าเป็นอากาศยาน Mugin-5 ผลิตจากประเทศจีน อากาศยานดังกล่าวเป็นที่รู้จักในสังคมออนไลน์ในชื่อ Alibaba Drone มีราคาขายในประเทศจีนอยู่ที่ 15,000 เหรียญดอลลาร์สหรัฐอเมริกา[518] แม้หน่วยความมั่นคงยูเครน (SBU) และนักวิชาการผู้เชี่ยวชาญด้านอาวุธจาก Staffordshire University คือนาย N.R. Jenzen-Jones ยืนยันว่ากรณีดังกล่าวเป็นการนำอากาศยานไร้คนขับเชิงพาณิชย์มาใช้ในสงคราม[519] และเชื่อว่าปฏิบัติการดังกล่าวน่าจะมาจากฝ่ายรัสเซียแต่ก็ไม่พบการแถลงการณ์รับผิดชอบโดยฝ่ายรัสเซียหรือฝ่ายใดๆ ซึ่งพฤติการณ์ดังกล่าวก็ไม่ได้แตกต่างจากการใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตี

กรณีการใช้อากาศยานไร้คนขับแต่ไม่ปรากฏการแสดงความรับผิดชอบนี้มีความแตกต่างจากการใช้ปฏิบัติการทางไซเบอร์อยู่บ้างในบางลักษณะเป็นต้นว่า อากาศยานไร้คนขับนั้นแสดงปฏิบัติการ

---

[517] Siobhan Gorman, “Georgia States Computers hit by Cyberattack,” The Wall Streat Journal, August 12, 2008, [online] Accessed: March 20, 2023. Available from: https://www.wsj. com /articles/SB121850756472932159

[518] Rebecca Wright, Ivan Watson, Olha Konovalova, and Tom Booth, “Chinese-made drone, retrofitted and weaponized, downed in eastern Ukraine,” CNN online, March 16, 2023.

[519] Ibid.

ทางกายภาพอย่างชัดเจนเพียงแต่การควบคุมทางไกลทำให้เกิดปัญหาของการพิสูจน์ว่าผู้สั่งปฏิบัติการคือใคร ในขณะที่ปฏิบัติการทางไซเบอร์อาจมีปัจจัยที่เกี่ยวข้องค่อนข้างมากทั้งลักษณะการปฏิบัติการที่อยู่ห่างกันโดยสถานที่และเวลา เนื่องจากปฏิบัติการทางไซเบอร์ไม่จำเป็นต้องนำไปสู่ผลเสียหายทันทีและอาจไม่เกิดความเสียหายเลยก็ได้และสื่อกลางที่นำปฏิบัติการให้เกิดขึ้นอยู่ในระบบดิจิทัลเป็นส่วนมาก เมื่อปฏิบัติการในระบบดิจิทัลสมบูรณ์ตามเงื่อนไขที่ผู้ออกคำสั่งกำหนดไว้จึงจะนำไปสู่ผลทางกายภาพเกิดขึ้น ความห่างระหว่างการสั่งการและผลที่เกิดขึ้นจึงค่อนข้างมีความไม่แน่นอน แต่อย่างไรก็ดีทั้งการปฏิบัติการทางไซเบอร์และการใช้อากาศยานไร้คนขับก็ยังนำไปสู่การปฏิเสธความเกี่ยวข้องและความรับผิดชอบของผู้กระทำการเช่นกัน

2.4.3 องค์ประกอบการทำงานที่ไม่แสดงผลทางกายภาพ

พื้นฐานการทำงานของเทคโนโลยีหลายชนิดอยู่บนเทคโนโลยีร่วมกันคือระบบดิจิทัลหรือการทำงานผ่านสัญญาณไฟฟ้าแบบไม่ต่อเนื่องที่มีค่าของสัญญาณแบบ 1 และ 0[520] ประกอบกับการทำงานของระบบคอมพิวเตอร์ซึ่งจะแสดงผลของสัญญาณดิจิทัลให้เป็นตัวหนังสือ ภาพ สัญญาณหรือการแสดงออกทางกายภาพของจักรกลหุ่นยนต์ คอมพิวเตอร์ประการใดประการหนึ่งจึงทำให้การทำงานของระบบดิจิทัลนี้มีกลไกส่วนใหญ่อยู่ที่สัญญาณดิจิทัลซึ่งไม่มีสถานะทางกายภาพเนื่องจากอยู่ในรูปแบบของคลื่นสัญญาณไฟฟ้าจึงต้องรอให้มีการแสดงผลขั้นสุดท้ายด้วยอุปกรณ์ที่เกี่ยวข้องจึงจะทราบได้ว่าสัญญาณนั้นมีความหมายอย่างไร ลักษณะการทำงานที่กล่าวมานี้มีผลย่างมากต่อการพิจารณาการโจมตีทางไซเบอร์ว่าจะเทียบเท่ากับการโจมตีตามแบบปกติที่มีการแสดงออกทางกายภาพได้อย่างไร อย่างไรก็ดีนอกจากปฏิบัติการทางไซเบอร์แล้วยังพบรูปแบบการทำงานของปัญญาประดิษฐ์ที่เกี่ยวข้องกับชุดคำสั่งทางคอมพิวเตอร์เพื่อทำให้ระบบอาวุธอิสระสามารถทำงานได้ก็มีความเกี่ยวข้องกับเทคโนโลยีดิจิทัลที่ไม่เป็นลักษณะของการดำเนินการทางกายภาพด้วย

2.4.3.1 เทคโนโลยีดิจิทัลกับปฏิบัติการทางไซเบอร์

ดังที่ได้กล่าวไปว่าการทำงานของไซเบอร์เป็นการเชื่อมต่อการสื่อสารของคอมพิวเตอร์กับมนุษย์และอุปกรณ์อื่นๆ โดยมีองค์ประกอบทั้งเชิงกายภาพคือเครื่องมือที่เกี่ยวข้องกับการสื่อสารเพื่อการรับ-ส่งข้อมูล[521] ระบบการสื่อสารในเครือข่าย www และแอปพลิเคชั่นการใช้งาน

---

[520] Linda Null, and Julia Lobur, The Essentials of Computer Organization and Architecture. (Massachusetts: Jones & Bartlett Publishers, 2006), p. 121.

[521] Serkan Savas and Suleyman Karatas, “Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance,” International Cybersecurity Law Review, Vol. 3, (2022): 9-11.

เครือข่ายคอมพิวเตอร์ในรูปแบบต่างๆ ซึ่งต้องอาศัยระบบการสื่อสารพื้นฐานเช่น เครือข่ายสัญญาณโทรศัพท์ไม่ว่าจะผ่านสายนำสัญญาณ หรือคลื่นความถี่โทรศัพท์เคลื่อนที่ รวมถึงการสื่อสารผ่านสัญญาณดาวเทียม และระบบกำหนดตำแหน่งบนพื้นโลก (GPS) เพื่อให้การเชื่อมต่อการทำงานของคอมพิวเตอร์เกิดขึ้นได้อย่างสมบูรณ์[522] และข้อมูลที่มีการส่งผ่านระบบหรือข้อมูลที่ส่งผ่านเครือข่ายไม่ว่าจะเป็นถ้อยคำ ภาษา เอกสาร รูปภาพ คำสั่ง ชุดคำสั่ง (โปรแกรม) ฯลฯ ในลักษณะของสัญญาณแม่เหล็กไฟฟ้า (Electro Magnetic) หรือสัญญาณไฟฟ้า ทั้งผ่านสายที่ทำหน้าที่ส่งข้อมูลและที่ส่งผ่านระบบไร้สาย[523]

ลักษณะของข้อมูลที่ส่งผ่านคลื่นแม่เหล็กไฟฟ้าหรือคลื่นไฟฟ้าทำให้ไม่สามารถระบุได้ว่า ณ ช่วงเวลาใดคลื่นดังกล่าวอยู่ที่ใดอยู่ในสถานะใดเนื่องจากพื้นที่การเดินทางของข้อมูลและตัวข้อมูลไม่มีตัวตนทางกายภาพเช่นเดียวกับโปรแกรมคอมพิวเตอร์และปฏิบัติทางไซเบอร์เพื่อการโจมตีซึ่งประกอบด้วยการทำงานของโปรแกรมในระบบดิจิทัลและจะแสดงผลเกิดขึ้นอย่างใดย่อมจะทราบได้เมื่อมีผลแสดงทางกายภาพไม่ว่าจะเป็นการใช้งานระบบอินเทอร์เน็ตไม่ได้ การเข้าถึงข้อมูลไม่ได้หรือการทำงานของระบบคอมพิวเตอร์ที่ผิดปกติ ทำให้ในปัจจุบันการพิจารณาการโจมตีทางไซเบอร์ยังคงยึดหลักผลที่เกิดขึ้นเป็นสำคัญ

2.4.3.2 เทคโนโลยีดิจิทัลกับการทำงานของปัญญาประดิษฐ์ในระบบอาวุธอิสระ

ระบบปัญญาประดิษฐ์เกี่ยวข้องกับคอมพิวเตอร์เป็นสำคัญเพราะเป็นการประมวลผ่านทั้งอุปกรณ์และโปรแกรมที่เป็นซอฟท์แวร์ ทั้งการทำงานของอัลกอริทึ่ม (Algorithm) การเรียนรู้ของจักรกล (Machine Learning) และการเรียนรู้เชิงลึก (Deep Learning) ซึ่งทั้งหมดเป็นการจำลองการทำงานของสมองมนุษย์ให้อยู่ในคอมพิวเตอร์ ระบบอาวุธอิสระจึงต้องประกอบด้วยสมองประมวลผลที่มีการคำนวณวิเคราะห์ ค้นหาเป้าหมายและโจมตีเป้าหมายได้เสมือนมนุษย์แต่อาจมีขีดความสามารถที่มากกว่ามนุษย์ เพราะปัญญาประดิษฐ์ในระบบอาวุธอิสระมีองค์ประกอบส่วนย่อยที่เป็นข้อมูลมหาศาล (Big Data) เพื่อการวิเคราะห์ สามารถเรียนรู้และการประมวลผลได้[524] จึงนับได้ว่าส่วนสำคัญของระบบอาวุธอิสระ (Autonomous Weapon System) คือการที่ระบบอาวุธตัดสินใจ

[522] Serkan Savas and Suleyman Karatas, “Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance,”: 9-11.

[523] Ibid.

[524] Iqbal H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,” SN Computer Science, Vol.2 No. 420 (2021), p. 425.

อิสระได้ด้วยตัวเองเสมือนมนุษย์ ปัญหาเกิดขึ้นว่าส่วนหนึ่งของการตัดสินใจของระบบอาวุธอิสระนั้นคือการทำงานของโปรแกรมคอมพิวเตอร์ซึ่งอยู่ในรูปแบบการประมวลผลทางดิจิทัลซึ่งแท้จริงแล้วก็คล้ายคลึงกับการคิดวิเคราะห์ในสมองของมนุษย์ เพียงแต่เป็นการจำลองมาอยู่ในเครื่องจักรกลจึงนำมาสู่ประเด็นว่าหากเครื่องจักรคิดได้เหมือนคนจะนำไปสู่ความรับผิดทางกฎหมายแบบเดียวกับคนหรือไม่ ซึ่งคำตอบค่อนข้างชัดเจนว่าไม่ เพราะกฎหมายมีเป้าหมายในการบังคับกับมนุษย์เป็นสำคัญ

การประมวลผลในระบบดิจิทัลของระบบอาวุธอิสระนี้เป็นรูปแบบเดียวกับที่ปรากฏในการปฏิบัติการทางไซเบอร์เพียงแต่ในระบบอาวุธอิสระมีการทำงานร่วมกันระหว่างโปรแกรมคอมพิวเตอร์ที่เป็นซอฟท์แวร์กับระบบอาวุธที่เป็นฮาร์ดแวร์ทำให้ผลที่เกิดขึ้นจากปฏิบัติการทางไซเบอร์กับการทำงานของระบบอาวุธอิสระมีความแตกต่างกันคือระบบไซเบอร์อาจเกิดผลอย่างไรก็ได้ไม่แน่นอนแต่ระบบอาวุธอิสระมีแนวโน้มที่จะเกิดผลเสียหายทางกายภาพมากกว่าเพราะเป็นการใช้งานระบบไซเบอร์ที่ประกอบรวมกับอาวุธ เมื่อมีอาวุธเข้ามาเกี่ยวข้องกับการทำงานจึงคาดหมายได้ว่าจะมีความเสียหายเกิดขึ้น อย่างไรก็ดีสาระสำคัญที่นักกฎหมายมนุษยธรรมระหว่างประเทศสนใจคือระบบการประมวลผล การวิเคราะห์และการตัดสินใจของระบบอาวุธนี้ว่าจะก่อให้เกิดนัยสำคัญต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศในมิติใดหรือไม่

2.4.4 เทคโนโลยีใหม่ที่พัฒนาเพื่อการทหาร

ในการขัดกันทางอาวุธระหว่างยูเครนและรัสเซียปรากฏการใช้งานระบบอาวุธเหนือเสียงโดยสำนักข่าว The Guardian ได้รายงานในวันที่ 20 มีนาคม พ.ศ.2565 ว่ากองทัพรัสเซียเพิ่มจำนวนอาวุธเหนือเสียง (Hypersonic Weapon) ชนิดติดตั้งบนเครื่องบิน Kinzhal ในสงครามยูเครน-รัสเซีย และในวันเดียวกันทางการรัสเซียได้กล่าวอ้างว่าอาวุธชนิดนี้สามารถทำลายคลังน้ำมันในเมืองนิโคลาเยฟ (Mykolaiv) ของยูเครนได้สำเร็จอีกด้วย[525]

การใช้งานอาวุธเหนือเสียงชนิดนี้ได้รับการจับตามองว่าเป็นอาวุธสมัยใหม่ (next-generation weapon) จุดเด่นของอาวุธชนิดนี้คือความเร็วเกือบ 10 เท่าของความเร็วเสียง แต่มีขีด

[525] ภูภุช กนิษฐชาติ, Hypersonic Weapon อาวุธเหนือเสียงนวัตกรรมเปื้อนเลือดเหนือน่านฟ้าสงครามยูเครน-รัสเซีย," Way Magazine online, 24 มีนาคม พ.ศ.2565, [online] เข้าถึงเมื่อ 15 มกราคม พ.ศ. 2566. สืบค้นจาก https://waymagazine.org/hypersonic-weapon-in-russia-ukraine-war/

ความสามารถในการเคลื่อนที่ขณะถูกยิงออกไปแล้วเหมือนกับขีปนาวุธร่อน (cruise missile) ทำให้ยังคงมีความแม่นยำ และทำให้การป้องกันการโจมตียากขึ้นกว่าเดิมมาก[526]

จากข้อมูลของ The Economist ระบุว่าอาวุธความเร็วเหนือเสียงสามารถเดินทางผ่านอากาศได้ด้วยความเร็วถึง 1.6 กิโลเมตรต่อ 1 วินาทีซึ่งเร็วพอๆ กับขีปนาวุธพิสัยไกล (long-range ballistic missile) ช่วงที่กำลังกลับเข้าสู่ชั้นบรรยากาศ แต่จุดเด่นของอาวุธดังกล่าวคือความสามารถในการควบคุมทิศทางได้หลังจากยิงออกไปแล้ว ทำให้ยากต่อการสกัดกั้นด้วยเทคโนโลยีทางการทหารทั่วไปในปัจจุบัน[527]

ชนิดของอาวุธเหนือเสียงในปัจจุบันถูกแบ่งอย่างกว้างออกเป็น 2 ประเภท ประเภทแรกคือขีปนาวุธร่อน มีรูปแบบคล้ายขีปนาวุธรูปแบบร่อนรุ่นก่อนๆ เช่น จรวดโทมาฮอว์ค (Tomahawk) แต่เร็วมากขึ้น ขณะที่อีกประเภทคือ hypersonic glide vehicles (HGVs) ที่ใช้จรวดบูสเตอร์ในการขับเคลื่อนขึ้นสู่ชั้นบรรยากาศก่อนตกลงมาสู่เป้าหมายด้วยความเร็วเหนือเสียงซึ่งทำให้การคาดการณ์เพื่อป้องกันทำได้ยากกว่าขีปนาวุธพิสัยไกลรุ่นก่อนๆ[528] ความสามารถในการควบคุมทิศทางระหว่างยิงออกไปแล้ว ไม่เพียงทำให้ขีปนาวุธสามารถหลบหลีกการสกัดกั้นได้เท่านั้น แต่สามารถทำได้แม้แต่การเปลี่ยนเป้าหมายกลางอากาศได้ด้วย ซึ่งตอนนี้ขีปนาวุธ Kinzhal ของรัสเซียถูกประเมินว่ามีพิสัยอยู่ที่ประมาณ 2,000 กิโลเมตร[529]

ถึงแม้พลังการทำลายล้างอาจจะไม่ได้สูงมากนักเมื่อเทียบกับจรวดรุ่นอื่นๆ ที่เคยมีมาในประวัติศาสตร์การทหารแต่ความรวดเร็วของจรวดอาจเปลี่ยนแปลงรูปแบบของการรบไปมากพอสมควร โดยเฉพาะเมื่ออาวุธชนิดนี้กำลังถูกทดลองใช้งานจริงในสงครามยูเครน-รัสเซีย[530]ประเทศที่ดำเนินโครงการขีปนาวุธเหนือเสียงมีอยู่ทั้งสิ้น 3 ประเทศ คือ สหรัฐอเมริกา สาธารณรัฐประชาชนจีน และรัสเซีย[531]

---

[526] ภูภุช กนิษฐชาติ, “Hypersonic Weapon อาวุธเหนือเสียงนวัตกรรมเปื้อนเลือดเหนือน่านฟ้าสงครามยูเครน-รัสเซีย,”

[527] เรื่องเดียวกัน.

[528] เรื่องเดียวกัน.

[529] เรื่องเดียวกัน.

[530] เรื่องเดียวกัน.

[531] เรื่องเดียวกัน.

สหรัฐเริ่มการทดลองขีปนาวุธเหนือเสียงในช่วงต้นปี 2000 เพื่อใช้ป้องกันหรือจู่โจมเป้าหมายที่มีลักษณะเร่งด่วน ก่อนที่กระทรวงกลาโหมสหรัฐจะเริ่มเพิ่มงบประมาณในโครงการอาวุธเหนือเสียงเหล่านี้เพื่อพัฒนาให้มันสามารถใช้งานในระดับภูมิภาคได้ดีมากขึ้น อย่างไรก็ตาม คำกล่าวของ CRS ได้ระบุว่า สหรัฐแตกต่างจากจีนและรัสเซียตรงที่ไม่ได้พยายามพัฒนาให้เทคโนโลยีนี้สามารถใช้งานได้กับหัวรบนิวเคลียร์[532]

ทางด้านรัสเซีย ก่อนที่จะมีขีปนาวุธ Kinzhal เคยมีโครงการ HGVs ในชื่อ Avangard ที่สามารถบรรจุหัวรบนิวเคลียร์ได้โดยยิงจากฐานยิงขีปนาวุธพิสัยไกล SS-19 ความน่ากลัวของ Avangard คือมันสามารถที่จะหลบหลีกจรวดต่อต้านขีปนาวุธของสหรัฐได้ (ตามที่รัสเซียกล่าวอ้าง) และทางการรัสเซียระบุว่า การทดสอบอาวุธชนิดนี้ประสบความสำเร็จแล้วในปี 2018 ซึ่งในปี 2019 กองทัพรัสเซียระบุต่อสาธารณะว่า มีขีปนาวุธ SS-19 อย่างน้อย 2 ลูกที่ติดตั้งจรวจ Avangard แบบพร้อมใช้งานเอาไว้แล้ว[533]

ขณะที่จีนมีโครงการขีปนาวุธเหนือเสียงของตนเองเช่นเดียวกันในชื่อ DF-ZF โดยได้ทำการทดสอบมาแล้วกว่า 9 ครั้ง ตั้งแต่ปี 2014 และจากข้อมูลของ CRS มีการคาดการณ์ว่าขีปนาวุธ DF-ZF มีความสามารถในการเคลื่อนไหวระดับสูงกว่าการเคลื่อนไหวทั่วไป จนอาจจะทำให้ระบบป้องกันขีปนาวุธพิสัยไกลของสหรัฐไม่สามารถป้องกันได้ และยังคาดการณ์ไว้อีกด้วยว่าขีปนาวุธ DF-ZF ตัวนี้อาจจะมีพิสัยอยู่ที่ 1,800-2,500 กิโลเมตร[534]

นอกเหนือไปจากข้อมูลของ CRS แล้ว สำนักข่าว The Economist ยังมองว่าไม่ใช่แค่ 3 ประเทศนี้เท่านั้นที่มีโครงการลักษณะดังกล่าว แต่ปัจจุบันนี้โครงการอาวุธเหนือเสียงยังถูกพัฒนาโดยประเทศออสเตรเลีย ฝรั่งเศส อินเดียและญี่ปุ่นขณะที่สำนักข่าว VOA News ระบุว่า เยอรมนี อิหร่าน อิสราเอล และเกาหลีใต้ก็ได้ดำเนินโครงการไปในระยะหนึ่งแล้วเช่นกัน[535]

การใช้ขีปนาวุธเหนือเสียงของรัสเซียในยูเครน ทำให้รัสเซียกลายเป็นชาติแรกที่ใช้งานอาวุธชนิดนี้จริงในประวัติศาสตร์ คำถามสำคัญที่น่าสนใจต่อมาคือทำไมรัสเซียถึงยอมใช้อาวุธที่มีราคาสูงเช่นนี้เมื่อขีปนาวุธพิสัยไกลทั่วไปก็สามารถบรรลุเป้าหมายได้เช่นเดียวกัน นักวิเคราะห์การทหารของ

---

[532] ภูภุช กนิษฐชาติ, “Hypersonic Weapon อาวุธเหนือเสียงนวัตกรรมเปื้อนเลือดเหนือน่านฟ้าสงครามยูเครน-รัสเซีย,”

[533] เรื่องเดียวกัน.

[534] เรื่องเดียวกัน.

[535] เรื่องเดียวกัน.

รัสเซีย พาเวล ฟิลกินฮาวเวอร์ (Pavel Felgenhauer) ให้ความเห็นว่าขีปนาวุธเหนือเสียงที่กำลังถูกใช้ในสงครามยูเครนครั้งนี้อาจจะไม่ได้เปลี่ยนแปลงภูมิทัศน์ทางการทหารมากนักเมื่อเทียบกับผลทางด้านจิตวิทยาและโฆษณาชวนเชื่อ ซึ่งยังมีความเป็นไปได้อีกว่าขีปนาวุธชนิดอื่นๆ ของรัสเซียเริ่มใช้งานไม่ได้เท่าที่คาดหวังสำหรับการจู่โจมยูเครน

จากการศึกษาวิเคราะห์การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธพบว่าพัฒนาการทางเทคโนโลยีในปัจจุบันมีแนวโน้มของการใช้เทคโนโลยีไซเบอร์และเทคโนโลยีปัญญาประกอบร่วมกับการใช้งานระบบอาวุธและปฏิบัติการทางทหารมากขึ้น ในขณะที่เทคโนโลยีเหล่านี้มีลักษณะเป็นเทคโนโลยีที่ใช้ร่วมกันระหว่างทหารและพลเรือนเป็นสำคัญ ด้วยลักษณะดังกล่าวเทคโนโลยีจึงอาจใช้งานในการสร้างประโยชน์เพื่อพลเรือนและเพื่อประโยชน์ทางการทหารได้ ในทำนองกลับกันเทคโนโลยีดังกล่าวอาจนำไปใช้ประกอบร่วมกับการใช้อาวุธ หรือใช้เยี่ยงอาวุธเพื่อการโจมตีและการทำลายได้ ข้อค้นพบดังกล่าวจะนำไปสู่การวิเคราะห์ในบทที่ 3 ในเรื่องการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับกรณีการใช้เทคโนโลยีใหม่ที่เปลี่ยนแปลงลักษณะการขัดกันทางอาวุธ

บทที่ 3

กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่

กฎหมายมนุษยธรรมระหว่างประเทศในยุคปัจจุบันโดยเฉพาะอย่างยิ่งที่ปรากฏในพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ปี ค.ศ.1977 มีเป้าหมายในการสร้างสมดุลระหว่างการปฏิบัติอย่างมีมนุษยธรรม (Humanity) และความจำเป็นทางการทหาร (Military necessity)[536] โดยเป็นการรวมกันระหว่างหลักเกณฑ์ว่าด้วยการขัดกันทางอาวุธของกฎเกณฑ์กรุงเฮก (Hague Rules) และหลักการเกี่ยวกับมนุษยธรรมระหว่างประเทศของอนุสัญญาเจนีวา ค.ศ. 1949 หรือกลุ่มกฎหมายเจนีวา (Geneva Law)[537] ลักษณะของกฎหมายมนุษยธรรมระหว่างประเทศในปัจจุบันจึงมีความหมายรวมทั้งกฎเกณฑ์ที่ควบคุมปฏิบัติการทางทหารและกฎเกณฑ์ในการคุ้มครองประชาชนพลเรือนในสถานการณ์การขัดกันทางอาวุธ[538]

ส่วนของกฎหมายว่าด้วยการขัดกันทางอาวุธ (Law of Armed Conflict) เป็นการห้ามหรือจำกัดลักษณะการทำสงครามบางรูปแบบรวมถึงการห้ามใช้อาวุธบางชนิดในการต่อสู้[539]สาระสำคัญของการจำกัดการทำสงครามจึงอยู่ที่การจำกัดวิธีการในการทำสงคราม การจำกัดปัจจัยซึ่งรวมถึงการจำกัดอาวุธในการทำสงครามและการจำกัดกระทำของทหารหรือพลรบในบางลักษณะที่อาจนำไปสู่การละเมิดต่อหลักการขัดกันทางอาวุธ ในขณะที่กฎหมายมนุษยธรรมระหว่างประเทศจะเป็นข้อกำหนดในการให้ความคุ้มครองบุคคลเฉพาะกลุ่มเพื่อไม่ให้สงครามมีความโหดร้ายเกินความจำเป็น ดังนั้นการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศจึงต้องคำนึงถึงหลักเกณฑ์ต่างๆ เหล่านี้

ลักษณะของการห้ามหรือจำกัดการใช้อาวุธของกฎหมายว่าด้วยการขัดกันทางอาวุธมีวัตถุประสงค์ในการลดความเสียหายของทหารในสงครามเพื่อไม่ต้องบาดเจ็บทุกข์ทรมานมากไปกว่าการเสียชีวิตจากการต่อสู้ การใช้อาวุธที่ไม่นำไปสู่ความตายโดยเฉียบพลันจึงเป็นสิ่งต้องห้าม ปัญหาคืออาวุธในแต่ละยุคมีความแตกต่างกัน ความรุนแรงของความทุกข์ทรมานที่เกิดจากอาวุธแต่ละประเภทก็แตกต่างกันขึ้นอยู่กับการนิยามที่เกิดขึ้นในแต่ละช่วงเวลา เช่นอาวุธในรูปแบบของธนูและหน้าไม้เป็นอาวุธที่ต้องห้ามในอดีตเพราะมีความเห็นว่าอาวุธดังกล่าวสร้างความทุกข์ทรมานมากกว่าความตาย

---

[536] Jean Pictet, Humanitarian Law and the Protection of War Victims, p. 28.

[537] Williams Boothby, Weapons and the Law of Armed Conflict, p. 2.

[538] Jean Pictet, Humanitarian Law and the Protection of War Victims, p. 29.

[539] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (Cambridge: Cambridge University Press, 2004) pp. 33-37.

แต่ต่อมาแนวคิดเรื่องอาวุธที่ก่อให้เกิดความทุกข์ทรมานก็เปลี่ยนไปเพราะมีการใช้สารพิษประกอบร่วมกับอาวุธรวมถึงการใช้พิษเป็นอาวุธในรูปแบบของแก๊ส อาวุธที่มีพิษและอาวุธแก๊สจึงเป็นอาวุธที่ต้องห้ามเพราะนำมาซึ่งความทุกข์ทรมานเกินความจำเป็น[540] เมื่ออาวุธปืนมีบทบาทมากขึ้นในสงครามยุคต่อมาก็นำไปสู่การพัฒนากระสุนปืนที่มีอำนาจทำลายล้างมากขึ้น อาวุธปืนบางชนิดที่ใช้กระสุนซึ่งอำนาจทำลายเกินความจำเป็นในการฆ่าก็จะเป็นอาวุธที่ก่อให้เกิดความทุกข์ทรมานเกินความจำเป็น เช่น กระสุนลูกปราย กระสุนระเบิด กระสุนที่ขยายตัวเมื่อถูกเป้าหมาย[541] ฯลฯ

หลังสงครามโลกครั้งที่ 2 เป็นต้นมาอาวุธที่ก่อให้เกิดความทุกข์ทรมานเกินความจำเป็นหมายถึงอาวุธที่มีอานุภาพทำลายโดยไม่สามารถจำกัดเป้าหมายหรือไม่สามารถจำกัดผลความเสียหายได้ เช่น อาวุธที่มีอานุภาพทำลายล้างสูง (อาวุธนิวเคลียร์ อาวุธเคมี อาวุธชีวภาพ) ทุ่นระเบิดสังหารบุคคลและทุ่นระเบิดทำลายรถถัง การใช้วิธีการทางเทคโนโลยีเพื่อเปลี่ยนแปลงสภาพแวดล้อมให้เป็นอาวุธในการทำลาย เป็นต้น[542]

การจำกัดหรือห้ามการใช้อาวุธในกฎหมายว่าด้วยการขัดกันทางอาวุธจึงมีความแตกต่างกันในแต่ละช่วงเวลาขึ้นอยู่กับพลวัตของการใช้อาวุธที่เปลี่ยนแปลงไป นอกจากนั้นทัศนะของนักกฎหมายระหว่างประเทศและสังคมระหว่างประเทศยังมีผลต่อการห้ามหรือจำกัดการใช้อาวุธหรือวิธีการที่มองว่าเป็นการสร้างความได้เปรียบในการสงครามเกินสมควร[543]

ความได้เปรียบทางสงครามที่เกินขอบเขตนี้เกี่ยวข้องกับหลายประเด็น ได้แก่การทำสงครามจะต้องไม่นำไปสู่ความทุกข์ทรมานเกินสมควรของผู้ที่มีส่วนเกี่ยวข้องกับการต่อสู้ การทำสงครามจะต้องเป็นไปเท่าที่ได้สัดส่วนเหมาะสมทางการทหารเพื่อผลแพ้ชนะในการรบ ความเสียหายที่ไม่สามารถจำกัดขอบเขตได้จึงเป็นสิ่งที่เกินความจำเป็นและการต่อสู้ในสงครามนี้จะต้องการแยกแยะเป้าหมายระหว่างพลเรือนและทหาร เฉพาะเป้าหมายทางทหารเท่านั้นที่เป็นเป้าหมายในการโจมตีในสงคราม กรณีการโจมตีใดที่อาจก่อให้เกิดความเสียหายหรือผลกระทบกับทั้งทหารและพลเรือนไปพร้อมกันโดยอาจเป็นความเสียหายกับพลเรือนมากกว่าทางทหารเป็นสิ่งที่เกินความจำเป็นในการรบ[544]

---

[540] Williams Boothby, Weapons and the Law of Armed Conflict, p. 16-17.

[541] Ibid., p. 10.

[542] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

[543] Ibid.

[544] Ibid., p. 37.

กฎหมายว่าด้วยการขัดกันทางอาวุธในยุคแรกจึงเป็นเรื่องหลักเกณฑ์การทำสงครามและความจำเป็นทางการทหารในการรบ ต่อมาในปี ค.ศ.1949 มีการสร้างอนุสัญญาเจนีวา ค.ศ.1949 ขึ้น โดยมีเนื้อหาเกี่ยวกับหลักการปฏิบัติต่อกันอย่างมีมนุษยธรรมของคู่พิพาทในสงครามคือเน้นการคุ้มครองพลเรือนและทหารที่บาดเจ็บ ป่วยไข้หรือทหารที่ไม่สามารถทำการต่อสู้ในการรบได้ (Hors de combat)[545] อนุสัญญาเจนีวาจึงมีลักษณะเป็นกฎหมายที่คุ้มครองบุคคลในการทำสงคราม แต่ไม่เกี่ยวข้องกับการห้ามหรือจำกัดรูปแบบการทำสงครามและการใช้อาวุธโดยตรง ต่อมามีการสร้างพิธีสารฉบับที่ 1 และฉบับที่ 2 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 พิธีสารทั้งสองฉบับนี้มีการนำหลักการห้ามใช้ปัจจัยและวิธีการทำสงครามรวมตลอดถึงการใช้อาวุธในบางลักษณะที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น[546] นอกจากนั้นยังมีการรวมเอาหลักการแยกแยะเป้าหมายในการโจมตี หลักความได้สัดส่วนในการโจมตี หลักความระมัดระวังล่วงหน้าก่อนการโจมตีรวมตลอดถึงหลักการคุ้มครองทรัพย์สิ่งของพลเรือนและสาธารณูปโภคต่างๆ ซึ่งเป็นส่วนหนึ่งของกฎหมายเกี่ยวกับขัดกันทางอาวุธมารวมไว้ในพิธีสาร (โดยเฉพาะอย่างยิ่งในพิธีสารฉบับที่ 1) จึงทำให้หลักความจำเป็นทางการทหารและหลักความมีมนุษยธรรมถูกรวบรวมอยู่ในพิธีสารเพิ่มเติมอนุสัญญาเจนีวา[547] ดังนั้นในยุคปัจจุบันเมื่อกล่าวถึงกฎหมายมนุษยธรรมระหว่างประเทศจึงหมายถึงกฎหมายระหว่างประเทศที่เกี่ยวกับเรื่องความจำเป็นทางการทหารและความมีมนุษยธรรมไปพร้อมกัน[548]

เนื่องจากกฎหมายมนุษยธรรมระหว่างประเทศจะมีผลบังคับตั้งแต่เกิดการขัดกันทางอาวุธขึ้นเกี่ยวข้องกับปฏิบัติการทางทหารที่จะต้องสอดคล้องต่อหลักการใช้ปัจจัยและวิธีการในการขัดกันทางอาวุธซึ่งรวมถึงการใช้อาวุธด้วยและปฏิบัติการทางทหารดังกล่าวจะต้องสอดคล้องต่อหลักการแยกแยะเป้าหมายในการโจมตี ในการโจมตีแต่ละครั้งจะต้องนำไปสู่ผลกระทบที่ได้สัดส่วนต่อความได้เปรียบทางการทหาร ปฏิบัติการทางทหารเพื่อการโจมตีแต่ละครั้งจึงต้องมีการประเมินความระมัดระวังล่วงหน้าก่อนการโจมตีรวมตลอดถึงการเคารพต่อกฎเกณฑ์อื่นๆ ที่กฎหมายกำหนดเอาไว้ ในบทที่ 3 นี้ผู้วิจัยจึงทำการศึกษาโดยใช้กฎหมายมนุษยธรรมระหว่างประเทศเป็นแกนหลักในการ

---

[545] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 159.

[546] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, available at: https://www.refworld.org/docid/3ae6b36b4.html [accessed 28 May 2021], Art 35 (2).

[547] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 33.

[548] Jean Pictet, Humanitarian Law and the Protection of War Victims, p. 13.

พิจารณาแต่ละขั้นตอนที่กฎหมายมนุษยธรรมระหว่างประเทศมีผลบังคับในสถานการณ์ต่างๆ และนำตัวอย่างการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธที่เกิดขึ้นในสถานการณ์ต่างๆ ซึ่งมีนัยสำคัญต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศในแต่ละกรณีมาพิจารณาวิธีการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อกรณีดังกล่าว

3.1 แนวคิดเรื่องการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่

การนำเทคโนโลยีใหม่มาใช้ในการขัดกันทางอาวุธก่อให้เกิดความเปลี่ยนแปลงของสมรภูมิรบอย่างมาก การใช้ปฏิบัติการทางไซเบอร์ในการรบและการโจมตีทางไซเบอร์ร่วมกับการรบตามแบบทำให้พลเรือนเข้ามามีส่วนร่วมมากขึ้นอย่างมีนัยสำคัญ[549] ลักษณะการใช้งานระบบไซเบอร์ซึ่งอยู่บนพื้นที่ซึ่งพลเรือนและทหารใช้ร่วมกันทำให้การจำแนกผู้มีส่วนร่วมในการรบตามกฎหมายทนุษยธรรมระหว่างประเทศทำได้ยากขึ้น[550] การใช้อากาศยานไร้คนขับในการรบเป็นที่นิยมมากขึ้นเป็นการช่วยลดความสูญเสียของกำลังพลในการลาดตระเวนสังเกตการณ์และยังช่วยให้การทำลายเป้าหมายเกิดความแม่นยำมากขึ้น[551]แต่ในทางปฏิบัตินั้นการใช้อากาศยานไร้คนขับก็ทำให้เป้าหมายของการโจมตีมีโอกาสตอบโต้ได้น้อยลง ขณะที่การใช้ระบบอาวุธอิสระ (Autonomous Weapon System) ซึ่งปรากฏในหลายรูปแบบทั้งระบบป้องกันภัยทางอากาศ หุ่นยนต์สังหารและอากาศยานไร้คนขับอัจฉริยะ[552] ฯลฯ ก็นำไปสู่ปัญหาที่วิพากษ์กันอย่างกว้างขวางว่าเครื่องจักรที่ทำงานด้วยระบบปัญญาประดิษฐ์เหล่านี้จะถูกใช้งานโดยสอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศได้หรือไม่[553]

ปรากฏการณ์การใช้เทคโนโลยีในการรบในปัจจุบันที่แตกต่างจากอดีต เช่นการขัดขวางระบบสื่อสารผ่านดาวเทียมเพื่อทำลายการสื่อสารของคู่ขัดแย้งในสงครามก่อให้เกิดความเสียหายต่อ

---

[549] Patricia Justino, “The Conflict in Ukraine – The Role of Civilians,” UNU Wider. (February 2022) [online] Accessed: March 26, 2022. Available from: https://www.wider.unu.edu/publication/conflict-ukraine-role-civilians

[550] Timothe Lopez, L’adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

[551] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law", p. 101.

[552] Annabelle Quince, “Future Drone Strikes Could See Execution by Algorithm,” ABC Online, January 21, 2013., [online] Accessed: July 24, 2020. Available from: https://www.abc.net.au/radionational/programs/rearvision/drones/4703792

[553] International Committee of the Red Cross. “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.” International Committee of the Red Cross. Paper, June 6, 2019, p. 6.

ทั้งการสื่อสารผ่านระบบอินเทอร์เน็ตและการใช้สัญญาณการกำหนดตำแหน่งบนพื้นโลก (GPS)[554] ซึ่งส่งผลกระทบต่อทั้งการสื่อสารทางทหารและการสื่อสารของพลเรือน ในขณะที่เทคโนโลยีใหม่บางชนิดก็ถูกสร้างขึ้นมาเพื่อคุ้มครองความปลอดภัยของพลรบเช่นเทคโนโลยีนาโนซึ่งเป็นส่วนประกอบของการออกแบบเครื่องแบบพรางกายของทหารและการออกแบบพื้นผิวยานพาหนะที่ใช้ในการรบเพื่อลดการตรวจจับจากทั้งการมองเห็นและการตรวจจับจากสัญญาณเรดาร์และอุปกรณ์อื่นๆ[555]

เทคโนโลยีเหล่านี้มีลักษณะสำคัญร่วมกันบางประการได้แก่การที่เทคโนโลยีเหล่านี้ไม่ใช่อาวุธโดยสภาพแต่เป็นการนำเอาความรู้หรืออุปกรณ์ที่ใช้งานทั่วไปมาใช้งานเพื่อมุ่งประสงค์ร้ายหรือการนำความรู้หรืออุปกรณ์ที่ใช้งานทั่วไปมาใช้งานประกอบร่วมกับการใช้งานอาวุธ ลักษณะดังกล่าวของเทคโนโลยีทำให้พลเรือนสามารถใช้งานเทคโนโลยีได้เช่นเดียวกับทหาร ในขณะที่การใช้งานระบบไซเบอร์ การใช้งานอุปกรณ์ในระบบดิจิทัล[556]และการใช้งานสัญญาณการสื่อสารผ่านระบบดาวเทียมซึ่งเป็นสิ่งที่พลเรือนและพลรบสามารถใช้ร่วมกันได้นั้นมีลักษณะของการทำงานที่ไม่ปรากฏการแสดงออกทางกายภาพแต่นำไปสู่ผลได้ทั้งเชิงกายภาพและผลที่ไม่เป็นกายภาพ[557]ก่อให้เกิดปัญหาต่อการพิจารณาลักษณะของการโจมตีว่าเทียบเท่ากับการโจมตีตามแบบด้วยอาวุธหรือไม่

ความเปลี่ยนแปลงที่เกิดขึ้นจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธดังกล่าวส่งผลต่อการพิจารณาการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศหลายประการและสร้างข้อวิพากษ์ทางวิชาการอย่างกว้างขวางว่ากฎหมายมนุษยธรรมระหว่างประเทศที่มีมาแต่เดิมนั้นยังคงเหมาะสมและเพียงพอต่อการปรับใช้กับสถานการณ์การทำสงครามในปัจจุบันที่เปลี่ยนแปลงไปหรือไม่ เป็นการสมควรหรือไม่ที่จะต้องมีการสร้างกฎหมายใหม่ให้ครอบคลุมถึงเทคโนโลยีที่เกิดขึ้น ความตระหนักถึงสถานการณ์ที่เปลี่ยนแปลงไปนี้ไม่ได้มีผลเฉพาะเพียงการพิจารณาเรื่องความเหมาะสมในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธเท่านั้นแต่ยังรวมไปถึงความเคลื่อนไหวขององค์การระหว่างประเทศในการแก้ไขปัญหาไม่ว่าจะเป็นความเคลื่อนไหวในการสร้างแนวปฏิบัติ ความพยายามสร้างอนุสัญญาระหว่างประเทศเพื่อควบคุมเทคโนโลยีและความพยายามในการสร้างความร่วมมือระหว่างประเทศหลากหลายรูปแบบซึ่งสะท้อนให้เห็นนัยสำคัญของ

---

[554] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 27.

[555] Hitoshi Nasu and McLaughlin, R, (eds), New Technologies and the Law of Armed Conflict, p. 152.

[556] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

[557] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 279.

เทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายมนุษยธรรมระหว่างประเทศเป็นอย่างดี รายละเอียดของข้อพิจารณาทางกฎหมาย ข้อวิพากษ์ทางวิชาการและบทบาทขององค์การระหว่างประเทศอาจอธิบายได้ดังต่อไปนี้

3.1.1 ข้อพิจารณาความเป็นไปได้ของการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับสถานการณ์ที่เปลี่ยนแปลงไปในการขัดกันทางอาวุธปัจจุบัน

การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับสถานการณ์การขัดกันทางอาวุธที่มีการใช้เทคโนโลยีใหม่เป็นวิธีการและปัจจัยในการรบไม่อาจกระทำได้โดยการใช้กฎหมายลายลักษณ์อักษรแต่เพียงอย่างเดียว แต่จะต้องคำนึงถึงบริบทแวดล้อมที่เป็นปัจจัยสำคัญในการก่อร่างสร้างกฎหมายขึ้นมา พัฒนาการของกฎหมายที่เปลี่ยนแปลงไปตามสังคมระหว่างประเทศในแต่ละช่วงเวลา และการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศนั้นจะต้องไม่บิดเบือนต่อเจตนารมณ์ของกฎหมายด้วย การพิจารณาความสามารถในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศจึงเป็นปัจจัยสำคัญที่จะชี้ได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นเพียงพอที่จะปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธหรือไม่ โดยอาจแยกประเด็นพิจารณาได้ดังนี้

ประเด็นที่ 1 การปรับใช้กฎหมายกับพัฒนาการของสังคมที่เปลี่ยนแปลงไป

ในฐานะที่เป็นกฎเกณฑ์ที่ใช้บังคับสำหรับตัวกระทำการระหว่างประเทศ กฎหมายระหว่างประเทศ ไม่ว่าจะเป็นสนธิสัญญา จารีตประเพณี หลักการทั่วไปของกฎหมายที่กำหนดสิทธิและภาระผูกพันของผู้ทรงสิทธิซึ่งไม่ใช่เฉพาะรัฐหรือหน่วยงานระหว่างประเทศแต่รวมถึงตัวบุคคลด้วย กฎหมายระหว่างประเทศจึงต้องตอบสนองต่อความต้องการที่เปลี่ยนแปลงไปของสังคมระหว่างประเทศ

กฎหมายระหว่างประเทศมีการเปลี่ยนแปลงอย่างช้าๆ ตลอดเวลาหรือบางครั้งมีปฏิกิริยาฉับพลันต่อเหตุการณ์สำคัญที่มีความเฉพาะเจาะจง รูปแบบและวิธีการที่ใช้ในการขัดกันทางอาวุธเป็นตัวอย่างหนึ่งของการปรับเปลี่ยนทิศทางของกฎเกณฑ์ระหว่างประเทศอย่างมีนัยสำคัญ โดยเฉพาะอย่างยิ่งพัฒนาการของรูปแบบและวิธีการในการสู้รบมีผลต่อการเปลี่ยนแปลงของกฎหมายมนุษยธรรมระหว่างประเทศที่นำไปสู่มิติใหม่ๆ ที่ไม่เคยมีมาก่อนในอดีตและได้รับการรับรองว่ากฎเกณฑ์พื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมีสถานะเป็น jus cogens ซึ่งหมายถึงว่า

เป็นกฎเกณฑ์ที่อยู่ระดับสูงสุดโดยไม่สามารถยกเว้นหรือตกลงเป็นอย่างอื่นได้[558] ดังนั้นการทำสงคราม/การขัดกันทางอาวุธ ไม่สามารถยกเป็นเหตุเพื่อปฏิเสธหลักการเหล่านี้ได้ ในทางตรงกันข้ามจะต้องเคารพหลักเกณฑ์เหล่านี้อย่างเคร่งครัด

อย่างไรก็ตาม ในขณะเดียวกันการเปลี่ยนแปลงไปในความสัมพันธ์ระหว่างประเทศและพัฒนาการของเทคโนโลยีเป็นข้อเท็จจริงที่ทำให้รูปแบบหรือวิธีการในการปฏิบัติการทางทหารในการขัดกันทางอาวุธได้เปลี่ยนแปลงไปอย่างมากด้วยในปัจจุบัน พลวัตของการขัดกันทางอาวุธซึ่งสอดคล้องกับการเปลี่ยนแปลงในธรรมชาติและความหลากหลายของตัวกระทำการ ตลอดจนวิวัฒนาการของปัจจัยและวิธีการทำสงครามที่เชื่อมโยงกับลักษณะ asymmetric และความก้าวหน้าทางเทคโนโลยีสร้างความท้าทายต่อกฎหมายมนุษยธรรมระหว่างประเทศในบริบทของความสามารถในการปรับตัว (Adaptability) ของกฎหมายมนุษยธรรมระหว่างประเทศให้เข้ากับความเป็นข้อเท็จจริงที่เปลี่ยนไป

ประเด็นการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศที่เกี่ยวกับการใช้เทคโนโลยีใหม่จึงมีความสัมพันธ์กับความสามารถในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศที่เป็นอยู่ปัจจุบันให้เข้ากับข้อเท็จจริงที่เกี่ยวกับพัฒนาการทางเทคโนโลยีและรูปแบบของการใช้เทคโนโลยีโดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีสองทางด้วย ดังนั้น ก่อนที่จะศึกษาวิเคราะห์ประเด็นเกี่ยวกับความสามารถในการปรับตัวและข้อจำกัดในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศจำเป็นอย่างยิ่งที่ต้องศึกษาถึงความหมายและเงื่อนไขของการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศ ดังนี้

(ก) ความสามารถในการปรับตัวและการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

ความสามารถในการปรับตัวของกฎหมายกับการเปลี่ยนแปลงไปของสถานการณ์หรือข้อเท็จจริงเป็นเงื่อนไขที่มาก่อนการปรับใช้กฎหมายว่าเป็นไปได้เพียงใด ซึ่งโดยทั่วไปกฎเกณฑ์ของกฎหมายมีลักษณะเป็นการทั่วไป การปรับใช้กฎหมายกับสถานการณ์ใดสถานการณ์หนึ่งอย่างเป็นรูปธรรม กฎหมายนั้นสามารถปรับตัวให้เข้ากับสถานการณ์ใดสถานการณ์หนึ่งที่เปลี่ยนแปลงไปด้วยได้

---

[558] ICJ, 1996 Legality of the Threats or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, para 79, p.257. "...Further these fundamental rules are to be observed by all States whether or not they have ratified the conventions that contain them, because they constitute intransgressible principles of international customary law."

หรือไม่ ดังนั้นการปรับใช้กฎหมายจึงเป็นวิธีการแสดงถึงความสามารถในการปรับตัวของกฎหมายให้เข้ากับข้อเท็จจริงที่เกิดขึ้น[559] David ได้ให้ข้อสังเกตในเรื่องนี้ว่า กฎเกณฑ์หนึ่งที่จะปรับเข้ากับสถานการณ์ใดสถานการณ์หนึ่งได้ก็ต่อเมื่อกฎเกณฑ์นั้นสามารถปรับใช้ได้โดยตรงกับสถานการณ์นั้นนั้นโดยปราศจากอุปสรรคและความยุ่งยากในการตีความ แต่ถ้าหากการปรับใช้มีความยุ่งยากแต่ถึงกระนั้นก็ตาม ก็ยังมีหนทางที่จะปรับใช้กฎเกณฑ์เหล่านั้นกับสถานการณ์หรือข้อเท็จจริงที่เกิดขึ้นได้ ก็ยังอาจจะเรียกได้ว่ากฎเกณฑ์นั้นมีความสามารถในการปรับตัวได้[560]

อนึ่ง การปรับใช้กฎหมายกับสถานการณ์และข้อเท็จจริงใดข้อเท็จจริงหนึ่งไม่ใช่จุดจบในตนเอง เนื่องจากบทบาทของการปรับใช้กฎหมายคือเพื่อตอบสนองความต้องการหรือสถานการณ์ที่เปลี่ยนแปลงไปของประชาคมระหว่างประเทศ เมื่อเป็นเช่นนั้น ความสามารถในการปรับตัวของกฎหมายจะต้องสะท้อนถึงความเหมาะสมพอเพียง (Adequacy) กับข้อเท็จจริงที่เปลี่ยนแปลงไปเพื่อที่จะใช้เป็นกฎเกณฑ์ได้แต่ถ้าหากกฎเกณฑ์ดังกล่าวไม่สะท้อนถึงความเหมาะสมพอเพียงกับสถานการณ์ที่เปลี่ยนแปลงไปแล้วก็เท่ากับว่ากฎเกณฑ์เหล่านั้นไม่สามารถปรับตัวและปรับใช้ได้กับสถานการณ์ที่เปลี่ยนแปลงไป[561]

(ข) ความสามารถในการปรับตัวและความเพียงพอ

กฎหมายทำหน้าที่หลัก 2 ประการ คือ ใช้เป็นกฎเกณฑ์และเป็นมาตรฐานพฤติกรรมและศีลธรรมที่ต้องสะท้อนสังคมและตอบสนองความต้องการและความท้าทายของสังคม[562] กฎหมายจึงต้องเหมาะสมกับสถานการณ์หรือข้อเท็จจริงที่เป็นอยู่ขณะนั้น และการปรับกฎหมายเข้ากับสถานการณ์หรือข้อเท็จจริงจะมีประสิทธิผลอย่างแท้จริงได้ (Effectiveness) ก็ต่อเมื่อกฎหมายนั้นสะท้อนและเหมาะสมกับความเป็นจริงในขณะนั้น

เมื่อความเหมาะสมเพียงพอคือคุณลักษณะที่สำคัญของความสามารถในการปรับตัวและเป็นเงื่อนไขสำคัญของการประสิทธิผลของกฎหมาย ดังนั้น เมื่อกฎหมายไม่สามารถปรับเปลี่ยน

---

[559] Eric David, Le droit international humanitaire face à ces évolutions: un droit adapté ou adaptable?, dans La pertinence du Droit international humanitaire pour les acteurs non-étatiques, Actes du Colloque de Bruges du 25-26 Octobre 2002, Bruges, CICR et Collège d'Europe, no. 27, 2003, p. 41.

[560] Ibid.

[561] Alain Pellet, " L'adaptation du droit international aux besoins changeants de la société internationale," RCADI, vol. 329, (2007): p. 17.

[562] Onuma Yasuaki, "International Law in and with the International Politics: The Functions of International Law in International Society," European Journal of International Law, vol. 14, no. 1, (2003); pp. 105-106.

อย่างเหมาะสมให้เข้ากับสถานการณ์หรือข้อเท็จจริงใหม่ๆ ที่เกิดขึ้นได้ กฎหมายจึงไม่สามารถปรับใช้กับสถานการณ์หรือข้อเท็จจริงเหล่านั้นได้ ในสมมติฐานนี้ การเปลี่ยนแปลงแก้ไขใหม่จึงเป็นสิ่งจำเป็นคือให้กฎหมายสอดคล้องรองรับและปรับใช้ได้กับข้อเท็จจริงหรือสถานการณ์ใหม่ๆ ที่เกิดขึ้นตามพลวัตที่เกิดขึ้นในประชาคมระหว่างประเทศ

(ค) ความสามารถในการการปรับตัวของกฎหมายและการพัฒนากฎหมายระหว่างประเทศ

ความสามารถในการปรับตัวและการพัฒนากฎหมายระหว่างประเทศ (Development of international Law) เป็นแนวคิดสองประการที่มีความเชื่อมโยงกันแต่รวมถึงความแตกต่างบางประการที่ทำให้สามารถแยกแยะได้ การพัฒนากฎหมายสอดคล้องกับการขยายสาขาที่สำคัญ การพัฒนากฎหมายเป็นวิธีการหนึ่งในการทำให้กฎหมายสามารถตอบสนองความต้องการใหม่ๆ ของสังคมระหว่างประเทศได้ ดังที่ Pellet ได้กล่าวไว้ว่าทฤษฎีเรื่องบ่อเกิดกฎหมายระหว่างประเทศไม่ว่าจะเป็นสนธิสัญญา จารีตประเพณีและหลักการทั่วไปของกฎหมายก็เป็นวิถีทางของการพัฒนากฎหมายระหว่างประเทศให้ปรับตัวเข้ากับพลวัตของสังคมระหว่างประเทศ อย่างไรก็ตาม ก็มีข้อจำกัดโดยเฉพาะอย่างยิ่งในสังคมระหว่างประเทศที่เป็นสังคมที่ไม่มีอำนาจแบบรวมศูนย์ สนธิสัญญาต่างๆ จะเกิดขึ้นได้ก็ด้วยความยินยอมของบรรดารัฐต่างๆ และในขณะเดียวกันสนธิสัญญาก็อาจเป็นกลไกที่มีลักษณะเคร่งครัดที่เป็นอุปสรรคที่ขัดขวางความสามารถในการปรับตัวให้เข้ากับพัฒนาการของสังคมระหว่างประเทศได้เสมอ[563] นอกจากนี้ จารีตประเพณีแม้จะเป็นวิธีการที่ตอบสนองพัฒนาการของสังคมระหว่างประเทศได้แต่อาศัยระยะเวลาและมีความไม่แน่นอน ซึ่งก็ถือเป็นข้อจำกัดประการหนึ่งในกรณีที่สังคมระหว่างประเทศต้องการหลักเกณฑ์ที่ชัดเจนและเร่งด่วนต่อสถานการณ์บางเรื่อง[564]

แม้บ่อเกิดตามรูปแบบของกฎหมายระหว่างประเทศจะมีข้อจำกัดในการตอบสนองการปรับตัวให้กฎเกณฑ์ระหว่างประเทศสามารถรองรับพัฒนาการของสังคมระหว่างประเทศได้อย่างเหมาะสม แต่หากพิจารณาบทบาทของศาลระหว่างประเทศจะเห็นได้ว่าศาลระหว่างประเทศมีบทบาทเป็น “ตัวปรับที่มีประสิทธิภาพ” ซึ่งศาลระหว่างประเทศได้ใช้อำนาจในการวินิจฉัยข้อพิพาทหรือทำความเห็น มีบทบาทในการให้ความกระจ่างหรือแสดงขอบเขตหรือความมีอยู่ของหลักกฎหมาย

---

[563] Alain Pellet, “L’adaptation du droit international aux besoins changeants de la société internationale,”: p. 18.

[564] Ibid., p.25.

ในมิติใหม่ๆ ซึ่งอาจเรียกได้ว่าเป็น“หน้าที่กึ่งนิติบัญญัติ[565] ดังนั้น การพัฒนากฎหมายหรือการปรับตัวของกฎหมายจึงไม่ได้ขึ้นอยู่กับบ่อเกิดของกฎหมายแบบดั้งเดิมอีกต่อไป แต่ยังขึ้นอยู่กับแนวคำวินิจฉัยและการตีความของศาลระหว่างประเทศด้วย

ในบริบทของกฎหมายมนุษยธรรมระหว่างประเทศ Meron ได้เน้นย้ำความสำคัญของคำวินิจฉัยและการตีความกฎหมายของบรรดาศาลอาญาระหว่างประเทศที่มีต่อพัฒนาการกฎหมายมนุษยธรรมระหว่างประเทศ[566] แม้จะมีผู้วิพากษ์วิจารณ์ว่าศาลเขียนกฎหมายใหม่โดยอำเภอใจให้ต่างไปจากกฎหมายจารีตประเพณีและอนุสัญญาเจนีวาโดยปราศจากความยินยอมของรัฐภาคี[567] อย่างไรก็ตาม สิ่งสำคัญอันเป็นที่ยอมรับก็คือแนวคำวินิจฉัยเหล่านั้นตั้งอยู่บน “ข้อพิจารณาพื้นฐานของหลักมนุษยธรรม”[568] ซึ่งเป็นหัวใจของตรรกะของกฎหมายมนุษยธรรมระหว่างประเทศ อย่างไรก็ตาม หากการตีความหรือความพยายามที่จะปรับใช้กฎหมายเกินไปกว่าขอบเขตของเนื้อหาหรือเจตนารมณ์ของกฎหมายโดยมุ่งหวังให้กฎหมายปรับตัวรองรับสถานการณ์ใหม่ การกระทำดังกล่าวก็เท่ากับเป็นการบิดเบือนกฎหมาย

(ง) ความสามารถในการปรับตัวของกฎหมายกับการฝืนหรือการบิดเบือนการปรับใช้กฎหมาย

กฎหมายระหว่างประเทศแผนกคดีเมืองมีพัฒนาการอย่างมากเมื่อเปรียบเทียบกับอดีตเพราะว่าโดยหลักแล้วจะเป็นกฎหมายที่ใช้บังคับในความสัมพันธ์ระหว่างบุคคลในระบบกฎหมายระหว่างประเทศ อย่างไรก็ตาม เห็นได้ว่าในปัจจุบันกฎหมายระหว่างประเทศแผนกคดีเมืองเข้าไปเกี่ยวข้องในลักษณะที่กำหนดสิทธิหรือบทบาทของตัวกระทำการที่ไม่ใช่รัฐอย่างมีนัยสำคัญเมื่อเปรียบเทียบกับอดีต[569] เช่นเดียวกันกับกฎหมายมนุษยธรรมระหว่างประเทศที่มีพัฒนาการจาก

---

[565] Alain Pellet, “L’adaptation du droit international aux besoins changeants de la société internationale,”: 21.

[566] Theodor Meron, “The Hague Tribunal: Working to Clarify International Humanitarian Law,” American University International Law Review, vol. 13, no. 6, (1998); p. 1152. “...There is no question that international humanitarian law has developed significantly since the atrocities in Yugoslavia began. This area of law has grown much more during these last few years than in the half-century following Nuremberg.”

[567] Peter W. Murphy, “Judging War Criminals,” Texas International Law Journal, vol. 35, no. 2, (2000): p. 332.

[568] Shane Darcy, Judges, Law and War: The Judicial Development of International Humanitarian Law, Cambridge, Cambridge University Press, 2014, p. 111.

[569] Shane Darcy, Judges, Law and War: The Judicial Development of International Humanitarian Law, Cambridge, Cambridge University Press, 2014, p. 111.

กฎเกณฑ์ที่มีลักษณะเป็นกฎหมายสงครามระหว่างรัฐที่ขยายขอบเขตครอบคลุมการกระทำของตัวกระทำการที่ไม่ใช่รัฐตลอดจนถึงการคุ้มครองบุคคลธรรมดาที่เป็นพลเรือนด้วย พัฒนาการของสังคมระหว่างประเทศมีผลเป็นการผลักดันให้เกิดการเปลี่ยนแปลงเนื้อหาและขยายขอบเขตของการบังคับใช้กฎหมาย การเปลี่ยนแปลงเช่นว่านี้ไม่ได้กระทบต่อเอกภาพของกฎหมายถ้าหากว่าไม่ได้เปลี่ยนแปลงเป้าหมายที่แท้จริงของกฎหมายดังกล่าว

จากข้อพิจารณาทั้งหมดข้างต้นจะเห็นได้ว่าการที่กฎหมายอื่นและโดยเฉพาะอย่างยิ่งในที่นี้คือกฎหมายมนุษยธรรมระหว่างประเทศจะสามารถนำไปปรับใช้กับสถานการณ์ใหม่ๆ ที่เกิดขึ้นได้หรือไม่นั้น ขึ้นอยู่กับความสามารถในการปรับตัวของกฎหมายหมายหรือกล่าวอีกนัยหนึ่งคือความสามารถของระบบกฎหมายในการปรับตัวให้เข้ากับความต้องการของสังคมระหว่างประเทศหรือสถานการณ์หรือปรากฏการณ์ของข้อเท็จจริงที่เปลี่ยนแปลงไปจากบริบทของสังคมหรือปรากฏการณ์ในขณะที่หลักกฎหมายดังกล่าวได้ก่อร่างสร้างตัวขึ้นและการปรับใช้นั้นไม่เป็นการบิดเบือนลักษณะหรือวัตถุประสงค์ของกฎหมายนั้นๆ เอง การพิจารณาว่ากฎหมายสามารถปรับใช้ได้กับสถานการณ์ใหม่ได้หรือไม่นั้น ความสามารถในการปรับตัวเกี่ยวข้องกับเทคนิคในการปรับกฎหมาย เช่น แบบแผน วิธีจารีตประเพณี หลักการ หรือแม้แต่การตีความ อย่างไรก็ตาม ตัวเลือกนี้ขึ้นอยู่กับลักษณะของสิทธิที่เป็นปัญหาและกฎของสิทธินั้น

ความเพียงพอเป็นผลการประเมินที่เกี่ยวข้องกับกฎหมายและเป็นวัตถุประสงค์ของการปรับกฎหมาย ความไม่เพียงพอสอดคล้องกับสถานการณ์ที่ไม่สามารถปรับใช้กฎหมายได้เนื่องจากไม่เพียงพอที่จะควบคุมสถานการณ์ที่เกี่ยวข้อง การปรับใช้กฎหมายโดยการฝืนความความเป็นไปได้ของกฎหมายที่ปรับให้เข้ากับสถานการณ์ใหม่นั้น เป็นการปรับใช้โดยการบิดเบือนกฎหมายเพราะขัดต่อลักษณะหรือวัตถุประสงค์ของกฎหมายนั้น

ประเด็นที่ 2 การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อความเปลี่ยนแปลงไปของสังคมระหว่างประเทศและปรากฏการณ์ในสถานการณ์การขัดกันทางอาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายสาขาหนึ่งของกฎหมายระหว่างประเทศที่มีความเป็นมาช้านาน ดังนั้นความท้าทายที่มีต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศที่เกิดขึ้นจากพลวัตของสังคมระหว่างประเทศที่เกี่ยวกับการขัดกันทางอาวุธจึงไม่ใช่เรื่องใหม่ ข้อพิจารณาเกี่ยวกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อความเปลี่ยนแปลงไปของสังคมระหว่างประเทศและปรากฏการณ์ในสถานการณ์การขัดกันทางอาวุธมีดังนี้

(ก) การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับปรากฏการณ์ใหม่ในการขัดกันทางอาวุธ

ความพยายามที่จะจำกัดผลกระทบของสงครามต่อมนุษย์มีปรากฏให้เห็นตั้งแต่ในอดีตกาล เนื่องจากเป็นที่ประจักษ์ว่าการใช้กำลังโดยปราศจากข้อจำกัดที่แต่ละฝ่ายที่สู้รบกันใช้ความรุนแรงประหัตประหารกันเพื่อที่จะได้มาซึ่งชัยชนะโดยไม่พิจารณาถึงมิติทางด้านมนุษย์เลย ส่งผลให้เกิดความหายนะอย่างที่สุดของทุกฝ่าย[570] สังคมระหว่างประเทศหลังยุคเวสฟาเลียได้ประสบความสำเร็จในการบรรลุข้อตกลงที่กำหนดกฎเกณฑ์เพื่อสร้างข้อจำกัดในเรื่องของวิธีการและปัจจัยในการสู้รบ โดยการรับรองอนุสัญญาที่เป็นผลมาจากการประชุมที่กรุงเฮกในปี ค.ศ. 1899 และ ค.ศ. 1907[571] ความตระหนักถึงมิติทางด้านมนุษยธรรมในข้อตกลงระหว่างประเทศสะท้อนให้เห็นถึงพัฒนาการของกฎหมายสงครามหรือที่เรียกในปัจจุบันว่ากฎหมายมนุษยธรรมระหว่างประเทศว่าเป้าประสงค์ของกฎหมายระหว่างประเทศไม่ได้อยู่ที่การอยู่ร่วมกันของรัฐในประชาคมระหว่างประเทศเท่านั้น แต่หมายถึงการร่วมกันสร้างสรรค์สันติภาพและการปกป้องคุ้มครองมนุษยชาติในสังคมที่ต่างต้องพึ่งพาอาศัยกันในประชาคมที่มีประชาชนและมนุษย์รวมอยู่ด้วย[572]กฎหมายมนุษยธรรมระหว่างประเทศจึงเป็นกฎหมายที่บังคับให้รัฐต้องเคารพต่อความเป็นมนุษย์ในทุกสถานการณ์ หน้าที่นี้สอดคล้องกับแนวความคิดที่ว่าสงครามไม่สามารถที่จะมีขึ้นได้ด้วยปราศจากความจำเป็น ความรุนแรงใดๆ ที่ไม่สามารถพิสูจน์ถึงความจำเป็นได้เป็นเพียงสิ่งที่โหดร้ายและโง่เขลาที่ไร้ประโยชน์ (Gratuitously cruel and stupid)[573] กฎหมายมนุษยธรรมระหว่างประเทศจึงเป็นกฎหมายที่สะท้อนความสมดุลระหว่างหลักการมนุษยธรรมและความจำเป็นทางการทหารที่กำหนดเงื่อนไขในการใช้อำนาจของฝ่ายที่เข้าร่วมในการขัดกันทางอาวุธที่จะปกป้องผลประโยชน์ของฝ่ายตนไม่ว่าฝ่ายในการสู้รบนั้นจะเป็นรัฐหรือกลุ่มติดอาวุธที่ไม่ใช่รัฐก็ตาม หลักการพื้นฐานของกฎหมายมนุษยธรรมเรื่องประเทศจึงถือว่าเป็นกฎเกณฑ์ที่ไม่ให้การใช้อาวุธต่อสู้กันกลายไปเป็นการประหัตประหารอย่างป่าเถื่อนที่ทำไปเพื่อการได้ชัยชนะเพียงแต่อย่างเดียว หลักเกณฑ์พื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศถือเป็น

---

[570] Mario Bettati, Le Droit de la Guerre, (Paris: Odile Jacob, 2016), p. 38.

[571] Alain Pellet, "L'adaptation du droit international aux besoins changeants de la société internationale,": p. 22.

[572] Mohamed Bedjaoui, "L'Humanité en quête de la Paix et le Développement," RCADI, vol.325, Martinus Nijhoff, (2006), p. 748.

[573] Jean Pictet, "The Formation of International Humanitarian Law," International Review of Red Cross, No. 244, January-February 1985. P. 5.

กฎเกณฑ์ที่มีลักษณะบังคับเด็ดขาดและการเคารพปฏิบัติตามหลักเกณฑ์เหล่านี้ไม่ได้อยู่ภายใต้เจตนารมณ์หรือการยินยอมของรัฐ[574]

(ข) การปรับเปลี่ยนของกฎหมายมนุษยธรรมระหว่างประเทศกับสถานการณ์ที่เปลี่ยนแปลงไป

กฎหมายมนุษยธรรมระหว่างประเทศมีการเปลี่ยนแปลงอยู่ตลอดเวลาโดยสะท้อนออกมาในรูปแบบของบ่อเกิดของกฎหมายระหว่างประเทศในรูปแบบต่างๆ ไม่ว่าจะเป็นสนธิสัญญา จารีตประเพณีระหว่างประเทศ หลักกฎหมายทั่วไปและรวมถึงการตีความและการปรับใช้กฎหมายโดยศาลระหว่างประเทศ

กฎหมายมนุษยธรรมระหว่างประเทศปรับเปลี่ยนให้ทันกับสถานการณ์ที่เปลี่ยนแปลงไปเพื่อให้เท่าทันกับสถานการณ์และความรุนแรงที่เกิดขึ้นในสงครามต่างๆ เช่น การมีอนุสัญญากรุงเจนีวา ค.ศ. 1929 ภายหลังสงครามโลกครั้งที่ 1 หรือการรับรองอนุสัญญากรุงเจนีวา 4 ฉบับ ค.ศ. 1949 ภายหลังสงครามโลกครั้งที่ 2 เช่นเดียวกันกับการรับรองพิธีสารเพิ่มเติมทั้งสองฉบับในปี ค.ศ. 1977 ที่ออกมาเพื่อรองรับสถานการณ์การขัดกันทางอาวุธที่มีลักษณะเปลี่ยนแปลงไปอย่างมีนัยสำคัญในช่วงหลังสงครามโลกครั้งที่ 2 การออกสนธิสัญญาเหล่านี้เป็นวิธีการอย่างหนึ่งในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศให้ทันกับสถานการณ์ที่เปลี่ยนแปลงไปโดยอยู่บนพื้นฐานของเจตนารมณ์ของบรรดารัฐต่างๆ ที่เป็นสมาชิกในประชาคมระหว่างประเทศ

การปรับตัวของฎหมายมนุษยธรรมระหว่างประเทศให้เหมาะสมกับสถานการณ์ที่เกิดขึ้นใหม่ๆ ไม่ได้ถูกจำกัดให้ขึ้นอยู่กับเจตนารมณ์ของรัฐโดยวิธีการปรับกฎหมายหรือสร้างหลักกฎหมายใหม่รูปแบบของสนธิสัญญาเท่านั้นแต่กฎหมายมนุษยธรรมระหว่างประเทศยังเป็นกฎหมายที่มีชีวิต (Living Law)[575]ที่มีปฏิกริยาเพื่อปรับเปลี่ยนให้เข้ากับสถานการณ์ใหม่หรือให้เข้ากับวิธีการหรือปัจจัยในการสู้รบที่เปลี่ยนแปลงไป[576] การปรับตัวให้เข้ากับสถานการณ์ใหม่ๆ เหล่านี้เป็นผลมาจากลักษณะความยืดหยุ่นของหลักการสำคัญของกฎหมายมนุษยธรรมและประเทศเองที่ไม่ได้ยึดติดอย่างเคร่งครัด

---

[574] 1996 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ Report 1996, pp. 257-258.

[575] Shane Darcy, Judges, Law and War: The Judicial Development of International Humanitarian Law, p. 5

[576] Jacques Meurant, "Inter Arma Caritas: Evolution and Nature of International Humanitarian Law," Journal of Peace Research, vol. 24, no. 3, 1987, p. 242.

ตามตัวบทของกฎหมายที่เป็นลายลักษณ์อักษรแต่อยู่เหนือกฎหมายที่เป็นลายลักษณ์อักษร[577] หลักการพื้นฐานสำคัญเหล่านี้เป็นฐานสำคัญที่ใช้ในการตีความเพื่อปรับใช้กฎหมายสำหรับสถานการณ์ใหม่ที่เกิดขึ้นหรือกับวิธีการและปัจจัยในการทำสงครามที่เปลี่ยนแปลงไปตามยุคสมัย หลักการเหล่านี้ได้แก่บรรดาหลักการต่างๆ ที่เกี่ยวข้องกับการปกป้องคุ้มครองพลเรือนและการเกี่ยวกับการปฏิบัติการหรือการสู้รบซึ่งได้แก่หลักการแยกแยะเป้าหมาย (Principle of Distinction) หลักความได้สัดส่วน (Principle of Proportionality) หลักความจำเป็นทางการทหาร (Principle of Military Necessity) หลักความระมัดระวังล่วงหน้า (Precautionary Principle) ตลอดจนการปกป้องคุ้มครองโดยคำนึงถึงข้อพิจารณาพื้นฐานทางด้านมนุษยธรรม (Elementary considerations of Humanity) ตาม Martens Clause[578]

ยิ่งไปกว่านั้น หลักการพื้นฐานสำคัญเหล่านี้ได้รับการยอมรับว่ามีลักษณะเป็นจารีตประเพณีและมีความสำคัญอย่างยิ่งที่มีความยืดหยุ่นในการปรับตัวและสามารถทำให้กฎหมายมนุษยธรรมระหว่างประเทศปรับใช้ได้กับสถานการณ์ใหม่ๆ ลักษณะความเป็นกฎหมายจารีตประเพณีของหลักการพื้นฐานสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศมีความสำคัญต่อการปรับใช้กฎหมายของศาลระหว่างประเทศอย่างยิ่ง เพราะในทางปฏิบัติเห็นได้อย่างชัดเจนว่าในการใช้อำนาจของศาลระหว่างประเทศมีบทบาทสำคัญอย่างยิ่งในการอธิบายเนื้อหาสาระและขอบเขตของกฎหมายจารีตประเพณีระหว่างประเทศที่สามารถปรับใช้กับสถานการณ์ใหม่ๆ ที่เกิดขึ้นได้[579] สถานะความเป็นกฎหมายจารีตประเพณีของกฎหมายมนุษยธรรมประเทศมีความสำคัญอย่างยิ่งอีกประการหนึ่งคือเป็นกฎหมายที่เปิดโอกาสให้ศาลนำมาปรับใช้โดยให้เหตุผลขยายความหรือให้ความหมายของขอบเขตกฎหมายที่มีนัยในทางปฏิบัติต่อสถานการณ์ที่เกิดขึ้นได้ง่ายกว่าเมื่อเปรียบเทียบกับกฎหมายลาย

---

[577] Ibid., p. 239.

[578] Theodor Meron, "The Martens Clause, Principles of Humanity, and Dictates of Public Conscience," The American Journal of International Law, Vol. 94 No.1, (January 2000); p. 79. Martens Clause คือหลักเกณฑ์ทั่วไปในการทำการรบที่จะต้องคำนึงถึงหลักกฎหมายระหว่างประเทศอันสืบเนื่องมาจากจารีตประเพณีซึ่งสอดคล้องต่อหลักมนุษยธรรมและข้อกำหนดแห่งมโนธรรมของสาธารณะแม้จะไม่มีข้อกฎหมายใดในอนุสัญญาระหว่างประเทศกำหนดเอาไว้ (...the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience.) หลักดังกล่าวได้รับการรับรองโดยอนุสัญญาเฮกว่าด้วยการทำสงคราม ค.ศ.1899 และฉบับแก้ไขปี ค.ศ. 1907 ในปัจจุบันหลัก Martens Clause อยู่ในข้อ 1 (2) ของพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949

[579] George Brand, "The Development of the International Law of War," Tulane Law Review, vol. 25, no. 2, (1951): p. 186.

ลักษณ์อักษร[580] และความยืดหยุ่นของกฎหมายจารีตประเพณีนี้เองเป็นคุณสมบัติสำคัญที่ทำให้กฎหมายปรับตัวให้เข้ากับสถานการณ์ใหม่ได้อย่างมีประสิทธิภาพ[581] และนำไปปรับใช้กับสถานการณ์ใหม่หรือเหตุการณ์ใหม่ที่เกิดขึ้นได้อย่างเหมาะสม

กฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายที่ได้รับประโยชน์จากบทบาทของศาลระหว่างประเทศที่มีต่อพัฒนาการของกฎหมายอย่างมากไม่ว่าจะเป็นศาลยุติธรรมระหว่างประเทศในการใช้อำนาจตัดสินข้อพิพาทระหว่างรัฐ[582]หรือในการทำความเห็นแนะนำ[583] ที่มีบทบาทในการชี้ความเป็นกฎหมายหรือสาธยายเนื้อหาและขอบเขตของกฎหมายที่จะใช้บังคับให้มีความกระจ่างชัดเจน เพื่อที่จะปรับใช้หลักเกณฑ์กฎหมายนั้นนั้นกับสถานการณ์ที่เกิดขึ้น เช่น คดี Military and Paramilitary Activities in and against Nicaragua[584] หรือความเห็นแนะนำ[585] นอกจากนี้ศาลอาญาระหว่างประเทศเช่นศาลอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวีย (ICTY) และศาลอาญาระหว่างประเทศสำหรับรวันดา (ICTR) ต่างก็มีบทบาทที่สำคัญอย่างยิ่งในการตีความปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศให้เข้ากับสถานการณ์ที่เกิดขึ้นซึ่งหลายกรณี การตีความและการอธิบายการวิเคราะห์กฎหมายโดยศาลมีความแตกต่างจากถ้อยคำที่ปรากฏอยู่ในกฎหมายลายลักษณ์อักษรอย่างเห็นได้ชัด ซึ่งนักกฎหมายบางคนเห็นว่าเป็นบทบาทที่สำคัญยิ่งของศาลอาญาระหว่างประเทศในการวิเคราะห์การปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศให้นำไปปรับใช้อย่างมีประสิทธิภาพกับสถานการณ์ใหม่ที่เกิดขึ้นโดยยังอยู่บนพื้นฐานสำคัญคือหลักความมีมนุษยธรรม (Principle of Humanity) ซึ่งเป็นพื้นฐานสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ ในลักษณะที่เรียกได้ว่าเรียกได้ว่าเป็นความสำเร็จที่ก้าวล้ำ (Ground-breaking Achievement) ของศาลอาญาระหว่างประเทศ[586]

---

[580] George Brand, “The Development of the International Law of War,”: 186.

[581] Alain Pellet, “L’adaptation du droit international aux besoins changeants de la société internationale,”: 21.

[582] Article 38, Statute of the International Court of Justice.

[583] Article 68, Statute of the International Court of Justice.

[584] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.392.

[585] 1996 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ Report 1996, p. 226.

[586] Theodor Meron, The Humanization of international Law, (The Nethelands: Matinus Nijjhof, 2006), pp.177-180.

แม้ว่าการวิเคราะห์ว่ากฎหมายมนุษยธรรมระหว่างประเทศจะปรับตัวได้เข้ากับสถานการณ์ที่เปลี่ยนแปลงไปและนำไปปรับใช้กับสถานการณ์เหล่านั้นได้หรือไม่จะมีกฎเกณฑ์เป็นเครื่องชี้วัดดังที่ได้กล่าวไว้แล้วข้างต้น แต่สิ่งที่ต้องคำนึงถึงก็คือไม่ว่ากฎหมายมนุษยธรรมระหว่างประเทศจะต้องปรับตัวไปโดยอาศัยกลไกอย่างใดอย่างหนึ่งเหล่านั้นจะต้องอาศัยเวลาและโอกาสที่มาถึงเนื่องจากการเกิดของกฎหมายระหว่างประเทศไม่สามารถเป็นไปได้ชั่วข้ามคืนจะต้องอาศัยระยะเวลาและเจตนารมณ์ของบรรดารัฐต่างๆ ในประชาคมระหว่างประเทศเป็นสำคัญหรือแม้แต่บทบาทของศาลในการวิเคราะห์และตีความกฎหมายก็ตามจะต้องอาศัยโอกาสที่มีประเด็นเหล่านั้นขึ้นสู่การพิจารณาของศาล ซึ่งในปัจจุบันการวิเคราะห์ว่ากฎหมายมนุษยธรรมระหว่างประเทศสามารถปรับใช้ได้กับเทคโนโลยีใหม่ที่ใช้ในฐานะเป็นวิธีการหรือปัจจัยในการสู้รบยังถือเป็นเรื่องใหม่และนำไปสู่การวิเคราะห์และมุมมองที่หลากหลายของนักวิชาการ

3.1.2 ข้อวิพากษ์ทางวิชาการในประเด็นการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่

ข้อวิพากษ์ทางวิชาการเกี่ยวกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธมีอยู่ค่อนข้างหลากหลาย ทั้งความเห็นว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศนั้นมีอยู่อย่างเพียงพอแล้ว[587]ความเห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่เพียงพอต่อการปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธ[588]ความเห็นว่าสถานการณ์การใช้เทคโนโลยีใหม่เป็นความตื่นตระหนกเกินความจำเป็นทั้งที่ความจริงเทคโนโลยีใหม่อาจไม่ได้สร้างผลกระทบต่อกฎหมายมนุษยธรรมระหว่างประเทศเลย[589] เป็นต้น ความคิดเห็นเหล่านี้อาจแบ่งกลุ่มได้ดังนี้

แนวคิดกลุ่มที่ 1 กฎหมายมนุษยธรรมมีความยืดหยุ่นเพียงพอต่อการปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธแต่อาจมีการแก้ไขเล็กน้อยเพื่อให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป

---

[587] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, pp. 30-31.

[588] Fatma Tasdemmir and Gokhan Albayrak, "The Law of Cyber Warfare In Terms of Jus Ad Bellum and Jus In Bello: Application of International Law to the Unknown." E-journal of Law. Vol 3 (2), (2017): 6.

[589] Myriam Dunn Cavelty. "The Militarisation of Cyberspace: Why Less May Be Better," pp. 141-153.

แนวคิดว่ากฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นเพียงพอต่อการปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธนี้เป็นแนวคิดหลักที่มีมากเท่ากับกลุ่มที่มองว่าควรมีการสร้างกฎหมายใหม่ในการควบคุมเทคโนโลยีในการขัดกันทางอาวุธ นักวิชาการที่มีแนวคิดว่ากฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นเพียงพอต่อการปรับใช้นี้มีแนวคิดร่วมกันว่ากฎหมายมนุษยธรรมระหว่างประเทศมีหลักพื้นฐานที่มีลักษณะทั่วไปสามารถปรับใช้กับวิธีการรบหรือปัจจัยในการรบที่มีความหลากหลายได้[590]หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศที่มีลักษณะเป็นกลางและใช้ได้เสมอ เช่น ข้อจำกัดการใช้ปัจจัยและวิธีการรบที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น หลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการโจมตี หลักความระมัดระวังล่วงหน้าก่อนการโจมตี ตลอดจนหลักการคุ้มครองทรัพย์สิ่งของพลเรือนและสถานที่เก็บพลังงานอันตราย เป็นต้น แม้เทคโนโลยีจะเปลี่ยนแปลงไปอย่างมากและพื้นที่ในการต่อสู้จะเปลี่ยนจากโลกจริงเป็นพื้นที่ไซเบอร์แต่หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศยังคงสามารถปรับใช้ได้เช่นเดิม[591] ทั้งนี้โดยคำนึงถึงแนวคิดพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศที่จะต้องทำการรบเท่าที่จำเป็นทางการทหารและคุ้มครองความมีมนุษยธรรมไปพร้อมกัน[592]นอกจากนั้นแนวทางการทำคำตัดสินและความเห็นแนะนำของศาลระหว่างประเทศยังช่วยให้เกิดการพัฒนาการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศให้เกิดความยืดหยุ่นยิ่งขึ้น เช่น ในการพิจารณาความชอบด้วยกฎหมายของการใช้อาวุธนิวเคลียร์ที่ไม่จำเป็นต้องอาศัยกฎหมายระหว่างประเทศเฉพาะเรื่อง เพียงการปรับใช้หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศก็เป็นการเพียงพอ[593]การวินิจฉัยของศาลยุติธรรมระหว่างประเทศในคดีดังกล่าวนำมาสู่แนวคิดว่าแม้จะไม่มีกฎหมายมนุษยธรรมเฉพาะเรื่องที่จะปรับใช้กับวิธีการหรือปัจจัยใหม่หรือแม้แต่อาวุธใหม่ที่เกิดขึ้นในปัจจุบัน แต่หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศยังคงมีผลใช้ได้และทุกรัฐรวมตลอดถึงคู่ความขัดแย้งในสงครามมีพันธกรณีที่จะต้องปฏิบัติตามเสมอ

นักวิชาการบางส่วนมองว่าการให้ความสนใจกับปัญหาการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธนี้เป็นเรื่องตื่นตระหนกเกินความจำเป็น[594]เพราะเทคโนโลยีบางลักษณะเช่นเทคโนโลยีไซเบอร์

---

[590] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, pp. 30-31.

[591] Mehmet Emin Erendor and Gurkan Tamer. "The New Face of The War: Cyber Warfare," p. 61.

[592] Jean Pictet, Humanitarian Law and the Protection of War Victims, (Geneva: Henry Dunant Institute, 1975), p. 28.

[593] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 31.

[594] Myriam Dunn Cavelty. "The Militarisation of Cyberspace: Why Less May Be Better." 4th International Conference on Cyber Conflict. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), Tallinn, (2012), p. 142.

เป็นสิ่งที่มีการใช้งานมายาวนานระยะหนึ่งแล้ว มีปรากฏกรณ์หลายกรณีที่สร้างความตื่นตัวของสังคมมากเกินความจำเป็นเช่นความหวาดกลัวเรื่องมัลแวร์คอมพิวเตอร์ไม่ว่าจะเป็นไวรัส หนอนคอมพิวเตอร์ โทรจัน ฯลฯ มัลแวร์เหล่านี้มักถูกกำจัดได้ด้วยโปรแกรมกำจัดไวรัสจนท้ายที่สุดความสนใจเรื่องมัลแวร์ก็หมดไป[595]แนวคิดของนักวิชาการกลุ่มนี้มองว่ากฎหมายอาจไม่ใช่คำตอบสำหรับทุกเรื่องเพราะปัญหาเกี่ยวกับการใช้เทคโนโลยีอาจแก้ไขได้ด้วยมาตรการอื่นนอกจากการใช้กฎหมาย ความคิดเห็นนี้อาจมีจุดอ่อนอยู่บ้าง

อย่างไรก็ดี แม้นักนักวิชาการกลุ่มนี้จะเห็นว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศจะสามารถนำมาปรับใช้กับเทคโนโลยีใหม่ได้อย่างยืดหยุ่นแต่ลักษณะการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธยังมีประเด็นท้าทายในเรื่องผลกระทบทางกายภาพที่เกิดจากการโจมตีทางไซเบอร์ ทั้งนี้เนื่องจากการโจมตีทางไซเบอร์อาจก่อให้เกิดผลได้หลายประการทั้งผลที่เป็นรูปธรรมทางกายภาพและผลที่ไม่แสดงทางกายภาพเช่นความเสียหายต่อข้อมูลของคอมพิวเตอร์ ข้อเสนอเดียวที่ยังคงเป็นที่ยอมรับในปัจจุบันคือการยอมรับว่าการโจมตีทางไซเบอร์จะมีผลเทียบเท่าการโจมตีตามด้วยอาวุธปกติคือจะต้องก่อให้เกิดความเสียหายทางกายภาพเท่านั้น[596]ทฤษฎีสัดส่วนความรุนแรงและผลกระทบ (Scale and effects)[597]จึงยังคงเป็นที่ยอมรับในปัจจุบันแม้จะยังคงมีข้อวิพากษ์อยู่บ้างก็ตาม

แนวคิดที่ว่าหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศยืดหยุ่นเพียงพอที่จะปรับใช้กับการโจมตีทางไซเบอร์ได้นี้มีตัวอย่างที่เป็นรูปธรรมคือคู่มือทาลลินน์ว่าด้วยการปรับใช้กฎหมายระหว่างประเทศต่อการสงครามทางไซเบอร์ ปี ค.ศ.2013 ซึ่งเป็นการแสดงให้เห็นว่ากฎหมายระหว่างประเทศและกฎหมายมนุษยธรรมระหว่างประเทศมีหลักการที่เพียงพอและเหมาะสมในการปรับใช้กับปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์โดยไม่ต้องมีการสร้างกฎหมายระหว่างประเทศใหม่เฉพาะเรื่องแต่อย่างใด

แนวคิดว่ากฎหมายมนุษยธรรมระหว่างประเทศมีความยืดหยุ่นเพียงพอต่อการปรับใช้กับการโจมตีทางไซเบอร์นี้ยังมีข้อโต้แย้งอยู่ โดยเฉพาะอย่างยิ่งในกรณีการใช้ไซเบอร์เพื่อการโจมตีในการขัดกันทางอาวุธก่อให้เกิดประเด็นท้าทายบางประการต่อหลักการแยกแยะเป้าหมายในการโจมตีที่ยังคงไม่สามารถอธิบายได้เนื่องจากพื้นที่ทางไซเบอร์โดยปกติมักเป็นพื้นที่ใช้งานร่วมกันระหว่างทหาร

---

[595] Ibid., p. 145.

[596] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare.”: p. 61.

[597] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, p. 43.

และพลเรือน ยิ่งไปกว่านั้นอุปกรณ์ที่ใช้งานทางไซเบอร์ยังเป็นสิ่งที่ใช้ได้สองทางทั้งเพื่อประโยชน์พลเรือนและประโยชน์ทางการทหาร[598] ลักษณะดังกล่าวเป็นปัจจัยให้พลเรือนเข้ามามีส่วนร่วมในการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธมากขึ้น นอกจากนั้นการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในปัจจุบันยังปรากฏอุปสรรคในเรื่องการพิสูจน์ตัวตนของผู้ปฏิบัติการ ข้อท้าทายดังกล่าวจึงไปไปสู่แนวความคิดเห็นของนักวิชาการอีกกลุ่มหนึ่งที่มองในทางตรงข้ามกับกลุ่มที่มองว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมีความเพียงพอ โดยมองว่าควรจะมีการสร้างกฎหมายใหม่หรือแก้ไขกฎหมายใหม่

แนวคิดกลุ่มที่ 2 ควรมีการสร้างกฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับการควบคุมการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ

แนวคิดว่าควรจะต้องมีการสร้างกฎหมายระหว่างประเทศเฉพาะเรื่องเพื่อจัดการหรือควบคุมการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธเกิดขึ้นกับเทคโนโลยีใหม่ 2 ลักษณะเป็นสำคัญคือเทคโนโลยีไซเบอร์และเทคโนโลยีอาวุธอิสระ (Autonomous Weapon Systems)

กรณีการใช้เทคโนโลยีไซเบอร์นั้นมีนักวิชาการที่มองว่าพื้นที่ทางไซเบอร์เป็นพื้นที่เฉพาะที่แตกต่างจากพื้นที่ทางกายภาพอย่างสิ้นเชิง ความเสียหายที่เกิดขึ้นจากการโจมตีทางไซเบอร์ก็มีหลากหลายกว่าการโจมตีด้วยอาวุธปกติ ในบางกรณีผลเสียหายที่เกิดขึ้นจากปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์อาจไม่สัมพันธ์โดยตรงกับความมุ่งหมายของผู้ปฏิบัติการก็ได้ การยอมรับให้พื้นที่ทางไซเบอร์เป็นพื้นที่ทางการรบรูปแบบหนึ่งและสร้างกฎหมายเฉพาะเรื่องสำหรับปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์จึงเป็นเรื่องจำเป็น[599]

กรณีการใช้เทคโนโลยีระบบอาวุธอิสระ (Autonomous Weapon Systems) มีประเด็นที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์และการตัดสินใจของจักรกลหรือคอมพิวเตอร์อยู่ค่อนข้างมาก นำไปสู่ข้อพิจารณาหลายประการ เช่น จักรกลหรือระบบอาวุธเหล่านี้ตัดสินใจทำลายเป้าหมายได้เองในระดับใด[600] ความสามารถในการตัดสินใจทำลายเป้าหมายของจักรกลนำมาสู่แนวทางในการพิจารณาความสัมพันธ์ระหว่างจักรกลกับมนุษย์ผู้สั่งการตามทฤษฎี Human-Centered

---

[598] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare.”: p. 67.

[599] Fatma Tasdemmir and Gokhan Albayrak, “The Law of Cyber Warfare In Terms of Jus Ad Bellum and Jus In Bello: Application of International Law to the Unknown.” E-journal of Law, Vol 3 (2), (2017): 6.

[600] Kjølv Egeland, "Lethal Autonomous Weapon Systems under International Humanitarian Law", p. 95.

Approach[601] ทั้งนี้เพื่อเชื่อมโยงผลที่เกิดขึ้นจากการปฏิบัติการของจักรกลไปสู่ความรับผิดชอบของมนุษย์ผู้สั่งการ โดยทัศนะว่ามนุษย์จะต้องเป็นผู้รับผิดชอบตามกฎหมาย

มีนักวิชาการหลายคนที่มองว่าระบบอาวุธสังหารอิสระ (Autonomous Weapon Systems) นี้มีความน่าวิตกกังวลมากกว่าเทคโนโลยีชนิดอื่น เนื่องด้วยการพัฒนาระบบปัญญาประดิษฐ์เพื่อการใช้งานของพลเรือนมีพัฒนาการที่ก้าวล้ำมากขึ้น จึงมีความเคลื่อนไหวขององค์การสหประชาชาติในการศึกษาพัฒนาการของระบบอาวุธตัดสินใจได้ด้วยตนเอง และความเป็นไปได้ในการสร้างอนุสัญญาระหว่างประเทศเพื่อควบคุมระบบอาวุธอิสระ[602] อย่างไรก็ดีท้ายที่สุดร่างอนุสัญญาระหว่างประเทศเพื่อควบคุมระบบอาวุธสังหารอิสระก็ไม่ได้รับมติจากชาติสมาชิกของสหประชาชาติ

ความพยายามดังกล่าวสะท้อนให้เห็นความต้องการของสังคมระหว่างประเทศในมิติหนึ่งว่าความต้องการกฎหมายระหว่างประเทศเฉพาะเรื่องเพื่อควบคุมหรือจัดการกับเทคโนโลยีใหม่ที่มีการพัฒนาอย่างรวดเร็วและมีการนำมาใช้ในการขัดกันทางอาวุธมากขึ้นอาจส่งผลกระทบต่อการพิจารณาความชอบด้วยกฎหมายของการใช้อาวุธนั้น นอกจากนั้นยังเป็นสิ่งสะท้อนว่ามีผู้ไม่มั่นใจว่ากฎหมายมนุษยธรรมระหว่างประเทศจะยังมีหลักการที่เหมาะสมเพียงพอต่อสถานการณ์ความเปลี่ยนแปลงทางเทคโนโลยีหรือไม่

แนวคิดของกลุ่มผู้ที่เห็นด้วยกับการสร้างกฎหมายระหว่างประเทศใหม่เฉพาะเรื่องเพื่อควบคุมปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์รวมตลอดถึงความพยายามในการสร้างอนุสัญญาระหว่างประเทศเพื่อควบคุมระบบอาวุธอิสระนี้ยังมีสิ่งที่น่าสงสัยอยู่ว่าการจะพิจารณาเฉพาะเรื่องการควบคุมการใช้งานเทคโนโลยีเหล่านี้ในการขัดกันทางอาวุธจะมีความจำเป็นมากเพียงใด หากสังเกตจากอนุสัญญาระหว่างประเทศหลายฉบับที่มีเจตนารมณ์ในการควบคุมอาวุธเฉพาะอย่างในกรอบกฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธ (Disarmament) นั้น มักจะเป็นเรื่องการควบคุมการผลิต ขาย ขนส่ง ถ่ายโอน ฯลฯ เป็นสำคัญ ในขณะที่การใช้งานอาวุธในการขัดกันทางอาวุธจะต้องไม่ขัดต่อหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศคือหลักการไม่ใช้อาวุธ

---

[601] International Committee of the Red Cross. “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.” International Committee of the Red Cross. Paper, June 6, 2019, p. 6.

[602] Amandeep Singh Gill, “The Roles of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,” UN Chronicle, Vol. LV No.3 & 4 (December 2018) [accessed June 10, 2021] Available from: https://www.un.org/en/un-chronicle/role-united-nations-addressing-emerging-technologies-area-lethal-autonomous-weapons

ที่ก่อให้เกิดความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นอยู่แล้ว[603] ในขณะที่การใช้ระบบอาวุธสังหารอิสระมีรูปแบบที่หลากหลายและมีวัตถุประสงค์ที่ไม่ใช่การทำลายชีวิตมนุษย์ทุกกรณีเสมอไปเช่นการใช้ระบบป้องกันภัยทางอากาศ หากจะมีการใช้งานอาวุธอิสระเพื่อการโจมตีฝ่ายคู่พิพาทในการรบก็ย่อมจะต้องใช้วิธีการที่สอดคล้องต่อหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศ แนวคิดเรื่องการสร้างกฎหมายใหม่เพื่อควบคุมเทคโนโลยีใหม่ในการขัดกันทางอาวุธจึงไม่นำไปสู่แนวทางในการแก้ไขปัญหาที่แท้จริงเสมอไป

แนวคิดกลุ่มที่ 3 ควรพิจารณาบริบทของกฎหมายอื่นและบริบทของสังคมระหว่างประเทศร่วมกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

แนวคิดกลุ่มนี้มองว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่ได้เป็นเอกเทศจากบริบททางสังคมและการเมืองระหว่างประเทศ[604]ปัญหาไม่ได้อยู่ที่กฎหมายมนุษยธรรมระหว่างประเทศทันสมัยหรือมีเพียงพอหรือไม่แต่ปัญหาอยู่ที่การนำกฎหมายมาบังคับใช้จริง แนวคิดนี้เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศมีเจตนารมณ์ที่ดีแต่การบังคับให้เป็นไปตามเจตนารมณ์นั้นเป็นเรื่องอุดมคติมากเกินความจริงเนื่องจากในการรบนั้นคู่พิพาทในสงครามต่างแสวงหาหนทางทุกประการเพื่อให้ตนเองเอาชนะคู่ต่อสู้ในสงครามให้ได้โดยสนใจการคุ้มครองตามกฎหมายน้อยมาก[605]ความได้เปรียบ-เสียเปรียบในการรบนั้นมักขึ้นอยู่กับความพร้อมทางเศรษฐกิจและอำนาจทางการเมืองระหว่างประเทศ[606] การรบอย่างเท่าเทียมกันจึงไม่เคยเกิดขึ้นในความเป็นจริงและการผลักภาระในการแก้ไขปัญหาที่เกิดขึ้นจากสงครามให้เป็นหน้าที่ของกฎหมายมนุษยธรรมระหว่างประเทศก็เป็นเรื่องที่ไม่เหมาะสมแต่ควรเป็นบทบาทของรัฐคู่พิพาทในการปฏิบัติตามพันธกรณีด้วย[607]

อย่างไรก็ดีความแตกต่างของความขัดแย้งซึ่งนำไปสู่สงครามนั้นมีความหลากหลายเกินกว่าที่จะสร้างกฎหมายหรือมาตรการแบบเดียวในการจัดการกับปัญหาแต่การมีกฎหมายมนุษยธรรมระหว่างประเทศอยู่ก็ยังมีข้อดีอยู่บ้าง อย่างน้อยที่สุดก็ทำให้มีแนวทางและมาตรฐานในการปฏิบัติเพื่อไม่ให้การรบเป็นไปอย่างไร้ขอบเขตจนเกินไป[608]

---

[603] Williams H. Boothby, Weapons and the Law of Armed Conflict, p. 33.

[604] David Kennedy, “Modern War and Modern Law,” University of Baltimore Law Review, Vol. 36, Issue 2, (2007): 472.

[605] David Kennedy, Reassessing International Humanitarianism: The Dark Side, p. 3.

[606] Ibid., p.7.

[607] Ibid., p.12.

[608] David Kennedy, Reassessing International Humanitarianism: The Dark Side, p. 12.

3.2 การขัดกันทางอาวุธโดยการใช้เทคโนโลยีใหม่

กฎหมายมนุษยธรรมระหว่างประเทศจะมีผลบังคับเมื่อเกิดการขัดกันทางอาวุธ ดังนั้นจึงต้องพิจารณาความหมายของการขัดกันทางอาวุธตามกฎหมายและความสัมพันธ์ระหว่างการเกิดการขัดกันทางอาวุธกับการใช้เทคโนโลยีใหม่ ดังนี้

3.2.1 การเกิดการขัดกันทางอาวุธ

ขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ (อนุสัญญาเจนีวา ค.ศ. 1949 และพิธีสารเพิ่มเติม ค.ศ. 1977) จะเริ่มต้นเมื่อเกิดสงครามที่มีการประกาศหรือการขัดกันทางอาวุธ[609] ทั้งนี้สงครามที่ชอบธรรมตามกฎหมายว่าด้วยการขัดกันทางอาวุธแต่เดิมนั้นหมายถึงสงครามที่มีการประกาศ[610] ขณะที่การขัดกันทางอาวุธเป็นส่วนหนึ่งของสงครามและสงครามที่ไม่มีการประกาศ[611] สาระสำคัญของการทำสงครามหรือการขัดกันทางอาวุธคือการพิพาทกันด้วยอาวุธ (Armed attack) โดยการขัดกันทางอาวุธนั้นมี 2 กรณี คือการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

การพิพาทกันด้วยอาวุธ (Armed attack) ไม่ปรากฏในอนุสัญญาเจนีวา ค.ศ. 1949 แต่ปรากฏคำว่าการโจมตี (Attack) ในข้อ 49 (1) ของพิธีสารฉบับที่ 1 ค.ศ. 1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1949 โดยการโจมตีหมายความถึงการกระทำในลักษณะรุนแรงต่อฝ่ายปฏิปักษ์ไม่ว่าจะเป็นเชิงรุกหรือเชิงรับ[612] ปัญหาว่าการพิพาทกันด้วยอาวุธหรือการโจมตีในลักษณะใดจึงจะเป็นการขัดกันทางอาวุธจึงไม่มีคำอธิบายโดยตรงในอนุสัญญาเจนีวาและพิธีสารเพิ่มเติม

การตีความความหมายของคำว่าการขัดกันทางอาวุธจึงอาศัยคำวินิจฉัยของศาลอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวีย (The International Criminal Tribunal for the Former

---

[609] Geneva Convention 1949, Article 2 and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 1.

[610] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Commentary of 1987, para 59. [online] Accessed: May 10; 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-1/commentary/1987?activeTab=undefined

[611] Françoise Bouchet-Saulnier, “The Practical Guide to Humanitarian Law,” [online] Accessed: May 10, 2022. Available from: https://guide-humanitarian-law.org/content/article/3/war/

[612] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 49 (1).

Yugoslavia: ICTY) ในคดี Prosecutor v. Dusko Tadic ซึ่งศาลอธิบายว่า "...การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐ..."[613] ดังนั้นเมื่อมีการใช้กำลังทางทหารระหว่างรัฐเกิดขึ้นก็จะเป็นสถานการณ์ที่กฎหมายมนุษยธรรมระหว่างประเทศมีผลบังคับ ซึ่งโดยปกติการใช้กำลังทางทหารตามแบบย่อมดำเนินไปพร้อมกับวิธีการต่อสู้ด้วยอาวุธ สถานการณ์ที่เกิดขึ้นนี้จึงเรียกว่าการขัดกันทางอาวุธ (Armed Conflict) ซึ่งหมายถึงการพิพาทกันระหว่างกองกำลังทางทหารและการพิพาทกันด้วยอาวุธระหว่างกองกำลังทางทหาร

3.2.2 เทคโนโลยีใหม่กับการเกิดการขัดกันทางอาวุธ

ปัญหาว่าเทคโนโลยีใหม่จะทำให้เกิดการขัดกันทางอาวุธได้หรือไม่มักเกิดขึ้นกับการโจมตีทางไซเบอร์ เนื่องจากลักษณะของการโจมตีทางไซเบอร์มักถูกนำมาเปรียบเทียบกับการโจมตีด้วยกำลังทางอาวุธตามแบบจนนำไปสู่แนวคิดว่าพื้นที่ทางไซเบอร์อาจเป็นสมรภูมิรบรูปแบบหนึ่งได้ การจะพิจารณาว่าการโจมตีทางไซเบอร์จะนำไปสู่การเกิดการขัดกันทางอาวุธได้หรือไม่นั้นจะต้องวิเคราะห์ว่าการโจมตีทางไซเบอร์เทียบเท่าการใช้กำลังทางทหารหรือเทียบเท่าการโจมตีตามแบบหรือไม่ หากการโจมตีทางไซเบอร์เป็นการใช้กำลังทางทหารหรือเทียบเท่ากับการโจมตีตามแบบ การโจมตีทางไซเบอร์ก็จะนำไปสู่การเกิดการขัดกันทางอาวุธได้

โดยทั่วไปการโจมตีทางไซเบอร์อาจเกิดขึ้นได้ใน 3 สถานการณ์ดังต่อไปนี้[614]

กรณีที่ 1 การโจมตีทางไซเบอร์ที่เป็นส่วนหนึ่งของปฏิบัติการทางทหารในการขัดกันทางอาวุธ

สถานการณ์ความขัดแย้งที่ประเทศจอร์เจียที่เกิดขึ้นในปี ค.ศ.2008 นำไปสู่การใช้ปฏิบัติการทางทหารในการขัดกันทางอาวุธประกอบกับการใช้ปฏิบัติการโจมตีทางไซเบอร์ระหว่างกลุ่มเซาท์ออสเซเทีย (South Ossetia) กับรัฐบาลจอร์เจีย[615] ปรากฏการโจมตีทางไซเบอร์ต่อเว็บไซต์ของรัฐบาลจอร์เจียด้วยปฏิบัติการปฏิเสธการเข้าถึงบริการทางอินเทอร์เน็ต (DDoS) ทำให้เว็บไซต์รัฐบาลจอร์เจียไม่สามารถทำงานได้นานถึง 24 ชั่วโมง[616] การโจมตีทางไซเบอร์พร้อมกับการโจมตีตามแบบปกติ

---

[613] The Prosecutor v. Dusko Tadic, The Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, The Appeal Chamber (ICTY) 2 October 1995 para.70.

[614] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 127.

[615] Kadri Kaska Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Center of Exxellence (CCD COE) (Z2012): 68.

[616] Williams C. Ashmore, "Impact of Alleged Russian Cyber Attacks," Baltic Security and Defense Review, 11 (2009): 10.

เกิดขึ้นอย่างน้อยสองครั้งในปีเดียวกันนี้[617] ความเสียหายสำคัญที่เกิดขึ้นคือการใช้งานเว็บไซต์รัฐบาลล้มเหลวและเจ้าหน้าที่ของรัฐบาลจอร์เจียต้องใช้เวลาหลายวันในการแก้ไขให้เว็บไซต์เพื่อให้กลับมาใช้ได้เหมือนเดิม[618]

กรณีการโจมตีทางไซเบอร์ไปพร้อมกับปฏิบัติการทางทหารตามแบบปกตินั้นย่อมเป็นส่วนหนึ่งของปฏิบัติการทางทหารในการขัดกันทางอาวุธ หากปฏิบัติการดังกล่าวเป็นการกระทำของกองกำลังของรัฐหรือของพลเรือนที่มีส่วนร่วมโดยตรงในการสู้รบ ซึ่งจะตกอยู่ภายใต้บังคับของกฎหมายว่าด้วยการขัดกันทางอาวุธ ข้อโต้แย้งเดียวที่อาจเกิดขึ้นในสถานการณ์ดังกล่าวคือ กฎหมายว่าด้วยการขัดกันทางอาวุธไม่สามารถปรับใช้แก่กรณีได้เพราะกฎหมายเกิดขึ้นก่อนเทคโนโลยีไซเบอร์ ซึ่งประเด็นเช่นนี้มีความไม่สมเหตุสมผลในสองประการกล่าวคือ

ประการแรก กฎหมายว่าด้วยการขัดกันทางอาวุธ เช่นพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ.1977 มีการกำหนดให้ขอบเขตการบังคับใช้กฎหมายครอบคลุมถึง อาวุธ ปัจจัย และวิธีการทำสงครามรูปแบบใหม่ด้วย เพราะผู้ร่างกฎหมายย่อมคำนึงถึงความเปลี่ยนแปลงทางเทคโนโลยีที่จะเกิดขึ้นในอนาคต และหวังให้กฎหมายที่สร้างขึ้นสามารถแก้ไขปัญหาที่อาจเกิดจากความเปลี่ยนแปลงทางเทคโนโลยีได้ด้วย

ประการที่สอง ในคดี Nuclear Weapons ค.ศ.1996 ศาลยุติธรรมระหว่างประเทศได้พิจารณาในสาระสำคัญว่า แม้อาวุธนิวเคลียร์จะได้รับการคิดค้นมาหลังหลักการทางกฎหมายมนุษยธรรมระหว่างประเทศหลายฉบับ และอาวุธนิวเคลียร์จะมีความแตกต่างจากอาวุธตามแบบอื่นๆ ทั้งในแง่ของความรุนแรงเชิงปริมาณและคุณภาพ แต่ก็มิได้หมายความว่ากฎหมายมนุษยธรรมระหว่างประเทศจะปรับใช้กับอาวุธนิวเคลียร์ไม่ได้ เพราะกฎหมายมนุษยธรรมระหว่างประเทศมีลักษณะเป็นหลักการที่มุ่งหมายจะให้มีผลปรับใช้ได้กับการทำสงครามทุกรูปแบบและอาวุธทุกชนิด ทั้งในปัจจุบันและในอนาคต[619] โดยคำอธิบายศาลยุติธรรมระหว่างประเทศในคดีดังกล่าว นักวิชาการหลายคนจึงใช้

---

[617] Ibid., p. 10.

[618] Ibid.

[619] *Nuclear Weapon Case*. Para 86. “Indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974-1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of legal principles in question which permeates the

ในการอธิบายว่าเหตุใดกฎหมายว่าด้วยการขัดกันทางอาวุธ หรือกฎหมายมนุษยธรรมระหว่างประเทศจึงควรปรับใช้กับการโจมตีทางไซเบอร์ได้ เพราะไม่ว่าเทคโนโลยีไซเบอร์จะเกิดขึ้นก่อนหรือหลังกฎหมายว่าด้วยการขัดกันทางอาวุธ ย่อมไม่ถือเป็นเหตุที่จะอ้างว่ากฎหมายว่าด้วยการขัดกันทางอาวุธไม่สามารถปรับใช้ได้ การพิจารณาของศาลยุติธรรมระหว่างประเทศกรณีดังกล่าวถือได้ว่าเป็นบทบาทในการตีความกฎหมายระหว่างประเทศซึ่งนำไปสู่การรับรองหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศว่ามีความเพียงพอต่อการปรับใช้กับสถานการณ์ใหม่

อย่างไรก็ดี ในคดี Armed Activities of Congo ปี ค.ศ.2005 และคดี Land and Maritime Boundary between Cameroon and Nigeria ปี ค.ศ.2002 นั้นศาลยุติธรรมระหว่างประเทศปรับใช้แนวคิดเรื่องความรุนแรงในการต่อสู้เพื่อการตัดสินคดี แม้โจทก์ในคดีทั้งสองคืออูกันด้าในคดี Armed Activities และคาเมรูนในคดี Land and Maritime Boundary มิได้พิสูจน์อย่างชัดเจนถึงระดับความรุนแรงที่เกิดขึ้นในเหตุการณ์ก็ตาม[620] ดังนั้นจึงหมายความว่าหากการโจมตีด้วยปฏิบัติการทางไซเบอร์มีความต่อเนื่องและพอจะพิสูจน์ความเสียหายในลักษณะที่รุนแรงอยู่บ้าง ย่อมถือได้ว่าการโจมตีทางไซเบอร์นั้นอยู่ในขอบเขตการบังคับตามพิธีสารฉบับที่ 2 นี้ได้[621]

ประเด็นที่น่าพิจารณาเป็นสำคัญคือการโจมตีทางไซเบอร์มีผลที่แตกต่างจากการโจมตีด้วยอาวุธตามแบบและอาวุธนิวเคลียร์ เนื่องจากอาวุธตามแบบและอาวุธนิวเคลียร์นั้นจะก่อให้เกิดความเสียหายทางตรงจากการใช้อาวุธเท่านั้น และส่วนใหญ่ความเสียหายมักจะเกิดทางกายภาพ ในขณะที่การโจมตีทางไซเบอร์อาจก่อให้เกิดความเสียหายต่อชีวิต และร่างกายของบุคคลก็ได้ หรืออาจเกิดความเสียหายต่อทรัพย์สินก็ได้ นอกจากนั้นยังอาจก่อให้เกิดความเสียหายที่ไม่มีลักษณะทางกายภาพด้วย เช่น การทำลายข้อมูล หรือระบบปฏิบัติการของคอมพิวเตอร์เป้าหมายซึ่งอาจไม่ก่อให้เกิดความเสียหายร้ายแรง อย่างไรก็ดี สิ่งที่ต้องคำนึงถึงคือแนวคิดในเรื่องการปฏิบัติที่เป็นปฏิปักษ์ (Conduct of Hostilities) นั้นครอบคลุมถึงการกระทำของปฏิบัติการทางทหารที่ก่อให้เกิดผลโดยตรงที่ไม่รุนแรงเพื่อต่อสู้กับฝ่ายศัตรูด้วย[622]

---

entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."

[620] *Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening)* (2002) ICJ Reports, International Court of Justice, para 323, Armed Activities Case, para 146.

[621] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 95.

[622] Yoram Dinstein, Conduct of Hostilities and the Law of War, p.2.

กรณีที่ 2 การโจมตีทางไซเบอร์ที่ไม่มีความเกี่ยวข้องกับสถานการณ์การขัดกันทางอาวุธเลย

สถานการณ์ที่ใกล้เคียงกับลักษณะกรณีที่ 2 นี้ได้แก่กรณีการโจมตีโรงงานผลิตยูเรเนียมของประเทศอิหร่านโดยมัลแวร์ Stuxnet ซึ่งเหตุการณ์นี้เกิดขึ้นระหว่างปี ค.ศ.2009-2010 โดยในเดือนพฤศจิกายน ค.ศ.2010 ประธานาธิบดี Mahmoud Ahmadinejad ได้แถลงว่ามัลแวร์ระบุชนิดไม่ได้นี้ถูกส่งมาจาก “ศัตรูตะวันตก” (Western enemies) โดยมีเป้าหมายในการรบกวนระบบคัดแยกยูเรเนียมที่เมือง Natanz ประเทศอิหร่าน แม้การโจมตีด้วยมัลแวร์ดังกล่าวจะไม่ก่อให้เกิดความเสียหายทางกายภาพ แต่ก็ทำให้เครื่องคัดแยกยูเรเนียม (Centrifuge) ทำงานผิดปกติไป โดย Stuxnet สั่งการให้ใบพัดเครื่องคัดแยกยูเรเนียมหมุนเร็วขึ้นอย่างมากในระยะเวลา 15 นาทีและบางครั้งมัลแวร์จะสั่งการให้ใบพัดเครื่องคัดแยกหมุนช้าลงกว่าปกติ รายงานของ ISIS Stuxnet ระบุว่าแกนเหวี่ยงหมุนแรงจนเกือบจะหลุดออกจากมอเตอร์เป็นผลให้ใบพัดเครื่องคัดแยกยูเรเนียมได้รับความเสียหาย อย่างไรก็ดีรายงานนี้ระบุว่าการโจมตีดังกล่าวไม่ได้มีผลทำลายระบบผลิตยูเรเนียมแต่เป็นการทำให้ชิ้นส่วนอุปกรณ์สึกหรอและชะลอการคัดแยกยูเรเนียมเท่านั้นเท่านั้น[623]

หากพิจารณาตามคำอธิบาย (Commentary) ของอนุสัญญาเจนีวาจะพบว่าหลักการที่ปรากฏในคดี Tadic นั้น ให้ความสำคัญกับองค์ประกอบของการกระทำที่เกิดจากรัฐ ตัวตนอื่นที่มีอำนาจกระทำการแทนรัฐ หรือกลุ่มกองกำลังอื่น โดยการกระทำดังกล่าวจะต้องก่อให้เกิดหรือมีความมุ่งหมายให้เกิดความเสียหายต่อชีวิต ร่างกาย หรือทรัพย์สิน เมื่อพิจารณาตามแนวทางนี้จะพบว่าการโจมตีทางไซเบอร์ซึ่งไม่เกี่ยวข้องกับสถานการณ์ใดๆ เลยนั้นก็อาจนำไปสู่การเกิดการขัดกันทางอาวุธได้ หากพิสูจน์ได้ว่าผู้กระทำนั้นปฏิบัติหน้าที่แทนรัฐ การพิจารณาว่าการโจมตีทางไซเบอร์โดยไม่ขึ้นอยู่กับสถานการณ์การขัดกันทางอาวุธ แต่อาจนำไปสู่การขัดกันทางอาวุธได้จึงจำเป็นต้องพิจารณาเงื่อนไขการกระทำดังกล่าวเป็นรายกรณีไป

กรณีที่ 3 การใช้การโจมตีทางไซเบอร์ควบคู่ไปกับการโจมตีด้วยอาวุธตามแบบ

แนวคิดเรื่องการโจมตีทางไซเบอร์ไปพร้อมกับการโจมตีด้วยอาวุธตามแบบนั้นเป็นกรณีที่ได้รับการยอมรับมากที่สุดว่าสัมพันธ์กับปฏิบัติการทางทหารในการขัดกันทางอาวุธ และเป็นวิธีการในการขัดกันทางอาวุธได้ด้วย อย่างไรก็ดีปฏิบัติการทางไซเบอร์หลายเหตุการณ์ไม่มีความสัมพันธ์กับลักษณะของปฏิบัติการทางทหารที่ก่อให้เกิดความได้เปรียบ-เสียเปรียบต่อกองทัพฝ่ายตรงข้ามเท่าไร

---

[623] David Albright, Paul Brannan, and Christina Walrond, “Stuxnet Malware and Natanz: update of ISIS December 2010,” Institute for Science and International Security Report; (2011). p.4.

นัก โดยมากมักเป็นการโจมตีเว็บไซต์ของรัฐบาล นักวิชาการส่วนหนึ่งจึงเสนอว่าควรจะต้องมีการพิสูจน์ความความสัมพันธ์ระหว่างปฏิบัติการทางไซเบอร์นั้นว่ามีความสัมพันธ์กับการโจมตีมากเพียงใด เช่น การพิสูจน์ไม่เพียงพอของการใช้อาวุธจึงต้องมีการใช้ปฏิบัติการทางไซเบอร์เสริม เช่น การแสดงให้เห็นว่าระบบเรดาร์ตรวจจับเป้าหมายถูกรบกวนหรือถูกทำลายโดยศัตรู จึงจำเป็นที่จะต้องมีการใช้ปฏิบัติการทางไซเบอร์ควบคู่ไปกับการโจมตีฝ่ายศัตรู[624]

การพิสูจน์การโจมตีทางไซเบอร์ว่าเป็นไปเพื่อประกอบกับการโจมตีด้วยอาวุธตามแบบเป็นเรื่องที่ค่อนข้างละเอียดอ่อนและอาจนำไปสู่ปัญหาบางประการ เช่น หากรัฐอ้างว่าระบบเรดาร์ของตนถูกโจมตีจึงเป็นเหตุให้การสั่งการทิ้งระเบิดจากอากาศยานเกิดความผิดพลาด หรือการอ้างว่าระบบนำวิถีของขีปนาวุธถูกรบกวนจึงทำให้การโจมตีเป้าหมายคลาดเคลื่อน[625] ข้ออ้างดังกล่าวจะรับฟังได้เพียงใด เนื่องจากการพิสูจน์ให้ทันท่วงทีอาจทำได้ยาก นอกจากนั้นการพิสูจน์ที่ล่าช้ายังอาจส่งผลต่อการตัดสินใจในการโต้ตอบของกองกำลังฝ่ายตรงข้ามซึ่งอาจทำให้การปฏิบัติตามหลักความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตีได้รับผลกระทบ

การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ ตามข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 กำหนดว่า “นอกจากบทบัญญัติที่ต้องใช้ในยามสงบแล้ว ให้ใช้อนุสัญญาฉบับนี้บังคับแก่บรรดากรณีสงครามที่ได้มีการประกาศ หรือกรณีพิพาทกันด้วยอาวุธอย่างอื่นใดซึ่งอาจเกิดขึ้นระหว่างอัครภาคีผู้ทำสัญญาสองฝ่ายหรือกว่านั้นขึ้นไป แม้ว่าฝ่ายหนึ่งฝ่ายใดจะมิได้รับรองว่ามีสถานะสงครามก็ตาม

อนุสัญญาฉบับนี้ให้ใช้บังคับแก่กรณีการยึดครองอาณาเขตบางส่วนหรือทั้งหมดของอัครภาคีผู้ทำสัญญาด้วย แม้ว่าการยึดครองดังกล่าวจะมิได้ประสบการต่อต้านด้วยอาวุธก็ตาม...”[626]

การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศจึงหมายถึง กรณีสงครามที่มีการประกาศหรือกรณีการพิพาทกันด้วยอาวุธอย่างอื่นระหว่างคู่ภาคีสองฝ่ายหรือกว่านั้น แม้จะไม่มีการรับสองสถานะสงครามก็ตาม และกรณีการยึดครองอาณาเขตบางส่วนแม้ไม่มีการต่อต้านด้วยอาวุธ[627]

---

[624] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 134.

[625] Ibid.

[626] Geneva Convention 1949, Common Article 2.

[627] Common Article 2, Geneva Convention 1949 “In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

การขัดกันทางอาวุธระหว่างรัฐหนึ่งรัฐใดกับองค์กรระหว่างประเทศจึงนับเป็นการขัดกันทางอาวุธระหว่างประเทศเช่นกัน ในขณะที่สงครามปลดแอกซึ่งประชาชนต่อสู้เพื่อปลดปล่อยตัวเองจากการเป็นอาณานิคมหรือ ต่อต้านการยึดครองโดยชาวต่างชาติ และการต่อสู้กับการเหยียดสีผิวโดยใช้สิทธิในการกำหนดเจตจำนงของตัวเอง จัดว่าเป็นการขัดกันทางอาวุธระหว่างประเทศภายใต้เงื่อนไขบางประการ ตามพิธีสารเพิ่มเติม ฉบับที่ 1 ข้อ 1 วรรค 4 และ ข้อ 96 วรรค 3[628]

การขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศซึ่งเป็นภาษากฎหมายระหว่างประเทศนั้นมักเรียกและเข้าใจกันในภาษาทั่วไปว่า “สงคราม” มีได้สองลักษณะคือ

ลักษณะที่ 1 มีการพิพาทกันด้วยอาวุธระหว่างรัฐคู่ภาคีสองฝ่ายหรือมากกว่านั้น

การพิพาทกันด้วยอาวุธหรือการขัดกันทางอาวุธ (Armed conflict) มีความหมายที่ค่อนข้างตรงตามตัวคือ การใช้ “อาวุธ” (Arm) เพื่อการต่อสู้ใน “ความขัดแย้ง” (Conflict)

อาวุธ (Arm) ย่อมหมายถึงสิ่งที่ออกแบบมาเพื่อการใช้งานให้เกิดความเสียหาย รวมถึงสิ่งที่ไม่ได้ออกแบบมาโดยสภาพเพื่อใช้ก่อให้เกิดความเสียหายแต่ผู้ใช้งานสามารถนำไปใช้ก่อให้เกิดความเสียหายได้ ความเสียหายนั้นได้แก่ ความเสียหายต่อร่างกาย ความเสียหายต่อชีวิต ความเสียหายที่เป็นผลกระทบต่อสุขภาพ ความเสียหายต่อทรัพย์สิน ความเสียหายต่อสิ่งแวดล้อม ฯลฯ ลักษณะของอาวุธจึงมีมักจะเกี่ยวข้องกับสิ่งของที่เป็นรูปธรรมในเชิงกายภาพและสามารถแสดงผลทางกายภาพ (kinetic) ได้ โดยหากจำแนกตามการออกแบบสิ่งที่สร้างขึ้นมาเพื่อเป็นอาวุธและสิ่งที่มิได้ออกแบบและสร้างขึ้นมาเพื่อเป็นอาวุธโดยตรงแต่สามารถใช้งานเป็นอาวุธได้ ย่อมพิจารณาได้ดังนี้

สิ่งที่ออกแบบและสร้างขึ้นมาเพื่อเป็นอาวุธ ได้แก่ ปืนเป็นสิ่งที่ออกแบบและสร้างขึ้นมาเพื่อการทำลาย ไม่ว่าจะเป็นการทำลายสิ่งมีชีวิตหรือทรัพย์สิน ปืนเป็นอาวุธที่มีสถานะเป็นวัตถุทางกายภาพ ยิ่งกระสุนปืนที่เป็นวัตถุทางกายภาพสู่เป้าหมายที่เป็นวัตถุทางกายภาพและทำให้วัตถุเป้าหมายถูกทำลาย ในทำนองเดียวกันระเบิดเป็นอาวุธที่มีสถานะเป็นวัตถุทางกายภาพที่สามารถทำลายเป้าหมายทางกายภาพได้ ปัญหาจะเริ่มมีความยุ่งยากมากขึ้นหากอาวุธที่ใช้ในการทำลาย

Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.”

[628] คณะกรรมการกาชาดระหว่างประเทศ, กฎหมายมนุษยธรรมระหว่างประเทศ ถาม-ตอบทุกคำถาม, (กรุงเทพฯ: คณะกรรมการกาชาดระหว่างประเทศ, 2562), หน้า 18.

เป้าหมายนั้นไม่ได้มีการกระทำหรือการแสดงออกในเชิงกายภาพ (Non-kinetic) เช่น ระเบิดนิวเคลียร์ซึ่งออกแบบมาเพื่อการทำลาย ย่อมไม่ได้เป็นที่สงสัยว่าเป็นอาวุธหรือไม่ เพราะโดยลักษณะการใช้งานมักเป็นการติดตั้งสารกัมมันตรังสีในหัวรบขีปนาวุธ (จรวด) เพื่อใช้ในการทำลาย เมื่อยิงขีปนาวุธไปยังเป้าหมายและเกิดการตกกระทบก็จะเกิดการระเบิด แต่สิ่งที่ทำให้ระเบิดนิวเคลียร์เป็นประเด็นในความขัดแย้งระดับระหว่างประเทศจนกระทั่งมีการฟ้องคดีต่อศาลยุติธรรมระหว่างประเทศคือปฏิกิริยาของสารกัมมันตรังสีไม่ได้ยุติเพียงการระเบิดในครั้งเดียวเท่านั้นเมื่อเปรียบเทียบกับระเบิดทั่วไป หากอธิบายให้ละเอียดขึ้นคือระเบิดทั่วไปเมื่อเกิดการระเบิดแล้วย่อมเกิดแรงอัดอากาศในปริมาณมากทำให้เป้าหมายถูกทำลาย ในบางกรณีวัตถุระเบิดดังกล่าวมีการผสมเศษโลหะหรือวัตถุอื่นๆ ด้วย เมื่อเกิดการระเบิดวัตถุที่บรรจุภายในระเบิดที่เรียกกันโดยทั่วไปว่า “สะเก็ดระเบิด” ก็จะกระจายไปสู่ทั้งคนและวัตถุรอบข้างก่อให้เกิดความเสียหายที่มากกว่าระเบิดที่ไม่ได้บรรจุวัตถุอื่น การทำงานของระเบิดรูปแบบนี้จึงมักมีผลกระทบครั้งเดียวจากการระเบิด (ไม่นับรวมการติดเชื้อที่อาจมาจากการถูกสะเก็ดระเบิด หรือความสูญเสียทางจิตใจซึ่งเป็นผลกระทบข้างเคียง)[629]

ขณะที่ระเบิดนิวเคลียร์มีผลกระทบที่มากกว่าแรงอัดอากาศปริมาณมหาศาล และสะเก็ดระเบิดที่สร้างความบาดเจ็บหรือเสียชีวิตแต่ปฏิกิริยาฟิวชั่นทางนิวเคลียร์ซึ่งหมายถึงการที่อนุภาคขนาดเล็กทางเคมีสามารถทำงานด้วยตัวเองได้โดยการระเบิดระดับนิวเคลียสหรือระดับเล็กที่สุด ซึ่งไม่สามารถมองเห็นได้ด้วยตาและปฏิกิริยาดังกล่าวสามารถทำงานได้ต่อไปจากการทำงานของระเบิดเพียงครั้งเดียว ยิ่งไปกว่านั้น แม้จะไม่มีการระเบิดเกิดขึ้น (หมายถึงไม่มีลักษณะการกระทำให้เกิดแรงอัดทางอากาศ) แต่เป็นการรั่วไหลของสารกัมมันตรังสีซึ่งเป็นปฏิกิริยาทางนิวเคลียร์ ก็สามารถส่งผลกระทบแบบเดียวกันกับผลกระทบที่เกิดจากระเบิดนิวเคลียร์ได้เช่นกัน เช่น ผู้โจมตีอาจทำลายเป้าหมายได้โดยการใช้อาวุธนิวเคลียร์ที่ไม่ต้องมีการระเบิด แต่ก่อให้เกิดการรั่วไหลของสารกัมกันตรังสี (แบบเดียวกับการปล่อยแก๊สพิษ) ก็สามารถก่อให้เกิดผลกระทบในวงกว้างได้ เป็นต้น ปฏิกิริยาที่เกิดขึ้นหลังจากการระเบิดของขีปนาวุธนิวเคลียร์นี้สามารถทำลายเป้าหมายได้โดยส่งผลกระทบในระยะยาว สิ่งที่ตามมาคือความป่วยไข้ ความพิการทุพลภาพ ความเสียหายทางพันธุกรรมของมนุษย์ซึ่งมีผลระยะยาว 1-2 ชั่วอายุขัยมนุษย์ และการปนเปื้อนสารกัมมันตรังสีในวัตถุ เหล่านี้เป็นสิ่งที่เป็นผลกระทบมากกว่าการใช้งานระเบิดทั่วไปและนำไปสู่ความพยายามในสังคมระหว่างประเทศเพื่อทำให้ระเบิดนิวเคลียร์เป็นอาวุธต้องห้ามตามกฎหมายระหว่างประเทศ ไม่ใช่เพราะแค่เป็นวัตถุระเบิด แต่

[629] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

เพราะปฏิกิริยานิวเคลียร์นั้นทำงานแตกต่างจากอาวุธทั่วไปที่เห็นการกระทำในเชิงกายภาพและส่งผลทางกายภาพแต่ปฏิกิริยานิวเคลียร์ไม่อาจเห็นการกระทำทางกายภาพ (นอกเหนือจากการระเบิดครั้งแรก) แต่เห็นผลความเสียหายที่เกิดขึ้นอย่างยาวนาน[630]

อย่างไรก็ตามอาจเกิดข้อสงสัยว่าลักษณะการทำงานของอาวุธบางประเภทก็ไม่เห็นการกระทำในเชิงกายภาพก็ไม่ปรากฏว่าจะมีปัญหาทางกฎหมายแต่อย่างใด เช่น หากระเบิดทำงานด้วยแรงอัดอากาศ แรงอัดอากาศดังกล่าวก็ไม่มีลักษณะทางกายภาพ เหตุใดจึงไม่มีปัญหาทางกฎหมาย หรือกรณีการใช้แก๊สพิษเพื่อการโจมตีก็ไม่มีลักษณะของการกระทำทางกายภาพ เหตุใดจึงไม่มีปัญหาทางกฎหมายเหมือนกรณีระเบิดนิวเคลียร์ ลักษณะการทำงานของอาวุธทั้งสองชนิดอาจอธิบายความแตกต่างจากการทำงานของระเบิดนิวเคลียร์ได้ดังนี้

การระเบิดด้วยแรงอัดอากาศแม้ไม่เห็นแรงอัดอากาศเป็นรูปธรรมเชิงกายภาพได้ แต่แรงอัดอากาศเป็นผลสืบเนื่องโดยทันทีจากการใช้วัตถุระเบิด และปรากฏชัดเจนว่าเมื่อมีการยิงระเบิด ขว้างระเบิดและมีการทำงานของระเบิด ไม่ว่าจะด้วยการจุดชนวนโดยอัตโนมัติหรือการตกกระทบหรือการใช้แรงกดทับ ระเบิดเหล่านี้จะมีการทำงานทันทีโดยปฏิกิริยาปล่อยแรงอัดอากาศ การทำงานของระเบิดที่ทันทีนี้ทำให้ความสัมพันธ์ระหว่างการใช้งานวัตถุระเบิดที่เป็นวัตถุทางกายภาพกับแรงอัดอากาศซึ่งเป็นปฏิกิริยาทางฟิสิกส์แต่ไม่เห็นลักษณะการกระทำทางกายภาพมีความเกี่ยวข้องกันอย่างแยกไม่ออก เมื่อพิจารณารวมแล้วจึงเป็นผลที่มาจากการใช้งานวัตถุระเบิดนั่นเอง

การใช้งานแก๊สพิษมีความใกล้เคียงกับการทำงานของอาวุธนิวเคลียร์ค่อนข้างมากเพราะไม่สามารถเห็นการทำงานของแก๊สพิษอย่างเป็นรูปธรรมได้และการทำงานของอาวุธแก๊สพิษอาจใช้งานได้โดยการติดตั้งกับหัวรบขีปนาวุธ บรรจุในวัตถุระเบิด หรือใช้งานโดยการปล่อยจากอุปกรณ์บรรจุแก๊สพิษก็ได้ แทบไม่แตกต่างจากการทำงานของนิวเคลียร์ แต่สิ่งที่แตกต่างคือผลของการทำงานของแก๊สพิษจะมีขอบเขตการทำลายที่ไม่กว้างขวางเท่าอาวุธนิวเคลียร์ ยิ่งไปกว่านั้นการทำงานของแก๊สพิษยังไม่ปรากฏผลกระทบในลักษณะยาวนานแบบเดียวกับที่เกิดขึ้นจากการใช้อาวุธนิวเคลียร์ ทำให้อาวุธนิวเคลียร์มีผลกระทบในระดับที่รุนแรงกว่าแก๊สพิษ ทั้งในแง่ของขอบเขตเชิงพื้นที่ในการทำลาย และขอบเขตเชิงผลกระทบระยะยาว เมื่อเทียบการทำงานของแก๊สพิษกับอาวุธนิวเคลียร์ในมิติทางด้านการทำลายล้าง อาวุธแก๊สพิษจึงมีผลกระทบที่คล้ายกับอาวุธตามแบบทั่วไปเท่านั้น คือเป็นอาวุธที่แสดงให้เห็นผลกระทบทันทีจากการใช้งาน ความพิเศษประการเดียวที่ทำให้อาวุธนิวเคลียร์แตกต่างจากอาวุธ

[630] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

อื่นๆ จึงเป็นเรื่องผลกระทบระยะยาวของปฏิกิริยานิวเคลียร์ที่สามารถทำงานได้โดยไม่ต้องสั่งการอีกและสามารถส่งผลการทำลายล้างในระยะยาวได้[631]

สิ่งที่มิได้ออกแบบและสร้างขึ้นมาเพื่อเป็นอาวุธโดยตรงแต่สามารถใช้งานเป็นอาวุธได้ สิ่งที่มิได้ออกแบบหรือสร้างขึ้นมาเพื่อให้เป็นอาวุธโดยตรงแต่ลักษณะสภาพของสิ่งนั้นสามารถนำมาใช้เป็นอาวุธ ได้แก่ แก๊ส (เชื้อเพลิง) ที่ปกติมีไว้เพื่อเป็นเชื้อเพลิงในการหุงต้มแต่หากมีการนำไปติดตั้งเข้ากับชนวนระเบิด แก๊สซึ่งบรรจุในถังดังกล่าวก็สามารถเป็นอาวุธที่ใช้ในการทำลายล้างได้

ในบางกรณีก็เกิดความสับสนของวัตถุที่อาจใช้ได้ทั้งการเป็นอาวุธและไม่ใช่อาวุธก็ได้ โดยผู้ออกแบบและสร้างขึ้นมาก็อาจมีวัตถุประสงค์ให้การใช้งานสิ่งนั้นมีความหลากหลาย เช่น มีดเป็นวัตถุมีคมหากใช้งานเป็นอาวุธก็ย่อมสามารถทำได้ เพราะโดยสภาพของโลหะที่แหลมและคมย่อมใช้ในการทำลายวัตถุสิ่งของหรือบุคคลได้ ด้วยการทิ่ม ฟัน ตัด หรือแทง ในขณะที่การใช้งานมีดเพื่อไม่ให้เป็นอาวุธก็ย่อมสามารถกระทำได้ โดยการนำมีดนั้นมาใช้เพื่อประโยชน์ทางอื่น เช่น การตัดต้นไม้ ตัด ผ่าสิ่งของต่างๆ ลักษณะของมีดจึงมีทั้งสองทางคือการทำลายและการใช้ประโยชน์รวมกันไปในเวลาเดียวกัน

อาวุธนิวเคลียร์ที่หมายถึงเฉพาะส่วนประกอบที่ก่อสารกัมมันตรังสี เช่น ธาตุยูเรเนียมเป็นสิ่งที่มีอยู่แล้วตามธรรมชาติแต่สามารถสกัดออกมาเพื่อสร้างปฏิกิริยาฟิวชั่นให้เกิดเป็นการทำงานของนิวเคลียร์ได้ ยูเรเนียมจึงไม่ใช่อาวุธโดยสภาพแต่จะเป็นอาวุธก็ต่อเมื่อมีการนำมาใช้งาน เป็นต้น

เมื่อพิจารณาจากความแตกต่างกันของสิ่งที่เป็นอาวุธโดยสภาพและสิ่งที่ไม่ใช่อาวุธโดยสภาพแล้ว ย่อมเกิดข้อสรุปในเบื้องต้นว่า การใช้ทั้งอาวุธและสิ่งที่ไม่ใช่อาวุธโดยสภาพแต่ถูกนำมาใช้งานให้เป็นอาวุธ และแม้กระทั่งสิ่งที่เป็นได้ทั้งอาวุธและไม่ใช่อาวุธ ย่อมสามารถก่อให้เกิดการขัดกันทางอาวุธได้ ปัญหาประการเดียวที่ยังคงเหลืออยู่คืออาวุธจำเป็นต้องมีลักษณะทางกายภาพเสมอไปหรือไม่

องค์ประกอบสำคัญ 2 ประการของการขัดกันทางอาวุธ คือ การกระทำของรัฐและกระทำที่เทียบเท่าปฏิบัติการทางทหาร

การกระทำของรัฐย่อมเกิดขึ้นได้จากตัวแทนของรัฐเช่นทหารที่สังกัดในกองทัพของรัฐหรือผู้ที่กระทำการแทนรัฐได้ปฏิบัติหน้าที่ตามได้รับมอบหมาย

---

[631] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

การกระทำที่เทียบเท่าปฏิบัติการทางทหาร มีข้อที่น่าสนใจคือ ในที่ประชุมของสมาชิกปฏิญญาแห่งสมัชชาใหญ่แห่งสหประชาชาติว่าด้วยหลักกฎหมายระหว่างประเทศเกี่ยวกับความสัมพันธ์ระหว่างประเทศและความร่วมมือระหว่างรัฐ ปี ค.ศ.1970 มีการวิพากษ์วิจารณ์อย่างกว้างขวางว่าคำว่า “การใช้กำลัง” (force) ในกฎบัตรสหประชาชาตินั้นมีความคลุมเครือ ด้วยเหตุว่าในขณะที่มีการร่างกฎบัตรสหประชาชาติมีสมาชิกสองกลุ่มที่มีความเห็นไม่ตรงกัน คือฝ่ายชาติตะวันตกเห็นว่าการใช้กำลังหมายถึงการใช้กำลังทางอาวุธเท่านั้น แต่ประเทศกลุ่มสหภาพโซเวียตเดิมและประเทศกำลังพัฒนามองว่า “การใช้กำลัง” ควรหมายถึงการกดดันรูปแบบอื่นๆ ด้วย เช่น มาตรการคว่ำบาตรทางเศรษฐกิจและมาตรการบีบบังคับทางการเมือง เพราะมาตรการเหล่านี้ส่งผลต่อความมั่นคงของ “บูรณภาพแห่งดินแดน” เช่นกัน แต่ท้ายที่สุดที่ประชุมปฏิญญาฯ แยกมาตรการทั้งสองนี้ออกจากกัน โดยให้เหตุผลว่าการใช้กำลังควรเกิดขึ้นเฉพาะกรณีที่มีการใช้อาวุธและกองกำลังทางทหารเท่านั้น แต่มาตรการบังคับทางเศรษฐกิจและการเมืองอยู่ในลักษณะการแทรกแซง (Intervention) จึงไม่ควรตีความไปในลักษณะเดียวกัน[632] ไม่ว่าจะด้วยอิทธิพลทางการเมืองของชาติตะวันตกที่เหนือกว่าหรือที่ประชุมสหประชาชาติเห็นว่านิยามดังกล่าวเหมาะสมที่สุดหรือไม่ ท้ายสุดแล้วปัญหาจึงตกมาสู่การตีความปัญหาเรื่องการใช้กำลังในปัจจุบันว่าจะรวมถึงสิ่งที่มิใช่การใช้กำลังทางทหารตามแบบได้หรือไม่

สิ่งที่น่าสนใจคือในคดี Nicaragua ศาลยุติธรรมระหว่างประเทศไม่ได้ปฏิเสธความรุนแรงในรูปแบบอื่นเสียทั้งหมด แม้ว่าศาลจะยอมรับเอาหลักการของกฎบัตรสหประชาชาติ ข้อ 2 (4) มาใช้และยังยอมรับเอาหลักการในปฏิญญาว่าด้วยหลักกฎหมายระหว่างประเทศเกี่ยวกับความสัมพันธ์ระหว่างประเทศและความร่วมมือระหว่างรัฐ ปี ค.ศ.1970 โดยถือว่าเป็นจารีตที่ปฏิบัติโดยทั่วไปในกฎหมายระหว่างประเทศ แต่ศาลมองว่ามาตรการบังคับทางเศรษฐกิจและการเมืองก็มีความรุนแรงไม่น้อยไปกว่าการใช้กำลังทางทหารเช่นกัน[633] ก่อนหน้าคดี Nicaragua เคยมีการวิฉัยของศาลยุติธรรมระหว่างประเทศในคดี Tehran Hostages เกี่ยวกับความรุนแรงที่เทียบเท่ากับการใช้กำลังทางทหาร ซึ่งคดี Tehran นี้ศาลไม่ได้วินิจฉัยตามหลักของปฏิญญา ค.ศ.1970 แต่ศาลก็มีมุมมองที่ไม่ได้แตกต่างจากคดี Nicaragua เท่าใดนัก ประเด็นสำคัญในคดีนี้เป็นเรื่องการพิจารณาสุนทรพจน์ของอยาตอลลาห์ โคมัยนี (Ayatollah Khomeini) ซึ่งได้แสดงต่อกลุ่มนักศึกษาและกองทัพและนำไปสู่การปิดล้อม

---

[632] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 47-48.

[633] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merit) (1986) ICJ 14, International Court of Justice, para 188.

สถานฑูตสหรัฐอเมริกาในกรุงเตห์ราน ศาลยุติธรรมระหว่างประเทศให้ความเห็นว่า แม้การกล่าวสุนทรพจน์ของโคมัยนีไม่อาจเทียบเท่ากับการใช้กำลัง (force) แต่การแสดงออกดังกล่าวก็นำไปสู่การใช้ความรุนแรงได้ ผลสืบเนื่องจากการกระทำดังกล่าวจึงเป็นการละเมิดต่อข้อ 2 (4) ของกฎบัตรสหประชาชาติได้และการกระทำด้วยการปิดล้อมสถานฑูตอเมริกาก็ถือเป็นการกระทำที่ละเมิดต่ออนุสัญญาเวียนนาว่าด้วยความคุ้มกันทางการฑูต[634]

ลักษณะที่ 2 กรณีที่เกิดการยึดครองอาณาเขตบางส่วนของรัฐแม้จะไม่มีการต่อต้านด้วยอาวุธก็ตาม

การยึดครองอาณาเขตบางส่วนอาจเกิดขึ้นได้ในกรณีที่มีการใช้กำลังฝ่ายเดียวเพื่อการทำสงคราม โดยการที่กองกำลังของรัฐหนึ่งทำการบุกเข้าไปยังดินแดนของอีกรัฐหนึ่งเพื่อความได้เปรียบทางการทหารในข้อพิพาท แม้ฝ่ายที่ถูกยึดครองอาณาเขตนั้นจะมิได้ทำการต่อสู้ป้องกันด้วยอาวุธก็ตาม

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ หมายถึง กรณีการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศอย่างกรณีแรก กล่าวคือเป็นการขัดกันทางอาวุธระหว่างกองกำลังของรัฐกับกองกำลังที่ไม่ใช่รัฐซึ่งอยู่ภายในเขตแดนของรัฐนั้นที่ทำการต่อสู้หรือ การขัดกันทางอาวุธที่เกิดขึ้นภายในดินแดนตนเอง

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศเป็นไปตามเงื่อนไขของข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 และข้อ 1 ของพิธีสารเพิ่มเติมฉบับที่ 2 แห่งอนุสัญญาเจนีวา ค.ศ.1977[635]

---

[634] Case Concerning the United States Diplomatic and Consular Staff in Tehran (United States v. Iran) (1980) 74 AJIL 746, International Court of Justice, para 59.

[635] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 1 — Material field of application

"1. This Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of applications, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.

คือการเผชิญหน้าทางอาวุธของกลุ่มติดอาวุธในดินแดนหนึ่งกลุ่มหรือมากกว่าหนึ่งกลุ่มในดินแดนของรัฐ โดยมีระดับความรุนแรงเกินกว่าเป็นความไม่สงบโดยปกติ โดยฝ่ายที่เกี่ยวข้องในการสู้รบจะต้องมีลักษณะเป็นองค์กรและมีการจัดตั้งอย่างเป็นระบบ

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศเป็นไปตามข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ซึ่งระบุว่า “ในกรณีที่การพิพาทกันด้วยอาวุธอันมิได้มีลักษณะเป็นกรณีระหว่างประเทศเกิดขึ้นในอาณาเขตของอัครภาคีผู้ทำสัญญาฝ่ายหนึ่งฝ่ายใด ภาคีคู่พิพาทแต่ละฝ่ายจะต้องมีความผูกพันที่จะใช้บทบัญญัติต่อไปนี้...”

นิยามของการขัดกันทางอาวุธ ตามข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 นั้น คงกำหนดไว้กว้างๆ เพียงกรณีการขัดกันทางอาวุธที่มิได้มีลักษณะเป็นสงครามระหว่างประเทศ ก็ย่อมถือเป็นสงครามภายในประเทศทั้งหมด แต่ตามข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 นี้ มีบทบัญญัติส่วนต่อมาที่กำหนดให้รัฐภาคีคู่พิพาทจะต้องผูกพันตามข้อกฎหมายดังต่อไปนี้เป็นอย่างน้อย คือ

“...(1) บุคคลซึ่งมิได้เข้าร่วมในการสู้รบโดยตรง รวมทั้งผู้สังกัดในกองทัพซึ่งได้วางอาวุธแล้ว และผู้ซึ่งถูกกันออกจากการต่อสู้ เพราะป่วยไข้ บาดเจ็บ ถูกกักคุม หรือเพราะเหตุอื่นใดก็ได้ ไม่ว่าในพฤติการณ์ใดๆ จะต้องได้รับการปฏิบัติด้วยมนุษยธรรมโดยไม่คำนึงถึงลักษณะความแตกต่างอันเป็นผลเสื่อมเสียเนื่องมาแต่ เชื้อชาติ ผิว ศาสนา หรือความเชื่อถือ เพศ กำเนิด หรือความมั่งมี หรือเหตุอื่นใดที่คล้ายคลึงกัน

เพื่อการนี้ บรรดาการกระทำต่อไปนี้ แก่บุคคลดังกล่าวข้างต้น เป็นอันห้ามและคงห้ามต่อไปไม่ว่า กาละ เทศะใด คือ

(ก) การประทุษร้ายต่อชีวิตและร่างกาย โดยเฉพาะอย่างยิ่งการฆาตกรรมทุกชนิด การตัดทอนอวัยวะส่วนหนึ่งส่วนใด การทำทารุณกรรมและการทรมาน

(ข) การจับตัวไปเป็นประกัน

(ค) การทำลายเกียรติยศแห่งบุคคล โดยเฉพาะอย่างยิ่งการปฏิบัติให้เป็นที่อับอายขายหน้าและเสื่อมทรามต่ำช้า

(ง) การตัดสินลงโทษและการปฏิบัติตามคำตัดสินโดยไม่มีคำพิพากษาของศาลที่ได้ตั้งขึ้นตามระเบียบอันเป็นการให้หลักประกันความยุติธรรมซึ่งอารยชนทั้งหลายยอมรับนับถือว่าเป็นสิ่งซึ่งไม่อาจละเว้นเสียได้

---

2. This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.”

(2) ให้รวบรวมและดูแลรักษาผู้บาดเจ็บ ป่วยไข้

องค์การมนุษยธรรมซึ่งไม่ลำเอียงทางฝ่ายใด เช่น คณะกรรมการกาดระหว่างประเทศอาจเสนอบริการของตนให้แก่ภาคีคู่พิพาทก็ได้

ภาคีคู่พิพาทควรพยายามนำบทบัญญัติอื่นๆ แห่งอนุสัญญาฉบับนี้ทั้งหมดหรือบางส่วนมาใช้บังคับอีกด้วย โดยทำความตกลงกันเป็นพิเศษ

การใช้บทบัญญัติข้างต้นนี้จะไม่กระทบกระเทือนฐานะทางกฎหมายของภาคีคู่พิพาท”

ข้อกฎหมายดังกล่าว เป็นเนื้อหาที่กำหนดให้รัฐภาคีจะต้องปฏิบัติตามหลักการในการให้ความคุ้มครองเหล่านี้แก่บุคคลบางกลุ่ม ปัญหาที่เกิดขึ้นจากการนำข้อกฎหมายนี้มาใช้อย่างน้อยมี 2 ประการคือ ได้แก่ ประการแรก เมื่อรัฐมีหน้าที่ในการให้ความคุ้มครองแก่บุคคลที่กฎหมายกำหนดแล้ว กองกำลังที่ไม่ใช่รัฐและเป็นฝ่ายต่อสู้กับรัฐจะมีหน้าที่ประการใดบ้าง ประการที่สอง รัฐมีหน้าที่เฉพาะตามที่ปรากฏในข้อ 3 นี้เท่านั้นหรือไม่ เพราะกฎหมายข้อนี้ใช้คำว่าอย่างน้อย เนื้อหากฎหมายส่วนอื่นในอนุสัญญาเจนีวาจะมีการนำมาใช้งานหรือไม่ เพียงใด

อย่างไรก็ดี ในปี ค.ศ.1977 คณะกรรมการกาชาดระหว่างประเทศได้ออกพิธีสารเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 มา 2 ฉบับ โดยฉบับที่ 1 เป็นข้อกฎหมายเพิ่มเติมเนื้อหาเกี่ยวกับการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ และฉบับที่ 2 ว่าด้วยเนื้อหาเพิ่มเติมเรื่องการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

ในพิธีสารฉบับที่ 2 ซึ่งว่าด้วยเรื่องการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศนี้ มีการกำหนดลักษณะของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศซึ่งจะตกอยู่ในบังคับของพิธีสารฉบับที่ 2 นี้ หมายถึง ข้อพิพาททางอาวุธที่เกิดขึ้นในอาณาเขตของภาคี ระหว่างกองทัพของตนและกองกำลังของฝ่ายต่อต้าน หรือกลุ่มกองกำลังที่ได้มีการจัดตั้งขึ้นอื่นๆ ซึ่งอยู่ภายใต้อำนาจการบังคับบัญชาที่รับผิดชอบ และสามารถควบคุมอาณาเขตส่วนหนึ่งของภาคีนั้น จนทำให้กองกำลังดังกล่าวสามารถปฏิบัติการทางทหารได้อย่างต่อเนื่องและพร้อมเพรียง สถานการณ์ดังกล่าวจะอยู่ในบังคับของพิธีสารเพิ่มเติมฉบับที่ 2 ค.ศ.1977 ทั้งนี้ไม่รวมสถานการณ์ความยุ่งยากภายในและความตึงเครียดต่างๆ เช่น การจลาจล การใช้กำลังรุนแรงที่เกิดขึ้นเป็นครั้งคราวและไม่ต่อเนื่อง[636]

องค์ประกอบของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศตามพิธีสารเพิ่มเติมฉบับที่ 2 นี้จึงได้แก่

---

[636] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 3.

1) ข้อพิพาททางอาวุธที่เกิดขึ้นในอาณาเขตของภาคี ระหว่างกองทัพของตนและกองกำลังของฝ่ายต่อต้าน หรือกลุ่มกองกำลังที่ได้มีการจัดตั้งขึ้นอื่นๆ

2) กองกำลังดังกล่าวอยู่ภายใต้อำนาจการบังคับบัญชาที่รับผิดชอบ

3) กองกำลังดังกล่าวสามารถควบคุมอาณาเขตส่วนหนึ่งของภาคีนั้น

4) กองกำลังดังกล่าวสามารถปฏิบัติการทางทหารได้อย่างต่อเนื่องและพร้อมเพรียง

โดยเนื้อหาดังกล่าวของพิธีสารเพิ่มเติมฉบับที่ 2 ทำให้สงครามภายในจะเกิดขึ้นได้ และอยู่ในบังคับของกฎหมาย (พิธีสารเพิ่มเติม) ก็ต่อเมื่อเป็นไปตามองค์ประกอบดังกล่าวเท่านั้น ซึ่งค่อนข้างมีความเฉพาะเจาะจงกว่าข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 นอกจากนั้นเนื้อหาของกฎหมายตามพิธีสารเพิ่มเติม ฉบับที่ 2 นี้ก็มีค่อนข้างมาก เพราะเป็นการขยายความเพิ่มเติมขึ้นมาจากเนื้อหาข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 แต่ก็ตามมาด้วยปัญหาประการสำคัญคือ พิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 2 นี้จะมีผลผูกพันเฉพาะกับรัฐที่เป็นภาคีเท่านั้น จึงก่อให้เกิดปัญหา 2 ประการ คือ ปัญหาประการที่ 1 ตัวตนที่จะเข้าเป็นภาคีตามพิธีสารระหว่างประเทศได้จะต้องเป็นรัฐหรือองค์การระหว่างประเทศเท่านั้น แต่ตัวตนที่ไม่ใช่รัฐย่อมไม่สามารถเข้าร่วมเป็นภาคีของพิธีสารระหว่างประเทศได้ จึงตามมาด้วยปัญหาประการที่ 2 คือ เมื่อตัวตนที่ไม่ใช่รัฐไม่สามารถเป็นภาคีตามพิธีสารได้ กองกำลังที่ไม่ใช่รัฐเหล่านั้นก็ย่อมไม่มีหน้าที่ปฏิบัติตามกฎหมายใช่หรือไม่

ปัญหาประการที่ 1 มีทางออกว่าแม้รัฐและองค์การระหว่างประเทศเท่านั้นที่จะสามารถเข้าร่วมเป็นภาคีพิธีสารระหว่างประเทศได้ กองกำลังที่ไม่ใช่รัฐไม่สามารถเป็นภาคีในพิธีสารระหว่างประเทศได้ แต่หลักเกณฑ์บางประการก็อาจได้รับการยอมรับให้ปฏิบัติเป็นการทั่วไปเช่นกฎหมายระหว่างประเทศ ในลักษณะการเป็นจารีตประเพณีระหว่างประเทศแล้ว ดังนั้น หากกองกำลังที่ไม่ใช่รัฐไม่ปฏิบัติตามหลักเกณฑ์ในการทำสงครามก็ย่อมมีความรับผิดชอบตามกฎหมายระหว่างประเทศเช่นกัน

ปัญหาประการที่ 2 หลักการตามอนุสัญญาเจนีวา ค.ศ.1949 เป็นกฎหมายที่ไม่ได้อาศัยหลักต่างตอบแทน ดังนั้นไม่ว่ากองกำลังที่ไม่ใช่รัฐจะดำเนินการอย่างไร กองทัพของรัฐก็จะต้องปฏิบัติตามหลักกฎหมายมนุษยธรรมระหว่างประเทศที่ปรากฏตามอนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติม ค.ศ.1977 เช่นเดิม และคำตอบเดียวกันที่จะตามมาคือ กรณีที่หลักเกณฑ์บางประการได้รับการยอมรับให้เป็นจารีตประเพณีระหว่างประเทศแล้ว ดังนั้น หากกองกำลังที่ไม่ใช่รัฐไม่ปฏิบัติตามหลักเกณฑ์ในการทำสงครามก็ย่อมมีความรับผิดชอบตามกฎหมายระหว่างประเทศเช่นกัน

ปัญหาประการสำคัญของการใช้ไซเบอร์เพื่อการโจมตีคือการโจมตีทางไซเบอร์จะถือเป็นการใช้กำลังทางทหารระหว่างรัฐได้หรือไม่ การพิจารณาปัญหาดังกล่าวจะต้องคำนึงถึงองค์ประกอบ 2 ประการ คือ 1) ปฏิบัติการทางไซเบอร์เพื่อการโจมตีนั้นเกิดขึ้นโดยเป็นปฏิบัติการของรัฐหรือไม่ และ 2) ปฏิบัติการทางไซเบอร์นั้นเทียบเท่ากับ “การใช้กำลังทางทหาร” อย่างไร

ปฏิบัติการใดเป็นปฏิบัติการของรัฐหรือไม่ย่อมต้องพิจารณาจากผู้ที่มีส่วนเกี่ยวข้องกับปฏิบัติการนั้นว่าเป็นการกระทำของรัฐหรือไม่ ซึ่งตามกฎหมายมนุษยธรรมระหว่างประเทศนั้นการกระทำดังกล่าวจะต้องเป็นการกระทำของทหารซึ่งสังกัดในกองทัพของรัฐหรือบุคลากรในลักษณะที่เป็นพลรบ แต่เนื่องด้วยลักษณะการทำงานของระบบไซเบอร์ซึ่งอยู่ในพื้นที่อิเล็กทรอนิกส์ที่พลเรือนและทหารต่างใช้ร่วมกัน ปัญหาของการใช้ปฏิบัติการทางไซเบอร์จึงเป็นเรื่องการพิสูจน์ว่าผู้ปฏิบัติการนั้นเป็นทหารของรัฐหรือเป็นพลเรือน ในทางปฏิบัตินั้นอาจมีการพิสูจน์ต้นทางการปฏิบัติการในเครือข่ายไซเบอร์ได้ โดยพิสูจน์จาก IP address ของคอมพิวเตอร์เครื่องนั้นว่ามาจากที่ใด แต่ปัญหาก็จะเกิดขึ้นอีกว่า หากพลเรือนแอบเข้าไปใช้งานระบบคอมพิวเตอร์ทางทหารหรือทหารใช้คอมพิวเตอร์พลเรือนเพื่อปฏิบัติการโจมตี ผู้ใดหรือวิธีการใดจึงจะสามารถพิสูจน์ได้ว่าผู้ปฏิบัติการที่แท้จริงคือใคร เป็นต้น

ปัญหาว่าการใช้กำลังทางทหารมีขอบเขตเพียงใด ศาลอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวียให้ความเห็นเพิ่มเติมว่านอกจากปฏิบัติการที่กระทำโดยทหารแล้ว ปัจเจกชนที่กระทำการภายในขอบเขตเกี่ยวกับกองกำลังทหารหรือสมรู้ร่วมคิดกับหน่วยงานของรัฐ อาจจัดว่าเป็นองค์กรของรัฐโดยพฤตินัยได้[637] ดังนั้นขอบเขตการกระทำที่ถือว่าเป็นการใช้กำลังทางทหารย่อมรวมถึงทั้งทหารและพลเรือนที่ทำหน้าที่แทนกองกำลังทางทหารด้วย[638]

การพิจารณาย้อนกลับไปสู่ปัญหาซึ่งเกิดขึ้นในองค์ประกอบที่ 1 ว่าจะตรวจสอบอย่างไรว่าการกระทำของพลเรือนนั้นเป็นการทำหน้าที่แทนกองกำลังทหารของรัฐ หากมีการปฏิเสธของรัฐว่าไม่เกี่ยวข้องกับปฏิบัติการของพลเรือนดังกล่าว หรือไม่สามารถหาหลักฐานพิสูจน์ถึงความสัมพันธ์ระหว่างปฏิบัติการของพลเรือนกับรัฐได้ การโจมตีทางไซเบอร์นั้นย่อมไม่ก่อให้เกิดลักษณะของการขัดกันทางอาวุธได้เช่นกัน เช่น กรณีการโจมตีทางไซเบอร์ซึ่งเกิดขึ้นที่เมืองทาลลินน์ ประเทศเอสโตเนีย พิสูจน์ได้เพียงว่าเป็นปฏิบัติการของกลุ่มแฮคเกอร์ที่ชาวรัสเซีย แต่ไม่สามารถเชื่อมโยงถึง

---

[637] Prosecutor v. Dusko Tadic, *(Appeal Judgement)*, Case it-94-1-A, 15 July 1999, para 144.

[638] อุบลวรรณ ภีระเป็ง, การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ: ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2558, หน้า 90.

การสั่งการหรือกระทำการแทนรัฐได้ จึงไม่อาจระบุได้ว่าเป็นการสร้างลักษณะการขัดกันทางอาวุธ คงเป็นได้เพียงการโจมตีทางไซเบอร์ปกติของพลเรือนเท่านั้น

คำอธิบายของคณะกรรมการกาชาดระหว่างประเทศให้ความสำคัญกับเงื่อนไขการใช้กำลังทางทหารในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ แต่ในคำพิพากษาศาลยุติธรรมระหว่างประเทศคดี Tadic มีความเห็นว่าการใช้กำลังทางทหารนั้นถือเป็นเงื่อนไขสำคัญของทั้งการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ[639] สิ่งที่แตกต่างกันคือในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศนั้นจะไม่มีการพิจารณาถึงความรุนแรงของการขัดกันทางอาวุธ ในขณะที่การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะมีการพิจารณาเรื่องความรุนแรงของการขัดกันทางอาวุธประกอบด้วย ทั้งนี้ก็เนื่องมาจาก ลักษณะของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศนั้นจะไม่ใช้กับกรณีความไม่สงบเรียบร้อยภายในประเทศ (Internal Disturbances) และความตึงเครียดภายในประเทศ (Internal Tensions) เช่น กรณีการประท้วงภายในประเทศ[640] เฉพาะการต่อสู้ที่รุนแรงเกินกว่าความไม่สงบเรียบร้อยภายในเท่านั้นจึงจะเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้

มุมมองของผู้เชี่ยวชาญซึ่งมีส่วนร่วมในการจัดทำคู่มือทาลลินน์ว่าด้วยกฎหมายระหว่างประเทศซึ่งปรับใช้สงครามทางไซเบอร์เห็นว่าการโจมตีทางไซเบอร์มีผลเทียบเท่ากับปฏิบัติการทางทหารได้ โดยในข้อ 20 วรรค 1 ของคู่มือทาลลินน์กำหนดว่ากฎหมายว่าด้วยการขัดกันทางอาวุธสามารถปรับใช้ได้กับปฏิบัติการทางไซเบอร์ซึ่งดำเนินอยู่ภายใต้ของบริบทการขัดกันทางอาวุธ[641] ซึ่งหากพิจารณาจากข้อ 20 นี้แล้วจะพบว่าเป็นหลักการที่ไม่ได้ช่วยให้การวิเคราะห์ว่าปฏิบัติการทางทหารนี้จะก่อให้เกิดการขัดกันทางอาวุธได้หรือไม่เลย หลักการนี้เพียงแต่ยืนยันว่าปฏิบัติการทางไซเบอร์มีผลเสมือนเป็นวิธีหรือปัจจัยในการขัดกันทางอาวุธได้ หากทหารเป็นผู้ใช้ปฏิบัติการทางไซเบอร์ก็มีผลเท่ากับเป็นส่วนหนึ่งของการขัดกันทางอาวุธเท่านั้น

สิ่งที่น่าสนใจคือผู้เชี่ยวชาญที่มีบทบาทสำคัญในการจัดทำคู่มือทาลลินน์ Michael N. Schmitt เคยเขียนบทความเรื่องหนึ่งชื่อ “Wired Warfare: Computer Network Attack and Jus

---

[639] คำพิพากษาคดี Tadic พิจารณาว่าการใช้กำลังทางทหารเป็นลักษณะโดยปกติของการขัดกันทางอาวุธทั้งที่มีลักษณะระหว่างประเทศและไม่มีลักษณะระหว่างประเทศ ทั้งนี้โดยการอ้างอิงถึงเหตุการณ์ที่เกิดขึ้นในบอลข่าน (Balkans)

[640] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Art. 1 (2).

[641] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013), Rule 20.

in Bello" ในบทความนี้ Schmitt มีความเห็นว่าเฉพาะกรณีการโจมตีทางไซเบอร์ที่ก่อให้เกิดผลทางกายภาพเท่านั้นจึงจะถือว่าเทียบเท่ากับปฏิบัติการทางทหารได้ โดยให้พิจารณาจากความเสียหายที่เกิดขึ้นซึ่งกระทบต่อชีวิต ร่างกาย หรือทรัพย์สิน (Scale and Effect)[642] แนวคิดนี้ของ Schmitt น่าจะมีผลไม่น้อยต่อการเขียนหลักการข้อ 20 ของคู่มือทาลลินน์ คือไม่ได้กำหนดให้ชัดเจนว่าปฏิบัติการทางไซเบอร์ที่เทียบเท่ากับปฏิบัติการทางทหารนี้จะนำไปสู่การเกิดการขัดกันทางอาวุธหรือไม่ เพราะผลที่เกิดจากปฏิบัติการทางไซเบอร์อาจมีได้ค่อนข้างหลากหลาย ในขณะที่ปฏิบัติการทางไซเบอร์โดยทหารซึ่งเกิดขึ้นขณะที่มีการขัดกันทางอาวุธสามารถยอมรับว่าเป็นส่วนหนึ่งในปฏิบัติการทางทหารได้ง่ายกว่า เพราะอย่างน้อยที่สุดปฏิบัติการทางไซเบอร์ย่อมเป็นวิธีการในการขัดกันทางอาวุธได้

โดยทั่วไปการใช้กำลังทางทหารนั้นค่อนข้างเป็นที่ยอมรับว่าหมายรวมถึงทั้งรูปแบบการใช้กำลังโดยตรง และการใช้รูปแบบอื่นทางอ้อม เช่นการสนับสนุนการใช้กำลังทางทหารด้วย[643] ดังนั้นการปฏิบัติการทางไซเบอร์ไม่ว่าโดยทางตรงหรือทางอ้อม หากเป็นผลให้เกิดความบาดเจ็บหรือการเสียชีวิต หรือก่อให้เกิดความเสียหายแก่ทรัพย์สินก็ย่อมเทียบเท่ากับการใช้กำลังทางทหาร ทั้งนี้ความเห็นของนักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายคนค่อนข้างสอดคล้องกับแนวคิดของ Schmitt คือยอมรับการปฏิบัติการทางไซเบอร์ว่าจะเป็นการใช้กำลังทางทหารได้ต่อเมื่อความเสียหายที่เกิดขึ้นจะต้องมีลักษณะทางกายภาพด้วย มิเช่นนั้นย่อมจะเป็นการพิสูจน์ได้ยากว่าปฏิบัติการทางไซเบอร์ดังกล่าวส่งผลกระทบต่อบุคคลที่กฎหมายคุ้มครองอย่างไร[644]

ความเห็นอื่นๆ ที่สนับสนุนแนวคิดเรื่องผลทางกายภาพของปฏิบัติการทางไซเบอร์ได้แก่ Cordula Droege นักวิชาการทางด้านกฎหมายมนุษยธรรมระหว่างประเทศ ผู้เชี่ยวชาญด้านกฎหมายของคณะกรรมการกาชาดระหว่างประเทศให้ความเห็นว่าหากการใช้งานไซเบอร์เพื่อการโจมตีก่อให้เกิดผลร้ายแรงเป็นอันตรายถึงตายได้ (Kinetic Force) ย่อมถือเป็นการกระทำที่เทียบเท่ากับการใช้กำลังทางทหารได้เช่นกัน เช่นการใช้งานระบบไซเบอร์ในการสั่งงานให้เครื่องบินตก หรือรถไฟชนกัน อย่างไรก็ดีการใช้งานไซเบอร์เพื่อการโจมตีโดยทั่วไปนั้นมักไม่ก่อให้เกิดผลร้ายแรงในทางกายภาพจึงถือไม่ได้ว่าเป็นการกระทำที่เสมือนปฏิบัติการทางทหารของรัฐ ดังนั้นปัจจัยที่จะต้อง

---

[642] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," International Review of the Red Cross, Vol 84, No 846, (June 2002): 397.

[643] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 123.

[644] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 123.

พิจารณาเป็นสำคัญคือเรื่องเป้าหมายในการกระทำการว่าเป็นการกระทำต่อกองกำลังทางทหารของรัฐหรือไม่ และการใช้ระบบไซเบอร์เพื่อการโจมตีนั้นก่อให้เกิดผลกระทบต่อโครงสร้างสำคัญทางการทหารและพลเรือนเช่นเดียวกับการโจมตีด้วยอาวุธหรือไม่ เป็นสำคัญ[645]

ปัญหาว่าปฏิบัติการทางไซเบอร์เกิดขึ้นบนพื้นที่ทางอิเล็กทรอนิกส์ปัจจัยด้านภูมิศาสตร์เข้ามาเกี่ยวข้องจะทำให้การวิเคราะห์ประเด็นการใช้กำลังทางทหารนี้ได้รับผลกระทบหรือไม่นั้น หากเปรียบเทียบกับแนวทางคำพิพากษาของศาลยุติธรรมระหว่างประเทศในคดี Corfu Channel จะพบว่าศาลยุติธรรมระหว่างประเทศวินิจฉัยว่าการที่อัลแบเนียทำการวางทุ่นระเบิดในช่องแคบคอร์ฟูทำให้เรือรบอังกฤษซึ่งผ่านเส้นทางดังกล่าวเสียหายนั้น เป็นการกระทำที่ละเมิดต่อหลักกฎหมายระหว่างประเทศ เพราะการปฏิเสธสิทธิในการผ่านไปสู่น่านน้ำสากลเป็นสิ่งต้องห้าม[646] หากเทียบกับกรณีการโจมตีทางไซเบอร์ต่อเว็บไซต์ด้วยปฏิบัติการปฏิเสธการเข้าถึงบริการ (DDoS) ย่อมมีลักษณะที่ไม่แตกต่างกัน เพราะเป็นการจำกัดการเข้าถึงช่องทางสากล ดังนั้น ปัจจัยทางด้านภูมิศาสตร์อาจไม่สำคัญเท่ากับลักษณะของการกระทำที่ก่อให้เกิดความเสียหายซึ่งรวมถึงการจำกัดการใช้ช่องทางสากลด้วย อย่างไรก็ดีสิ่งที่ศาลได้นำมาใช้ในการพิจารณาคดี Corfu Channel นั้น เกี่ยวข้องกับหลักการตามกฎหมายทะเลในขณะที่หากจะนำแนวทางดังกล่าวมาใช้กับปฏิบัติการทางไซเบอร์ก็จะต้องมีฐานตามกฎหมายระหว่างประเทศที่สามารถปรับใช้ได้ ซึ่งย่อมแตกต่างจากคดี Corfu Channel

กรณีการใช้เทคโนโลยีอื่นๆ ก็พบว่ามีการใช้งานอุปกรณ์ที่มีลักษณะร่วมกันของทหารและพลเรือนมากขึ้น โดยผู้ใช้งานเทคโนโลยีก็เป็นกลุ่มที่มีความหลาหหลายมากขึ้น โดยเฉพาะอย่างยิ่งการใช้อากาศยานไร้คนขับเพื่อการโจมตี มีหลายกรณีที่อากาศยานไร้คนขับถูกใช้โดยกลุ่มที่ไม่ใช่รัฐ ตัวอย่างเช่น กรณีเหตุการณ์วันที่ 13 มกราคม ค.ศ.2006 มีรายงานว่าหน่วยข่าวกรองของสหรัฐอเมริกา (The United States Central Intelligence Agency) ได้ใช้อากาศยานสังหารแบบไร้คนขับ (Predator Drone) ยิงขีปนาวุธโจมตีเป้าหมายซึ่งคาดว่าเป็นกลุ่มผู้ก่อการร้ายในเขตพื้นที่เมืองดามาโดลา (Damadola) ของประเทศปากีสถานใกล้เขตพรมแดนประเทศอัฟกานิสถาน[647] โดยก่อน

---

[645] อุบลวรรณ ภีระเป็ง, การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ: ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ, หน้า 105.

[646] Corfu Channel Case *(UK v. Albania) (Merit)* (1949) ICJ Reports 4, International Court of Justice, para 29.

[647] Dafna Linzer and Griff Witte, "U.S. Airstrike Targets Al Qaeda's Zawahiri", Washington Post, 14 January 2006. [online] Accessed December 10, 2020. Available from: https://www.washingtonpost.com/archive/politics/2006/01/14/us-airstrike-targets-al-qaedas-zawahiri/235b61c5-0c8d-477d-868c-54565c3f30fa/

การโจมตีนั้นได้มีการระบุว่าเป้าหมายดังกล่าวเป็นที่อยู่ของเป้าหมายระดับสูงของ Al Qaeda แต่ปรากฏว่าข้อมูลผิดพลาด ภารกิจทำลายเป้าหมายจึงล้มเหลว แต่การโจมตีดังกล่าวเป็นผลให้ประชาชนเสียชีวิตราว 18 คน โดยกองทัพสหรัฐอเมริกาได้ปฏิเสธความเกี่ยวข้องกับปฏิบัติการดังกล่าว[648]

ในสถานการณ์การใช้อากาศยานไร้คนขับเพื่อการโจมตีนี้ค่อนข้างแตกต่างจากปฏิบัติการทางไซเบอร์เพื่อการโจมตีอยู่ค่อนข้างมาก เพราะการระบุตัวตนผู้ปฏิบัติการทางไซเบอร์เป็นเรื่องที่ค่อนข้างยาก แต่การควบคุมอากาศยานไร้คนขับนั้นแม้จะมีระยะห่างระหว่างผู้ควบคุมอากาศยานและตัวอากาศยานก็ตาม แต่การพิสูจน์ความสัมพันธ์ระหว่างอากาศยานไร้คนขับกับผู้ควบคุมหรือผ็ที่เกี่ยวข้องกับอากาศยานนั้นอาจกระทำได้ง่ายกว่า ทั้งนี้อยู่ในเงื่อนไขว่าจะต้องทำลายอากาศยานหรือควบคุมอากาศยานไร้คนขับนั้นได้ก่อน ประเด็นการปฏิบัติการของหน่วยข่าวกรองสหรัฐอเมริกาซึ่งโจมตีเป้าหมายในประเทศปากีสถานนั้นไม่มีการทำลายอากาศยานไร้คนขับโดยฝ่ายที่ถูกโจมตีจึงไม่สามารถระบุความสัมพันธ์ระหว่างอากาศยานไร้คนขับกับหน่วยงานใดได้ แต่เรื่องนี้ก็ไม่ได้แตกต่างจากกรณีการโจมตีด้วยอาวุธทั่วไป เช่น การวางระเบิดเพื่อการก่อการร้าย ที่เมื่อมีการกล่าวหาผู้กระทำความผิดก็มักจะมีการปฏิเสธความรับผิดชอบเสมอ การพิสูจน์ความสัมพันธ์ระหว่างการใช้อากาศยานไร้คนขับจึงแตกต่างจากปฏิบัติการทางไซเบอร์อยู่ค่อนข้างมาก

นอกจากการใช้งานอากาศยานไร้คนขับโดยกลุ่มกองกำลังของรัฐแล้วยังพบว่ากลุ่มก่อการร้ายก็นิยมการใช้อากาศยานไร้คนขับเพื่อการโจมตีเช่นกัน เช่น เหตุการณ์ในปี ค.ศ. 1994 กลุ่มโอมซินริเคียว (Aum Shinrikyo) ในประเทศญี่ปุ่นใช้เฮลิคอปเตอร์บังคับวิทยุทำการปล่อยแก๊สซารินในที่สาธารณะแต่ภารกิจไม่สำเร็จเนื่องจากเฮลิคอปเตอร์ดังกล่าวประสบอุบัติเหตุตก[649] เหตุการณ์ในปี ค.ศ.2013 กลุ่มฮามาสในปาเลสไตน์ได้ควบคุมอากาศยานไร้คนขับบรรทุกวัตถุระเบิดบินเข้าไปในเขตของอิสราเอลแต่ถูกสกัดเอาไว้ได้ก่อน[650] และเหตุการณ์ในปี ค.ศ.2014 กลุ่ม Islamic State: IS ใช้

---

[648] Ibid.

[649] Robert j. Bunker, Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications. Carlisle, (Pennsylvania: Strategic Studies Institute U.S. Army War College, 2015), p. 7. [online] Accessed December10, 2020. Available from: https://apps.dtic.mil/sti/citations/ADA623134

[650] Ibid., p. 11.

อากาศยานไร้คนขับเชิงพาณิชย์และอากาศยานไร้คนขับประดิษฐ์เอง เพื่อปฏิบัติการทางทหารในประเทศอิรักและซีเรีย[651] เป็นต้น

3.3 การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่

กฎหมายมนุษยธรรมระหว่างประเทศมีเป้าหมายในการควบคุมปฏิบัติการทางทหารในการรบ จึงเป็นกฎหมายที่มุ่งควบคุมการกระทำของบุคคลในการรบเป็นสำคัญ การควบคุมการกระทำของบุคคลจึงต้องรวมถึงการใช้อาวุธ การใช้วิธีการในการรบ รวมตลอดถึงการกำหนดมาตรการในการป้องกันผลที่อาจก่อให้เกิดความเสียหายต่อบุคคลและทรัพย์สิ่งของที่กฎหมายมุ่งคุ้มครอง กฎหมายมนุษยธรรมระหว่างประเทศจึงวางหลักการเอาไว้เป็นลักษณะทั่วไปเพื่อให้กฎหมายมีความยืดหยุ่นเพียงพอต่อการปรับใช้ในสถานการณ์ที่หลากหลายได้ การปรับใช้หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธอาจพิจารณาได้ดังนี้

3.3.1 การจำกัดปัจจัยและวิธีการในสงคราม

วิธีการ (Methods) และปัจจัย (Means) ในสงครามมีความหมายรวมถึงอาวุธ การใช้อาวุธและวิธีการที่เกี่ยวข้องกับการใช้อาวุธและวิธีการทำรบ กฎหมายมนุษยธรรมระหว่างประเทศจำกัดการใช้ปัจจัยและวิธีการในสงครามเพื่อไม่ให้การขัดกันทางอาวุธนั้นเป็นไปโดยไร้ข้อจำกัด การขัดกันทางอาวุธหรือสงครามจะต้องกระทำเท่าที่เป็นความจำเป็นทางทหารเพื่อมุ่งต่อผลแพ้ชนะทางทหารในสงครามเท่านั้น คำว่าความจำเป็นทางทหารนั้นไม่มีความหมายที่ชัดเจนในตัวเองจึงต้องมีการสร้างหลักการเพื่อกำหนดขอบเขตของการกระทำลักษณะต่างๆ ให้สอดคล้องกับความจำเป็นทางการทหาร โดยในพิธีสารฉบับที่ 1 เพื่อเพิ่มเติมอนุสัญญาเจนีวาได้นำเอาแนวคิดของกฎหมายว่าด้วยการขัดกันทางอาวุธในยุคก่อนหน้าอนุสัญญาเจนีวา ค.ศ.1949 มาจำกัดการทำสงคราม โดยเน้นที่คำสำคัญ 2 ประการคือปัจจัย (Means) และวิธีการ (Methods) ในการทำสงครามและกำหนดให้การใช้ปัจจัยและวิธีการในการขัดกันทางอาวุธหรือสงครามนั้นจะต้องไม่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น (Superfluous Injuries and Unnecessary Suffering)

---

[651] Joby Warrick, “Use of Weaponized Drones by Isis Spurs Terrorism Fears,” *Washington Post*, 21 February 2017. [online] accessed May 10, 2021. Available from: https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017 /02/21/ 9d83d51e-f382-11e6-8d72-263470bf0401_story.html,

การจำกัดปัจจัยและวิธีการในสงครามเริ่มขึ้นมาจากความพยายามในการจำกัดการใช้อาวุธในสงครามโดยในยุคสงครามโลกครั้งที่ 1 ช่วงปี ค.ศ.1917 เริ่มมีการใช้แก๊สพิษเป็นที่แพร่หลายในการทำสงครามแก่แก๊สน้ำตาและแก๊สคลอรีน โดยแก๊สคลอรีนนั้นมีฤทธิ์ส่งผลต่อระบบการหายใจของมนุษย์โดยตรงก่อให้เกิดสภาวะขาดออกซิเจนเฉียบพลัน (Asphyxia) และทำให้เสียชีวิตได้ นอกจากนั้นยังมีการใช้แก๊สมัสตาร์ด (Mustard Gas or Sulfur Mustard) ด้วย[652] ในการประชุมที่เฮกก็มีความตระหนักถึงปัญหาการใช้แก๊สพิษและกำหนดเป็นข้อห้ามในการทำสงครามก่อนล่วงหน้าแล้ว แต่เมื่อเข้าสู่ยุคสงครามโลกครั้งที่ 1 อาวุธแก๊สพิษกลับเป็นที่แพร่หลายเสมือนว่าข้อห้ามที่เกิดขึ้นในสังคมระหว่างประเทศนั้นไม่มีผลบังคับในสถานการณ์สงครามแต่อย่างใด

พัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศในช่วงเริ่มต้นไปในทิศทางเดียวว่าปฏิบัติการทางทหารในยามสงครามที่เป็นไปโดยความจำเป็นนี้จะต้องเคารพต่อหลักมนุษยธรรมคือการไม่ก่อให้เกิดความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นเท่านั้นและหลักการนี้จะกลายเป็นสิ่งที่ปรากฏในพิธีสารเพิ่มเติม ฉบับที่ 1 ของอนุสัญญาเจนีวา ค.ศ.1977[653]

แม้จะมีความพยายามสร้างกฎหมายที่เกี่ยวข้องกับการรบทางบกมาช่วงระยะเวลาหนึ่ง แต่ก็ยังไม่มีกฎหมายระหว่างประเทศที่เป็นลายลักษณ์อักษรอย่างเป็นรูปธรรม จนกระทั่งในปี ค.ศ.1907 มีการประชุมว่าด้วยสันติภาพที่กรุงเฮก (Hague Peace Conference) และมีการอนุวัติการอนุสัญญาเฮก ฉบับที่ 4 ซึ่งได้รับการยอมรับอย่างกว้างขวางว่าเป็นอนุสัญญาระหว่างประเทศที่เป็นการประกาศจารีตประเพณีเกี่ยวกับการทำสงครามที่มีมาแต่เดิม[654] อนุสัญญาเฮกฉบับที่ 4 นี้พยายามอ้างอิงถึงความเป็นอารยะกับการสร้างหลักมนุษยธรรมในสงคราม โดยหลักการสำคัญของการทำสงครามรู้จักกันเป็นการทั่วไปในชื่อหลักมาร์ติน (Marten's clause) ซึ่งต้องการให้การขัดกันทางอาวุธ หรือการสงครามนั้นจะต้องคำนึงถึงความมีมนุษยธรรมอยู่ด้วย โดยความมีมนุษยธรรมเช่นว่านั้นจะต้องเป็นบงการของจิตสำนึกสาธารณะด้วย (Dictates of Public conscience)[655] คำว่า "บงการของจิตสำนึก

---

[652] Boothby, W., Weapons and the Law of Armed Conflict, p. 33.

[653] Ibid.

[654] Adam Roberts, "The Equal Application of the Law of War: A Principle under Pressure," International Review of the Red Cross, Vol. 90, No. 872, (December 2008): 942-943. [online] Accessed: June 10, 2022. Available from: https://international-review.icrc.org/sites/default/files/irrc-872-6.pdf

[655] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899. Para 9. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-ii-1899/preamble?activeTab=undefined

สาธารณะ” หรือ Dictates of public conscience นี้ค่อนข้างสื่อไปในลักษณะการสร้างองค์ประกอบทางศีลธรรมขึ้นมาเป็นการเฉพาะในกฎหมายว่าด้วยการขัดกันทางอาวุธ[656] แต่หากตีความโดยคำนึงถึงบริบทการเกิดขึ้นของ “จารีตประเพณี” ทางกฎหมาย ก็อาจพิจารณาได้ว่า dictates of public conscience นี้น่าจะเป็นความรับรู้ร่วมกันของสาธารณะซึ่งเป็นพัฒนาการของจารีตประเพณี (Custom) ก่อนจะมีการบัญญัติเป็นกฎหมาย[657]

ในขณะที่ Professor Dinstein มีข้อสังเกตว่าหลักมนุษยธรรมที่ปรากฏในอารัมภบทของอนุสัญญาเฮก ฉบับที่ 4 ซึ่งอ้างอิงถึง dictates of public conscience นี้ไม่เกี่ยวข้องโดยตรงกับกฎหมายว่าด้วยการขัดกันทางอาวุธในเรื่องความชอบด้วยกฎหมายของการใช้อาวุธในสงคราม แต่ dictates of public conscience น่าจะเกี่ยวข้องกับลักษณะโดยทั่วไปของหลักการกระทำอันเป็นปรปักษ์ (Conduct of hostilities) มากกว่า[658] ความเห็นของ Professor Dinstein อาจอธิบายได้ว่าการใช้อาวุธตามหลักการมาร์ตินที่จะต้องจะต้องคำนึงถึงความมีมนุษยธรรมพร้อมไปกับบงการของจิตสำนึกสาธารณะเกี่ยวข้องกับการกระทำของทหารว่าควรปฏิบัติการอยู่ในเงื่อนไขความเหมาะสมระดับใด การกระทำใดเป็นการต้องห้ามเพราะเกินขอบเขตความจำเป็นทางการทหาร แต่หลักมาร์ตินนี้ไม่ได้บอกว่าอาวุธใดใช้ได้หรือไม่ เพราะหลักการมาร์ตินเป็นหลักเกี่ยวกับปฏิบัติการทางทหารไม่ใช่หลักกฎหมายควบคุมอาวุธ

กฎเกณฑ์พื้นฐานข้อ 35 เกี่ยวกับวิธีการและปัจจัยในการทำสงคราม กำหนดว่าในการขัดกันทางอาวุธนั้นมีข้อจำกัด โดยข้อจำกัดได้แก่ การห้ามใช้อาวุธ กระสุน วัตถุ และวิธีการทำสงครามในลักษณะที่ก่อให้เกิดการบาดเจ็บเกินสมควรหรือความทุกข์ทรมานเกินความจำเป็น รวมตลอดถึงการใช้วิธีการหรือปัจจัยในการทำสงครามที่จะทำให้สภาพแวดล้อมทางธรรมชาติเสียหายในลักษณะขยายเป็นวงกว้าง มีระยะเวลายาวนาน และมีลักษณะรุนแรง[659]

---

[656] Theodor Meron, "The Martens Clause, Principles of Humanity, and Dictates of Public Conscience," The American Journal of International Law, Vol. 94, No. 1, (January 2000): 78–89, [online] Accessed: June 10, 2022. Available from: https://www.jstor.org/stable/2555232

[657] William Boothby, Weapons, and the Law of Armed Conflict, p. 14.

[658] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 57.

[659] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 35 Basic Rules “

1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.

กฎเกณฑ์ข้อ 35 นี้เป็นกฎเกณฑ์ที่มีความกว้างขวาง ครอบคลุมต่อการจำกัดทั้งการใช้อาวุธ และสิ่งที่ไม่ใช่อาวุธ คือทั้งวิธีการและปัจจัยอื่นๆ ที่เกี่ยวข้องกับการทำสงคราม ดังนั้นเทคโนโลยีใหม่ซึ่งมีการนำมาใช้ในการขัดกันทางอาวุธย่อมอยู่ภายใต้บทบัญญัติข้อ 35 นี้ หากเทคโนโลยีดังกล่าวเป็นอาวุธ ถูกนำมาใช้เยี่ยงอาวุธ หรือแม้แต่การใช้เป็นวิธีการหรือปัจจัยในการสงคราม โดยหากการใช้งานเทคโนโลยีนั้นก่อให้เกิดการบาดเจ็บเกินสมควรหรือความทุกข์ทรมานเกินความจำเป็น หรือทำให้สภาพแวดล้อมทางธรรมชาติเสียหายในลักษณะขยายเป็นวงกว้าง มีระยะเวลายาวนาน และมีลักษณะรุนแรง

ด้วยเหตุที่การใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นมีลักษณะที่เปลี่ยนแปลงไปจากการใช้อาวุธ วิธีการและปัจจัยในรูปแบบเดิม ทั้งในแง่ของการใช้เทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพ และการใช้เทคโนโลยีที่ไม่ก่อให้เกิดผลอย่างร้ายแรงต่อบุคคล เช่น การใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีนั้นอาจก่อให้เกิดผลกระทบที่ร้ายแรงต่อร่างกายของบุคคลหรือไม่ก็ได้ ในกรณีที่การโจมตีทางไซเบอร์นั้นไม่ถึงขั้นก่อให้เกิดความเสียหายในรูปแบบของความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น หรือไม่ก่อให้เกิดผลกระทบต่อสภาพแวดล้อมทางธรรมชาติอย่างกว้างขวางแล้วย่อมไม่เป็นการขัดต่อหลักเกณฑ์ดังกล่าว เช่นเดียวกับการใช้ระบบอาวุธที่ไม่ก่อให้เกิดความร้ายแรงต่อร่างกาย (Non-lethal weapons) เช่น อาวุธยิงคลื่นแม่เหล็กไฟฟ้า (Electromagnetic weapons)

แนวโน้มความเปลี่ยนแปลงทางเทคโนโลยีใหม่ในการขัดกันทางอาวุธมักเป็นการลดความเสียหายที่อาจเกิดขึ้นแก่ทั้งตัวพลรบและพลเรือน รวมทั้งสร้างความแม่นยำในการปฏิบัติต่อเป้าหมาย ประเด็นในเรื่องการพิจารณาบทบัญญัติข้อ 35 นี้จึงอาจเกิดขึ้นกับการใช้เทคโนโลยีที่ทำให้เกิดผลกระทบต่อสภาพแวดล้อมทางธรรมชาติ เช่นหากมีการพัฒนาระบบอาวุธทางอวกาศที่สามารถก่อให้เกิดสภาวะการเปลี่ยนแปลงทางภูมิอากาศได้ หรือการใช้เทคโนโลยีที่อาจก่อให้เกิดภัยพิบัติทางธรรมชาติได้ย่อมเป็นการต้องห้ามตามหลักกฎหมายในเรื่องนี้[660]

ทั้งนี้ พึงสังเกตว่าบทบัญญัติข้อ 35 นี้เป็นการสร้างข้อจำกัดเกี่ยวกับการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามเท่าที่จำเป็นต่อปฏิบัติการทางทหารแบบกว้างเท่านั้น โดยคำนึงถึงผลที่จะเกิดจากการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามบางลักษณะ แต่หากเป็นการพิจารณาหลักเกณฑ์การกระทำที่เป็น

---

2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.

3. It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment."

[660] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 35.

ปรปักษ์ (Conduct of Hostilities) ประการอื่นๆ เช่นการปฏิบัติต่อเป้าหมาย ความได้สัดส่วนในการใช้กำลัง การแยกแยะเป้าหมาย และการระมัดระวังในการโจมตี เช่นนี้ต้องดูบทบัญญัติเฉพาะเรื่องในส่วนนั้นไป

นอกเหนือจากการใช้ข้อ 35 กับการจำกัดการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามแล้ว ยังปรากฏว่ามีความพยายามในการสร้างอนุสัญญาระหว่างประเทศอีกหลายฉบับเพื่อการจำกัดและควบคุมการใช้อาวุธเฉพาะอย่าง

ประเด็นสำคัญที่เกิดขึ้นกับเทคโนโลยีที่มีการนำมาใช้ทางการทหารและทางพลเรือนในปัจจุบันคือการใช้เทคโนโลยีร่วมกันทั้งทางการทหารและพลเรือน ลักษณะดังกล่าวอาจมีความแตกต่างกันเล็กน้อยจากพัฒนาการทางทหารในยุคเดิมที่อาวุธมักถูกออกแบบและสร้างขึ้นมาเพื่อการรบโดยเฉพาะ เทคโนโลยีทางการทหารจึงมักเป็นการสร้างอาวุธ ในขณะที่ปัจจุบันมีการใช้เทคโนโลยีของพลเรือนประกอบกับเทคโนโลยีทางการทหารค่อนข้างมาก[661] เช่นการใช้ระบบปฏิบัติการทางไซเบอร์เน็ตเวิร์คของคอมพิวเตอร์เพื่อปฏิบัติการจารกรรมข้อมูล รวมตลอดถึงการก่อวินาศกรรมทางไซเบอร์ ตั้งแต่การปล่อยไวรัส มัลแวร์ รวมตลอดถึงการเข้าไปควบคุมระบบการทำงานของคอมพิวเตอร์และทำลายระบบปฏิบัติการของคอมพิวเตอร์เป้าหมาย ซึ่งปฏิบัติการทางไซเบอร์ลักษณะนี้จะกระทำผ่านระบบเครือข่ายการทำงานของคอมพิวเตอร์ซึ่งใช้ร่วมกันระหว่างพลเรือนและทหาร ในขณะที่คอมพิวเตอร์นั้นก็ถูกออกแบบมาให้ใช้งานได้ทั่วไปของพลเรือนนั้นคอมพิวเตอร์เป็นประโยชน์ในการใช้งานในชีวิตประจำวันแต่เมื่อคอมพิวเตอร์เป็นส่วนหนึ่งของเครื่องมือที่ใช้เพื่อปฏิบัติการทางทหาร การควบคุมการใช้งานคอมพิวเตอร์เพื่อการโจมตีทางทหารจึงต้องคำนึงถึงผลลัพท์จากการกระทำเป็นสำคัญแต่จะควบคุมคอมพิวเตอร์ทุกเครื่องไม่ได้เพราะคอมพิวเตอร์มิใช่อาวุธเพื่อการทำลายในตัวเอง การตรวจสอบการใช้งานไซเบอร์ที่อาจก่อให้เกิดการโจมตีในการขัดกันทางอาวุธจึงเป็นเรื่องจำเป็น[662]

ประเด็นท้าทายต่อมาสำหรับการใช้งานระบบไซเบอร์คือการไม่ปรากฏตัวตนของผู้ใช้งานว่าเป็นทหารหรือพลเรือน การจำแนกพลรบและพลเรือนดังที่ปรากฏตามกฎเกณฑ์ในการขัดกันทางอาวุธ เช่น การสวมเครื่องแบบและการถืออาวุธย่อมไม่สามารถกระทำได้ แต่จะต้องตรวจสอบจาก IP address ของ

---

[661] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p. 26.

[662] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p. 29.

คอมพิวเตอร์ว่ามีการใช้งานมาจากแหล่งใด ก่อให้เกิดปัญหาในการแยกแยะเป้าหมายที่สามารถตอบโต้ได้ และปัญหาต่อหลักความระมัดระวังในการโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศ[663]

นอกเหนือจากการใช้งานระบบไซเบอร์แล้วเทคโนโลยีอื่นๆ เช่น การใช้โดรนในการลาดตระเวนตรวจตราในทางการทหารก็มีลักษณะการใช้งานร่วมทั้งพลเรือนและทหาร เนื่องจากเป็นเทคโนโลยีที่สามารถใช้ได้ทั้งสองลักษณะ เช่นเดียวกันกับพัฒนาการทางด้านหุ่นยนต์ซึ่งมีทั้งระบบจักรกลตัดสินใจได้ด้วยตนเองและระบบที่ต้องอาศัยการควบคุมจากมนุษย์ก็เป็นเทคโนโลยีที่เป็นประโยชน์ในทางอุตสาหกรรมและเป็นประโยชน์ทางการทหารเพื่อลดการสูญเสียพลรบด้วย พัฒนาการทางเทคโนโลยีเหล่านี้อาจไม่สามารถควบคุมการพัฒนาทั้งหมดได้ แต่จะต้องทำการจำแนกว่าการพัฒนาเพื่อการทหารจะต้องอยู่ภายใต้การควบคุมของกฎหมายหรือองค์กรใด ในขณะที่การใช้งานเทคโนโลยีดังกล่าวก็จะต้องพิจารณาผลที่เกิดขึ้นจากการใช้งานด้วยเช่นกันว่าเป็นไปเพื่อวัตถุประสงค์ทางการทหารหรือเพื่อประโยชน์ในทางพลเรือนซึ่งจะทำให้การควบคุมเทคโนโลยีดังกล่าวมีความชัดเจนมากยิ่งขึ้น

3.3.1.1 การจำกัดวิธีการและปัจจัยในการขัดกันทางอาวุธกับเทคโนโลยีใหม่

ข้อจำกัดการใช้วิธีและปัจจัยที่ใช้ในการขัดกันทางอาวุธนั้น ปรากฏตามข้อ 35 แห่งพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ.1977 ของอนุสัญญาเจนีวา ค.ศ.1949 ซึ่งมีเป้าหมายในการควบคุมความรุนแรงของการขัดกันทางอาวุธให้เป็นไปเท่าที่จำเป็นต่อปฏิบัติการทางทหารเท่านั้น การจำกัดวิธีและปัจจัยในการขัดกันทางอาวุธนี้มีความหมายรวมถึงอาวุธและการใช้อาวุธด้วย

คำว่า “อาวุธ” ในทางกฎหมายนั้นมีสองรูปแบบ คืออาวุธโดยสภาพกับอาวุธโดยการใช้งาน เช่น ปืนถูกออกแบบมาเพื่อการใช้งานในการทำลาย และต่อสู้เป็นสำคัญ ปืนจึงเป็นอาวุธโดยสภาพ ในขณะที่มีดอาจถูกออกแบบมาเพื่อการใช้งานครัว มีดโดยทั่วไปจึงอาจไม่ใช่อาวุธโดยสภาพ แต่อาจเป็นอาวุธโดยการใช้งาน ในขณะที่ท่อนไม้ไม่ใช่ทั้งอาวุธโดยสภาพและการออกแบบ เพราะเป็นสิ่งที่มีอยู่แล้วตามธรรมชาติ ก็อาจถูกนำมาใช้งานเพื่อให้กลายเป็นอาวุธในการต่อสู้หรือป้องกันตัวได้

กฎหมายมนุษยธรรมระหว่างประเทศนั้น อาวุธ (Weapons) ที่ใช้ในการขัดกันทางอาวุธย่อมหมายถึง สิ่งที่ออกแบบมาเพื่อใช้ในการต่อสู้ต่อพลรบฝ่ายตรงข้าม หรือเพื่อการโจมตีเป้าหมายทางการทหารฝ่ายตรงข้าม[664] เช่น ปืนที่พลรบหรือทหารมีไว้ใช้ประจำกาย ย่อมเป็นสิ่งที่ออกแบบมา

---

[663] Ibid.

[664] William Boothby, Weapons, and the Law of Armed Conflict, p. 4.

เพื่อการต่อสู้และการป้องกันตัว ปืนประจำกายจึงเป็นอาวุธโดยสภาพ ระเบิดที่ทหารพกไว้เพื่อการรบมีเป้าหมายเพื่อใช้ในการทำลาย จึงเป็นอาวุธโดยสภาพ ในขณะที่รถหุ้มเกราะเพื่อใช้ลำเลียงทหารมิได้ถูกออกแบบมาเพื่อการทำลาย จึงไม่ใช่อาวุธโดยสภาพ แต่หากมีการติดตั้งอาวุธเข้าไปเพื่อการทำลายย่อมเป็นการนำเอายานพาหนะไปรวมเข้ากับการใช้งานอาวุธ จึงเป็นการใช้งานยานพาหนะให้เป็นสิ่งประกอบการใช้อาวุธ เครื่องมือสื่อสารทางการทหารมิใช่อาวุธ แต่มีไว้เพื่อประกอบการใช้งานสั่งการโจมตีและป้องกัน โดยนัยนี้เครื่องมือสื่อสารจึงไม่ใช่อาวุธแต่ถูกใช้งานเพื่ออำนวยประโยชน์ต่อการรบฯลฯ ดังนี้ย่อมสังเกตได้ว่าการใช้งานสิ่งต่างๆ ในการรบนั้น อาจอยู่ในหลายสถานะตั้งแต่การเป็นอาวุธโดยการออกแบบ การใช้สิ่งที่มิใช่อาวุธมาประกอบกับการใช้อาวุธ และสิ่งที่มิใช่อาวุธมาประกอบการรบ การควบคุมการใช้อาวุธจึงไม่อาจคุ้มครองบุคคลในสถานการณ์การขัดกันทางอาวุธในทุกกรณีได้ จึงมีการใช้ถ้อยคำทางกฎหมายที่ก่อให้เกิดความครอบคลุมมากขึ้น โดยปรากฏคำว่า วิธี (Methods) และปัจจัย (Means)

ปัจจัย (Means) หมายถึง อาวุธ เครื่องกระสุน ส่วนประกอบ ชิ้นส่วน และอุปกรณ์ที่ใช้ประกอบกับอาวุธนั้น โดยนัยนี้ ปัจจัยย่อมรวมถึงอาวุธทุกชนิดที่ใช้ในการสงคราม สิ่งประกอบการใช้อาวุธ แท่นยิง เครื่องกระสุน ในขณะที่วิธี (Methods) หมายถึง วิธีการใช้อาวุธต่อศัตรู หรือวิธีการในการใช้กำลังกับศัตรู[665] วิธีการจึงมีความกว้างขวางมากกว่าอาวุธ และย่อมครอบคลุมถึงพฤติกรรมในการใช้กำลังในการขัดกันทางอาวุธในหลายกรณี

ด้วยเหตุที่กฎหมายมนุษยธรรมระหว่างประเทศจำกัดปัจจัยและวิธีการในการขัดกันทางอาวุธว่าจะต้องไม่ก่อให้เกิดความเสียหายเกินขนาดและความทุกข์ทรมานเกินความจำเป็น โดยปัจจัยมีความหมายรวมถึงอาวุธและวิธีการมีความหมายทั้งวิธีการใช้อาวุธและวิธีการทำสงคราม ซึ่งการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นอาจเป็นได้ทั้งปัจจัยคือใช้เป็นอาวุธและเป็นวิธีการในการขัดกันทางอาวุธ จึงจำเป็นต้องพิจารณาเทคโนโลยีที่อาจนำมาใช้เป็นปัจจัยและวิธีการในการขัดกันทางอาวุธและส่งผลต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศดังต่อไปนี้

(ก) การใช้ไซเบอร์เป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธ

อาวุธทางไซเบอร์ที่มีการกล่าวถึงมากที่สุดคือปฏิบัติการ Stuxnet หรือการส่งหนอนคอมพิวเตอร์ (Computer worm) เข้าไปทำลายระบบคัดแยกแร่ยูเรเนียม (Uranium Enrichment) ของโรงงานในเมืองนาธานซ์ (Natanz) ประเทศอิหร่าน ผลกระทบจากการติดเชื้อหนอนคอมพิวเตอร์

---

[665] Ibid., p. 4.

ที่เป็นรูปธรรมคือการทำให้เครื่องปั่นยูเรเนี่ยม (Centrifuge) ทำงานผิดปกติเป็นผลให้ใบพัดซึ่งทำหน้าที่แยกองค์ประกอบธาตุยูเรเนียมชำรุดจนส่งผลสุดท้ายให้การแยกธาตุยูเรเนียมใช้เวลานานขึ้นกว่าปกติ[666]

หากพิจารณาจากผลทางกายภาพที่เกิดขึ้นจากการใช้ปฏิบัติการ Stuxnet จะพบว่ามัลแวร์คอมพิวเตอร์ชนิดนี้สามารถสร้างความเสียหายแก่อุปกรณ์คัดแยกแร่ยูเรเนียมได้แต่ไม่ได้ทำให้โรงงานคัดแยกแร่ยูเรเนียมได้รับความเสียหายลักษณะเดียวกับการทำลายด้วยอาวุธ เป็นเพียงการชะลอการผลิตยูเรเนียมให้ช้าลงและทำให้เครื่องปั่นยูเรเนี่ยมสึกหรอเร็วขึ้น[667] การกระทำดังกล่าวย่อมมีผลกระทบต่อการนำยูเรเนียมที่ถูกคัดแยกแล้วไปใช้งานในประเทศอิหร่านไม่ว่าจะเป็นการใช้งานเพื่อผลิตกระแสไฟฟ้าหรือเพื่อการสร้างอาวุธนิวเคลียร์ก็ตาม หากมองในมุมการทำลายของ Stuxnet แล้ว Stuxnet จะมีลักษณะไม่แตกต่างจากการใช้อาวุธทางกายภาพเพื่อทำลายระบบคัดแยกยูเรเนียม แต่หากมองในมิติว่าปฏิบัติการ Stuxnet เป็นมาตรการป้องกันก็อาจเกิดข้อโต้แย้งได้ผลที่เกิดขึ้นจาก Stuxnet เป็นการป้องกันไม่ให้เกิดการผลิตอาวุธนิวเคลียร์ซึ่งเท่ากับเป็นการปฏิบัติที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศ

นอกจากการโจมตีทางไซเบอร์โดยตรงต่อเป้าหมายเป็นการเฉพาะเช่นกรณี Stuxnet แล้วการโจมตีทางไซเบอร์เพื่อทำลายระบบการสื่อสารยังปรากฏในหลายเหตุการณ์ เช่น การโจมตีทางไซเบอร์ร่วมกับการโจมตีตามแบบปกติในความขัดแย้งที่เมืองเซาท์ออสเซเทีย ประเทศจอร์เจียและความขัดแย้งระหว่างประเทศยูเครนและรัสเซีย วิธีการโจมตีทางไซเบอร์ที่นิยมใช้ร่วมกับการโจมตีตามแบบมักเป็นวิธีการ DDoS หรือการโจมตีระบบการสื่อสารของเว็บไซต์อินเทอร์เน็ตซึ่งทำให้ระบบสาธารณูปโภคที่เชื่อมต่อกับอินเทอร์เน็ตไม่สามารถใช้การได้[668] การโจมตีในรูปแบบนี้อาจพิจารณาได้ว่ามีผลเท่ากับการใช้อาวุธปกติทำลายระบบการสื่อสารได้ เพียงแต่ความเสียหายทางกายภาพที่เกิดขึ้นกับอุปกรณ์อาจไม่เป็นรูปธรรมเช่นเดียวกับการทำลายด้วยอาวุธตามแบบ

การใช้ปฏิบัติการทางไซเบอร์เพื่อวัตถุประสงค์อื่นทางการทหารยังสามารถเกิดขึ้นได้ เช่นการใช้ปฏิบัติการทางไซเบอร์เพื่อการจารกรรมข้อมูลทางการทหารหรือการใช้ปฏิบัติการทาง

---

[666] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: update of ISIS December 2010," Institute for Science and International Security Report; (2011). p.4.

[667] Ibid., p.4.

[668] Williams C. Ashmore, "Impact of Alleged Russian Cyber Attacks," Baltic Security and Defense Review, 11 (2009): 10.

สารสนเทศเพื่อสร้างข่าวลวงในการสงคราม ฯลฯ กรณีการใช้ปฏิบัติการทางไซเบอร์เพื่อวัตถุประสงค์ทางการทหารเหล่านี้ย่อมถือเป็นวิธีการในการขัดกันทางอาวุธ

การใช้ไซเบอร์ในลักษณะเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธหากไม่ก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นย่อมถือว่าไม่เป็นการขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศและเมื่อพิจารณาจากเหตุการณ์ที่เกิดขึ้นในกรณีต่างๆ จะพบว่าการใช้ไซเบอร์ไม่ว่าจะในฐานะเป็นอาวุธ ปัจจัยหรือวิธีการในการขัดกันทางอาวุธมักไม่นำไปสู่ความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นแบบเดียวกับที่อาวุธตามแบบสามารถทำให้เกิดผลเสียหายดังกล่าวได้ การโจมตีทางไซเบอร์หรือการใช้ปฏิบัติการทางไซเบอร์ย่อมไม่เป็นการต้องห้ามในกฎหมายมนุษยธรรมระหว่างประเทศเสมอไป ทั้งนี้จะต้องคำนึงถึงผลที่เกิดขึ้นจากการใช้ไซเบอร์ในแต่ละกรณีเป็นสำคัญ

(ข) การใช้อากาศยานไร้คนขับเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธ

อากาศยานไร้คนขับอาจใช้งานได้ในรูปแบบเดียวกับเครื่องบินรบเพื่อการโจมตี เมื่ออากาศยานไร้คนขับสามารถใช้เพื่อการโจมตีได้อากาศยานดังกล่าวย่อมมีสถานะเป็นปัจจัยในการรบคือเป็นอาวุธในการโจมตีและเป็นวิธีการใช้อาวุธในการโจมตี ในขณะที่การใช้อากาศยานไร้คนขับเพื่อการจารกรรมข้อมูลและการลาดตระเวนย่อมถือเป็นวิธีการในการขัดกันทางอาวุธ การใช้งานอากาศยานไร้คนขับทั้งเพื่อเป็นปัจจัยและเป็นวิธีการในการขัดกันทางอาวุธนี้จะต้องสอดคล้องกับหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศด้วยคือจะต้องไม่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น

ในทางปฏิบัติไม่พบรายงานว่าอากาศยานไร้คนขับก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นแต่ประการใดจึงไม่สามารถกล่าวได้ว่าการใช้อากาศยานไร้คนขับในปัจจุบันเป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศเรื่องการใช้ปัจจัยและวิธีการในการขัดกันทางอาวุธแต่อย่างใด

(ค) การใช้ระบบอาวุธอิสระเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธ

ระบบอาวุธอิสระ (Autonomous Weapon Systems) ในปัจจุบันปรากฏในรูปแบบของระบบป้องกันภัยทางอากาศเป็นสำคัญ ได้แก่ระบบป้องกันภัยทางอากาศของประเทศ

อิสราเอล[669]และระบบป้องกันภัยทางอากาศ Patriot ของประเทศสหรัฐอเมริกา[670] ขณะที่การใช้งานหุ่นยนต์สังหาร (Killer Robot) เพื่อการขัดกันทางอาวุธนั้นยังไม่พบรายงานที่เป็นทางการแต่อย่างใด

ลักษณะของการใช้ระบบอาวุธอิสระย่อมเป็นปัจจัยในการรบคือเป็นอาวุธที่ใช้เพื่อการป้องกันประเทศในขณะที่มีแนวโน้มการพัฒนาในอนาคตซึ่งอาจเป็นไปเพื่อการโจมตีได้ ระบบอาวุธอิสระจึงต้องใช้งานโดยสอดคล้องกับหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศคือไม่ก่อให้เกิดความเสียหายเกินขนาดและความทุกข์ทรมานเกินความจำเป็น ประเด็นซึ่งเป็นที่วิพากษ์ในแวดวงกฎหมายมนุษยธรรมระหว่างประเทศและทางการทหารในปัจจุบันไม่ใช่เรื่องความเสียหายที่เกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นแต่อย่างใด แต่มักเป็นประเด็นเรื่องความวิตกกังวลเกี่ยวกับความผิดพลาดที่เกิดขึ้นจากระบบอาวุธอิสระซึ่งอาจส่งผลกระทบต่อพลเรือน ดังนั้นการใช้งานระบบอาวุธอิสระในปัจจุบันจึงยังคงไม่มีประเด็นเรื่องการใช้งานที่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานแต่อย่างใด

(ง) การใช้เทคโนโลยีนาโนเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธ

เทคโนโลยีนาโนที่นิยมในปัจจุบันและมีการนำมาใช้งานอย่างแพร่หลายคือเทคโนโลยีลดการตรวจจับ (Low Observable Technology) หรือเทคโนโลยี Stealth ซึ่งประกอบด้วยการออกแบบทางวัสดุศาสตร์และการใช้สารเคลือบผิววัตถุซึ่งใช้เทคโนโลยีนาโนเพื่อทำให้ยานพาหนะ เครื่องแบบหรืออาวุธที่ใช้ในการทหารมองเห็นได้ยากขึ้นหรือตรวจจับด้วยอุปกรณ์ตรวจจับยากขึ้น[671]

การใช้เทคโนโลยีนาโนเพื่อการลดการตรวจจับนี้เป็นวิธีการในการขัดกันทางอาวุธแต่ไม่ใช่วิธีการที่นำไปสู่ความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นเพียงแต่เป็นวิธีการลวงหรือพรางไม่ให้ฝ่ายศัตรูในการสงครามโจมตีได้ง่ายเท่านั้น ดังนั้นการใช้เทคโนโลยีลดการตรวจจับจึงไม่เป็นการขัดต่อการจำกัดปัจจัยและวิธีการในการขัดกันทางอาวุธ

---

669 Emily B. Landau, and Azriel Bermant. "Iron Dome protection: missile defense in Israel's security concept." The lessons of operation protective edge (2014): 37.

670 Eliot A. Cohen, Gulf War Air Power Survey, Washington, D.C.: U.S. Government Printing, 1993). p.30.

671 Serdar Cadirci, RF Stealth (or Low Observable) and Counter- RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for Turkish Air Force, Naval Postgraduate School, Monterey California, PhD Thesis. March 2009, p. 52.

ในขณะที่การใช้เทคโนโลยีนาโนสำหรับอาวุธนิวเคลียร์ อาวุธเคมีและอาวุธชีวภาพอาจนำมาซึ่งผลเสียหายที่เกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นได้ การใช้เทคโนโลยีนาโนเพื่อประกอบการใช้อาวุธที่มีอานุภาพทำลายล้างสูงดังกล่าวจึงเป็นการละเมิดต่อข้อจำกัดของการใช้ปัจจัยและวิธีการในการขัดกันทางอาวุธได้

(จ) การใช้ระบบอาวุธอวกาศเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธ

ระบบอาวุธอวกาศที่มีการกล่าวถึงทางการทหารในปัจจุบันแบ่งเป็น 2 รูปแบบคือ 1) การใช้ดาวเทียมเพื่อประกอบการใช้อาวุธในโลกและ 2) การใช้ระบบอาวุธที่ติดตั้งบนดาวเทียม โดยการใช้งานระบบอาวุธอวกาศที่พบในปัจจุบันคือลักษณะที่ 1 หรือการใช้งานดาวเทียมเพื่อการระบุตำแหน่งบนพื้นโลก (Global Positioning System: GPS) เพื่อการใช้งานระบบอาวุธนำวิถี[672]

การใช้งานระบบการกำหนดตำแหน่งบนพื้นโลก (GPS) ร่วมกับระบบอาวุธนำวิถีย่อมเป็นวิธีการในการขัดกันทางอาวุธที่มีเป้าหมายเพื่อการทำให้การใช้งานระบบอาวุธนำวิถีมีความแม่นยำมากขึ้นจึงไม่ถือว่าเป็นการกระทำที่ละเมิดต่อข้อจำกัดปัจจัยและวิธีการในการขัดกันทางอาวุธเพราะวัตถุประสงค์การใช้งานระบบอาวุธนำวิถีมีเพื่อทำให้ความเสียหายอยู่ในขอบเขตที่กำหนดได้ การใช้ระบบการกำหนดตำแหน่งบนพื้นโลกร่วมกับระบบอาวุธนำวิถีจึงไม่ขัดต่อข้อจำกัดการใช้ปัจจัยและวิธีการในการขัดกันทางอาวุธ

กรณีการใช้งานระบบอาวุธที่ติดตั้งบนดาวเทียมในฐานะเป็นปัจจัยในการขัดกันทางอาวุธหากไม่ก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นย่อมไม่เป็นการขัดต่อหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับข้อจำกัดในการใช้ปัจจัย และวิธีการในการขัดกันทางอาวุธ อย่างไรก็ดีตามสนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศรวมทั้งดวงจันทร์และเทหะฟากฟ้าอื่น ค.ศ. 1967 มีข้อห้ามติดตั้งอาวุธนิวเคลียร์และอาวุธที่มีอานุภาพทำลายล้างสูงบนดาวเทียม[673] การใช้ดาวเทียมเพื่อวัตถุประสงค์ในเชิงสันติตามสนธิสัญญาฉบับนี้ย่อมเป็นการป้องกันไม่ให้เกิดการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศแม้ว่าสนธิสัญญานี้จะไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศก็ตาม

---

[672] Duncan Blake, "Military Strategic Use of Outer Space," in Nasu, H. and McLaughlin, R, (editors), New Technologies and the Law of Armed Conflict. (The Hague: T.M.C. Asser Press, 2014), p. 105.

[673] 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Art. IV.

3.3.1.2 การจำกัดการใช้อาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศมีหลักการสำคัญในการจำกัดการทำสงครามหรือการขัดกันทางอาวุธให้คู่พิพาทในสงครามจะต้องไม่ใช้วิธีการหรือปัจจัยที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น (Superfluous injury and unnecessary suffering)[674] คำว่า “ปัจจัย” นั้นหมายถึงอาวุธที่ใช้ในสงครามรวมตลอดถึงสิ่งที่เกี่ยวข้องกับการทำให้อาวุธนั้นสามารถทำงานได้ และ “วิธีการ” หมายความถึงวิธีในการใช้อาวุธในสงครามและวิธีการที่เกี่ยวข้องกับการทำสงคราม[675] หมายความว่าการใช้อาวุธในการขัดกันทางอาวุธนั้นจะใช้โดยก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นไม่ได้ เพราะเป็นการละเมิดต่อหลักการขั้นพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศ

หากพิจารณาความหมายของคำว่า “ความเสียหายเกินขนาดและความทุกข์ทรมานเกินความจำเป็น” ตามกฎหมายมนุษยธรรมระหว่างประเทศก็ย่อมหมายความว่า การใช้อาวุธนั้นจะต้องไม่ก่อให้เกิดความเสียหายที่เกินไปกว่าความจำเป็นทางการทหารในการขัดกันทางอาวุธ ความจำเป็นทางการทหารย่อมหมายความว่าการกระทำที่ก่อให้เกิดผลเสียหายทางการทหารที่จะทำให้เกิดการแพ้-ชนะในสงครามเท่านั้น[676] เช่น ทหารทำการรบย่อมมีเป้าหมายในการฆ่าทหารฝ่ายตรงข้ามหรือทำลายอาคาร ยานพาหนะของฝ่ายตรงข้าม การกระทำอย่างอื่นที่ไม่ได้เป็นไปเพื่อฆ่าฝ่ายตรงข้ามทันทีอันได้แก่การทำให้ทรมานด้วยอาวุธหรือวิธีการใดๆ ย่อมเป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศ นอกจากนั้นความจำเป็นทางการทหารยังหมายถึงความเสียหายจากปฏิบัติการทางทหารจะต้องเกิดผลกระทบต่อพลเรือนอย่างน้อยที่สุดด้วย เช่น การโจมตีทางทหารจะต้องมีการประเมินว่าสถานที่ซึ่งเป็นเป้าหมายนั้นอยู่ใกล้แหล่งที่อยู่ของพลเรือนหรือไม่ การใช้อาวุธบางชนิดจะส่งผลกระทบในวงกว้างซึ่งย่อมกระทบต่อพลเรือนอย่างมากหรือไม่ เป็นต้น

ข้อจำกัดการใช้ปัจจัยและวิธีการที่จะก่อให้เกิดความเสียหายที่เกินขนาดและความทุกข์ทรมานเกินความจำเป็นตามกฎหมายมนุษยธรรมระหว่างประเทศนี้มีปัญหาในการบังคับใช้กับอาวุธใน

---

[674] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, available at: https://www.refworld.org/docid/3ae6b36b4.html [accessed 28 May 2021], Art 35 (2).

[675] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 37.

[676] Williams Boothby, Weapons and the Law of Armed Conflict, p. 5.

บางลักษณะที่ความเสียหายและความบาดเจ็บไม่ชัดเจนว่าจะเกินขนาดหรือเกินความจำเป็นหรือไม่ เช่น ประเด็นเรื่องการใช้กระสุนลูกปรายชนิดแท่งโลหะ (Flechette) ซึ่งนิยมใช้ในกระสุนปืนลูกซอง กระสุน 90 มิลลิเมตรประจำรถถังรวมถึงกระสุนปืนใหญ่ขนาด 106 มิลลิเมตร[677] กระสุนลูกปรายชนิดนี้มีการใช้งานมาตั้งแต่สมัยสงครามโลกครั้งที่ 1 แต่กลับพบว่าในการใช้งานจริงนั้นอาวุธชนิดนี้มีอานุภาพทำลายต่ำเป้าหมายต่ำมาก เนื่องจากแท่งเหล็กแหลมที่อยู่ในกระสุนซึ่งมีขนาดเล็กนั้นจะทำให้ผู้ถูกยิงเสียชีวิตได้เมื่อแรงปะทะมากพอและถูกอวัยวะส่วนที่สำคัญ มีข้อน่าสังเกตว่าในที่ประชุมของคณะกรรมการทบทวนการบังคับใช้อนุสัญญาว่าด้วยการห้ามอาวุธตามรูปแบบบางชนิด (CCW) เห็นว่ากระสุนชนิดนี้ไม่ต้องห้ามตามกฎหมายระหว่างประเทศ เพราะความรุนแรงน้อยกว่าลักษณะ “ความเสียหายที่เกินขนาดและความทุกข์ทรมานเกินความจำเป็น”[678] นอกจากนั้นในคดี Physicians for Human Rights v. OC Southern Command case โจทก์กล่าวหากองกำลังป้องกันตนเองของอิสราเอลว่ามีการใช้กระสุนลูกปรายชนิดแท่งเหล็ก (Flechette shells) ในการทำลายเป้าหมาย กองกำลังอิสราเองอ้างว่าไม่มีกฎหมายระหว่างประเทศหรือกฎหมายใดห้ามการใช้กระสุนชนิดนี้ ยิ่งไปกว่านั้นศาลสูงสุดของประเทศอิสราเอล (Supreme Court of Israel) ยังยืนยันว่าไม่มีกฎหมายใดห้ามการใช้กระสุนลูกปรายชนิดแท่งเหล็ก (Flechette shells) อันสังเกตได้จากที่อนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิด (CCW) ไม่มีข้อห้ามอาวุธชนิดนี้ จึงเป็นการไม่ถูกต้องที่จะกล่าวหาว่าการใช้อาวุธชนิดนี้เป็นเรื่องผิดกฎหมาย[679]

ความเสียหายทางการทหารที่จะส่งผลต่อความได้เปรียบ-เสียเปรียบ หรือแพ้-ชนะในสงครามนั้นจะต้องคำนึงถึงความมีมนุษยธรรม (Humanity) ด้วย ความมีมนุษยธรรมเช่นว่าคือในการต่อสู้กับฝ่ายตรงข้ามจะต้องต่อสู้ด้วยความเท่าเทียมกันระหว่างทหารที่ถืออาวุธ หากมีการแสดงเจตนาของทหารฝ่ายตรงข้ามว่าวางอาวุธแล้วก็จะต้องไม่ทำการโจมตี[680] ในกรณีที่พบว่าทหารฝ่ายตรงข้ามไม่อยู่ในสถานะที่สู้ได้อันเนื่องจากการบาดเจ็บหรือป่วยไข้ก็จะต้องไม่ทำร้ายทหารผู้นั้น เป็นต้น ในขณะที่บางกรณีการมีมนุษยธรรมอาจทับซ้อนกับหลักความจำเป็นทางการทหาร เช่นการใช้อาวุธทาง

---

[677] Ibid., P. 241.

[678] Ibid.

[679] David Turns, “Weapons in the ICRC Study on Customary International Law,” Journal of Conflict and Security Law, Vol. 11, Issue 2, (2006): 224 - 225. [online] Accessed: June 8, 2021. Available from: https://academic.oup.com/jcsl/article/11/2/201/836156

[680] Yoram Dinstein, (2004), The Conduct of Hostilities under the Law of International Armed Conflict, p. 39.

การทหารเพื่อการรบในสงครามนั้นจะต้องไม่เป็นไปเพื่อสร้างความทุกข์ทรมานแทนที่จะทำให้ศัตรูเสียชีวิตในทันที[681]

พึงสังเกตว่าในการต่อสู้กันนั้นคงเป็นไปได้ยากที่จะหลีกเลี่ยงความบาดเจ็บและการสูญเสียชีวิต ผลที่เกิดจากการสู้รบโดยปกติจึงเป็นเรื่องที่หลีกเลี่ยงไม่ได้ และกฎหมายมนุษยธรรมระหว่างประเทศก็ไม่ได้ห้ามการต่อสู้เสียทีเดียวเพียงแต่จำกัดการต่อสู้ไม่ให้เกินขอบเขตที่เหมาะสมเท่านั้น ประเด็นสำคัญที่เกิดขึ้นในประวัติศาสตร์การทำสงครามคือคู่พิพาทมักจะมีการใช้อาวุธหรือวิธีการที่เหี้ยมโหดมากกว่าการสังหารโดยทันที เพื่อให้เกิดผลในทางจิตวิทยาคือความหวาดกลัวแก่คู่พิพาท ซึ่งจะทำให้ได้เปรียบในเชิงการรบมากขึ้น ตัวอย่างที่เห็นได้ชัดได้แก่การใช้สารพิษในการรบ ซึ่งปรากฏมาตั้งแต่ยุคก่อนที่จะมีกฎหมายว่าด้วยการขัดกันทางอาวุธ พิษที่มีการใช้กันในยุคแรกๆ คือการใช้พิษอาบที่ลูกศรธนูหรือหน้าไม้ กฎหมายในยุคแรกที่ปรากฏการห้ามการใช้ธนูอาบยาพิษคือคัมภีร์พระธรรมศาสตร์ (Code of Manu) ก่อนยุคคริสตกาลราว 200 ปี[682]

การต่อสู้ด้วยธนูและหน้าไม้นั้นมีความรุนแรงอยู่ในระดับหนึ่งแล้วคือบุคคลที่เป็นเป้าหมายการโจมตีอาจบาดเจ็บหรือเสียชีวิตก็ได้ขึ้นอยู่กับตำแหน่งอวัยวะสำคัญที่ถูกทำลาย แต่การเพิ่มความรุนแรงด้วยการอาบยาพิษที่ลูกศร มีผลให้การยิงลูกศรที่ไม่ตรงกับอวัยวะสำคัญก็อาจทำให้ผู้ถูกยิงเสียชีวิตจากพิษได้ การสูญเสียชีวิตจึงไม่ใช้ผลโดยตรงที่มาจากลูกศรแต่เป็นผลที่มาจากยาพิษ ความพยายามในการจำกัดการใช้อาวุธในยุคแรกๆ จึงเป็นความพยายามในการสร้างกฎหมายเพื่อจำกัดการใช้อาวุธที่จะไม่ก่อให้เกิดความเสียหายในลักษณะดังกล่าว[683]

ข้อสังเกตคือคำว่า “ความเสียหายเกินขนาดและความทุกข์ทรมานเกินความจำเป็น” ที่ปรากฏในพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 นั้นไม่ใช้จุดเริ่มต้นของแนวคิดดังกล่าว แต่เป็นการประมวลเอาความคิดที่เกิดขึ้นจากแนวปฏิบัติของหลักเกณฑ์การขัดกันทางอาวุธในหลายยุคมารวมกัน โดยจุดเริ่มต้นนั้นไม่มีถ้อยคำดังกล่าวปรากฏ เช่นในกฎเกณฑ์ก่อนยุค Lieber Code ว่าด้วยเรื่องการห้ามใช้อาวุธยิงลูกศรอาบยาพิษ ไม่มีการอ้างถึงหลักการความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นแต่อย่างใด เป็นเพียงแต่การห้ามใช้อาวุธที่มียาพิษ

---

[681] Ibid., pp. 33-37.

[682] Adam Roberts and Richard Guelff, Documents on the Laws of War, 3rd edn, (Oxford: Oxford University Press, 2000), p. 53.

[683] William Boothby, Weapons and the Law of Armed Conflict, pp. 8-9.

เป็นส่วนประกอบเท่านั้น แต่ใน Lieber Code มีการใช้คำว่า “ความเสียหายเกินขนาด” (Superfluous injury) เท่านั้น

หลักเกณฑ์ Lieber Code เกิดจากข้อเสนอของ DR. Francis Lieber จากมหาวิทยาลัยโคลัมเบีย (Columbia University) ในช่วงทศวรรษ ค.ศ.1860 โดย Dr. Lieber ตีพิมพ์หลักเกณฑ์เรื่องการรบทางบกในปี ค.ศ. 1863 เพื่อให้กองทัพ Union Army ได้นำไปใช้ในช่วงสงครามกลางเมืองของสหรัฐอเมริกา Lieber Code มีหลักการทั้งสิ้น 157 ข้อ ซึ่งรวมถึงหลักการกระทำอันเป็นปรปักษ์ (Conduct of Hostilities) วิธีการ (Methods) และปัจจัย (Means) ในการกระทำอันเป็นปรปักษ์ นอกจากนั้นยังมีการอธิบายว่า “ความจำเป็นทางการทหาร” (military necessity) หมายถึงมาตรการที่จำเป็นและไม่สามารถหลีกเลี่ยงได้เพื่อทำให้สงครามยุติลง (measures which are indispensable for securing the end of the war) และการกระทำดังกล่าวจะต้องชอบด้วยกฎหมายที่เกี่ยวข้อง[684] ความจำเป็นทางการทหารที่กล่าวถึงใน Lieber Code นี้ขยายความไปถึงการจำกัดวิธีการและปัจจัยในการขัดกันทางอาวุธด้วย เช่น การห้ามการกระทำที่ก่อให้เกิดความทรมานเพื่อการแก้แค้น และการห้ามใช้สารพิษ[685] แม้จะไม่ปรากฏคำว่า “ความบาดเจ็บที่เกินขนาดและความทุกข์ทรมานเกินความจำเป็น” (Superfluous injury and unnecessary suffering) อย่างชัดเจนแต่ก็ทำให้เห็นได้ว่าอย่างน้อย Lieber Code ก็เป็นยุคเริ่มต้นของหลักการดังกล่าว สิ่งที่ Lieber Code น่าจะแตกต่างจากหลักกฎหมายว่าด้วยการขัดกันทางอาวุธในยุคหลังคือ Lieber Code ห้ามการล้างแค้นที่เกิดขึ้นจากเจตนาของผู้กระทำเอง ในขณะที่กฎหมายว่าด้วยการขัดกันทางอาวุธในยุคหลังนั้นการล้างแค้นที่มาจากคำสั่งของผู้บังคับบัญชาปฏิบัติก็ถือเป็นความผิดด้วย[686]

นักกฎหมายในยุคต่อมาเริ่มตระหนักถึงการห้ามการใช้อาวุธที่เกินความจำเป็นในการทำสงคราม เช่นการใช้ยาพิษ ว่าจะต้องอยู่บนพื้นฐานของหลักการบางอย่าง หลักการที่ว่าคือ “หลักการไม่ก่อความบาดเจ็บที่เกินขนาด” และมีทัศนะว่าการใช้ยาพิษ สารพิษ แก๊สพิษ คือการก่อให้เกิดความบาดเจ็บเกินขนาด แนวคิดเรื่องการห้ามใช้สารพิษในการทำสงครามปรากฏเรื่อยมาจนถึงยุคหลังสงครามโลกครั้งที่ 2 ก็ยังคงปรากฏอนุสัญญาว่าด้วยการห้ามใช้แก๊สพิษในการรบ โดยมีแนวคิดที่

---

[684] Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863, Art 14. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863

[685] Ibid., Art 16.

[686] William Boothby, Weapons and the Law of Armed Conflict, p. 9.

สอดคล้องกับ Lieber Code บ้างไม่มากก็น้อยว่าการใช้พิษในการทำสงครามเป็นการกระทำที่เกินความจำเป็นทางการทหารในการรบ[687]

ในยุคหลังสงครามโลกครั้งที่ 2 นับจากการก่อตั้งองค์การสหประชาชาติ เริ่มมีความเปลี่ยนแปลงรูปแบบของกฎหมายระหว่างประเทศเกี่ยวกับการควบคุมอาวุธและการใช้อาวุธในการขัดกันทางอาวุธมากขึ้น โดยหลักการไม่ก่อให้เกิดความบาดเจ็บที่เกินขนาดไม่ได้เปลี่ยนแปลงไป แต่มีความเปลี่ยนแปลงมิติของอาวุธที่ควบคุมหลากหลายมากไปกว่าสารพิษ ซึ่งแท้จริงแล้วก่อนยุคสหประชาชาติก็มีความเคลื่อนไหวในการสร้างกฎหมายระหว่างประเทศที่จำกัดการใช้อาวุธอื่นนอกจากสารพิษอยู่บ้าง แต่ไม่มีกฎหมายระหว่างประเทศเกินขึ้นอย่างมากมายจะแสดงนัยสำคัญ เช่น St. Petersburg Declaration ที่ห้ามใช้กระสุนระเบิดที่มีน้ำหนักต่ำกว่า 400 กรัม เพราะจะก่อให้เกิดความบาดเจ็บที่เกินความจำเป็นทางการทหาร

ปฏิญญาเซนต์ปีเตอร์สเบิร์กเกิดขึ้นจากสงครามในรัสเซียสมัยกษัตริย์ Tsar Alexander II ซึ่งมีการใช้กระสุนระเบิดบางชนิดในการต่อสู้ ทำให้เกิดการประชุมของคณะกรรมาธิการระหว่างประเทศด้านการทหาร (International Military Commission)[688] เพื่อพิจารณาความเสียหายที่เกิดขึ้นจากการใช้อาวุธดังกล่าว โดยปรากฏในอารัมภบทของปฏิญญาฯ ได้กล่าวว่า เป็นหน้าที่ของรัฐในการพิจารณาว่าอาวุธที่ใช้ในการรบนั้นจะต้องเป็นไปเพื่อการทำลายกองทัพฝ่ายตรงข้ามซึ่งเป็นผลต่อความได้เปรียบทางการรบแต่จะต้องไม่เป็นการใช้อาวุธเพื่อก่อให้เกิดความทุกข์ทรมานและต้องไม่ใช้อาวุธที่ไม่ได้ทำให้บุคคลเสียชีวิตในทันที โดยประนามว่าการกระทำที่ก่อให้เกิดความทุกข์ทรมานแต่ไม่ได้นำไปสู่ความตายโดยตรงนี้เป็นการละเมิดต่อหลักกฎหมายมนุษยธรรม (Laws of Humanity)[689] ปฏิญญาเซนต์ปีเตอร์สเบิร์กจึงเป็นการตอกย้ำหลักการเรื่องความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นอีกครั้งต่อจาก Lieber Code แม้หลักการเรื่องความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นจะยังไม่ได้ปรากฏอย่างชัดเจนเช่นในปัจจุบัน อย่างไรก็ดี ในปฏิญญาเซนต์ปีเตอร์สเบิร์กมีการกล่าวเอาไว้อย่างชัดเจนถึงความสัมพันธ์ระหว่างความจำเป็นทางการทหาร (Military Necessity) กับการคุ้มครองหลักมนุษยธรรม (Laws of Humanity) ซึ่งทำให้เริ่ม

---

[687] Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863, Art 14.

[688] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, 29 November/11 December 1868. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868

[689] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, 29 November/11 December 1868., Preamble, Para 2-6.

เห็นพัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศในยุคเริ่มต้นก่อนพัฒนามาเป็นกฎหมายมนุษยธรรมในยุคปัจจุบันซึ่งให้ความสำคัญกับการสร้างความสมดุลระหว่างหลักการทั้งสองนี้ในกรณีที่เกิดการขัดกันทางอาวุธขึ้น[690]

ในปี ค.ศ.1874 มีการประชุมระหว่างประเทศเกิดขึ้นที่เมืองบรัสเซล ประเทศเบลเยี่ยมและเป็นที่มาของปฏิญญาบรัสเซล (Brussels Declaration 1874) ซึ่งห้ามใช้วิธีการที่ก่อให้เกิดความบาดเจ็บบางประการแก่ฝ่ายศัตรู เช่น การใช้พิษและการใช้อาวุธที่มีพิษ (Poison or poisoned weapons) รวมตลอดถึงการห้ามใช้อาวุธ อาวุธยิง หรือวัตถุอื่นใดที่อาจก่อให้เกิดความทุกข์ทรมานเกินความจำเป็น (Unnecessary suffering) โดยอ้างอิงถึงกระสุนหรืออาวุธยิงที่ปรากฏในปฏิญญาเซนต์ปีเตอร์สเบิร์กด้วย[691]

ขณะที่ในปี ค.ศ.1880 มีการจัดทำคู่มือออกซ์ฟอร์ด (Oxford Manual 1880) ขึ้นมา โดยมีการอ้างอิงหลักการที่ปรากฏในปฏิญญาเซนต์ปีเตอร์สเบิร์ก เช่น หลักการเรื่องความจำเป็นทางการทหาร และมีการอ้างอิงถึงหลักการในปฏิญญาบรัสเซล ได้แก่หลักข้อจำกัดในการทำสงครามที่จะต้องไม่ก่อให้เกิดความบาดเจ็บบางลักษณะแก่ศัตรู (no unlimited liberty as to the means of injuring the enemy) รวมถึงการกระทำที่ไม่จำเป็นในการสงครามและการการทำที่ไม่ชอบธรรมในการสงครามด้วย[692] นอกจากนั้นในข้อ 8 ของปฏิญญาฉบับนี้ยังให้ความสำคัญกับการคุ้มครองผู้บาดเจ็บให้ไม่ตกเป็นเป้าหมายของการโจมตีด้วย โดยยังคงให้ความสำคัญกับการห้ามใช้พิษไม่ว่าจะอยู่ในรูปแบบใดๆ ก็ตาม ในข้อ 9 มีการห้ามใช้อาวุธ อาวุธยิง และวัตถุอื่นใดที่อาจก่อให้เกิดความบาดเจ็บเกินขนาดหรือก่อให้เกิดบาดแผลที่รุนแรง

ในปี ค.ศ.1899 มีการประชุมที่เมืองเฮก ประเทศเนเธอร์แลนด์ (Hague Peace Conference 1899) ยังมีการนำเอาประเด็นเรื่องการจำกัดการใช้งานอาวุธบางชนิดในสงครามมากล่าวถึง เช่น การห้ามใช้อาวุธพิษ และการห้ามใช้กระสุนระเบิดที่มีน้ำหนักต่ำกว่า 400 กรัม ในขณะที่สิ่งที่พัฒนามากกว่าเดิมในการประชุมครั้งนี้คือการเสนอห้ามใช้แก๊สพิษที่ส่งผลต่อระบบหายใจ (Asphyxiating Gas)

---

[690] Ibid., Preamble, Para 2-6.

[691] International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874, Art 12 and 13 (a) and (e). [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874

[692] The Laws of War on Land, Manual published by the Institute of International Law (Oxford Manual), Adopted by the Institute of International Law at Oxford, September 9, 1880. Art 3 and art 4. [online] Accessed: June 9, 2022. Available from: http://hrlibrary.umn.edu/instree/1880a.htm

และแก๊สที่เป็นอันตรายในการสงคราม[693] และการห้ามใช้กระสุนที่หัวขยายออกเมื่อเข้าสู่เป้าหมาย (Expanding bullet)[694] การประชุมครั้งนี้สร้างประเด็นที่น่าสังเกตหลายประการได้แก่

1) พัฒนาการของกฎหมายระหว่างประเทศเกี่ยวกับการควบคุมอาวุธในการทำสงครามหยุดนิ่งหรือไม่

เมื่อพิจารณาหลักการที่มีการกล่าวอ้างในการประชุมที่เฮกจะพบว่ายังมีการกล่าวอ้างถึงหลักการเดิมที่ปรากฏขึ้นมาตั้งแต่อดีต เช่น การห้ามใช้กระสุนระเบิดที่มีน้ำหนักต่ำกว่า 400 กรัม ซึ่งเป็นหลักการของปฏิญญาเซนต์ปีเตอร์สเบิร์ก การห้ามใช้อาวุธพิษที่ปรากฏมาตั้งแต่ Lieber Code จนถึง Oxford Manual สะท้อนให้เห็นว่าในช่วงเวลาดังกล่าวไม่มีสถานการณ์การใช้อาวุธที่เปลี่ยนแปลงไปเลย (ทั้งนี้อาจหมายความว่าพัฒนาการทางอาวุธในช่วงเวลาดังกล่าวอาจมีเพียงเท่านั้น) และหลักการของกฎหมายระหว่างประเทศไม่มีแนวโน้มว่าจะพัฒนาการไปอย่างใด แม้จะมีส่วนขยายเพิ่มขึ้นมาเรื่องการห้ามใช้แก๊สพิษและกระสุนหัวขยาย แต่ก็ไม่ได้แสดงนัยสำคัญของเทคโนโลยีทางอาวุธที่เปลี่ยนแปลงไปในช่วงทศวรรษ ค.ศ.1980 หลักการเดียวที่ยังมั่นคงคือหลักความจำเป็นทางการทหารที่จะต้องไม่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นเท่านั้น

2) การสร้างหลักการห้ามใช้อาวุธขึ้นมาไม่ได้มีผลต่อการจำกัดการใช้อาวุธในยามสงครามเลย

ในยุคสงครามโลกครั้งที่ 1 ช่วงปี ค.ศ.1917 เริ่มมีการใช้แก๊สพิษเป็นที่แพร่หลายในการทำสงคราม โดยกองทัพฝรั่งเศสนิยมใช้แก๊สน้ำตาและกองทัพเยอรมันนิยมใช้อาวุธแก๊สคลอรีน แก๊สคลอรีนนั้นมีฤทธิ์ส่งผลต่อระบบการหายใจของมนุษย์โดยตรงก่อให้เกิดสภาวะขาดออกซิเจนเฉียบพลัน (Asphyxia) และทำให้เสียชีวิตได้ นอกจากนั้นยังมีการใช้แก๊สอื่นๆ ด้วย เช่น แก๊สมัสตาร์ด (Mustard Gas or Sulfur Mustard)[695] ซึ่งในการประชุมที่เฮกก็มีความตระหนักถึงปัญหาการใช้แก๊สพิษและกำหนดเป็นข้อห้ามในการทำสงครามก่อนล่วงหน้าแล้ว แต่เมื่อเข้าสู่ยุคสงครามโลกครั้งที่ 1

---

[693] Declaration (IV,2) concerning Asphyxiating Gases. The Hague, 29 July 1899, para 1-2. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-decl-iv-2-1899/declaration?activeTab=undefined

[694] Declaration (IV,3) concerning Expanding Bullets. The Hague, 29 July 1899. para 1-2. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-decl-iv-3-1899/declaration?activeTab=undefined

[695] Boothby, W., Weapons and the Law of Armed Conflict, p. 33.

อาวุธแก๊สพิษกลับเป็นที่แพร่หลายเสมือนว่าข้อห้ามที่เกิดขึ้นในสังคมระหว่างประเทศนั้นไม่มีผลบังคับในสถานการณ์สงครามแต่อย่างใด

ข้อสังเกตเหล่านี้สะท้อนให้เห็นพัฒนาการของกฎหมายมนุษยธรรมระหว่างประเทศในช่วงเริ่มต้นไปในทิศทางเดียวว่าปฏิบัติการทางทหารในยามสงครามที่เป็นไปโดยความจำเป็นนี้จะต้องเคารพต่อหลักมนุษยธรรมคือการไม่ก่อให้เกิดความบาดเจ็บเกินขนาดและความทุกข์ทรมานเกินความจำเป็นเท่านั้น และหลักการนี้จะกลายเป็นสิ่งที่ปรากฏในพิธีสารเพิ่มเติม ฉบับที่ 1 ของอนุสัญญาเจนีวา ค.ศ.1977 แต่หลักการนี้ไม่ได้สะท้อนให้เห็นพัฒนาการของเทคโนโลยีทางอาวุธในช่วงเริ่มต้นเลย[696]

แม้จะมีความพยายามสร้างกฎหมายที่เกี่ยวข้องกับการรบทางบกมาช่วงระยะเวลาหนึ่ง แต่ก็ยังไม่มีกฎหมายระหว่างประเทศที่เป็นลายลักษณ์อักษรอย่างเป็นรูปธรรม จนกระทั่งในปี ค.ศ.1907 มีการประชุมว่าด้วยสันติภาพที่กรุงเฮก (Hague Peace Conference) และมีการอนุวัติการอนุสัญญาเฮก ฉบับที่ 4 ซึ่งได้รับการยอมรับอย่างกว้างขวางว่าเป็นอนุสัญญาระหว่างประเทศที่เป็นการประกาศจารีตประเพณีเกี่ยวกับการทำสงครามที่มีมาแต่เดิม[697] อนุสัญญาเฮกฉบับที่ 4 นี้พยายามอ้างอิงถึงความเป็นอารยะกับการสร้างหลักมนุษยธรรมในสงคราม โดยหลักการสำคัญของการทำสงครามรู้จักกันเป็นการทั่วไปในชื่อหลักมาร์ติน (Marten's clause) ซึ่งต้องการให้การขัดกันทางอาวุธ หรือการสงครามนั้นจะต้องคำนึงถึงความมีมนุษยธรรมอยู่ด้วย โดยความมีมนุษยธรรมเช่นว่านั้นจะต้องเป็นสอดคล้องกับข้อกำหนดแห่งมโนธรรมสาธารณะด้วย (Dictates of Public conscience)[698] คำว่า "ข้อกำหนดแห่งมโนธรรมสาธารณะ" หรือ Dictates of public conscience นี้ค่อนข้างสื่อไปในลักษณะการสร้างองค์ประกอบทางศีลธรรมขึ้นมาเป็นการเฉพาะในกฎหมายว่าด้วยการขัดกันทางอาวุธ[699] แต่หากตีความโดยคำนึงถึงบริบทการเกิดขึ้นของ "จารีตประเพณี" ทางกฎหมาย ก็อาจ

---

[696] Ibid., p. 33.

[697] Adam Roberts, "The Equal Application of the Law of War: A Principle under Pressure," International Review of the Red Cross, Vol. 90, No. 872, (December 2008): 942-943. [online] Accessed: June 10, 2022. Available from: https://international-review.icrc.org/sites/default/files/irrc-872-6.pdf

[698] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899. Para 9. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-ii-1899/preamble?activeTab=undefined

[699] Theodor Meron, "The Martens Clause, Principles of Humanity, and Dictates of Public Conscience," The American Journal of International Law, Vol. 94, No. 1, (January 2000): 78–89, [online] Accessed: June 10, 2022. Available from: https://www.jstor.org/stable/2555232

พิจารณาได้ว่า dictates of public conscience นี้น่าจะเป็นความรับรู้ร่วมกันของสาธารณะซึ่งเป็นพัฒนาการของจารีตประเพณี (Custom) ก่อนจะมีการบัญญัติเป็นกฎหมาย[700]

ในขณะที่ Professor Dinstein มีข้อสังเกตว่าหลักมนุษยธรรมที่ปรากฏในอารัมภบทของอนุสัญญาเฮก ฉบับที่ 4 ซึ่งอ้างอิงถึง dictates of public conscience นี้ไม่เกี่ยวข้องโดยตรงกับกฎหมายว่าด้วยการขัดกันทางอาวุธในเรื่องความชอบด้วยกฎหมายของการใช้อาวุธในสงคราม แต่ dictates of public conscience น่าจะเกี่ยวข้องกับลักษณะโดยทั่วไปของหลักการกระทำอันเป็นปฏิปักษ์ (Conduct of hostilities) มากกว่า[701] ความเห็นของ Professor Dinstein อาจอธิบายได้ว่าการใช้อาวุธตามหลักการมาร์ตินที่จะต้องจะต้องคำนึงถึงความมีมนุษยธรรมพร้อมไปกับข้อกำหนดแห่งมโนธรรมสาธารณะเกี่ยวข้องกับการกระทำของทหารว่าควรปฏิบัติการอยู่ในเงื่อนไขความเหมาะสมระดับใด การกระทำใดเป็นการต้องห้ามเพราะเกินขอบเขตความจำเป็นทางการทหาร แต่หลักมาร์ตินนี้ไม่ได้บอกว่าอาวุธใดใช้ได้หรือไม่ เพราะหลักการมาร์ตินเป็นหลักเกี่ยวกับปฏิบัติการทางทหารไม่ใช่หลักกฎหมายควบคุมอาวุธ

ประเด็นความชอบด้วยกฎหมายในการใช้อาวุธนี้ ศาลยุติธรรมระหว่างประเทศในคดี The Legality of the Use by a State of Nuclear Weapons มีความเห็นที่ค่อนข้างไม่ชัดเจนว่าการใช้อาวุธนิวเคลียร์ชอบด้วยกฎหมายระหว่างประเทศหรือไม่ ศาลจึงมีความเห็นว่าให้พิจารณาแนวปฏิบัติทั่วไปของนานาอารยประเทศในช่วงเวลาดังกล่าว[702] หากรัฐที่ถูกคุกคามจากอาวุธนิวเคลียร์มีจำนวนมากและมองว่าอาวุธนิวเคลียร์เป็นภัยต่อความสงบเรียบร้อยของโลกก็อาจนำไปสู่การห้ามใช้อาวุธนิวเคลียร์ได้ แต่ปรากฏว่าในช่วงเวลาดังกล่าวยังมีความไม่ชัดเจนในประเด็นการใช้งานนิวเคลียร์เพื่อสันติภาพและการมีไว้ในครอบครองเพื่อการป้องกันตัว จึงทำให้ไม่มีบทกฎหมายระหว่างประเทศใดกำหนดว่าการใช้อาวุธนิวเคลียร์ต้องห้าม

ต่อมาในอนุสัญญาเฮก ฉบับที่ 4 ค.ศ.1907 ในข้อ 22 และ ข้อ 23 ยังคงยืนยันหลักการว่าสิทธิของคู่สงครามในการใช้วิธีการเพื่อสร้างความบาดเจ็บแก่คู่พิพาทนั้นไม่ใช่ว่าไม่มีข้อจำกัด[703] และ

---

[700] William Boothby, Weapons, and the Law of Armed Conflict, p. 14.

[701] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 57.

[702] Legality of the Use by State of Nuclear Weapons in Armed Conflicts (1996) ICJ 26, International Court of Justice, 265 para 105 (2) E.

[703] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, Art. 22. [online] Accessed: June 10, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907

กำหนดข้อห้ามในการใช้พิษและอาวุธพิษในการสงคราม[704] และการห้ามใช้อาวุธ เครื่องยิงกระสุนหรือวัตถุอื่นใดที่จะก่อให้เกิดความทุกข์ทรมานเกินความจำเป็น[705]

การพัฒนาทางเทคโนโลยีทางทหารอย่างรวดเร็วในยุคก่อนสงครามโลกครั้งที่ 1 และความตื่นตัวของสังคมระหว่างประเทศในช่วงเวลาที่มีการประชุมที่เฮกเพื่อสร้างอนุสัญญาเฮก ฉบับที่ 4 นั้น มีการหยิบยกประเด็นเทคโนโลยีที่พัฒนาอย่างรวดเร็วในช่วงเวลาดังกล่าวซึ่งสังคมระหว่างประเทศเกรงว่าจะเป็นเครื่องมือหลักในการสงครามต่อไปในอนาคต เทคโนโลยีที่พัฒนาอย่างรวดเร็วในช่วงเวลาดังกล่าวคืออากาศยานรบทางทหาร โดยในปฏิญญาเฮก ฉบับที่ 1 ค.ศ.1899 นั้นได้มีข้อกำหนดห้ามการใช้อาวุธยิงและวัตถุระเบิดซึ่งปล่อยจากบอลลูน รวมถึงวิธีการอื่นๆ ในลักษณะเดียวกัน (launching of projectiles and explosives from balloons and other methods of a similar nature) คำว่าวิธีการอื่นๆ ในลักษณะเดียวกันนี้สะท้อนให้เห็นว่าพัฒนาการทางอาวุธบางชนิดเกิดขึ้นรวดเร็วมากจนไม่อาจสร้างกฎหมายเฉพาะเรื่องขึ้นเพื่อควบคุมได้ หรือแม้กระทั่งไม่สามารถสร้างคำจำกัดความที่ครอบคลุมถึงทุกกรณีได้ ทั้งนี้ในที่ประชุมเพื่อสันติภาพที่เฮกมองว่าการสร้างคำจำกัดความที่ยืดหยุ่นจะเป็นการเปิดโอกาสให้สามารถใช้กฎหมายบังคับกับเทคโนโลยีที่พัฒนาอย่างรวดเร็วได้มากกว่า[706]

ขณะที่ในปี ค.ศ.1907 มีการเปลี่ยนถ้อยคำใหม่โดยปฏิญญาเฮก ฉบับที่ 14 ค.ศ.1907 (Hague Declaration XIV 1907) กำหนดข้อห้ามในการใช้กระสุนปล่อยและวัตถุระเบิดจากบอลลูน (discharge of projectiles and explosives from balloons)[707] ซึ่งยังเป็นข้อความที่ไม่ได้มีสาระสำคัญแตกต่างจากเดิม แต่ก็ไม่ได้ยืนยันว่ากฎหมายก้าวทันต่อความเปลี่ยนแปลงทางเทคโนโลยี เพราะหลังจากการประชุมในปี ค.ศ.1899 เป็นต้นมาก็ยังคงมีการใช้บอลลูนและเครื่องยิงกระสุนและระเบิดจากบอลลูนอยู่เช่นเดิม

พัฒนาการของเทคโนโลยีการรบทางอากาศเริ่มเปลี่ยนแปลงไปอย่างมีนัยสำคัญและมีการนำมาพิจารณาแนวทางในการสร้างข้อกำหนดเกี่ยวกับการรบทางอากาศในการประชุมที่เมืองวอชิงตันในปี ค.ศ.1921-1922 โดยคณะกรรมาธิการยกร่างหลักเกณฑ์การรบทางอากาศ (Rules of Aerial

---

[704] Ibid. Art. 23 (a)

[705] Ibid. Art. 23 (e)

[706] William Boothby, Weapons, and the Law of Armed Conflict, p. 16.

[707] Adam Roberts and Richard Guelff, Documents on the Laws of War, p. 140.

Warfare)[708] แต่หลักการดังกล่าวก็ไม่ได้มีการพัฒนาให้เป็นกฎหมายระหว่างประเทศแต่อย่างใด ในหลักเกณฑ์การรบทางอากาศนี้มีเพียงข้อ 18 ข้อเดียวที่มีข้อกำหนดเกี่ยวกับเรื่องอาวุธ โดยกล่าวถึงข้อห้ามใช้การแกะรอย อาวุธไฟ เครื่องยิงลูกระเบิดซึ่งปล่อยจากอากาศยานหรือยิงต่อต้านอากาศยาน ซึ่งในสังคมระหว่างประเทศในช่วงเวลานั้นมองว่าข้อกำหนดนี้ขัดแย้งกับปฏิญญาเซนต์ปีเตอร์สเบิร์ก ทำให้หลักเกณฑ์การรบทางอากาศนี้มีผลผูกพันเฉพาะชาติสมาชิกเท่านั้น[709]

นอกจากพัฒนาการเกี่ยวกับเรื่องหลักเกณฑ์เกี่ยวกับการรบทางอากาศที่กำลังพัฒนาในช่วงเวลาดังกล่าว สิ่งที่ยังคงไม่เปลี่ยนแปลงไปคือการใช้แก๊สพิษ นับตั้งแต่ความพยายามในทศวรรษ ค.ศ.1980 มาจนถึงหลังสงครามโลกครั้งที่ 1 ยังปรากฏข้อห้ามในกฎหมายระหว่างประเทศในการใช้อาวุธแก๊สพิษ เช่น ในข้อ 171 ของสนธิสัญญาแวร์ซาย ค.ศ.1919 ก็ยังคงปรากฏข้อห้ามในการใช้แก๊สพิษอยู่เช่นกัน ล่วงเลยมาจนถึงการก่อตั้งองค์การสันนิบาตชาติ ซึ่งมีการจัดประชุมระหว่างประเทศว่าด้วยเรื่องการควบคุมการค้าระหว่างประเทศที่เกี่ยวกับอาวุธ เครื่องกระสุน และสิ่งที่เกี่ยวข้องในการสงคราม ค.ศ.1925 (International Conference on the Control of the International Trade in Arms, Munitions and Implements of War 1925)[710]

การประชุมครั้งนี้ได้มีการรับรองพิธีสารเจนีวาว่าด้วยแก๊ส (The Geneva Gas Protocol) โดยมีข้อกำหนดว่าด้วยเรื่องการห้ามใช้แก๊สพิษในการทำสงครามที่มีเนื้อหาที่ละเอียดขึ้นมากกว่าหลักการที่เกิดขึ้นในอดีต โดยกล่าวถึงลักษณะของการใช้แก๊สในหลายลักษณะ ตั้งแต่แก๊สพิษที่ส่งผลต่อระบบทางเดินหายใจ แก๊สอื่นๆ ของเหลว วัตถุ หรืออุปกรณ์อื่นใดที่เกี่ยวข้องกับการใช้แก๊สพิษ เพื่อหลีกเลี่ยงการใช้คำว่าแก๊สพิษที่ส่งผลต่อระบบทางเดินหายใจแต่เพียงอย่างเดียว นอกจากนั้นยังมีข้อกำหนดเรื่องการห้ามใช้แบคทีเรียเป็นวิธีในการทำสงครามด้วย[711] พิธีสารเจนีวานี้แสดงให้เห็นพัฒนาการทางกฎหมายที่ตอบสนองต่อรูปแบบการทำสงครามที่เปลี่ยนแปลงไปอย่างเด่นชัด แม้จะไม่ได้ครอบคลุมถึงอาวุธที่กำลังจะเกิดขึ้นในช่วงเวลาต่อมา เช่นอาวุธที่มีอานุภาพทำลายล้างสูงอย่าง

---

[708] “Commission of Jurists to Consider and Report Upon the Revision of the Rules of Warfare, General Report.” American Journal of International Law, Vol. 32, No. S1, (1938): 1–56. [online] Accessed: June 10, 2022. Available from: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/commission-of-jurists-to-consider-and-report-upon-the-revision-of-the-rules-of-warfare-general-report1/F25B66816C13A812DE257DBB37CDFE96

[709] William Boothby, Weapons, and the Law of Armed Conflict, p. 16.

[710] William Boothby, Weapons, and the Law of Armed Conflict, p. 16.

[711] Ibid., p. 17.

อาวุธนิวเคลียร์ อาวุธเคมีและอาวุธชีวภาพ แต่ก็เป็นจุดเริ่มต้นในการปูทางให้เกิดกฎหมายระหว่างประเทศเกี่ยวกับการห้ามใช้อาวุธ เช่น อนุสัญญาว่าด้วยอาวุธชีวภาพในปี ค.ศ.1972 และอนุสัญญาว่าด้วยอาวุธเคมี ค.ศ.1993

หลังสงครามโลกครั้งที่ 2 สังคมระหว่างประเทศเริ่มมีความกังวลเกี่ยวกับการใช้สิ่งแวดล้อมให้กลายเป็นอาวุธในการสงคราม ตัวอย่างที่ปรากฏเด่นชัดคือในสงครามเวียดนาม กองทัพสหรัฐอเมริกาได้มีการใช้วิธีการทำฝนเหลือง (Orange Agent) เพื่อดัดแปลงฝนให้กลายเป็นสารพิษสร้างความได้เปรียบในการทำสงคราม หลักการในการทำฝนเหลืองใช้วิธีการเดียวกับการทำฝนเทียม คือการใช้สารเคมีในกลุ่ม silver iodide, potassium iodide และ solid carbon dioxide (dry ice) รวมตลอดถึง liquid propane สารเคมีเหล่านี้จะถูกบรรทุกไปบนเครื่องบินและปล่อยที่ชั้นบรรยากาศ เมื่อสารเคมีเหล่านี้ทำปฏิกิริยากับไอน้ำและอุณหภูมิในชั้นบรรยากาศก็จะก่อตัวเป็นเมฆฝนและตกลงสู่พื้นดิน โดยมีการผสมสารเคมีกำจัดศัตรูพืชไปในการผลิตฝน หรือปล่อยสารเคมีกำจัดศัตรูพืชโดยตรงในชั้นบรรยากาศ สารเคมีเหล่านั้นได้แก่ phenoxy herbicides, dichlorophenoxyacetic acid และ trichlorophenoxyacetic acid ผลกระทบที่เกิดจากการรับสารเคมีจากฝนเหลืองคือ มะเร็งเม็ดเลือดขาว มะเร็งต่อมน้ำเหลือง มะเร็งต่อมลูกหมาก มะเร็งระบบทางเดินหายใจ มะเร็งปอด และเนื้องอกเนื้อเยื่ออ่อน[712]

นอกจากนั้นยังมีปฏิบัติการ Sober Popeye (Operation Sober Popeye, Project Controlled Weather Popeye) ของกองทัพสหรัฐอเมริกาในพื้นที่เมืองโฮจิมินท์เพื่อสกัดกั้นการโจมตีของฝ่ายเวียตนามเหนือ โดยการสร้างฝนเทียมเพื่อทำให้ดินอ่อนตัวและเกิดการถล่มของดิน (landslide) ซึ่งส่งผลทำให้เกิดปรากฏการณ์น้ำหลากเนื่องจากแม่น้ำถล่มเข้าสู่พื้นที่

จากเหตุที่มีการใช้วิธีการเปลี่ยนแปลงสภาพแวดล้อมหลายกรณีในการขัดกันทางอาวุธ ทำให้สหประชาติต้องสร้างอนุสัญญาระหว่างประเทศว่าด้วยการห้ามใช้ปฏิบัติการทางทหารหรือการกระทำที่เป็นศัตรูโดยการใช้เทคนิคเปลี่ยนแปลงสภาพแวดล้อม ค.ศ.1976

ในปี ค.ศ.1977 มีการประกาศใช้พิธีสารเพิ่มเติมอนุสัญญาเจนีวา 2 ฉบับ โดยในฉบับที่ 1 ว่าด้วยเรื่องการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ ได้มีหลักการในข้อ 35 กำหนดให้ในการใช้

[712] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

อาวุธ วิธีการและปัจจัยในการขัดกันทางอาวุธจะต้องมีข้อจำกัด[713] ข้อจำกัดประการสำคัญได้แก่ การห้ามใช้วิธีการหรือปัจจัยในการขัดกันทางอาวุธที่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น[714] การห้ามดัดแปลงสิ่งแวดล้อมเพื่อการสงคราม[715] และกำหนดหน้าที่ของรัฐสมาชิกในการพิจารณาความเหมาะสมในการพัฒนาอาวุธใหม่[716]

ต่อมาปี ค.ศ.1980 สหประชาชาติได้มีการประกาศใช้อนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัดเป้าหมาย (Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects 1980: CCW) อนุสัญญาฉบับนี้มีเป้าหมายในการสร้างหลักการจำกัดการใช้อาวุธโดยตระหนักว่าเทคโนโลยีทางอาวุธจะมีการพัฒนาอยู่เสมอ แต่การพัฒนาเทคโนโลยีทางอาวุธนั้นจะต้องคำนึงถึงการเคารพต่อหลักการไม่ก่อให้เกิดความเสียหายเกินขนาดด้วย[717] อนุสัญญาฉบับนี้มีการแก้ไขอีกครั้งในปี ค.ศ.2001 โดยแก้ไขข้อ 1 ให้อนุสัญญาฉบับนี้มีผลบังคับกับการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ เพื่อให้สอดคล้องกับข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ทั้ง 4 ฉบับ

ภายใต้อนุสัญญาอนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัดเป้าหมายนี้ มีการสร้างพิธีสารเพิ่มเติมทั้งสิ้น 5 ฉบับ ได้แก่

1) พิธีสารเพิ่มเติมฉบับที่ 1 ว่าด้วยเรื่องอาวุธที่ไม่สามารถตรวจพบได้โดยการเอกซ์เรย์ (Protocol I on non-detachable Fragment) ค.ศ.1980

2) พิธีสารเพิ่มเติมฉบับที่ 2 ว่าด้วยเรื่องการห้ามหรือจำกัดการใช้ทุ่นระเบิด กับระเบิดและวัตถุระเบิดอื่นๆ (Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-traps and Other Devices) ค.ศ.1980 ซึ่งต่อมามีการแก้ไขในปี ค.ศ.1996 เรื่องขอบเขตในการบังคับใช้กฎหมายให้ครอบคลุมถึงการบังคับใช้กฎหมายในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่าง

---

[713] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 35 (1).

[714] Ibid., Art. 35 (2).

[715] Ibid., Art. 35 (3) and art 55.

[716] Ibid., Art. 51.

[717] William Boothby, Weapons, and the Law of Armed Conflict, p. 18.

ประเทศ และไม่บังคับใช้กฎหมายกับสถานการณ์ความตึงเครียดภายในประเทศที่ไม่ใช่การขัดกันทางอาวุธ นิยามของทุ่นระเบิดที่มีความละเอียดมากขึ้น รวมถึงการนิยามของระเบิดสั่งการทางไกล และการแก้ไขมาตรการทางกฎหมายในการจัดการกับทุ่นระเบิด กับระเบิด และวัตถุระเบิดเพื่อให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงไป โดยกำหนดให้รัฐภาคีจะต้องมีนโยบายภายในประเทศในการจัดการกับปัญหาทุ่นระเบิด

3) พิธีสารเพิ่มเติมฉบับที่ 3 ว่าด้วยเรื่องการห้ามและจำกัดการใช้อาวุธเพลิง (Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons) ค.ศ.1980

4) พิธีสารเพิ่มเติมฉบับที่ 4 ว่าด้วยเรื่องการห้ามอาวุธเลเซอร์ที่ทำให้ตาบอด (Protocol on Blinding Laser Weapons) ค.ศ.1995

5) พิธีสารเพิ่มเติมฉบับที่ 5 ว่าด้วยเรื่องวัตถุระเบิดซึ่งตกค้างจากสงคราม (Protocol on Explosive Remnants of War) ค.ศ.2003

ขณะที่ในปี ค.ศ.2008 มีการเจรจานอกกรอบของที่ประชุมอนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบและก่อให้เกิดการสร้างอนุสัญญาว่าด้วยระเบิดแบบกลุ่ม (Convention on Cluster Munition)

ปัญหาสำคัญที่ทำให้อนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัดเป้าหมายไม่สามารถแก้ไขปัญหาทุ่นระเบิดได้ประสบผลสัมฤทธิ์เนื่องจากมีการสร้างกฎหมายระหว่างประเทศในเรื่องเดียวกันขึ้นมาถึงสองฉบับในเวลาเดียวกัน[718] โดยระหว่างที่พิธีสารฉบับที่ 2 ว่าด้วยการห้ามทุ่นระเบิดต้องรอผลใช้บังคับโดยอาศัยฉันทามติของรัฐภาคีในการบังคับให้เป็นไปตามกฎหมาย ก็เกิดอนุสัญญาออตตาวาว่าด้วยทุ่นระเบิดสังหารบุคล ค.ศ.1997 (Ottawa Convention on Anti-Personnel Landmines 1997) ขึ้นมา อนุสัญญาออตตาวาเป็นผลมาจากการเจรจานอกกรอบอนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัดเป้าหมาย ปรากฏการณ์ดังกล่าวจึงสะท้อนให้เห็นว่าแม้จะมีกฎหมายเฉพาะเรื่องที่สร้างขึ้นมาเพื่อแก้ไขปัญหาการใช้อาวุธบางชนิดแต่ก็ไม่สามารถรับรองได้ว่ากฎหมายดังกล่าวจะถูกนำมาใช้แก้ไขปัญหาได้อย่างเป็นรูปธรรมเสมอไป เพียงแต่เป็นการสร้างทางเลือกในการนำกฎหมายไปใช้แก้ไขปัญหาของอาวุธบางประการให้กับสังคมระหว่างประเทศเท่านั้น

[718] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

ในธรรมนูญจัดตั้งศาลอาญาระหว่างประเทศมีการกำหนดลักษณะการกระทำที่เป็นอาชญากรรมสงคราม (War Crime) ในข้อ 8 โดยให้รวมถึงการใช้พิษและอาวุธพิษ[719] นอกจากนั้นการใช้แก๊สที่ส่งผลต่อระบบทางเดินหายใจ แก๊สพิษ และแก๊สอื่นๆ ในลักษณะเดียวกัน ไม่ว่าจะอยู่ในรูปแบบของเหลว วัตถุ หรืออุปกรณ์อื่นๆ[720] และการใช้กระสุนที่ขยายหรือกระจายเมื่อถูกร่างกาย[721] แนวคิดในการสร้างหลักการของธรรมนูญศาลอาญาระหว่างประเทศดังกล่าวย่อมถือได้ว่าได้รับอิทธิพลอย่างมากจากกฎหมายว่าด้วยการขัดกันทางอาวุธหลายฉบับที่เกิดขึ้นตลอดช่วงเวลาที่ผ่านมาในอดีต ดังสังเกตได้จากหลักการที่ปรากฏในกฎหมายว่าด้วยการขัดกันทางอาวุธทุกฉบับที่เกิดขึ้นมานั้นต่างมีบทบาทในการประกอบสร้างหลักการไม่ก่อให้เกิดความเสียหายเกินขนาดและความทุกข์ทรมานเกินความจำเป็นเพื่อจำกัดการใช้อาวุธและวิธีการในการขัดกันทางอาวุธให้สอดคล้องกับหลักความจำเป็นทางการทหาร ในขณะที่ช่วงเวลาต่อมาหลักข้อจำกัดในการใช้อาวุธและวิธีการขัดกันทางอาวุธนี้ได้ขยายไปจนถึงเรื่องการห้ามใช้อาวุธที่ไม่สามารถจำแนกเป้าหมายเฉพาะได้[722]

หลักเกณฑ์ที่เกิดขึ้นในธรรมนูญจัดตั้งศาลอาญาระหว่างประเทศดังกล่าวถือเป็นการสร้างหลักการที่เชื่อมระหว่างกฎหมายมนุษยธรรมระหว่างประเทศกับเขตอำนาจในการพิจารณาคดีของศาลอาญาระหว่างประเทศ แม้จะไม่ได้เป็นไปโดยชัดแจ้งแต่ความผิดฐานอาชญากรรมสงครามหรือการละเมิดกฎหมายมนุษยธรรมระหว่างประเทศก็ถือเป็นประเด็นที่ศาลอาญาระหว่างประเทศมีเขตอำนาจในการพิจารณาคดีดังกล่าวได้ นอกจากนั้นในปี ค.ศ.2001 มีการประชุมทบทวนการปฏิบัติตามอนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดที่ก่อให้เกิดการบาดเจ็บร้ายแรงเกินความจำเป็นหรือก่อให้เกิดผลโดยไม่จำกัดเป้าหมาย (CCW) เพื่อเชื่อมโยงประเด็นการห้ามใช้อาวุธบางชนิดที่จะเป็นความผิดฐานอาญากรรมสงคราม รวมถึงการขยายขอบเขตการบังคับใช้อนุสัญญาว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิดในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศด้วย ทำให้เกิดมิติในการเชื่อมโยงกฎหมายระหว่างประเทศหลายประเด็นมากขึ้น

ปรากฏการณ์ที่กล่าวมาทั้งหมดแสดงให้เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศในยุคสหประชาชาตินั้นมีพัฒนาการอย่างรวดเร็วและต่อเนื่อง มีความพยายามสร้างอนุสัญญาระหว่างประเทศที่ควบคุมอาวุธหลากหลายประเภท เช่น การควบคุมอาวุธปืนประจำกายทหาร อนุสัญญา

---

[719] Rome Statute of the International Criminal Court, 17 July 1998, Art. 8 (2) (b) (xvii), [online] Accessed: June 10, 2021. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/icc-statute-1998?activeTab=undefined

[720] Ibid, Art. 8 (2) (b) (xviii)

[721] Ibid., Art. 8 (2) (b) (xix)

[722] Ibid., Art. 8 (2) (b) (xx)

ควบคุมอาวุธตามแบบ อนุสัญญาห้ามใช้อาวุธเคมี อนุสัญญาห้ามใช้อาวุธชีวภาพ อนุสัญญาห้ามใช้อาวุธเลเซอร์ที่ทำให้ตาบอด มาจนถึงสนธิสัญญาห้ามใช้อาวุธนิวเคลียร์ ฯลฯ

หากมองแต่เพียงผิวเผินจะเห็นว่ากฎหมายระหว่างประเทศเกี่ยวกับการควบคุมอาวุธเหล่านี้มีผลต่อการสร้างมายาคติในกฎหมายระหว่างประเทศว่าเมื่อใดก็ตามที่เกิดเทคโนโลยีทางอาวุธใหม่ๆ เกิดขึ้น ก็ควรจะสร้างกฎหมายระหว่างประเทศเรื่องใหม่ขึ้นมาเสมอ จนหลายครั้งนักกฎหมายระหว่างประเทศอาจลืมไปว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศที่ปรากฏในอนุสัญญาเจนีวาและพิธีสารเพิ่มเติมนั้นควรจะมีบทบาทอย่างไร เพราะในความเป็นจริงแล้วกฎหมายระหว่างประเทศหลายฉบับก็ไม่ได้มีการใช้งานเสมอไป นอกจากนั้นในบางกรณีก็ไม่สามารถแก้ไขปัญหาได้

การจำกัดการใช้อาวุธในสถานการณ์การขัดกันทางอาวุธตามหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศที่ปรากฏในพิธีสารฉบับที่ 1 เพื่อเพิ่มเติมอนุสัญญาเจนีวานั้นเป็นการห้ามใช้อาวุธ กระสุน และวัตถุที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น (Superfluous Injury and Unnecessary Suffering) และแม้จะมีการสร้างอนุสัญญาระหว่างประเทศเฉพาะเรื่องในการห้ามใช้อาวุธบางชนิด อนุสัญญาระหว่างประเทศเหล่านั้นก็ใช้หลักการพื้นฐานคือการห้ามใช้อาวุธที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นเช่นเดียวกัน

กรณีของการใช้เทคโนโลยีใหม่ในฐานะเป็นอาวุธในการขัดกันทางอาวุธจึงต้องสอดคล้องกับหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศคือการใช้เทคโนโลยีเหล่านี้จะต้องไม่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น

หลักเกณฑ์เกี่ยวกับการจำกัดการใช้อาวุธในยุคแรกที่ปรากฏในทางสังคมระหว่างประเทศคือ Lieber Code ของ Dr. Francis Lieber ในปี ค.ศ.1861[723] หลักเกณฑ์ดังกล่าวมีวัตถุประสงค์เพื่อใช้บังคับกับกรณีสงครามกลางเมืองในประเทศสหรัฐอเมริกา สาระสำคัญของหลักเกณฑ์คือการคำนึงถึงความจำเป็นทางการทหารที่จะต้องไม่ก่อให้เกิดผลกระทบที่เกินความจำเป็น อันได้แก่ การห้ามใช้วิธีการที่ก่อให้เกิดความทุกข์ทรมานแก่ศัตรู การห้ามกระทำที่มีลักษณะเป็นแก้นแค้น หรือการห้ามใช้สารพิษในการรบ[724] ซึ่งต่อมาในภายหลังหลักการดังกล่าวปรากฏในลักษณะข้อห้ามตามพิธีสารฉบับที่

[723] Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863. [online] Accessed: June 9, 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863

[724] Williams Boothby, Weapons and the Law of Armed Conflict, p. 5.

1 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 ในเรื่องการห้ามใช้อาวุธ วิธี หรือปัจจัยในการขัดกันทางอาวุธจะต้องไม่ก่อให้เกิดอันตรายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น[725]

ดังที่ได้กล่าวแล้วว่ากฎหมายมนุษยธรรมระหว่างประเทศมีเป้าหมายในการสร้างสมดุลระหว่างการปฏิบัติอย่างมีมนุษยธรรมและความจำเป็นทางการทหาร (Humanity and necessity)[726] ซึ่งพัฒนาการของกฎหมายทั้งสองแนวทางนี้มีจุดเริ่มต้นมาจากหลักเกณฑ์ว่าด้วยการขัดกันทางอาวุธของกฎเกณฑ์กรุงเฮกและหลักกฎหมายมนุษยธรรมระหว่างประเทศของอนุสัญญาเจนีวา ค.ศ. 1949 โดยในยุคเริ่มต้นของกฎหมายที่เกี่ยวข้องกับการควบคุมอาวุธในการขัดกันทางอาวุธนั้นเกิดขึ้นในช่วงปลายศตวรรษที่ 19 โดยเป็นที่รู้จักกันดีในชื่อของกฎหมายกรุงเฮก (Hague Law) ซึ่งว่าด้วยเรื่องการควบคุมการใช้อาวุธ วิธีการและปัจจัยในการสงคราม กฎหมายดังกล่าวนี้มีการใช้ควบคู่ไปกับกฎหมายอีกกลุ่มหนึ่งที่สร้างขึ้นมาเพื่อคุ้มครองบุคคลจากการขัดกันทางอาวุธ ซึ่งเป็นที่รู้จักกันดีในชื่อของกลุ่มกฎหมายเจนีวา (Geneva Law)[727] หรือที่ปรากฏในปัจจุบันคืออนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติม 2 ฉบับในปี ค.ศ.1977 ซึ่งพิธีสารเพิ่มเติมอนุสัญญาเจนีวาในปี ค.ศ.1977 นี้เป็นการรวมกันระหว่างกฎเกณฑ์กรุงเฮกและอนุสัญญาเจนีวา ทำให้การคุ้มครองความมีมนุษยธรรมในการขัดกันทางอาวุธและข้อกำหนดเกี่ยวกับความจำเป็นทางการทหารมาบรรจบกันในกฎหมายฉบับเดียวกัน

แม้จะมีกฎหมายว่าด้วยการขัดกันทางอาวุธกำหนดหลักการทั่วไปเกี่ยวกับการจำกัดการใช้อาวุธ วิธีการและปัจจัยที่ใช้ในการขัดกันทางอาวุธ แต่ก็ยังมีกฎหมายอีกกลุ่มหนึ่งที่ว่าด้วยเรื่องการควบคุมอาวุธ และการลดอาวุธในกรณีนอกเหนือการขัดกันทางอาวุธด้วย เช่น อนุสัญญาว่าด้วยอาวุธเคมี ค.ศ.1993 อนุสัญญาว่าด้วยอาวุธชีวภาพ ค.ศ.1992 หรืออนุสัญญาออตตาวาว่าด้วยทุ่นระเบิดสังหารบุคคล ค.ศ.1997 ฯลฯ ซึ่งอนุสัญญาเหล่านี้ ไม่ได้บังคับใช้แต่เฉพาะในกรณีที่เกิดการขัดกันทางอาวุธเท่านั้น แต่มีเป้าหมายในการห้ามการผลิต สะสม ถ่ายโอน และอื่นๆ[728] ทั้งนี้กฎหมายในสองกลุ่มดังกล่าวมีเป้าหมายในการบังคับใช้ที่แตกต่างกัน เช่นอนุสัญญาเฉพาะเรื่องที่ควบคุมอาวุธมักจะมีสาระสำคัญในการควบคุมการผลิต การพัฒนา การมีไว้ครอบครอง รวมถึงการแพร่กระจายอาวุธ ฯลฯ ในกรณีก่อนเกิดการขัดกันทางอาวุธและภายหลังการขัดกันทางอาวุธ ในขณะที่หลักการทั่วไปใน

---

[725] Geneva Convention 1949, Article 2 and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 35.

[726] Jean Pictet, Humanitarian Law and the Protection of War Victims, p. 28.

[727] Williams Boothby, Weapons and the Law of Armed Conflict, p. 2.

[728] Williams Boothby, Weapons and the Law of Armed Conflict, p. 3.

กฎหมายว่าด้วยเรื่องการใช้อาวุธเช่นพิธีสารเพิ่มเติมอนุสัญญาเจนีวาและกลุ่มกฎหมายกรุงเฮกเป็นหลักการที่บังคับใช้เมื่อเกิดการขัดกันทางอาวุธ (Jus in bello) กฎหมายทั้งสองกลุ่มจึงมีบทบาทในแต่ละช่วงเวลาที่แตกต่างกันตามเป้าหมายในการบังคับใช้ที่แตกต่างกัน อย่างไรก็ดีแม้อนุสัญญาเฉพาะเรื่องที่ควบคุมการใช้อาวุธเฉพาะอย่างจะมีข้อกำหนดที่ใช้นอกเหนือสถานการณ์การขัดกันทางอาวุธ แต่ก็ไม่ได้หมายความว่าอนุสัญญาเหล่านั้นจะสิ้นผลบังคับในระหว่างที่เกิดการขัดกันทางอาวุธ ในช่วงเวลาที่เกิดการขัดกันทางอาวุธจึงอาจมีกฎหมายที่บังคับใช้ทั้งสองกลุ่มแต่กฎหมายว่าด้วยเรื่องการใช้อาวุธจะเกี่ยวข้องโดยตรงกับกฎหมายมนุษยธรรมระหว่างประเทศ

ในยุคที่คณะกรรมการกาชาดระหว่างประเทศได้มีการประกาศใช้อนุสัญญาเจนีวา ค.ศ. 1949 มีการกำหนดขอบเขตที่อนุสัญญาฯ สามารถปรับใช้ได้ในกรณีที่เกิดการขัดกันทางอาวุธ (Armed Conflict) ซึ่งมีความหมายแตกต่างจากคำว่าสงคราม (War) โดยเดิมนั้นสงครามคือการต่อสู้ระหว่างรัฐและที่ยอมรับกันในอดีตว่าเป็นสงครามที่ชอบธรรมจะต้องเป็นสงครามที่มีการประกาศ[729]ในขณะที่ความขัดแย้งระหว่างประเทศในยุคสงครามโลกครั้งที่ 2 ซึ่งเป็นที่มาของการจัดทำอนุสัญญาเจนีวา ค.ศ.1949 นั้นได้มีการคำนึงถึงความขัดแย้งในรูปแบบอื่นทั้งในกรณีที่ไม่ใช่การทำสงครามระหว่างรัฐและกรณีสงครามที่ไม่ได้มีการประกาศ จึงมีการใช้คำว่าการขัดกันทางอาวุธ (Armed Conflict) เป็นขอบเขตหนึ่งที่กฎหมายมนุษยธรรมระหว่างประเทศสามารถนำมาปรับใช้ได้ อย่างไรก็ดีหากสังเกตขอบเขตการปรับใช้อนุสัญญาเจนีวา ค.ศ. 1949 และพิธีสารเพิ่มเติมจะปรากฏทั้งคำว่าสงครามและการขัดกันทางอาวุธ[730]หรืออาจกล่าวได้ว่ากฎหมายมนุษยธรรมระหว่างประเทศปรับใช้ได้กับทั้งกรณีที่เกิดสงครามและการขัดกันทางอาวุธซึ่งอาจเป็นส่วนหนึ่งของสงครามหรือที่อยู่นอกเหนือจากนิยามของสงครามโดยปกติก็ได้[731]

---

[729] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Commentary of 1987, para 59. [online] Accessed: May 10; 2022. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-1/commentary/1987?activeTab=undefined

[730] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Commentary of 1987, para 59, "...the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them"

[731] Françoise Bouchet-Saulnier, "The Practical Guide to Humanitarian Law," [online] Accessed: May 10, 2022. Available from: https://guide-humanitarian-law.org/content/article/3/war/

กฎหมายว่าด้วยเรื่องหลักเกณฑ์ที่ใช้ระหว่างที่เกิดการขัดกันทางอาวุธ (Jus in bello) หรือกฎหมายมนุษยธรรมระหว่างประเทศปรากฏในรูปแบบของอนุสัญญาระหว่างประเทศ เช่น อนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติม ค.ศ.1977 รวมตลอดถึงอนุสัญญากรุงเฮก ค.ศ.1907 เป็นต้น กฎหมายกลุ่มนี้เป็นกฎหมายระหว่างประเทศหลักที่ใช้ในการพิจารณาในงานวิจัยนี้เพื่ออธิบายว่าเมื่อมีการใช้เทคโนโลยีใหม่เกิดขึ้นในการขัดกันทางอาวุธแล้ว หลักการที่ปรากฏในกฎหมายมนุษยธรรมระหว่างประเทศจะนำมาปรับใช้ได้อย่างไร

ลักษณะการใช้งานเทคโนโลยีทางการทหารในปัจจุบันนั้นค่อนข้างมีความทับซ้อนกับการใช้งานเทคโนโลยีของพลเรือนอยู่พอสมควร เช่น การใช้งานระบบไซเบอร์ในสถานการณ์การขัดกันทางอาวุธย่อมมีทั้งการใช้งานของทหารและพลเรือน การใช้งานระบบไซเบอร์ของทหารและพลเรือนสามารถใช้ได้ทั้งนอกสถานการณ์การขัดกันทางอาวุธและในสถานการณ์การขัดกันทางอาวุธ ในอากาศยานไร้คนขับก็มีลักษณะการใช้งานที่ไม่แตกต่างกันคือทหารและพลเรือนสามารถใช้งานอากาศยานไร้คนขับในช่วงเวลาใดๆ ก็ได้ เทคโนโลยีไซเบอร์และการใช้อากาศยานไร้คนขับต่างก็มีไว้เพื่อวัตถุประสงค์ทางสันติ (เพื่อความบันเทิง การสันทนาการ ฯลฯ) และยังสามารถใช้เพื่อการโจมตีได้ (การโจมตีเครือข่ายการสื่อสารทางไซเบอร์ การใช้อากาศยานไร้คนขับในการทิ้งระเบิดหรือยิงอาวุธโจมตีเป้าหมาย ฯลฯ) เทคโนโลยีเหล่านี้จึงเป็นสิ่งที่มีอยู่ทั้งในและนอกสถานการณ์การขัดกันทางอาวุธ ในขณะที่วิธีการใช้จะเปลี่ยนแปลงไปตามผู้ใช้งาน[732]

นอกจากนั้น ลักษณะเฉพาะของเทคโนโลยีบางประการยังส่งผลต่อการพิจารณาสถานะทางกฎหมายมนุษยธรรมระหว่างประเทศด้วย เช่น การโจมตีทางไซเบอร์จะถือว่าเป็นการใช้กำลังทางทหารหรือไม่ การกระทำทางไซเบอร์มีผลเท่ากับการใช้อาวุธ (armed force) หรือไม่ หรือแม้แต่การโจมตีทางไซเบอร์จะทำให้เกิดการขัดกันทางอาวุธ (armed conflict) ได้หรือไม่[733]

กฎหมายว่าด้วยการขัดกันทางอาวุธให้ความสำคัญกับเรื่องการห้ามหรือจำกัดการใช้อาวุธหรือวิธีการในการขัดกันทางอาวุธที่จะก่อให้เกิดความทุกข์ทรมานเกินความจำเป็น[734]เพื่อไม่ให้รัฐคู่พิพาทใช้อาวุธหรือวิธีการที่เกินความจำเป็นทางการทหาร ประเด็นที่ต้องพิจารณาในการใช้อาวุธ

---

[732] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 28.

[733] Ibid., p. 26.

[734] International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, available at: https://www.refworld.org/docid/3ae6b36b4.html [accessed 28 May 2021], Art 35 (2).

หรือวิธีการในการการขัดกันทางอาวุธจึงได้แก่ 1) อาวุธหรือวิธีการใดที่สามารถใช้ในการขัดกันทางอาวุธได้ และ 2) อาวุธหรือวิธีการใดที่ห้ามใช้ในการขัดกันทางอาวุธ แม้การจำแนกกฎหมาย 2 ลักษณะดังกล่าวจะมีลักษณะในทางตรงข้ามกัน แต่ผู้วิจัยต้องการแยกประเด็นเป็น 2 ลักษณะ ดังนี้

ลักษณะที่ 1 อาวุธหรือวิธีการใดที่สามารถใช้ในการขัดกันทางอาวุธได้ หมายถึง หากอาวุธใดหรือวิธีการใดไม่เป็นการต้องห้ามตามกฎหมายอาวุธหรือวิธีการนั้นย่อมสามารถใช้ได้ เพราะในปฏิบัติการทางทหารเป็นไปเพื่อการทำลายฝ่ายตรงข้ามเพื่อให้เกิดความได้เปรียบในการรบ การใช้อาวุธหรือวิธีการเพื่อการต่อสู้เป็นเรื่องปกติที่ต้องเกิดขึ้น เพียงแต่อาวุธดังกล่าวจะต้องไม่สร้างความเสียหายเกินกว่าความจำเป็นทางการทหาร อาวุธหรือวิธีการขัดกันทางอาวุธที่สามารถใช้ได้ในการขัดกันทางอาวุธจึงหมายถึงกรณีที่ไม่ต้องมีกฎหมายระหว่างประเทศกำหนดหลักเกณฑ์ใดๆ ไว้[735]

ลักษณะที่ 2 อาวุธหรือวิธีการใดที่ห้ามใช้ในการขัดกันทางอาวุธ หมายถึง อาวุธและวิธีการในการขัดกันทางอาวุธบางลักษณะเป็นการต้องห้ามตามกฎหมาย ไม่ว่าจะเป็นไปตามพิธีสารเพิ่มเติมอนุสัญญาเจนีวาหรืออนุสัญญาระหว่างประเทศเฉพาะเรื่องที่ห้ามใช้อาวุธดังกล่าวก็ตาม การห้ามหรือจำกัดการใช้อาวุธหรือวิธีการขัดกันทางอาวุธจึงต้องมีกฎหมายกำหนดเอาไว้ ไม่ว่าจะเป็นไปโดยหลักพื้นฐานที่กำหนดไว้ในกฎหมายหรือเป็นไปตามหลักการเฉพาะของกฎหมายเฉพาะเรื่อง[736]

ดังนั้น การใช้อาวุธหรือวิธีการในขัดกันทางอาวุธที่เกี่ยวข้องกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธจึงต้องพิจารณาจากมุมมองทั้งสองประการด้วย หมายความว่าหากไม่มีข้อห้ามใดๆ ตามกฎหมาย เทคโนโลยีที่ถูกใช้เป็นอาวุธหรือวิธีการขัดกันทางอาวุธนั้นย่อมใช้ได้ แต่หากมีลักษณะการใช้เทคโนโลยีใดๆ ที่เป็นการละเมิดต่อหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศหรือเป็นการละเมิดต่ออนุสัญญาเฉพาะเรื่องเทคโนโลยีดังกล่าวต้องถูกจำกัดหรือห้ามใช้ในการขัดกันทางอาวุธ[737]

การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธสร้างความแตกต่างจากการใช้อาวุธและวิธีการในการขัดกันทางอาวุธในแบบเดิมคือเทคโนโลยีใหม่หลายชนิดไม่ได้ถูกออกแบบมาให้เป็นอาวุธแต่เป็นส่วนประกอบการใช้งานอาวุธในขณะที่เทคโนโลยีบางชนิดเป็นอาวุธโดยการออกแบบ ในขณะที่อาวุธตามแบบดั้งเดิมนั้นถูกออกแบบมาให้เป็นอาวุธโดยสภาพ

[735] Williams Boothby, Weapons and the Law of Armed Conflict, p. 5.

[736] Williams Boothby, Weapons and the Law of Armed Conflict, p. 5.

[737] Ibid., p. 9.

เทคโนโลยีที่ถูกออกแบบมาให้เป็นอาวุธย่อมถือเป็นปัจจัยในการขัดกันทางอาวุธ หากมีการใช้เทคโนโลยีเหล่านี้ให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นย่อมถือเป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศ เช่นการใช้อากาศยานไร้คนขับหรือการใช้หุ่นยนต์สังหารเพื่อการโจมตีจะต้องมีผลเท่ากับการต่อสู้ตามแบบในสงครามคือเป็นไปเพื่อทำลายเป้าหมายเฉพาะและการใช้งานตามปกติของอุปกรณ์จะต้องไม่ก่อให้เกิดความบาดเจ็บที่ไม่ใช่ความตายเช่นการทำให้พิการหรือทำให้ได้รับความทุกข์ทรมานเกินสมควร[738]

นอกจากนั้นการออกแบบอาวุธตามแบบแต่เดิมมีเป้าหมายในการทำลายทางกายภาพเป็นสำคัญแต่เทคโนโลยีใหม่ในการขัดกันทางอาวุธบางกรณีไม่มีลักษณะการทำลายทางกายภาพ[739] เช่นปฏิบัติการโจมตีทางไซเบอร์โดยทั่วไปมักก่อให้เกิดผลเสียหายต่อระบบสารสนเทศเป็นสำคัญ[740]แต่ในบางกรณีการโจมตีทางไซเบอร์ก็นำไปสู่ความเสียหายทางกายภาพได้เช่นปฏิบัติการ Stuxnet[741] การปรับใช้หลักการห้ามใช้ปัจจัยหรือวิธีการที่จะไม่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นนี้อาจเกิดข้อจำกัดในกรณีที่ไม่มีความเสียหายทางกายภาพเกิดขึ้นเนื่องจากความบาดเจ็บเกินขนาดเกี่ยวข้องกับผลทางกายภาพเช่นการบาดเจ็บทางกายเป็นสำคัญ ในขณะที่ความทุกข์ทรมานเกินความจำเป็นย่อมเกี่ยวข้องกับความรู้สึกทางจิตใจ[742] แต่ความเสียหายต่อระบบสารสนเทศอาจไม่เกี่ยวข้องกับทั้งความเสียหายทางกายและทางใจอย่างชัดเจน ตัวอย่างเช่นปฏิบัติการทางไซเบอร์เพื่อการทำลายการสื่อสารทางอินเทอร์เน็ตด้วยวิธีการ DDoS (Distribute Denial of Service) โดยปกติย่อมมีผลทำให้เว็บไซต์ไม่สามารถทำงานได้ตามปกติย่อมมีความหมายว่าการสื่อสารทางอินเทอร์เน็ตล้มเหลว การปฏิบัติการแบบ DDoS ในสถานการณ์การขัดกันทางอาวุธโดยพลรบย่อมถือเป็นปฏิบัติการทางทหาร โดยใช้เทคโนโลยีเป็นวิธีการทำลายการสื่อสารแต่การทำลายการสื่อสารดังกล่าวไม่ก่อให้เกิดความเสียหายทางกายภาพรวมถึงความเสียหายทางจิตใจอย่างชัดเจน ปฏิบัติการ DDoS ย่อมไม่เป็นการละเมิดต่อหลักการใช้วิธีการในการขัดกันทางอาวุธ เว้นแต่ว่า

---

[738] Stuart Casey-Maslen and Steven Haines, Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict, (London: Bloomsbury Publishing, 2018), p. 211.

[739] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

[740] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare.” Cyberpolitik Journal. 2 (4). (2018), p. 63.

[741] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 3.

[742] Stuart Casey-Maslen and Steven Haines, Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict, p. 211.

ในการโจมตีระบบการสื่อสารในปฏิบัติการ DDoS นี้จะมีผลกระทบต่อเนื่องประการอื่นเช่นเมื่อเว็บไซต์ล่มแล้วส่งผลให้ระบบการรักษาพยาบาลล้มเหลวหรือเว็บไซต์ล่มแล้วทำให้ระบบสาธารณูปโภคพื้นฐานไม่สามารถใช้การได้ ปฏิบัติการดังกล่าวแม้จะไม่เป็นการต้องห้ามตามหลักความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นแต่ย่อมถือเป็นการกระทำที่ไม่สอดคล้องต่อหลักความได้สัดส่วน (Proportionality) ในการโจมตีหรืออาจเป็นการละเมิดต่อหลักการคุ้มครองทรัพย์สินที่ใช้ร่วมกันของพลเรือน เป็นต้น

บางกรณีเทคโนโลยีใหม่ถูกนำมาใช้ประกอบร่วมกับการใช้อาวุธแต่เป็นไปเพื่อเพิ่มความแม่นยำในการโจมตีและลดความสูญเสียทางกำลังพล[743] เช่นการใช้อากาศยานไร้คนขับเพื่อการโจมตีหรือการใช้ระบบอาวุธสังหารอิสระอาจเป็นไปเพื่อการป้องกันประเทศ นอกจากนั้นเทคโนโลยีใหม่ยังถูกนำมาใช้ในการป้องกันการโจมตีและการให้ความช่วยเหลือทางมนุษยธรรม เช่น การใช้ระบบอาวุธป้องกันภัยทางอากาศ การใช้ระบบพาหนะไร้คนขับเพื่อการเก็บกู้ระเบิดและการใช้พาหนะไร้คนขับเพื่อค้นหาผู้บาดเจ็บ เป็นต้น การพิจารณาว่าเทคโนโลยีใดสามารถใช้ได้และเทคโนโลยีใดจะเป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศจึงต้องพิจารณาเป็นรายกรณีไป หากการใช้งานเทคโนโลยีเป็นไปเพื่อการให้ความช่วยเหลือทางมนุษยธรรมเช่นการใช้หุ่นยนต์เก็บกู้วัตถุระเบิดในหรือการใช้หุ่นยนต์ช่วยเหลือผู้บาดเจ็บและลำเลียงผู้บาดเจ็บในสนามรบย่อมเป็นวิธีการในการสงครามกระทำที่สอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศและไม่เป็นการต้องห้ามกระทำ

ปัจจัยสำคัญที่เปลี่ยนแปลงไปคือการห้ามใช้อาวุธที่ก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นนั้นอาจไม่สามารถใช้ได้กับเทคโนโลยีใหม่นี้ทั้งหมดได้ จะต้องพิจารณาความเสียหายที่เกิดขึ้นจากการใช้งานเทคโนโลยีแต่ละประเภทเป็นรายกรณีไป

3.3.1.3 การห้ามใช้อุบายล่อลวง (Perfidy)

หลักการห้ามล่อลวงเป็นการจำกัดวิธีการในสงครามโดยห้ามการกระทำที่ทำให้ฝ่ายปฏิปักษ์เกิดความไว้วางใจหรือความเข้าใจผิดว่าผู้ล่อลวงนั้นมีสิทธิได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศและมีเจตนาหักหลังความไว้วางใจนั้น อันได้แก่ การแสร้งว่ายอมจำนนหรือพักรบ การแสร้งว่าไร้ความสามารถ บาดเจ็บหรือป่วย หารแสร้งว่ามีสถานภาพเป็นพลเรือน และ

[743] Ibid., p. 28.

การแสร้งว่าเป็นผู้ได้รับความคุ้มครองโดยแสดงเครื่องหมายหรือสัญญาณที่ได้รับความคุ้มครอง[744] ขณะที่การใช้กลอุบายบางลักษณะไม่ถือว่าเป็นการล่อลวงตามกฎหมายมนุษยธรรมระหว่างประเทศ เพราะไม่ใช่การชักจูงให้เกิดความวางใจในเรื่องการคุ้มครองตามกฎหมาย เช่น การใช้เครื่องอำพราง เครื่องล่อ ปฏิบัติการลวง และการให้ข้อมูลที่ไม่ถูกต้อง

ปฏิบัติการทางไซเบอร์ซึ่งเป็นที่นิยมใช้ทั้งในสถานการณ์การขัดกันทางอาวุธและนอกสถานการณ์การขัดกันทางอาวุธคือปฏิบัติการทางข้อมูลข่าวสาร (Information Operation) โดยในสถานการณ์ความขัดแย้งระหว่างยูเครนและรัสเซียก็ปรากฏการใช้ปฏิบัติการทางข้อมูลข่าวสาร เช่น การเผยแพร่ภาพกองกำลังรัสเซียที่เข้าไปในพื้นที่ต่างๆ ของยูเครนและความพยายามสื่อสารว่ากองกำลังรัสเซียเหล่านั้นเข้ามาในพื้นที่ยูเครนโดยไม่ทราบข้อมูลว่าต้องทำอะไร ในขณะที่บางกรณีมีการสื่อสารในสื่อโซเชียลเน็ตเวิร์คว่าทหารรัสเซียเหล่านั้นไม่พร้อมรบและต้องการกลับบ้าน แม้กระทั่งภาพนิ่งและภาพเคลื่อนไหวการปฏิบัติการตอบโต้ของกองทัพยูเครนต่อกองทัพรัสเซียในพื้นที่ต่างๆ โดยเฉพาะอย่างยิ่งภาพความสำเร็จในการทำลายกองกำลังรัสเซียฯลฯ ข้อมูลเหล่านี้แม้จะไม่มีผลโดยตรงต่อการแพ้ชนะในสงครามแต่เป็นการสื่อสารที่ทำลายความน่าเชื่อถือของกองทัพรัสเซียต่อสายตาชาวโลกและเป็นการเพิ่มขวัญและกำลังใจให้กองทัพยูเครน

ภาพข่าวที่ปรากฏในปฏิบัติการทางข้อมูลข่าวสารดังกล่าวไม่ว่าจะเป็นเรื่องจริงหรือไม่ก็ไม่มีลักษณะเป็นการล่อลวงตามหลักกฎหมายมนุษยธรรมระหว่างประเทศเนื่องจากไม่ใช่การที่พลรบยูเครนทำการล่อลวงพลรบรัสเซียให้เข้าใจผิดว่าพลรบยูเครนได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศแต่เป็นการปฏิบัติการทางข้อมูลข่าวสารที่มีผลต่อขวัญและกำลังใจของพลรบและพลเรือนชาวยูเครนและอาจมีผลกระทบเชิงจิตวิทยาต่อพลรบรัสเซียเท่านั้น ลักษณะการปฏิบัติการทางข้อมูลข่าวสารที่ปรากฏในสถานการณ์ความขัดแย้งระหว่างประเทศยูเครนและประเทศรัสเซียจึงไม่มีลักษณะเป็นการล่อลวงแต่อย่างใด

ปฏิบัติการทางไซเบอร์ลักษณะหนึ่งที่นิยมใช้เพื่อนำไปสู่การโจมตีทางไซเบอร์คือการใช้โทรจันคอมพิวเตอร์ซึ่งมีมัลแวร์หรือโปรแกรมประสงค์ร้ายอยู่ในโทรจัน เมื่อเครื่องคอมพิวเตอร์เครื่องใดดาวน์โหลดโปรแกรมคอมพิวเตอร์ที่มีโทรจันแฝงอยู่ก็จะรับเอาโปรแกรมประสงค์ร้ายเข้าไปด้วย ลักษณะการทำงานของโทรจันคอมพิวเตอร์นี้มีความคล้ายคลึงกับอุบายที่ทหารสปาร์ต้าใช้ล่อลวงพลเมืองชาวทรอยให้นำม้าไม้ซึ่งบรรจุทหารอยู่ภายในเข้าไปในเมืองทรอยทำให้ทหารสปาร์ต้าสามารถรบชนะเมือง

[744] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 37 (1).

ทรอยได้ หากเทียบการใช้งานโปรแกรมโทรจันกับม้าไม้เมืองทรอยจะมีลักษณะที่ไม่แตกต่างกัน แต่สิ่งที่แตกต่างกันอย่างมากคือม้าไม้เมืองทรอยเป็นการใช้อุบายเพื่อนำไปสู่การฆาตกรรมแต่การใช้โปรแกรมโทรจันนำไปสู่การติดเชื้อมัลแวร์ในคอมพิวเตอร์ไม่ได้นำไปสู่การฆาตกรรม โปรแกรมโทรจันคอมพิวเตอร์จึงไม่มีลักษณะเป็นการหลอกให้ศัตรูหลงเชื่อว่าตนเองได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศจึงไม่เป็นการล่อลวงตามกฎหมาย

การใช้เทคโนโลยีลดการตรวจจับเช่นเทคโนโลยี Stealth มีวัตถุประสงค์เพื่อทำให้ศัตรูมองเห็นได้ยากขึ้นหรือตรวจจับด้วยอุปกรณ์ตรวจจับได้ยากขึ้น เทคโนโลยี Stealth นิยมใช้กับยานพาหนะเป็นสำคัญ อย่างไรก็ดีเทคโนโลยีลดการตรวจจับในรูปแบบอื่นนอกเหนือจาก Stealth มีการนำมาใช้งานกับเครื่องแต่งกายและอาวุธประจำกายพลรบในรูปแบบเครื่องแบบพราง (Camouflage)[745] หรืออาวุธพราง โดยพัฒนาการในยุคปัจจุบันสามารถใช้เทคโนโลยีวัสดุศาสตร์ออกแบบชุดพรางของทหารให้สามารถหักเหแสงทำให้ดวงตามนุษย์ไม่สามารถมองเห็นได้ในบางมุม เครื่องแบบชนิดนี้ทำให้ทหารอยู่ในสภาพคล้ายการล่องหนทำให้ประสิทธิภาพของพลรบมีสูงขึ้นและมีโอกาสถูกโจมตีลดลง

โดยปกติเครื่องแบบพรางของทหารไม่ถือเป็นการล่อลวงตามกฎหมายมนุษยธรรมระหว่างประเทศตามข้อ 37 วรรค 2 เพราะไม่มีวัตถุประสงค์ทำให้ฝ่ายศัตรูเข้าใจผิดว่าผู้ใช้เครื่องแบบพรางเป็นบุคคลที่ได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ การใช้เครื่องแบบล่องหนก็มีผลไม่แตกต่างจากการใช้เครื่องแบบพรางเพราะเป็นไปเพื่อความได้เปรียบในการรบแต่ไม่ได้เป็นไปเพื่อให้เกิดความเข้าใจผิดว่าบุคคลที่ใช้เครื่องแบบล่องหนได้รับความคุ้มครองตามกฎหมาย ในกรณีนี้ย่อมรวมถึงการใช้อาวุธที่ใช้เทคโนโลยีลดการตรวจจับหรืออาวุธล่องหนด้วย อาวุธล่องหนจึงไม่ถือเป็นการล่อลวงเช่นกัน อย่างไรก็ดีหากมีการใช้เครื่องแบบล่องหนหรืออาวุธล่องหนร่วมกับอุบายว่าตนเองไม่สามารถทำการสู้รบได้ก็อาจนำไปสู่การล่อลวงได้ เช่นการแสร้งว่ายอมจำนนในขณะที่มีการซ่อนอาวุธที่มองไม่เห็นไว้แต่เมื่อฝ่ายศัตรูจะเข้าทำการควบคุมตัวกลับถูกฝ่ายที่ยอมจำนนโจมตีตอบโต้เป็นต้น อย่างไรก็ดีพฤติการณ์ดังกล่าวจะทำให้การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต้องคำนึงถึงปัจจัยที่มีความซับซ้อนมากขึ้นและอาจเป็นการยากที่จะพิสูจน์การละเมิดกฎหมายมนุษยธรรมระหว่างประเทศในกรณีที่เกิดเหตุการณ์ดังกล่าวขึ้น

[745] เครื่องแบบพรางของทหารสามารถใช้ได้โดยสอดคล้องกับข้อ 37 (2) ของพิธีสารฉบับที่ 1 ค.ศ.1977 เพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1949

ปัญหาที่น่าสนใจคือหากมีการใช้หุ่นยนต์สังหารแทนการใช้ทหารที่เป็นมนุษย์โดยหุ่นยนต์ดังกล่าวมีความสามารถในการใช้อุบายล่อลวงทหารที่เป็นมนุษย์ได้ว่าหุ่นยนต์ดังกล่าวไม่สามารถทำการต่อสู้ได้หรือทำการยอมแพ้จนทหารที่เป็นมนุษย์หลงเชื่อในอุบายดังกล่าวและนำไปสู่การที่หุ่นยนต์ฆาตกรรมทหารมนุษย์ซึ่งหลงเชื่ออุบายล่อลวงดังกล่าว เช่นนี้จะถือว่าเป็นการกระทำที่เป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ หากการกระทำดังกล่าวเป็นการล่อลวง (Perfidy) ตามกฎหมายมนุษยธรรมระหว่างประเทศใครจะเป็นผู้รับผิดชอบจากการกระทำดังกล่าว

3.3.2 หลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศกับเทคโนโลยีใหม่ในการขัดกันทางอาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศมีเป้าหมายสำคัญในการจำกัดการทำสงครามให้สอดคล้องกับความจำเป็นทางการทหารโดยจะต้องควบคุมไม่ให้เกิดการกระทำที่ไร้มนุษยธรรม หลักการพื้นฐานสำคัญประการแรกที่กฎหมายมนุษยธรรมระหว่างประเทศให้ความสำคัญคือหลักการแยกแยะระหว่างเป้าหมายทางการทหารและเป้าหมายพลเรือนโดยในการโจมตีแต่ละครั้งจะต้องกระทำต่อเป้าหมายทางการทหารเท่านั้น การโจมตีต่อเป้าหมายพลเรือนโดยตรงย่อมเป็นการต้องห้าม

อย่างไรก็ดีการโจมตีเฉพาะเป้าหมายทางการทหารในทางปฏิบัติย่อมเป็นไปได้ค่อนข้างยาก หากการโจมตีอาจนำไปสู่ผลกระทบต่อพลเรือนด้วยจะต้องคำนึงถึงสัดส่วนความเสียหายแก่พลเรือนที่จะเกิดขึ้นจากการโจมตีนั้นด้วยและเพื่อป้องกันไม่ให้การโจมตีแต่ละครั้งจะนำไปสู่ความเสียหายแก่พลเรือนที่เกินความจำเป็นทางการทหารในการรบการโจมตีแต่ละครั้งจึงต้องคำนึงถึงความระมัดระวังล่วงหน้าก่อนการโจมตีด้วย หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศเหล่านี้จะนำมาปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธได้มากน้อยเพียงไรจึงเป็นประเด็นที่ต้องพิจารณา

3.3.2.1 หลักการแยกแยะเป้าหมาย

หลักการแยกแยะเป้าหมายได้มีการบัญญัติเอาไว้ในข้อ 48 ข้อ 51 (4), (5) และข้อ 52 (2) ของพิธีสารฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ. 1949 โดยเป็นข้อห้ามการใช้กำลังทางทหารเพื่อโจมตีพลเรือนโดยตรง และหลักเกณฑ์ข้อนี้สอดคล้องกับหลักเกณฑ์ ข้อ 8 (2) (b) (ii)

ของธรรมนูญศาลยุติธรรมระหว่างประเทศ กล่าวคือ การกระทำโดยเจตนาเพื่อโจมตีต่อพลเรือนโดยตรง โดยมิใช่เป้าหมายทางการทหาร การกระทำนั้นย่อมเป็นความผิดฐานอาชญากรรมสงคราม[746]

หลักการแยกแยะตามข้อ 51 ของพิธีสาร ฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 ตามข้อ 51 การคุ้มครองประชากรพลเรือนกำหนดว่า

"1. ประชากรพลเรือน และพลเรือนปัจเจกบุคคลจักได้รับความคุ้มครองทั่วไปจากภยันตรายที่เกิดขึ้นจากปฏิบัติการทางทหาร ในการอำนวยผลในเรื่องความคุ้มครองดังกล่าว จักต้องให้การพิจารณาในทุกพฤติการณ์ถึงกฎต่างๆ ซึ่งผนวกเพิ่มเติมต่อหลักของกฎหมายระหว่างประเทศที่ใช้บังคับอื่นๆ ดังที่จักได้กล่าวถึงต่อไป

2. ประชากรพลเรือนดังกล่าว ตลอดจนพลเรือนปัจเจกบุคคล จักไม่ตกเป็นเป้าหมายของการโจมตี ห้ามมิให้มีการกระทำ หรือการคุกคามว่าจะใช้ความรุนแรง โดยมีวัตถุประสงค์เบื้องต้นเพื่อเป็นการสร้างความหวาดกลัวให้แพร่หลายไปในหมู่ประชากรพลเรือน

3. พลเรือนจักได้รับความคุ้มครองตามที่ได้บัญญัติไว้ในหมวดนี้ เว้นแต่ว่าและตราบเท่าช่วงเวลาที่พลเรือนนั้นเข้ามีส่วนร่วมในการสู้รบโดยตรง

4. ห้ามมิให้มีการโจมตีในลักษณะการไม่เลือกปฏิบัติ การโจมตีในลักษณธการไม่เลือกปฏิบัติได้แก่

(ก) การโจมตีโดยไม่ได้กระทำโดยตรงต่อเป้าหมายทางการทหารในลักษณะเฉพาะ

(ข) การโจมตีโดยใช้วิธีการหรือปัจจัยการรบ ซึ่งไม่สามารถเพ่งเล็งต่อเป้าหมายทางทหารในลักษณะเฉพาะได้ หรือ

(ค) การโจมตีโดยใช้วิธีการหรือปัจจัยการรบซึ่งก่อให้เกิดผลอันไม่สามารถจำกัดขอบเขตได้ตามที่กำหนดไว้ในพิธีสารฉบับนี้และจักเป็นผลให้การโจมตีแต่ละกรณีเช่นว่ามีลักษณะเป็นการทำลายเป้าหมายทางทหารและพลเรือน หรือทรัพย์สิ่งของพลเรือนโดยปราศจากซึ่งการจำแนก

5. นอกจากกรณีอื่นๆ แล้ว รูปแบบของการโจมตีต่อไปนี้ให้ถือว่าเป็นการโจมตีที่มีลักษณะไม่เลือกปฏิบัติ

(ก) การโจมตีในลักษณะการระดมการใช้วิธีการหรือปัจจัยใดๆ ซึ่งปฏิบัติการต่อเป้าหมายทางทหารหลายจุดที่แยกกันอย่างเห็นได้ชัด ซึ่งตั้งอยู่ในนคร เมือง หมู่บ้าน หรือบริเวณอื่นใด

---

[746] Jean-Marie Hanckaerts, and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, (New York: Cambridge University Press, 2009), p. 25.

อันมีการจุกตัวกันอยู่ของพลเรือน หรือเป้าหมายพลเรือนโดยถือเสมือนว่าเป็นเป้าหมายทางทหารอยู่แห่งเดียว

(ข) การโจมตีซึ่งอาจคาดได้ว่าจะยังผลให้เกิดการสูญเสียชีวิตของพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์สิ่งของพลเรือน หรือความเสียหายดังกล่าวรวมกัน ซึ่งทั้งนี้เป็นความสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหารที่มีลักษณะเป็นรูปธรรม และโดยตรงอันได้คาดหมายไว้

6. ห้ามมิให้มีการโจมตีต่อประชากรพลเรือน หรือพลเรือนในลักษณะการตอบโต้

7. จักไม่ให้มีการใช้ การที่มี หรือการเคลื่อนย้ายของประชากรพลเรือนหรือพลเรือนปัจเจกบุคคล เพื่อประโยชน์บางแห่ง หรือบางท้องที่ได้รับความคุ้มกันจากการปฏิบัติการทางทหาร โดยเฉพาะในความพยายามที่จะปกป้องเป้าหมายทางการทหารจากการโจมตี หรือจะปกป้องสนับสนุน หรือขัดขวางการปฏิบัติการทางทหาร ภาคีคู่พิพาทจักไม่สั่งการเคลื่อนย้ายประชากรพลเรือนหรือพลเรือนปัจเจกบุคคล เพื่อวัตถุประสงค์ที่จะปกป้องเป้าหมายทางทหารจากการโจมตี หรือปกป้องกันการปฏิบัติการทางทหาร

8. การละเมิดในข้อห้ามดังกล่าว จักไม่ทำให้ภาคีคู่พิพาทพ้นจากพันธกรณีทางกฎหมายที่เกี่ยวกับประชากรพลเรือน และพลเรือนปัจเจกบุคคลตลอดจนพันธกรณีที่จักใช้มาตรการการระมัดระวังล่วงหน้าตามที่ได้กำหนดไว้ในข้อ 57”

หลักการนี้ได้มีการกล่าวอ้างถึงในคดีสำคัญ เช่น คดี 1996 Legality of the Threats or Use of Nuclear Weapons โดยในความเห็นเชิงแนะนำของศาลยุติธรรมระหว่างประเทศให้ทัศนะว่า เป็นหลักจารีตประเพณีระหว่างประเทศที่จะล่วงละเมิดมิได้ (intransgressible principles of international law)[747] ทั้งนี้ เป้าหมายทางการทหารย่อมหมายถึง เป้าหมายซึ่งโดยสภาพ ที่ตั้ง วัตถุประสงค์ หรือการใช้งานเป็นไปเพื่อประสิทธิภาพในการปฏิบัติงานทางทหาร ซึ่งจะต้องถูกแยกออกมาเป็นลักษณะเฉพาะเพื่อประโยชน์ทางการทหารเท่านั้น[748]

ขณะที่เป้าหมายพลเรือน หมายถึง พื้นที่ทั่วไปที่พลเรือนใช้ประโยชน์ เมือง หมู่บ้าน ที่พักอาศัย อาคาร บ้าน โรงเรียน โรงพยาบาล ศาสนสถาน อนุสาวรีย์ รวมถึงทรัพย์สินทางวัฒนธรรม และ

---

[747] ICJ, 1996 Legality of the Threats or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, para 79, p.257.

[748] Jean-Marie Hanckaerts, and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.29.

สิ่งแวดล้อมทางธรรมชาติ[749] อย่างไรก็ดี หากเป้าหมายพลเรือนถูกนำไปใช้เพื่อประโยชน์ทางการทหารเพื่อการขัดกันทางอาวุธ เป้าหมายพลเรือนดังกล่าวย่อมไม่ได้รับความคุ้มครองตามหลักการนี้อีกต่อไป เว้นเสียแต่ในกรณีที่เกิดความไม่ชัดเจนว่าสถานที่ของพลเรือนนั้นถูกใช้เพื่อประโยชน์ทางการทหารหรือไม่ พื้นที่ดังกล่าวจะได้รับความคุ้มครองตามหลักบทสันนิษฐานว่าเป็นเป้าหมายทางพลเรือน (Presumption of Civilian Character)[750] จึงยังคงได้รับความคุ้มครองตามกฎหมาย

นอกเหนือจากการกำหนดเรื่องการคุ้มครองเป้าหมายที่เกี่ยวกับทรัพย์สินพลเรือนแล้ว การคุ้มครองร่างกายพลเรือนยังแสดงผ่านหลักการแยกพลรบออกจากพลเรือนตามอนุสัญญาเจนีวา ค.ศ. 1949 3 ฉบับแรก โดยพลรบที่แบ่งแยกจากพลเรือนได้จะต้องมีเครื่องหมายกำหนดไว้เด่นชัดและเห็นได้ในระยะไกล ถืออาวุธโดยเปิดเผย และปฏิบัติการรบตามกฎและประเพณีสงคราม[751] ทั้งนี้เพื่อให้พลเรือนมีลักษณะแตกต่างจากพลรบ และพลเรือนจะไม่ตกเป็นเป้าหมายของการโจมตีนั่นเอง หลักเกณฑ์นี้ยังสอดคล้องกับข้อ 1 ของ 1907 Hague Regulation ด้วยเช่นกัน

หลักการแยกแยะเป้าหมายเป็นหลักการพื้นฐานสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ โดยเป็นส่วนหนึ่งของหลักการกระทำอันเป็นปรปักษ์ซึ่งรวมถึงการใช้วิธี (methods) และปัจจัย (means) ในการขัดกันทางอาวุธ[752] ทั้งนี้ ปัจจัยย่อมหมายรวมถึงอาวุธที่ใช้ในการขัดกันทางอาวุธ และอุปกรณ์ที่เกี่ยวข้องกับการใช้งานอาวุธเหล่านั้น ส่วนวิธีการย่อมหมายความถึงการใช้อาวุธและวิธีการในการใช้กำลังเพื่อการขัดกันทางอาวุธ[753] โดยนัยนี้ การกระทำไม่ว่าจะเป็นการใช้วิธีการหรือการใช้อาวุธใดๆ หากเป็นไปเพื่อประโยชน์ในการขัดกันทางอาวุธ และผู้ใช้วิธีการหรืออาวุธนั้นสังกัดอยู่ในกองทัพหรืออาจจำแนกได้ว่าเป็นผู้มีส่วนร่วมโดยตรงในการสู้รบ ย่อมถือว่าการกระทำนั้นๆ อยู่ในบังคับของกฎหมายมนุษยธรรมระหว่างประเทศด้วย

ปัญหาที่เกิดขึ้นในปัจจุบันคือการใช้งานสาธารณูปโภคขั้นพื้นฐาน เช่น การสื่อสาร และการคมนาคมขนส่ง ทั้งทางการทหารและทางพลเรือนมักจะมีการใช้งานร่วมกัน (Dual-use facilities) จึงเกิดประเด็นว่า เป้าหมายทางการทหารมีความหมายครอบคลุมถึงพื้นที่ หรือการใช้งานในลักษณะใด พบว่าในทางปฏิบัตินั้น คู่มือในการปฏิบัติการทางทหารของหลายประเทศได้ทำการจำแนกเป้าหมายทางการทหารโดยพิจารณาจากรูปแบบการใช้งานว่าเป็นไปเพื่อการทหารมากน้อยเพียงไรเป็นสำคัญ

---

[749] Ibid., p.34.

[750] Ibid., p.35

[751] ปรากฏในข้อ 13 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 และฉบับที่ 2 และข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3

[752] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 1.

[753] Ibid., p. 1.

หากมีการใช้งานการสื่อสาร หรือช่องทางการคมนาคมใดเพื่อประโยชน์ทางการทหารเป็นสำคัญ ย่อมอาจจำแนกได้ว่าพื้นที่ หรือช่องทางดังกล่าวคือเป้าหมายทางการทหารด้วยเช่นกัน[754]

ในปัจจุบันปรากฏการใช้เทคโนโลยีเพื่อประโยชน์ในการขัดกันทางอาวุธมากขึ้น โดยเฉพาะอย่างยิ่งการใช้ระบบไซเบอร์เพื่อการโจมตี การใช้ระบบสื่อสารผ่านดาวเทียมเพื่อประโยชน์ในการระบุตำแหน่งเป้าหมายการโจมตี และการใช้ระบบประมวลผลของอาวุธที่สามารถตัดสินใจทำลายเป้าหมายได้ด้วยตนเอง ซึ่งนำไปสู่ข้อพิจารณาถึงการนำกฎหมายมนุษยธรรมระหว่างประเทศในส่วนที่เกี่ยวข้องกับการพิจารณาการกระทำอันเป็นปรปักษ์ โดยเฉพาะเรื่องการแยกแยะเป้าหมายในการโจมตีว่ากฎหมายมนุษยธรรมระหว่างประเทศจะสามารถคุ้มครองบุคคลที่ไม่มีส่วนเกี่ยวข้องโดยตรงกับการสู้รบได้อย่างไร เนื่องจากเทคโนโลยีที่มีการใช้ในปัจจุบันนี้ปรากฏในลักษณะการใช้งานทั้งทางการทหารและเพื่อวัตถุประสงค์ของพลเรือน จึงจำเป็นต้องมีการพิจารณาถึงเงื่อนไขในการปรับใช้กฎหมายในกรณีต่างๆ อย่างชัดเจนมากขึ้น

แนวคิดพื้นฐานเรื่องการแยกแยะเป้าหมายเป็นหัวใจสำคัญเพื่อไม่ให้การขัดกันทางอาวุธนำไปสู่ความรุนแรงหรือความเสียหายมากเกินขอบเขตความจำเป็น หลักการนี้ปรากฏในกฎเกณฑ์พื้นฐานข้อ 35 ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ. 1949 โดยกำหนดให้คู่พิพาทในการขัดกันทางอาวุธจะต้องจำกัดวิธีการ (Methods) และปัจจัย (Means) ในการทำสงคราม[755] นอกจากนั้น สิ่งที่รัฐผู้ทำการสู้รบกันจะต้องให้ความสำคัญเป็นลำดับแรกคือการแยกแยะระหว่างพลเรือนกับทหาร โดยแนวคิดว่าพลเรือนคือผู้บริสุทธิ์ที่ควรได้รับความคุ้มครองเฉพาะทหารและผู้มีส่วนร่วมโดยตรงในการสู้รบเท่านั้นจึงจะตกเป็นเป้าหมายในการโจมตีได้[756] หลักการแยกแยะนี้จึงนับได้ว่าเป็นหลักพื้นฐานที่สำคัญประการแรกในกฎหมายมนุษยธรรมระหว่างประเทศ[757] และปรากฏหลักการนี้ในตราสารทางด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายฉบับ

หลักการแยกแยะปรากฏในข้อ 48 ข้อ 51 (4), (5) และข้อ 52 (2) ของพิธีสารฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ. 1949 โดยเป็นข้อห้ามการใช้กำลังทางทหารเพื่อโจมตีพลเรือน

---

[754] Ibid., p. 32.

[755] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 35, "1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited."

[756] W. J. Fenrick, "The Law Applicable to Targeting and Proportionality after Operation Allied Force: A View from the Outside," Yearbook of International Humanitarian Law, Vol. 3 (2000): pp. 53-66.

[757] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 62.

โดยตรง ในการขัดกันทางอาวุธจึงต้องมีการแยกแยะพลเรือนและทรัพย์สินพลเรือนออกจากพลรบซึ่งเป็นเป้าหมายทางทหาร และหลักเกณฑ์ข้อนี้สอดคล้องกับหลักเกณฑ์ ข้อ 8 (2) (b) (ii) ของธรรมนูญศาลยุติธรรมระหว่างประเทศ กล่าวคือ การกระทำโดยเจตนาเพื่อโจมตีต่อพลเรือนโดยตรง โดยมิใช่เป้าหมายทางการทหาร การกระทำนั้นย่อมเป็นความผิดฐานอาชญากรรมสงคราม[758] นอกจากนั้น ยังปรากฏหลักการแยกแยะนี้ในข้อ 1 ของกฎเกณฑ์กรุงเฮก ค.ศ. 1907 เรื่องการกำหนดคุณสมบัติของคู่พิพาทในการขัดกันทางอาวุธ[759] หลักการนี้ได้มีการกล่าวอ้างถึงในคดีสำคัญ เช่น คดี 1996 Legality of the Threats or Use of Nuclear Weapons โดยในความเห็นเชิงแนะนำของศาลยุติธรรมระหว่างประเทศให้ทัศนะว่า เป็นการแยกแยะนี้เป็นหลักจารีตประเพณีระหว่างประเทศที่จะล่วงละเมิดมิได้ (Intransgressible principle)[760]

การแยกแยะระหว่างพลเรือนและพลรบนี้เป็นไปเพื่อกำหนดเป้าหมายการโจมตีที่ชอบด้วยกฎหมายในการขัดกันทางอาวุธ ซึ่งจะต้องเป็นเป้าหมายทางการทหารเท่านั้น ทั้งนี้ เป้าหมายทางการทหารหมายถึง เป้าหมายซึ่งโดยสภาพ ที่ตั้ง วัตถุประสงค์ หรือการใช้งานเป็นไปเพื่อประสิทธิภาพในการปฏิบัติงานทางทหาร ซึ่งจะต้องถูกแยกออกมาเป็นลักษณะเฉพาะเพื่อประโยชน์ทางการทหารเท่านั้น[761] โดยนัยนี้การแยกแยะเป้าหมายจึงมีความหมายทั้งการแยกระหว่างพลเรือนและพลรบ รวมถึงการแยกแยะทรัพย์สินสิ่งของของพลเรือนและพลรบด้วยเช่นกัน[762]

ขณะที่เป้าหมายพลเรือน หมายถึง พื้นที่ทั่วไปที่พลเรือนใช้ประโยชน์ เมือง หมู่บ้าน ที่พักอาศัย อาคาร บ้าน โรงเรียน โรงพยาบาล ศาสนสถาน อนุสาวรีย์ รวมถึงทรัพย์สินทางวัฒนธรรม และสิ่งแวดล้อมทางธรรมชาติ[763] อย่างไรก็ดี หากเป้าหมายพลเรือนถูกนำไปใช้เพื่อประโยชน์ทางการทหารเพื่อการขัดกันทางอาวุธ เป้าหมายพลเรือนดังกล่าวย่อมไม่ได้รับความคุ้มครองตามหลักการนี้อีกต่อไป เว้นเสียแต่ในกรณีที่เกิดความไม่ชัดเจนว่าสถานที่ของพลเรือนนั้นถูกใช้เพื่อประโยชน์ทางการทหาร

---

[758] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.25.

[759] Article 1 of Annex to the Convention Regulations Respecting the Laws and Customs of War on Land 1907.

[760] ICJ, 1996 Legality of the Threats or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, para 79, p.257.

[761] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.29.

[762] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p 62.

[763] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules,, p.34.

หรือไม่ พื้นที่ดังกล่าวจะได้รับความคุ้มครองตามหลักบทสันนิษฐานว่าเป็นเป้าหมายทางพลเรือน (Presumption of Civilian Character)[764] จึงยังคงได้รับความคุ้มครองตามกฎหมาย

นอกเหนือจากการกำหนดเรื่องการคุ้มครองเป้าหมายที่เกี่ยวกับทรัพย์สินพลเรือนแล้ว การคุ้มครองร่างกายพลเรือนยังแสดงผ่านหลักการแยกพลรบออกจากพลเรือนตามอนุสัญญาเจนีวา ค.ศ. 1949 3 ฉบับแรก โดยพลรบที่แบ่งแยกจากพลเรือนได้จะต้องมีเครื่องหมายกำหนดไว้เด่นชัดและเห็นได้ในระยะไกล ถืออาวุธโดยเปิดเผย และปฏิบัติการรบตามกฎและประเพณีสงคราม[765] ทั้งนี้เพื่อให้พลเรือนมีลักษณะแตกต่างจากพลรบ และพลเรือนจะไม่ตกเป็นเป้าหมายของการโจมตีนั่นเอง นอกจากนี้หลักเกณฑ์การแยกแยะนี้ยังสอดคล้องกับข้อ 1 ของ Hague Regulation ค.ศ. 1907 ด้วยเช่นกัน

หลักการคุ้มครองพลเรือนโดยการแยกเป้าหมายระหว่างพลเรือนออกจากพลรบนั้นเกิดขึ้นเฉพาะพลเรือนที่ไม่มีส่วนร่วมโดยตรงในการสู้รบเท่านั้น ทั้งนี้ตามข้อ 51 (3) ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ.1949 กำหนดว่า “พลเรือนจักได้รับความคุ้มครองตามที่ได้บัญญัติไว้ในหมวดนี้ เว้นแต่ว่าและตราบเท่าช่วงเวลาที่พลเรือนนั้นเข้ามีส่วนในการสู้รบโดยตรง” [766] อย่างไรก็ดี กฎหมายมนุษยธรรมระหว่างประเทศกลับไม่มีนิยามคำว่า “ส่วนในการสู้รบโดยตรง” (Direct participation) คืออะไร การตีความจึงจำต้องพิจารณาจากพฤติการณ์แต่ละกรณีบนพื้นฐานความหมายตามปกติและสอดคล้องกับวัตถุประสงค์ของกฎหมายมนุษยธรรมระหว่างประเทศ[767] ตามหลักการกระทำอันเป็นปฏิปักษ์ (Conduct of Hostilities) ในการขัดกันทางอาวุธ

หลักการแยกแยะนี้สามารถพิจารณาได้ใน 2 มิติ คือ มิติที่หนึ่งการแยกแยะโดยพิจารณาจากการมีส่วนร่วมในการสู้รบโดยตรง และมิติที่สองคือการแยกแยะโดยพิจารณาที่การจำกัดขอบเขตของความเสียหายที่จะเกิดจากการใช้อาวุธหรือวิธีการในการสู้รบ ดังพิจารณาได้จากความเห็นเชิงแนะนำของศาลยุติธรรมระหว่างประเทศในคดีความชอบด้วยกฎหมายของการคุกคามหรือใช้อาวุธนิวเคลียร์ โดยศาลยุติธรรมระหว่างประเทศมีทัศนะว่า *“...รัฐจะต้องไม่ทำให้พลเรือนตก*

---

[764] Ibid., p.35

[765] ปรากฏในข้อ 13 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 และฉบับที่ 2 และข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3

[766] Geneva Convention 1949, Article 2 and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 51 (3).

[767] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, (Geneva: International Committee of the Red Cross, 2009), p. 41. [online] Accessed: June 10, 2021. Available from: https://www.refworld.org/docid/4a670dec2.html

เป็นเป้าหมายในการโจมตี นอกจากนั้นยังต้องห้ามใช้อาวุธที่ไม่สามารถแบ่งแยกระหว่างเป้าหมายทางพลเรือนและเป้าหมายทางทหารได้..."[768] การปรับใช้หลักการแยกแยะจึงอาจพิจารณาได้ใน 2 ประการ คือ

ประการที่หนึ่ง การพิจารณาหลักการในการแยกแยะระหว่างพลเรือนและพลรบ โดยการพิจารณาการปฏิบัติตามธรรมธรรมเนียมการทำสงครามที่ปรากฏในกฎหมายมนุษยธรรมระหว่างประเทศ เช่น การพิจารณาเรื่องการสวมเครื่องแบบ การถืออาวุธ การสังกัดในกองทัพ หรือแม้แต่การมีส่วนร่วมโดยตรงในการสู้รบ เป็นต้น ซึ่งกรณีเช่นนี้จะมีความสัมพันธ์กับการพิจารณาเรื่องหลักการเกี่ยวกับวิธีการ (Methods) ในการสู้รบเป็นสำคัญ

ประการที่สอง การพิจารณาหลักการในการแยกแยะเป้าหมายในการโจมตี โดยพิจารณาจากหลักเกณฑ์ที่ควบคุมการใช้อาวุธในการสู้รบ ซึ่งจะต้องเป็นอาวุธที่จำกัดเป้าหมายในการทำลายได้ มิใช้อาวุธที่มีอานุภาพทำลายล้างสูง หรืออาวุธที่ไม่สามารถระบุการทำลายเป้าหมายโดยเฉพาะเจาะจงได้ กรณีนี้จึงเป็นส่วนที่สัมพันธ์กับหลักการในการจำกัดปัจจัย (Means) ในการสู้รบเป็นสำคัญ

ปัญหาที่เกิดขึ้นในปัจจุบันคือการใช้งานสาธารณูปโภคขั้นพื้นฐาน เช่น การสื่อสาร และการคมนาคมขนส่ง ทั้งทางการทหารและทางพลเรือนมักจะมีการใช้งานร่วมกัน (Dual-use facilities) จึงเกิดประเด็นว่า เป้าหมายทางการทหารมีความหมายครอบคลุมถึงพื้นที่ หรือการใช้งานในลักษณะใด พบว่าในทางปฏิบัตินั้น คู่มือในการปฏิบัติการทางทหารของหลายประเทศได้ทำการจำแนกเป้าหมายทางการทหารโดยพิจารณาจากรูปแบบการใช้งานว่าเป็นไปเพื่อการทหารมากน้อยเพียงไรเป็นสำคัญ หากมีการใช้งานการสื่อสาร หรือช่องทางการคมนาคมใดเพื่อประโยชน์ทางการทหารเป็นสำคัญย่อมอาจจำแนกได้ว่าพื้นที่หรือช่องทางดังกล่าวคือเป้าหมายทางการทหารด้วยเช่นกัน[769]

ในปัจจุบันปรากฏการใช้เทคโนโลยีเพื่อประโยชน์ในการขัดกันทางอาวุธมากขึ้น โดยเฉพาะอย่างยิ่งการใช้ระบบไซเบอร์เพื่อการโจมตี การใช้ระบบสื่อสารผ่านดาวเทียมเพื่อประโยชน์ในการระบุตำแหน่งเป้าหมายการโจมตี และการใช้ระบบประมวลผลของอาวุธที่สามารถตัดสินใจทำลายเป้าหมายได้ด้วยตนเอง ซึ่งนำไปสู่ข้อพิจารณาถึงการนำกฎหมายมนุษยธรรมระหว่างประเทศในส่วนที่เกี่ยวข้องกับการพิจารณาการกระทำอันเป็นปรปักษ์ โดยเฉพาะเรื่องการแยกแยะเป้าหมายในการ

---

[768] ICJ, 1996 Advisory Opinion on the Legality of Threat or Use of Nuclear Weapons, p. 257. "...States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets..."

[769] ICJ, 1996 Advisory Opinion on the Legality of Threat or Use of Nuclear Weapons, p. 32.

โจมตีว่ากฎหมายมนุษยธรรมระหว่างประเทศจะสามารถคุ้มครองบุคคลที่ไม่มีส่วนเกี่ยวข้องโดยตรงกับการสู้รบได้อย่างไร เนื่องจากเทคโนโลยีที่มีการใช้ในปัจจุบันนี้ปรากฏในลักษณะการใช้งานทั้งทางการทหารและเพื่อวัตถุประสงค์ของพลเรือน จึงจำเป็นต้องมีการพิจารณาถึงเงื่อนไขในการปรับใช้กฎหมายในกรณีต่างๆ อย่างชัดเจนมากขึ้น

เป้าหมายในการโจมตีนั้นมีความหมายทั้งในกฎหมายมนุษยธรรมระหว่างประเทศและในเชิงการปฏิบัติการทางทหาร ในปฏิบัติการทางทหารมีคำว่า Targeting หรือการกำหนดเป้าหมายซึ่งเป็นกระบวนการในการคัดเลือกเป้าหมายหรือกำหนดความสำคัญของเป้าหมายให้เหมาะสมกับปฏิบัติการ โดยจะต้องพิจารณาถึงขีดความสามารถของฝ่ายตนเอง โดยเป้าหมายอาจเป็นบุคคล สถานที่ สิ่งของใดๆ ทั้งที่จับต้องได้ และจับต้องไม่ได้ซึ่งเกี่ยวข้องกับการทำลายขีดความสามารถของฝ่ายตรงข้าม[770] การจัดลำดับความสำคัญของเป้าหมายจึงขึ้นอยู่กับลักษณะของเป้าหมายนั้นว่าเกี่ยวข้องกับขีดความสามารถในการรบของฝ่ายตรงข้ามเพียงใด ขณะที่เป้าหมายที่ชอบด้วยกฎหมายมนุษยธรรมระหว่างประเทศหมายถึงเป้าหมายทางการทหาร ไม่ว่าจะเป็นการกระทำต่อตัวทหาร สถานที่ทางการทหาร หรือทรัพย์สิ่งของทางการทหาร ฯลฯ เป้าหมายในปฏิบัติการทางทหารตามหลักนิยมในการทำสงครามจึงอาจไม่สอดคล้องกับเป้าหมายของกฎหมายมนุษยธรรมระหว่างประเทศเสมอไป เช่น การกำหนดเป้าหมายทางการทหารอาจหมายถึงการโจมตีโรงไฟฟ้าซึ่งจะส่งผลต่อระบบการใช้อาวุธทางการทหาร ในขณะที่ในกฎหมายมนุษยธรรมระหว่างประเทศ การโจมตีโรงไฟฟ้าอาจต้องคำนึงถึงผลกระทบต่อพลเรือนด้วยว่าปฏิบัติการดังกล่าวจะส่งผลกระทบต่อพลเรือนมากเกินความจำเป็นทางการทหารหรือไม่ อย่างไรก็ตามแม้หลักการกำหนดเป้าหมายของทั้งสองแนวทางจะไม่สอดคล้องกันในทุกมิติ แต่กระบวนการในการจัดลำดับความสำคัญในการโจมตีทางยุทธศาสตร์ก็อาจช่วยคัดกรองเป้าหมายที่ไม่ได้เป็นการลดขีดความสามารถทางการทหารออกไป หมายความว่าเป้าหมายที่จะก่อให้เกิดผลกระทบต่อพลเรือนมากกว่าย่อมไม่ใช่เป้าหมายลำดับต้นในการโจมตีทางทหาร[771]

เหตุที่กฎหมายมนุษยธรรมระหว่างประเทศให้ความสำคัญกับการแยกพลเรือนออกจากการทำลายทางการทหารก็เนื่องจาก “ความมีมนุษยธรรม” ที่สมดุลกับ “ความจำเป็นทางการทหาร” นั้นจะต้องหมายถึงการคุ้มครองพลเรือนที่ไม่เกี่ยวข้องกับการสู้รบตลอดระยะเวลาที่มีการขัดกันทางอาวุธ

---

[770] U.S. Army, Joint Targeting, Joint Publication 3-60, 31 January 2013, vii. [online] Accessed: June 10, 2021. Available from: https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf

[771] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

เกิดขึ้น ดังนั้นคู่พิพาทในการขัดกันทางอาวุธจึงต้องแยกแยะพลเรือนออกจากทหาร รวมตลอดถึงจะต้องมีการแยกระหว่างทรัพย์สิ่งของของพลเรือนและทรัพย์สิ่งของของทหารด้วย ปฏิบัติการทางทหารจะต้องมุ่งกระทำโดยตรงต่อทรัพย์สิ่งของของทหารเท่านั้น[772]

ปัญหาอาจเกิดขึ้นกับบางกรณีได้เช่น ในการกำหนดเป้าหมายทางทหารนั้น เป้าหมายที่ไม่ใช่สิ่งของทางกายภาพ เช่น เครือข่ายไซเบอร์ก็ถือเป็นเป้าหมายทางการทหารได้แต่การโจมตีเครือข่ายไซเบอร์นั้นย่อมกระทบต่อความเสียหายของพลเรือนและทหารไปพร้อมกัน การจำแนกความเสียหายว่าเป็นของทหารหรือพลเรือนมากกว่ากันย่อมเป็นเรื่องยากเพราะเครือข่ายการเชื่อมต่อทางไซเบอร์เป็นพื้นที่ร่วมกันของพลเรือนและทหาร [773]

นิยามคำว่า “พลเรือน” ตามพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ. 1949 หมายถึงผู้ที่ไม่ใช่ทหารหรือพลรบตามนิยามของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3 ข้อ 4 A (1), (2), (3) และ (6) และข้อ 43 ของพิธีสารฉบับที่ 1 ค.ศ.1977 หากกรณีที่มีข้อสงสัยว่าบุคคลใดเป็นทหารหรือพลเรือน กฎหมายให้สันนิษฐานไว้ก่อนว่าบุคคลดังกล่าวเป็นพลเรือน[774] เหตุที่กฎหมายจะต้องสร้างนิยามของพลเรือนที่ชัดเจนรวมตลอดถึงบทสันนิษฐานเรื่องพลเรือนขึ้นมานี้ก็เนื่องจากกฎหมายมนุษยธรรมระหว่างประเทศมีหลักสำคัญเพื่อคุ้มครองพลเรือนไม่ให้เป็นเป้าหมายในปฏิบัติการทางทหาร

ความคุ้มครองต่อพลเรือนที่กฎหมายมนุษยธรรมระหว่างประเทศมุ่งประสงค์คือการปกป้องพลเรือนจากภัยอันตรายที่เกิดขึ้นเพราะปฏิบัติการทางทหาร พลเรือนจึงต้องไม่ตกเป็นเป้าหมายโดยตรงของการโจมตี รวมตลอดถึงพลเรือนจะต้องไม่ตกเป็นเป้าหมายของคุกคามว่าจะมีการใช้ความรุนแรง การละเมิดต่อพลเรือนถือเป็นการต้องห้ามตามกฎหมาย สิทธิของพลเรือนที่จะได้รับการคุ้มครองนี้จะมีอยู่ตราบเท่าที่พลเรือนนั้นไม่เข้าไปมีส่วนร่วมโดยตรงในการสู้รบ (Direct participation in hostility)[775] ดังนั้นหากประชาชนไปมีส่วนเกี่ยวข้องโดยตรงในการสู้รบย่อมสูญเสียสิทธิในการได้รับความคุ้มครอง แม้การเข้าไปมีส่วนเกี่ยวข้องโดยตรงในการสู้รบจะไม่ได้ทำให้พลเรือน

---

[772] International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art 48.

[773] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 29.

[774] International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art 50 (1)

[775] Ibid., Art. 50 (1)-(3)

รายดังกล่าวกลายเป็นทหาร แต่พลเรือนผู้ที่มีส่วนโดยตรงในการสู้รบย่อมตกเป็นเป้าหมายการโจมตีทางทหารได้

การแยกแยะเป้าหมายการโจมตีทางการทหารในการขัดกันทางอาวุธจึงมีข้อห้ามสำคัญคือการห้ามโจมตีในลักษณะที่ไม่สามารถแบ่งแยกเป้าหมายได้ หมายถึงการโจมตีในปฏิบัติการทางทหารนั้นจะต้องกระทำโดยตรงต่อเป้าหมายเฉพาะทางการทหารเท่านั้น ปฏิบัติการทางทหารใดๆ ที่จะก่อให้เกิดผลกระทบต่อพลเรือนมากกว่าย่อมถือเป็นการโจมตีที่ห้ามกระทำตามกฎหมาย การแยกแยะเป้าหมายในกรณีแรกนี้จึงปัจจัยด้านพื้นที่ซึ่งทหารและพลเรือนอยู่เป็นสำคัญ ในขณะที่อีกมุมมองหนึ่งการแยกแยะเป้าหมายย่อมหมายถึงการใช้อาวุธ วิธีการและปัจจัยในการขัดกันทางอาวุธที่จะต้องจำกัดขอบเขตผลกระทบได้ด้วย มุมมองที่สองนี้จึงว่าด้วยเรื่องการจำกัดผลกระทบที่จะเกิดจากการกระทำโดยไม่ได้จำกัดขอบเขตพื้นที่ เช่น การโจมตีด้วยอาวุธนิวเคลียร์แม้จะกระทำในพื้นที่ทางการทหาร แต่ผลกระทบอาจเกิดขึ้นในวงกว้างขวางเกินพื้นที่เป้าหมายทางการทหารได้ เพราะสารกัมมันตรังสีอาจลอยไปในอากาศ ปนเปื้อนในน้ำ รวมถึงผลกระทบที่ยาวนานย่อมเป็นผลเสียหายต่อพลเรือนได้ เป็นต้น ดังนั้นการใช้อาวุธ วิธีการและปัจจัยในการขัดกันทางอาวุธที่ไม่สามารถแยกแยะเป้าหมาย รวมถึงไม่สามารถแยกแยะผลกระทบที่อาจเกิดขึ้นได้นั้น ย่อมถือเป็นการกระทำที่ละเมิดต่อกฎหมายระหว่างประเทศ[776]

การกระทำที่ถือว่าเป็นการโจมตีอย่างไม่เลือกปฏิบัติหรือไม่แบ่งแยกได้แก่

1) การโจมตีในลักษณะการระดมการใช้วิธีการหรือปัจจัยใดๆ ซึ่งปฏิบัติการต่อเป้าหมายทางการทหารหลายจุดที่แยกกันอย่างเห็นได้ชัดซึ่งตั้งอยู่ในนคร เมือง หมู่บ้าน หรือบริเวณอื่นใดอันมีการจุกตัวกันอยู่ของพลเรือนหรือเป้าหมายพลเรือนโดยถือเสมือนว่าเป็นเป้าหมายทางการทหารเพียงแห่งเดียว[777]

2) การโจมตีซึ่งอาจคาดได้ว่าจะยังผลให้เกิดการสูญเสียชีวิตของพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือนความเสียหายต่อทรัพย์สิ่งของพลเรือนหรือความเสียหายดังกล่าวรวมกันซึ่ง

---

[776] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 51 (4)

[777] Ibid., Art. 51 (5) (a)

ทั้งนี้เป็นการสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหารที่มีลักษณะเป็นรูปธรรมและโดยตรงอันได้คาดหมายไว้[778]

การโจมตีในลักษณะสุดท้ายนี้มีการอธิบายในทางวิชาการว่าเป็นหลักความได้สัดส่วน (Proportionality rules) ซึ่งสามารถนำมาพิจารณาปรับใช้กับการใช้อาวุธในการขัดกันทางอาวุธได้ แต่ไม่เกี่ยวข้องกับความชอบด้วยกฎหมายของอาวุธที่ใช้ในการขัดกัน

การใช้พลเรือนเป็นตัวแทนหรือการเคลื่อนย้ายประชากรพลเรือนเพื่อให้กองทัพทหารได้รับความคุ้มกันจากการห้ามโจมตีพลเรือน หรือเพื่อเป็นโล่ห์มนุษย์ในการป้องกันการโจมตีจากฝ่ายตรงข้ามในการขัดกันทางอาวุธเป็นเรื่องต้องห้ามตามกฎหมายมนุษยธรรมระหว่างประเทศ[779] นอกจากนั้นรัฐภาคีในข้อพิพาทยังมีหน้าที่ตามกฎหมายในการเคลื่อนย้ายประชากรพลเรือนออกไปจากพื้นที่ซึ่งเป็นเป้าหมายทางการทหาร[780] หลีกเลี่ยงการตั้งเป้าหมายทางการทหารภายในพื้นที่หรือใกล้เคียงพื้นที่ที่มีประชาชนอาศัยอยู่อย่างหนาแน่น[781] และจะต้องใช้ความระมัดระวังล่วงหน้าอื่นๆ เพื่อคุ้มครองประชากรพลเรือน พลเรือนปัจเจกบุคคลและทรัพย์สิ่งของพลเรือนซึ่งอยู่ภายใต้การควบคุมของตนให้พ้นจากภยันตรายต่างๆ อันเป็นผลมาจากการปฏิบัติการทางทหาร[782] การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธจะต้องเคารพต่อหลักการดังกล่าวด้วย

หลักสำคัญประการต่อมาคือการคุ้มครองทรัพย์สิ่งของพลเรือนหมายถึงทรัพย์สิ่งของที่ไม่ได้เป็นของทหารจะได้รับความคุ้มครองจากการไม่ตกเป็นเป้าหมายในการโจมตี[783] ข้อห้ามการโจมตีทรัพย์สิ่งของพลเรือนใช้กับกรณีการโจมตีที่กระทำต่อเป้าหมายทางพลเรือนโดยตรงเท่านั้น ส่วนปฏิบัติการโจมตีเป้าหมายทางการทหารและก่อให้เกิดผลกระทบจากการโจมตี (Collateral damage) กับพลเรือนหรือทรัพย์สิ่งของพลเรือนด้วยนั้นไม่ได้เป็นการต้องห้ามตามหลักการนี้ นอกจากนั้นหลักการดังกล่าวนี้ยังไม่มีผลบังคับกับกรณีที่มีการโจมตีเป้าหมายทางการทหารโดยตรง แต่เกิดความ

---

[778] Ibid., Art. 51 (5) (b)

[779] Ibid., Art. 51 (7)

[780] Ibid., Art. 58 (a)

[781] Ibid., Art. 58 (b)

[782] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 58 (c)

[783] Ibid., Art. 58

ผิดพลาดของผู้ปฏิบัติการ ความผิดพลาดทางเทคนิคหรือเหตุแทรกแซงอื่นๆ ที่ทำให้การโจมตีนั้นเกิดความคลาดเคลื่อนหรือล้มเหลวด้วย[784]

กฎหมายมนุษยธรรมระหว่างประเทศแบ่งบุคคลในการสู้รบออกเป็น 2 กลุ่ม คือ พลเรือนและพลรบ โดยพลรบเท่านั้นที่จะตกเป็นเป้าหมายหลักในการโจมตี แต่พลเรือนต้องอยู่ภายใต้การคุ้มครองของรัฐ อย่างไรก็ดี ข้อยกเว้นอาจเกิดขึ้นในบางกรณีที่การจำแนกระหว่างพลเรือนและพลรบอาจทำได้ยากขึ้น เช่นการโจมตีค่ายทหารซึ่งอยู่ใกล้กับพื้นที่ชุมชน หรือการทำลายสาธารณูปโภคทางการทหารที่อาจส่งผลต่อพลเรือน ดังนั้นประเด็นในการพิจารณาการใช้เทคโนโลยีใหม่เพื่อการขัดกันทางอาวุธจึงได้แก่สาระสำคัญดังต่อไปนี้

การพิจารณาสถานะพลรบถือเป็นเงื่อนไขประการสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ โดยเป็นไปตามหลักการแยกแยะ (Principle of Distinction) ซึ่งตามข้อ 43 (2) ของพิธีสารเพิ่มเติม ฉบับที่ 1 บัญญัติว่า “บุคคลผู้สังกัดในกองทัพของภาคีคู่พิพาทจักเป็นพลรบ (ยกเว้นบุคคลที่เป็นพนักงานแพทย์ หรืออนุศาสนาจารย์ ตามที่ได้บัญญัติไว้ในข้อ 33 ของอนุสัญญาฉบับที่ 3) กล่าวคือบุคคลดังกล่าวมีสิทธิในการเข้ามีส่วนในการสู้รบโดยตรง” ในขณะที่คำว่า “กองทัพ” ตามข้อ 43 (1) ของพิธีสารฉบับนี้ หมายถึง “...กองทัพ กลุ่ม และหน่วยต่างๆ ซึ่งมีการจัดตั้งเป็นระบบและอยู่ภายใต้การบังคับบัญชารับผิดชอบของภาคีนั้นสำหรับการปฏิบัติการของผู้ใต้บังคับบัญชา ถึงแม้ว่าภาคีดังกล่าวจะมีตัวแทนเป็นรัฐบาลหรือคณะเจ้าหน้าที่ซึ่งไม่ได้รับการรับรองโดยฝ่ายปฏิปักษ์ กองทัพเช่นว่าจักอยู่ภายใต้ระบบวินัยภายในซึ่งจักบังคับให้มีการปฏิบัติสอดคล้องกับกฎแห่งกฎหมายระหว่างประเทศที่ใช้บังคับในกรณีข้อพิพาททางอาวุธ เป็นอาทิ”

พลรบ มีความหมายตามอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 ฉบับที่ 2 ข้อ13 และฉบับที่ 3 ข้อ 4 เนื่องจากการมีสถานะเป็นพลรบจะส่งผลต่อการมีสถานะเป็นเชลยศึกตาม ข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3 ด้วย โดยปกติพลรบจึงหมายถึง

(1) ผู้สังกัดในกองทัพของภาคีคู่พิพาท

(2) ผู้สังกัดในมิลิเชีย และผู้สังกัดหน่วยอาสาสมัครอื่นใด รวมทั้งผู้สังกัดในขบวนต่อต้านที่ได้จัดตั้งขึ้นโดยมีระเบียบ

(3) ผู้สังกัดในกองทัพประจำ

(4) บุคคลที่ร่วมอยู่แต่มิได้สังกัดอยู่ในกองทัพนั้นโดยตรง

---

[784] Statement (j) (2) made by the UK on ratification of API on January 1998. The issue of collateral damage is considered under 4.2.4 “Indiscriminate attacks.”

(5) บุคคลประจำเรือ และอากาศยาน

(6) พลเมืองในอาณาเขตที่มิได้ถูกยึดครองซึ่งสมัครใจจับอาวุธต่อต้านกองทหาร โดยไม่มีเวลาเข้าเป็นทหารกองประจำ (levée en mass)

นิยามดังกล่าวเป็นการแยกแยะพลเรือนออกจากพลรบในการขัดกันทางอาวุธ แต่กระนั้นข้อ 50 (1) ของพิธีสารเพิ่มเติม ฉบับที่ 1 ได้ให้นิยามว่า “พลเรือน ได้แก่ บุคคลใด ผู้ซึ่งไม่ได้จัดอยู่ในประเภทของบุคคลตามที่ได้กำหนดไว้ในข้อ 4 a (1) (2) (3) และ (6) แห่งอนุสัญญาฉบับที่ 3 และในข้อ 43 แห่งอนุสัญญาฉบับนี้ ในกรณีเป็นที่สงสัยว่าบุคคลนั้นเป็นพลเรือนหรือไม่ บุคคลนั้นจักได้รับการพิจารณาว่าเป็นพลเรือน” จากนิยามของข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3 และข้อ 50 (1) ของพิธีสารเพิ่มเติม ฉบับที่ 1 นี้ทำให้บุคคลที่เข้าไปมีส่วนร่วมในการรบแต่มิใช่สมาชิกของกองทัพย่อมตกอยู่ในสถานะเชลยศึกได้ แต่บุคคลดังกล่าวไม่ใช่พลรบ ซึ่งน่าจะก่อให้เกิดความสับสนอยู่ไม่น้อยในทางปฏิบัติ และยังส่งผลในการจำแนกบุคคลที่มีส่วนในการสู้รบให้เป็น 2 ลักษณะ คือ 1) บุคคลที่สังกัดในกองทัพหรือกลุ่มกองกำลังอื่น ย่อมเป็นพลรบตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าบุคคลเหล่านั้นจะมีส่วนในการสู้รบมากน้อยเพียงใด 2) บุคคลที่ไม่ได้สังกัดในกองทัพหรือกลุ่มกองกำลังอื่น แต่ไปมีบทบาทในการสู้รบ กลุ่มหลังนี้ย่อมไม่มีสถานะเป็นพลรบตามกฎหมาย[785] คำว่าพลรบจึงมีความหมายทั้งผู้ที่มีส่วนร่วมโดยตรงในการสู้รบและผู้ที่เกี่ยวข้องกับการสู้รบในนามของตัวแทนรัฐคู่สงคราม

บุคคลที่มิใช่พลรบตามกฎหมายแต่เข้าไปมีส่วนร่วมในการรบย่อมตกเป็นเป้าหมายในการโจมตีตามหลักการในการทำสงครามได้ ในขณะที่บุคคลเหล่านี้จะไม่ได้รับการคุ้มครองตามกฎหมายมนุษยธรรมเช่นเดียวกับพลรบที่ถูกกฎหมาย และไม่ได้รับการคุ้มครองเช่นเดียวกับที่พลเรือนพึงได้รับตามกฎหมาย[786] อย่างไรก็ดี บุคคลดังกล่าวจะยังคงมีสิทธิขั้นพื้นฐานที่ได้รับการคุ้มครองอยู่ตามข้อ 3 ร่วม ของอนุสัญญาเจนีวา ค.ศ.1949 และข้อ 75 ของพิธีสารเพิ่มเติม ฉบับที่ 1[787]

Yoram Dinstein ได้จำแนกองค์ประกอบความเป็นพลรบตามกฎหมายไว้ 7 ประการ[788] โดย 4 ประการแรกมาจาก Hague Regulation และอนุสัญญาเจนีวา คือ[789]

---

[785] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 141.

[786] Ibid., p. 142.

[787] Michael N. Schmitt, “The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis.” Harvard National Security Journal, Vol. 1, 55, (2010): 14.

[788] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, pp. 33-37.

[789] ข้อ 13 (2) อนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 และฉบับที่ 2 และข้อ 4 (2) อนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3

(1) มีผู้บัญชาสั่งการอันเป็นบุคคลที่รับผิดชอบสำหรับผู้อยู่ใต้บังคับบัญชา

(2) มีเครื่องหมายที่กำหนดไว้เด่นชัดเจน สามารถเห็นได้ในระยะไกล

(3) ถืออาวุธโดยเปิดเผย

(4) ปฏิบัติการรบตามกฎและประเพณีการทำสงคราม

2 ประการต่อมามาจากข้อ 4 (A) (2) ของอนุสัญญาเจนีวา ฉบับที่ 3 คือ

(5) ผู้สังกัดในขบวนต่อต้านที่ได้จัดตั้งขึ้นโดยมีระเบียบ

(6) เป็นสมาชิกของภาคีคู่พิพาท

ข้อ 7 มาจากแนวทางคำพิพากษาคดี Public Prosecutor v. Koi (1968)[790]

(7) เจ้าหน้าที่ที่มิได้รับการรับรองจากผู้ปฏิบัติงานภายใต้บังคับบัญชาของรัฐผู้กักคุมตัว

การพิจารณาสถานะพลรบซึ่งเกิดจากการใช้เทคโนโลยีใหม่จะเกิดขึ้นกับกรณีการใช้งานระบบไซเบอร์ซึ่งไม่สามารถใช้หลักการพื้นฐานของกฎหมายว่าด้วยการขัดกันทางอาวุธได้ เนื่องจากในขณะปฏิบัติการนั้นจะไม่พบการสวมเครื่องแบบและการถืออาวุธของผู้ปฏิบัติการณ์ กิจกรรมทั้งหมดจะอยู่บนเครือข่ายการทำงานของคอมพิวเตอร์ การพิจารณาสถานะพลรบเพื่อการโจมตีตอบโต้จึงอาจกระทำได้โดยการตรวจสอบข้อมูลว่าการสั่งการดังกล่าวมาจากคอมพิวเตอร์ของหน่วยงานทหารหรือกองกำลังอื่นหรือไม่ ซึ่งส่งผลต่อการตอบโต้อย่างทันท่วงทีที่ไม่สามารถดำเนินได้[791]

กรณีการใช้หุ่นยนต์สังหารอัตโนมัติหรือการใช้อากาศยานไร้คนขับนั้น หากพิจารณาว่าอุปกรณ์หรือจักรกลดังกล่าวเป็นเครื่องมือเช่นอาวุธ ก็จะไม่พบตัวพลรบที่กระทำการ เพราะผู้สั่งการหรือควบคุมจะอยู่ไกลกว่าระบบอาวุธดังกล่าว

การใช้เครื่องแบบทหารและอาวุธชนิดที่ล่องหนได้จากเทคโนโลยีนาโนมีประเด็นที่ต้องพิจารณาเรื่องสถานะของพลรบที่ไม่สามารถมองเห็นได้ว่าแม้จะไม่เป็นการทำให้เข้าใจว่าเป็นพลเรือนแต่จะยังคงสถานะความเป็นพลรบได้หรือไม่ ส่วนกรณีการถืออาวุธล่องหนนั้นต้องถือว่าเป็นการกระทำที่ขัดต่อหลักเกณฑ์ในการขัดกันทางอาวุธอย่างแน่นอน

ข้อพิจารณาเกี่ยวกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศเกี่ยวกับการแยกแยะเป้าหมายในการโจมตีทางไซเบอร์เป็นประเด็นที่มีความซับซ้อนอยู่ค่อนข้างมากเนื่องจากการใช้งานระบบไซเบอร์เกี่ยวข้องกับคอมพิวเตอร์ อินเตอร์เน็ตและโปรแกรมคอมพิวเตอร์ซึ่งเป็นทรัพยากรที่ทั้ง

---

[790] Public Prosecutor v. Koi (1968) AC 829 in A.P.V. Rogers, Law on the Battlefield, 2nd edition, (Manchester: Manchester University Press, 2004) p.32.

[791] Jean Pictet, Humanitarian Law and the Protection of War Victims, (Geneva: Henry Dunant Institute, 1975) p.15.

ทหารและพลเรือนใช้รูปแบบเดียวกัน กล่าวคือคอมพิวเตอร์ทั่วไปสามารถใช้งานได้ทั้งเพื่อวัตถุประสงค์ของพลเรือนและวัตถุประสงค์ทางการทหาร ระบบอินเตอร์เน็ตที่ใช้งานทั้งทางทหารและทางพลเรือนก็ใช้ระบบอินเตอร์เน็ตเดียวกัน ในขณะที่การใช้งานโปรแกรมคอมพิวเตอร์อาจมีทั้งโปรแกรมคอมพิวเตอร์ทั่วไปที่ใช้ได้ทั้งทางทหารและพลเรือนรวมถึงโปรแกรมคอมพิวเตอร์เฉพาะทางการทหารก็ได้

การแยกแยะเป้าหมายเครื่องคอมพิวเตอร์ซึ่งเป็นเป้าหมายในการโจมตีทางไซเบอร์นั้นในทางเทคนิคจะต้องจำแนกจาก IP address ของเครื่องคอมพิวเตอร์ IP address หรือ Internet Protocol address เป็นชุดของกฎและคำสั่งเพื่อใช้ในการติดต่อสื่อสารระหว่างเครือข่ายอินเทอร์เน็ตและยังเป็นสิ่งระบุตัวตนของเครือข่ายและอุปกรณ์คอมพิวเตอร์ที่ติดต่อสื่อสารกันในระบบอินเทอร์เน็ตด้วย IP address ของคอมพิวเตอร์หรืออุปกรณ์ที่เชื่อมต่อระบบอินเทอร์เน็ตได้นั้นจะมีรหัสเฉพาะของแต่ละอุปกรณ์ที่แตกต่างกันจึงใช้ในการจำแนกอุปกรณ์และบอกตำแหน่งที่ตั้งของอุปกรณ์ที่ใช้ในการติดต่อสื่อสารได้[792]

แม้ IP address จะใช้ในการจำแนกอุปกรณ์ในเครือข่ายอินเทอร์เน็ตและอุปปกรณ์ในระบบไซเบอร์ได้แต่ก็ไม่สามารถบอกได้ว่าบุคคลใดหรือหน่วยงานใดเป็นผู้ใช้งานอุปกรณ์ดังกล่าว การจำแนกอุปกรณ์ว่าเป็นของพลเรือนหรือทหารจึงต้องรู้ข้อมูลที่ซับซ้อนมากขึ้นคือรู้ว่าอุปกรณ์ที่มีรหัสแสดงตัวตนเฉพาะอยู่ที่ใดและทำงานเพื่อวัตถุประสงค์อะไร เช่นกณีการโจมตีโรงงานเพิ่มประสิทธิภาพยูเรเนียมของอิหร่านที่เมืองนาธานซ์ (Natanz) ด้วยมัลแวร์สตักเน็ต (Stuxnet) ผู้ออกแบบมัลแวร์สามารถเจาะจงให้มัลแวร์ทำลายคอมพิวเตอร์ควบคุมเครื่องคัดแยกยูเรเนี่ยมได้โดยที่เครื่องคอมพิวเตอร์เครื่องอื่นที่ไม่เกี่ยวข้องจะไม่ได้รับความเสียหายเลย[793]

ในกรณีการโจมตีทางไซเบอร์ที่เมืองเซาท์ออสเซเทีย ประเทศจอร์เจียและการโจมตีทางไซเบอร์ที่เมืองทาลลินน์ ประเทศเอสโตเนียใช้วิธีการแบบ DDoS หรือการทำให้เว็บไซต์ล่มด้วยการส่งคำขอเข้าถึงเว็บไซต์พร้อมกันจำนวนมหาศาลนั้นเป็นการโจมตีเป้าหมายเฉพาะซึ่งเป็นเว็บไซต์ของหน่วยงานราชการแต่ก่อให้เกิดผลเสียหายอย่างกว้างขวางต่อการเข้าใช้บริการทางอินเทอร์เน็ตของพลเรือนและการเข้าใช้บริการอินเทอร์เน็ตของทหาร[794] นอกจากนั้นเครื่องคอมพิวเตอร์ซึ่งถูกมัลแวร์

---

[792] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: update of ISIS December 2010," Institute for Science and International Security Report; (2011). p. 4.

[793] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: update of ISIS December 2010," Institute for Science and International Security Report; (2011). p.4.

[794] Ibid.

ควบคุมให้ทำหน้าที่โจมตีเครื่องคอมพิวเตอร์เป้าหมายอาจเป็นเครื่องคอมพิวเตอร์ของทหารหรือของพลเรือนก็ได้ วิธีการโจมตีแบบ DDoS จึงก่อให้เกิดผลกระทบโดยไม่แยกแยะเป้าหมาย

สถานการณ์ความขัดแย้งระหว่างประเทศยูเครนและประเทศรัสเซียเป็นอีกกรณีหนึ่งที่สะท้อนให้เห็นปัญหาของการโจมตีเครือข่ายการสื่อสารผ่านดาวเทียมซึ่งน่าพิจารณาว่าเป็นการโจมตีที่สอดคล้องต่อหลักการแยกแยะหรือไม่เนื่องจากการสื่อสารผ่านดาวเทียมและการใช้สัญญาณดาวเทียมเพื่อระบุที่ตั้งบนพื้นโลก (Global Positioning System) ย่อมส่งผลกระทบต่อทั้งพลเรือนและทหารไปพร้อมกันและคงจำแนกได้ยากว่าเป็นผลกระทบที่เกี่ยวข้องกับทหารหรือพลเรือนมากกว่า เนื่องจากการใช้งานระบบการระบุที่ตั้งบนพื้นโลก (GPS) ของทั้งทหารและพลเรือนเป็นการใช้สัญญาณดาวเทียมทำงานร่วมกับอุปกรณ์อื่นเพื่อค้นหาตำแหน่งและค้นหาความเร็วของการเคลื่อนที่ของวัตถุแบบเดียวกัน แม้ทางการทหารจะมีการใช้งานสัญญาณ GPS ประกอบร่วมกับระบบอาวุธนำวิถีก็ตาม

การรบกวนสัญญาณดาวเทียมโดยกองทัพรัสเซียซึ่งกระทำต่อยูเครนก่อให้เกิดผลกระทบต่อการสื่อสารของระบบอินเทอร์เน็ตด้วยและผลกระทบดังกล่าวก็ไม่สามารถแยกระหว่างเป้าหมายพลเรือนและเป้าหมายทางการทหารได้เช่นเดียวกัน การนำหลักการแยกแยะเป้าหมายมาปรับใช้กับกรณีการรบกวนสัญญาณดาวเทียมจึงก่อให้เกิดข้อท้าทายต่อการแยกแยะเป้าหมายในการโจมตี อย่างไรก็ดี แม้การปรับการแยกแยะเป้าหมายในการโจมตีจะไม่สามารถกระทำได้แต่อาจนำหลักความได้สัดส่วนในการโจมตีมาพิจารณาในขั้นต่อไปได้ว่าการโจมตีระบบการสื่อสารผ่านดาวเทียมดังกล่าวจะถือว่าเป็นการกระทำที่ขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่

3.3.2.2 หลักความได้สัดส่วนในการโจมตี

ความได้สัดส่วนในการโจมตีหมายถึงคู่พิพาทในการขัดกันทางอาวุธนั้นจะต้องไม่ก่อความรุนแรงมากไปกว่าสัดส่วนที่จำเป็นต้องใช้เพื่อวัตถุประสงค์ในการทำสงคราม การทำลายกองทัพฝ่ายตรงข้ามเพื่อความได้เปรียบทางการทหารเท่านั้น[795] การใช้กำลังทางทหารจึงไม่ใช่ว่าจะทำได้โดยปราศจากข้อจำกัด[796] นอกจากนั้น ในการโจมตีด้วยปฏิบัติการทางทหารจะต้องคาดหมายล่วงหน้าถึงความเสียหายที่อาจกระทบต่อ ชีวิต และทรัพย์สินของพลเรือนด้วย หากความเสียหายดังกล่าวเกินขอบเขตจากการทำลายเป้าหมายทางการทหารฝ่ายตรงข้ามมากเกินไปย่อมถือว่าเป็นการต้องห้าม

[795] Jean Pictet, Humanitarian Law and the Protection of War Victims, p. 31.

[796] Ibid., p. 33.

ตามกฎหมาย[797] โดยปกติหลักการสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศหลักการแรกที่ต้องปฏิบัติตามคือหลักการแยกแยะเป้าหมาย เมื่อแยกแยะเป้าหมายแล้วจะต้องคำนึงถึงหลักต่อมาคือการโจมตีนั้นเป็นไปโดยได้สัดส่วนหรือไม่

ปัญหาว่า ความเกี่ยวข้องต่อประโยชน์ทางการทหารโดยตรงและเป็นรูปธรรม (concrete and direct military advantage anticipate) ซึ่งเป็นสัดส่วนที่สามารถโจมตีได้นั้น เป็นอย่างไร ทางปฏิบัติโดยรัฐส่วนมากพิจารณาจากสาระสำคัญและความใกล้ชิดอย่างยิ่ง (substantial and relatively close) ว่าพื้นที่หรือปฏิบัติการใดเป็นไปเพื่อการใช้กำลังทางหทารมากที่สุดย่อมตกเป็นเป้าหมายของการโจมตีได้ แม้กระนั้นก็ตามการพิสูจน์ดังกล่าวยังเป็นเรื่องที่ค่อนข้างยาก จึงต้องอาศัยการวางแผนและการพิจารณาถึงความจำเป็นในการปฏิบัติการเพื่อการโจมตีเป้าหมายดังกล่าวก่อนที่จะมีการตัดสินใจโจมตีด้วย[798]

หลักความได้สัดส่วนในการโจมตีปรากฏในข้อ 57 2. (ก) (3) “ละเว้นจากการตัดสินใจที่จะโจมตีซึ่งอาจคาดหมายได้ว่าจะก่อให้เกิดความสูญเสียต่อชีวิตของพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์พลเรือน หรือความเสียหายดังกล่าวรวมกัน ซึ่งทั้งนี้เป็นการสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหาร ที่มีลักษณะเป็นรูปธรรมและโดยตรงอันได้คาดหมายไว้” และข้อ 57 3. “ในกรณีที่อาจมีทางเลือกได้สำหรับเป้าหมายทางทหารหลายแห่งเพื่อจะบรรลุความได้เปรียบทางการทหารที่มีลักษณะคล้ายคลึงกัน เป้าหมายที่ได้รับเลือกโจมตีจักต้องเป็นเป้าหมายซึ่งอาจคาดหมายได้ว่าจะก่อให้เกิดอันตรายต่อชีวิตของพลเรือน และทรัพย์สิ่งของพลเรือนในลักษณะที่น้อยที่สุด”

ในส่วนของระบบอาวุธที่ตัดสินใจได้ด้วยตนเองนั้น ยังมีข้อพิจารณาเรื่องความรับผิดขอบของ ผู้วางแผน ผู้ตัดสินใจ ผู้ควบคุมการโจมตี หลักการนี้จะต้องนำมาปรับใช้กับทุกการโจมตี โดยคำนึงถึงปัจจัยและวิธีที่นำมาใช้ และพิจารณาความรับผิดของพลรบซึ่งเป็นบุคคลที่ต้องคำนึงถึงหลักเกณฑ์ดังกล่าว ทั้งนี้จะกล่าวอ้างความผิดที่เกิดจากจักรกล ระบบข้อมูลการประมวลผล หรือ

[797] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.46.

[798] Ibid., p. 50.

ระบบการใช้อาวุธไม่ได้ จึงต้องมีการกำหนดพันธกรณีตามกฎหมายให้มีเกณฑ์ขั้นต่ำเรื่องการใช้มนุษย์ควบคุมระบบอาวุธเหล่านี้[799]

การตรวจสอบเรื่องการควบคุมระบบอาวุธตัดสินใจอัตโนมัติโดยมนุษย์นี้ จะพิจารณาจากการคาดหมายได้ (Predictabilities) ของการปฏิบัติการ การควบคุมโดยมนุษย์ซึ่งสามารถแทรกแซงปฏิบัติการของระบบอาวุธอัตโนมัติได้ (human supervision and ability to intervene) ข้อจำกัดในการปฏิบัติการในประเด็นต่างๆ เช่น ภารกิจ ลักษณะของเป้าหมายที่จะโจมตี สภาพแวดล้อมการปฏิบัติการ กำหนดระยะเวลาการปฏิบัติการณ์ และขอบเขตการปฏิบัติการ นอกจากนั้นความจำเป็น ประสิทธิภาพและความพอเพียงในการพิจารณาเรื่องการควบคุมระบบอาวุธโดยมนุษย์นั้น ผู้ปฏิบัติการณ์จะต้องจัดเตรียมข้อมูลให้เพียงพอ เข้าใจระบบอาวุธ และสภาพแวดล้อมในการปฏิบัติการณ์ รวมถึงปฏิสัมพันธ์ระหว่างผู้ใช้อาวุธกับอาวุธด้วย

ปัจจัยเรื่องการควบคุมระบบอาวุธโดยมนุษย์นี้ จะต้องเชื่อมโยงให้เห็นถึงการตัดสินใจระหว่างผู้บังคับบัญชา และผู้ปฏิบัติการณ์ที่เป็นมนุษย์ด้วย สิ่งที่น่าพิจารณาเพิ่มเติมคือเรื่องการออกแบบอาวุธที่อาจนำไปสู่ความไม่สามารถคาดการณ์ปฏิบัติการณ์ของอาวุธได้ เช่น การใช้จักรกลอัจฉริยะ (AI: Artificial Intelligence) ซึ่งใช้ชุดคำสั่งอัลกอริทึ่ม (Algorithms)[800] ประมวลผลการระบุเป้าหมาย ซึ่งจะก่อให้เกิดปัญหาเรื่องการปรับใช้หลักกฎหมายกับระบบประมวลผลดังกล่าว นอกจากนั้นประเด็นเรื่องจริยธรรมในการใช้อาวุธ (Ethic) คณะกรรมการกาชาดระหว่างประเทศ มองว่าประเด็นสำคัญอยู่ที่ปฏิบัติการของจักรกล และความรับผิดชอบในการตัดสินใจสังหารหรือทำลายล้าง เมื่อความรับผิดชอบในด้านจริยธรรมนี้ไม่อาจใช้กับจักรกลได้ จึงต้องมีการกำหนดประเภทและระดับการควบคุมจักรกลซึ่งต้องมีมนุษย์เข้ามาเกี่ยวข้องในการตัดสินใจในการสังหารและทำลาย เพื่อกำหนดความรับผิดของผู้ควบคุมได้ด้วย[801]

---

[799] ICRC, Expert Meeting on Lethal Autonomous Weapons Systems, Statement, November 15, 2017. P. 23. [online] Accessed: November 16, 2017. Available from: https://www.icrc.org/en/document/expert-meeting-lethal-autonomous-weapons-systems

[800] Algorithm คือ กระบวนการแก้ปัญหาที่สามารถอธิบายออกมาเป็นขั้นตอนที่ชัดเจน เมื่อนำเข้าอะไร แล้วจะต้องได้ผลลัพธ์เช่นไร กระบวนการนี้ประกอบด้วยจะประกอบด้วย วิธีการเป็นขั้นๆ และมีส่วนที่ต้องทำแบบวนซ้ำอีก จนกระทั่งเสร็จสิ้นการทำงาน Algorithm ไม่ใช่คำตอบแต่เป็นชุดคำสั่งที่ทำให้ได้คำตอบ วิธีการในการอธิบาย Algorithm ได้แก่

1. Natural Language อธิบายแบบใช้ภาษาที่เราสื่อสารกันทั่วไป

2.Pseudocode อธิบายด้วยรหัสจำลองหรือรหัสเทียม

3.Flowchart อธิบายด้วยแผนผัง

[801] ICRC, Expert Meeting on Lethal Autonomous Weapons Systems, Statement, November 15, 2017.

ในการโจมตีทางไซเบอร์นั้นมีประเด็นว่าความเสียหายที่เกิดขึ้นได้สัดส่วนกับความจำเป็นทางการทหารหรือหรือไม่ในบางกรณี ได้แก่กรณีการโจมตีด้วยวิธีการ DDoS มีปัญหาว่าเป็นการกระทำที่ก่อให้เกิดความสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหารที่มีลักษณะเป็นรูปธรรมซึ่งอาจคาดหมายได้โดยตรงหรือไม่ หากการโจมตีทางไซเบอร์ที่กระทำต่อเว็บไซต์ส่งผลต่อความเสียหายของพลเรือนมากกว่า การโจมตีทางไซเบอร์ดังกล่าวย่อมเป็นการโจมตีที่ไม่สอดคล้องต่อหลักความได้สัดส่วนในการโจมตี ปัญหาที่น่าคิดต่อมาคือความเสียหายที่เกิดจากการโจมตีทางไซเบอร์นั้นมีความเป็นรูปธรรมเพียงใดเนื่องจากการโจมตีด้วยวิธีการ DDoS นั้นมีผลให้การใช้บริการอินเทอร์เน็ตขัดข้องเป็นสำคัญแต่โดยทั่วไปไม่มีผลให้เกิดความเสียหายแก่ร่างกายหรือทรัพย์สิน ในขณะที่การโจมตีทางไซเบอร์บางกรณีก่อให้เกิดผลกระทบต่อการรักษาพยาบาลคนไข้ในโรงพยาบาลและการโจมตีเครือข่ายไซเบอร์ที่เกี่ยวข้องกับวัตถุอันตรายที่นำมาซึ่งความบาดเจ็บ การเสียชีวิตหรือความเสียหายต่อทรัพย์สินของพลเรือนย่อมถือว่าเป็นการโจมตีที่ไม่ได้สัดส่วนตามกฎหมายมนุษยธรรมระหว่างประเทศ

กรณีการใช้อาวุธอิสระอาจแบ่งได้เป็น 2 ลักษณะคือการใช้อาวุธอิสระเพื่อการป้องกันและการใช้อาวุธอิสระเพื่อการโจมตี ประเด็นการใช้ระบบอาวุธอิสระเพื่อการป้องกันภัยคุกคามทางอากาศนั้นมีประเด็นพิจารณาเรื่องความแม่นยำของระบบอาวุธในการทำลายภัยคุกคามทางอากาศจากอากาศยานและขีปนาวุธรวมตลอดถึงความเสียหายข้างเคียงที่อาจเกิดขึ้นต่อพลเรือน ในทางปฏิบัติพบรายงานความผิดพลาดจากการทำลายภัยคุกคามอยู่บ้าง กล่าวคือระบบป้องกันภัยทางอากาศไม่สามารถทำลายภัยคุกคามทางอากาศได้ทั้งหมดแต่ยังถือว่ามีความแม่นยำค่อนข้างมาก ในขณะที่ความเสียหายจากระบบป้องกันภัยคุกคามทางอากาศต่อพลเรือนไม่ปรากฏรายงานความเสียหายแต่อย่างใดเนื่องจากระบบดังกล่าวไม่ได้ออกแบบมาเพื่อการโจมตีและไม่มีลักษณะการทำงานที่จะนำไปสู่ผลกระทบข้างเคียงเท่าไรนัก

ระบบอาวุธอิสระเพื่อการโจมตีมีได้ในหลายรูปแบบ เช่น อากาศยานไร้คนขับที่ตัดสินใจได้เอง หุ่นยนต์สังหาร ฯลฯ ในปัจจุบันยังไม่พบรายงานเกี่ยวกับการใช้หุ่นยนต์สังหารที่ตัดสินใจทำลายเป้าหมายได้ด้วยตัวเองแต่มีการอ้างถึงการใช้ระบบอากาศยานไร้คนขับที่สามารถคัดเลือกและทำลายเป้าหมายได้ด้วยตัวเองเช่นอากาศยานไร้คนขับ KUB-BLA ของประเทศรัสเซีย อย่างไรก็ดียังไม่พบรายงานว่าอากาศยานไร้คนขับดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามที่ฝ่ายรัสเซียกล่าวอ้างจริงหรือไม่[802]

[802] Cecilia Anderson, Killer Robot-Autonomous Weapons and Their Compliance with IHL, p.26.

นักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายคนตั้งข้อสงสัยเกี่ยวกับความสามารถในการคัดเลือกและทำลายเป้าหมายโดยระบบปัญญาประดิษฐ์ของอาวุธอิสระว่าจะมีความแม่นยำและสามารถควบคุมผลที่ไม่สามารถคาดหมายได้เพียงไร หากระบบหุ่นยนต์สังหารทำงานผิดพลาดจนก่อให้เกิดความเสียหายแก่พลเรือนอย่างมากจะถือว่าเป็นปฏิบัติการที่เกินสัดส่วนตามกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ ข้อพิจารณาที่เกี่ยวข้องกับการทำงานที่ผิดพลาดของหุ่นยนต์สังหารอิสระอาจไม่ใช่เรื่องความได้สัดส่วนการในการโจมตีของหุ่นยนต์สังหารอิสระแต่น่าจะเกี่ยวข้องกับประเด็นความรับผิดชอบของผู้ใช้งานระบบอาวุธอิสระรวมตลอดถึงผู้ออกแบบและโปรแกรมการทำงานของระบบอาวุธเป็นสำคัญ ซึ่งปัจจัยเรื่องความสัมพันธ์ระหว่างมนุษย์กับระบบอาวุธอิสระนำมาสู่ประเด็นการกำหนดระดับความสัมพันธ์ของมนุษย์กับการใช้งานระบบอาวุธอิสระเพื่อจำแนกความรับผิดชอบในแต่ละกรณีที่แตกต่างกัน

กรณีการขัดขวางระบบการสื่อสารผ่านดาวเทียมในความขัดแย้งระหว่างประเทศยูเครนและประเทศรัสเซียนั้นมีข้อพิจารณาเรื่องความได้สัดส่วนในการโจมตีเนื่องจากปฏิบัติการดังกล่าวก่อให้เกิดผลกระทบต่อการสื่อสารทั้งของพลเรือนและทหาร แม้ปฏิบัติการดังกล่าวจะก่อให้เกิดความได้เปรียบเสียเปรียบทางการทหารแต่ก็นำไปสู่ความเสียหายต่อการสื่อสาร การใช้งานอินเทอร์เน็ตและการใช้สัญญาณ GPS ของพลเรือนด้วยการปฏิบัติการขัดขวางระบบสัญญาณดาวเทียมโดยกองทัพรัสเซียดังกล่าวอาจถือได้ว่าเป็นการโจมตีที่ไม่ได้สัดส่วนตามกฎหมายมนุษยธรรมระหว่างประเทศ อย่างไรก็ดีมีข้อน่าพิจารณาว่าความเสียหายต่อการสื่อสารดังกล่าวไม่มีความเสียหายทางกายภาพปรากฏ ไม่นำไปสู่ความตายความบาดเจ็บของบุคคลและอาจไม่นำไปสู่ความเสียหายต่อทรัพย์สินอย่างเป็นรูปธรรม เช่นนี้จะถือว่าเป็นความเสียหายที่เกินสัดส่วนที่กฎหมายมนุษยธรรมระหว่างประเทศมุ่งประสงค์หรือไม่

3.3.2.3 หลักความระมัดระวังล่วงหน้าในการโจมตี

กรณีที่ไม่แน่ชัดว่าการโจมตีใดเป็นไปโดยชอบต่อหลักความได้สัดส่วนหรือไม่ย่อมสามารถนำหลักความระมัดระวังล่วงหน้าในการโจมตีมาปรับใช้ได้ว่าปฏิบัติการโจมตีนั้นได้กระทำไปโดยสอดคล้องต่อแนวทางของกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ โดยพิเคราะห์ว่าในการโจมตีแต่ละครั้งนั้นได้มีการตรวจสอบเป้าหมายในการโจมตีหรือไม่ มีการเลือกปัจจัยและวิธีการที่

เหมาะสมเพียงไรและมีมาตรการในการละเว้นการโจมตีที่คาดได้ว่าอาจเกิดความสูญเสียต่อพลเรือนหรือไม่ อย่างไร

หลักความระมัดระวังล่วงหน้าในการโจมตีปรากฏในข้อ 57 ของพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949[803] โดยกำหนดว่า

1. ในปฏิบัติการทางทหาร จักต้องใช้ความระมัดระวังตลอดเวลา เพื่อมิให้ประชากรพลเรือนและทรัพย์สิ่งของพลเรือนต้องถูกกระทบกระเทือน

2. ส่วนที่เกี่ยวกับการโจมตี จักต้องให้มีการระมัดระวังล่วงหน้า ดังนี้

(ก) ผู้วางแผนหรือผู้ตัดสินใจในการโจมตี จัก

(1) กระทำทุกวิถีทางเท่าที่จะเป็นไปได้เพื่อตรวจสอบว่าเป้าหมายในการโจมตี มิได้เป็นพลเรือน หรือทรัพย์สิ่งของพลเรือน และมิใช่กรณีที่ได้รับความคุ้มครองเป็นพิเศษ แต่เป็นเป้าหมายทางการทหาร ภายใต้ความหมายที่บัญญัติไว้ในวรรค 2 ข้อ 52 และซึ่งไม่ใช่กรณีต้องห้ามการโจมตีตามบทบัญญัติของพิธีสารฉบับนี้

(2) ดำเนินการทั้งปวงเพื่อการระมัดระวังล่วงหน้าที่เป็นไปได้ในการเลือกปัจจัยและวิธีการเข้าโจมตีโดยมีวัตถุประสงค์เพื่อการหลีกเลี่ยงและอย่างน้อยก็เพื่อลดการสูญเสียชีวิตของพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือนและความเสียหายต่อทรัพย์สิ่งของพลเรือน

(3) ละเว้นจากการตัดสินใจที่จะโจมตีซึ่งอาจคาดหมายได้ว่าจะก่อให้เกิดความสูญเสียต่อชีวิตของพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์พลเรือน หรือความเสียหายดังกล่าวรวมกัน ซึ่งทั้งนี้เป็นการสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหาร ที่มีลักษณะเป็นรูปธรรมและโดยตรงอันได้คาดหมายไว้

(ข) การโจมตีจักถูกระงับหรือเลื่อนเวลาออกไป หากปรากฏว่าเป้าหมายแห่งการโจมตีนั้นไม่ใช่เป้าหมายทางการทหาร หรือเป็นเป้าหมายที่ได้รับความคุ้มครองเป็นพิเศษ หรือการโจมตีนั้นอาจคาดหมายได้ว่าจะก่อให้เกิดการสูญเสียชีวิตพลเรือนที่อาจพลอยเกิดขึ้น การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์สิ่งของพลเรือนหรือความเสียหายดังกล่าวรวมกัน ซึ่งทั้งนี้เป็นการสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหารที่มีลักษณะเป็นรูปธรรมและโดยตรงอันได้คาดหมายไว้

---

[803] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 57.

(ค) จักให้มีการเตือนล่วงหน้าอย่างเป็นผลก่อนการโจมตีใดๆ ซึ่งอาจส่งผลกระทบต่อประชากรพลเรือน เว้นไว้แต่ว่าพฤติการณ์ไม่อำนวยให้

3. ในกรณีที่อาจมีทางเลือกได้สำหรับเป้าหมายทางทหารหลายแห่งเพื่อจะบรรลุความได้เปรียบทางการทหารที่มีลักษณะคล้ายคลึงกัน เป้าหมายที่ได้รับเลือกโจมตีจักต้องเป็นเป้าหมายซึ่งอาจคาดหมายได้ว่าจะก่อให้เกิดอันตรายต่อชีวิตของพลเรือน และทรัพย์สิ่งของพลเรือนในลักษณะที่น้อยที่สุด

4. ในการปฏิบัติภารกิจทางทหารในทะเลหรือในอากาศ ภาคีคู่พิพาทแต่ละฝ่ายจักใช้ความระมัดระวังล่วงหน้าอย่างสมเหตุสมผลทั้งปวง เพื่อหลีกเลี่ยงการก่อให้เกิดความสูญเสียต่อชีวิตของพลเรือน และความเสียหายต่อทรัพย์สิ่งของพลเรือน ทั้งนี้โดยสอดคล้องต่อสิทธิและหน้าที่ตามกฎแห่งกฎหมายระหว่างประเทศที่ใช้บังคับในกรณีข้อพิพาททางอาวุธ

5. จักไม่มีบทบัญญัติใดแห่งข้อนี้ที่อาจตีความไปในทางที่เป็นการให้อำนาจในการเข้าโจมตีประชากรพลเรือน พลเรือน หรือทรัพย์สิงของพลเมือง

หลักความระมัดระวังก่อนการโจมตีจะต้องอยู่บนพื้นฐานของการพิจารณาว่าการปฏิบัติการทางทหารเพื่อการโจมตีฝ่ายตรงข้ามนั้นจะต้องคาดหมายได้ว่าจะเกิดผลกระทบต่อพลเรือนอย่างน้อยที่สุด และหลีกเลี่ยงจากการก่อความเสียหายแก่พลเรือน หรือความเสียหายดังกล่าวจะต้องเกิดน้อยที่สุดด้วย จึงต้องมีการตรวจสอบเป้าหมายทางการทหารที่ย่อมตกอยู่ภายใต้การทำลายได้เสมอ นอกจากนั้นยังต้องมีการเลือกวิธีและปัจจัยในการโจมตีที่จะไม่ก่อให้เกิดความเสียหายต่อพลเรือนหรือความเสียหายที่อาจเกิดขึ้นแก่พลเรือนจะต้องน้อยที่สุด ต้องมีการประเมินความเสียหายล่วงหน้า ปฏิบัติการจะต้องอยู่ภายใต้การควบคุมที่อาจมีการยกเลิกหรือเลื่อนการปฏิบัติการได้หากเป้าหมายดังกล่าวไม่ใช่เป้าหมายทางการทหาร ต้องมีการเตือนภัยล่วงหน้าแก่พลเรือนถึงผลกระทบที่อาจเกิดขึ้น และในกรณีที่สามารถเลือกเป้าหมายในการโจมตีได้ การโจมตีนั้นจะต้องกระทำต่อเป้าหมายที่จะเกิดความเสียหายน้อยที่สุดต่อพลเรือนด้วย ทั้งนี้ ย่อมรวมถึงกรณีจำเป็นที่อาจมีการเคลื่อนย้ายพลเรือนออกจากพื้นที่ปฏิบัติการทางทหารด้วย[804]

[804] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p. 51-68.

ปัญหาในทางปฏิบัติจึงเกิดขึ้นว่าในการปฏิบัติการทางทหารแต่ละกรณีที่จะต้องมีการพิจารณาปัจจัยหลายประการนั้นจะสามารถนำไปสู่การตอบโต้ได้รวดเร็วเพียงใด[805] เพราะมาตรการตอบโต้นั้นจะต้องทำบนพื้นฐาน 3 ประการ คือ

1) ต้องกระทำตอบโต้ต่อรัฐผู้กระทำความผิดโดยตรง

2) รัฐผู้เสียหายจะต้องเรียกร้องให้รัฐผู้กระทำความผิดยุติการละเมิดแล้ว แต่รัฐผู้กระทำความผิดเพิกเฉย

3) มาตรการตอบโต้จะต้องได้สัดส่วนกับความเสียหายที่เกิดขึ้น

มาตรการตอบโต้ทั้งสามประการมาจากการพิจารณาคดี Gabcikovo-Nagymaros Project ของศาลยุติธรรมระหว่างประเทศ[806] หากใช้มาตรการตอบโต้เพื่อการป้องกันตัวตามแนวทางของคดีดังกล่าว จะเกิดปัญหาที่ต้องพิจารณาอย่างมากกับกรณีการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธอย่างแน่นอน เพราะหากการตอบโต้ไม่ได้กระทำโดยตรงต่อผู้ละเมิดพันธกรณีตามกฎหมายระหว่างประเทศย่อมไม่ถือว่าเป็นการป้องกันตัวเองโดยชอบด้วยกฎหมาย เช่นในกรณี the Construction of the Wall in Occupied Palestinian Territory อิสราเอลไม่ได้ทำการป้องกันตัวเองด้วยการตอบโต้โดยตรงต่อผู้ละเมิดอิสราเอล ศาลจึงไม่ยอมรับว่าการกระทำของอิสราเอลชอบด้วยกฎหมายระหว่างประเทศ[807]

นอกเหนือจากหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศซึ่งจะนำมาปรับใช้แก่กรณีวิธีและปัจจัยในการขัดกันทางอาวุธแล้ว หลักพื้นฐานเกี่ยวกับเรื่องการใช้อาวุธในการขัดกันทางอาวุธที่จะต้องพิจารณายังได้แก่กฎการห้ามใช้อาวุธที่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น กฎความได้สัดส่วนในการใช้อาวุธ กฎการห้ามใช้อาวุธที่ไม่สามารถจำแนกเป้าหมายได้ กฎข้อจำกัดในการใช้ปัจจัยและวิธีการในการรบ และพันธกรณีของรัฐภาคีในการทบทวนการพัฒนา การศึกษา การได้มา และการยอมรับซึ่งอาวุธใหม่[808]

ความคิดเห็นของนักวิชาการกลุ่มหนึ่ง โดยเฉพาะอย่างยิ่ง William H. Boothby มองว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศนั้นได้กำหนดนิยามศัพท์ที่ค่อนข้างมีทั้ง

---

[805] Ibid., p. 64.

[806] Case Concerning the Gabcikovo-Nagymaros Project (1997) ICJ Reports 3, International Court of Justice, para 85.

[807] Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory. (2004) ICJ 136, International Court of Justice, Para 139.

[808] William Boothby, Weapons, and the Law of Armed Conflict, p. 348 and Article 36 of Additional Protocol 1 of Geneva Convention 1977.

ความยืดหยุ่นและปรับใช้ได้กับในหลายกรณีอยู่แล้ว แม้ว่าอาจมีข้อท้าทายบางประการเกิดขึ้นจากเทคโนโลยีซึ่งไม่อาจทราบได้ว่าจะเป็นอย่างไรในอนาคตก็ตาม ความล้าหลังของกฎหมายที่เกี่ยวกับอาวุธจึงไม่ใช่เรื่องที่น่าวิตก เพราะกฎหมายสร้างลักษณะความเป็นพลวัตในตัวเองอยู่แล้ว[809]

การตรวจสอบเป้าหมายในการโจมตีเป็นประเด็นสำคัญประการหนึ่งของปฏิบัติการทางทหาร โดยปรากฏในข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 โดยระบุว่าการโจมตีจะต้องกระทำอย่างเคร่งครัดต่อเป้าหมายทางทหาร ในกรณีที่เกี่ยวกับทรัพย์สินสิ่งของนั้น เป้าหมายทางทหารจำกัดเฉพาะทรัพย์สินสิ่งของซึ่งโดยลักษณะ สถานที่ตั้ง วัตถุประสงค์ หรือการใช้ ก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร และการทำลายล้างไม่ว่าทั้งหมดหรือบางส่วน การยึดหรือทำให้หมดสมรรถภาพซึ่งทรัพย์สิน สิ่งของในสภาวการณ์ที่ปฏิบัติการนั้น จะก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน

บทบัญญัติดังกล่าวเป็นพื้นฐานสำคัญที่จะต้องพิจารณาว่าการใช้เทคโนโลยีในการขัดกันทางอาวุธนั้นก่อให้เกิดผลกระทบต่อกฎหมายหรือไม่ โดยจะต้องคำนึงถึงสถานที่ตั้ง และความได้เปรียบทางการทหาร เช่น ระบบการสื่อสารทางไซเบอร์โดยปกติเป็นช่องทางของพลเรือน หากมีการใช้งานเพื่อเป้าหมายทางการทหารและตกอยู่ภายใต้การถูกตอบโต้ได้ จะต้องพิจารณาด้วยว่าการตอบโต้ดังกล่าวนั้นจะก่อให้เกิดความได้เปรียบทางการทหารมากกว่าผลเสียหายที่จะเกิดแก่พลเรือนหรือไม่ และการกระทำต่อระบบดังกล่าวกระทำบนพื้นฐานที่ช่องทางการสื่อสารดังกล่าวต้องมีวัตถุประสงค์หลักในปฏิบัติการทางทหารเป็นสำคัญด้วย

การเลือกปัจจัยและวิธีการในการเข้าโจมตีเป็นกระบวนการหนึ่งซึ่งจะต้องกระทำในปฏิบัติการทางทหารเพื่อให้การโจมตีนั้นเป็นไปด้วยความได้สัดส่วนและเป็นไปเพื่อประโยชน์ในความได้เปรียบทางการทหารเท่านั้น ปัญหาจึงอยู่ที่ว่าระบบอาวุธที่ตัดสินใจได้ด้วยตนเองนั้นใช้วิธีการประมวลผลแบบอัลกอริทึมซึ่งกระทำได้โดยไม่ผ่านการตัดสินใจของมนุษย์ หากมีความผิดพลาดเกิดขึ้นจากการตัดสินใจในการโจมตี จะเชื่อมโยงผลดังกล่าวสู่ความรับผิดชอบของผู้ใด ในขณะที่ระบบการโจมตีทางไซเบอร์อาจเกิดได้ทั้งสองทางคือการใช้ระบบอัลกอริทึมประมวลและตัดสินใจโจมตีเองกับการที่ระบบไซเบอร์ทำตามเงื่อนไขที่ผู้ใช้งานกำหนดเอาไว้ กรณีที่มีมนุษย์เป็นผู้มีส่วนร่วมในการตัดสินใจจึงเป็นประเด็นที่สามารถวิเคราะห์ความรับผิดชอบได้ง่ายกว่า

[809] Ibid, p. 370.

การเลือกเป้าหมายในการโจมตีที่จะต้องกระทำต่อเป้าหมายทางทหารเท่านั้น และจะต้องพยายามให้ความเสียหายเกิดขึ้นแก่พลเรือนน้อยที่สุด เช่นเดียวกันกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธที่จะต้องคำนึงถึงความเสียหายที่อาจเกิดขึ้นแก่พลเรือนทั้งต่อระบบสาธารณูปโภคขั้นพื้นฐานและปัจจัยสำคัญประการอื่นๆ ด้วย

ในการพิจารณาตามปกตินั้นมนุษย์จะมีส่วนเกี่ยวข้องในการตัดสินใจเพื่อโจมตี หากเทคโนโลยีที่ใช้ในการขัดกันทางอาวุธนั้นสามารถระงับการปฏิบัติการเพื่อรอการตัดสินใจจากผู้ที่เกี่ยวข้องได้ ย่อมถือว่าเป็นการปฏิบัติตามหลักการ แต่หากระบบอาวุธนั้นตัดสินใจได้ด้วยตนเอง และมีความผิดพลาดจากการประมวลผลเกิดขึ้นปัญหาย่อมตามมาว่าจะถือเป็นการละเมิดต่อหลักกฎหมายหรือไม่ และความรับผิดชอบตกแก่ผู้ใด[810]

การโจมตีทางไซเบอร์มีประเด็นที่ยากต่อการพิจารณาหลายประการทั้งการตรวจสอบเป้าหมายในการโจมตีว่าจะสามารถกระทำได้เพียงใดเนื่องจากเทคโนโลยีไซเบอร์มีลักษณะการใช้งานร่วมกันของทหารและพลเรือน ในขณะที่การเลือกปัจจัยและวิธีการสำหรับการโจมตีทางไซเบอร์นั้นอาจมีได้หลายหลายแต่ปัญหาที่ยากต่อการพิจารณามากที่สุดคือการละเว้นการโจมตีที่อาจเกิดความสูญเสียต่อพลเรือนซึ่งจะสัมพันธ์กับวิธีปฏิบัติการที่เลือกใช้ด้วย[811]

ปฏิบัติการ Stuxnet อาจเป็นตัวอย่างของการโจมตีทางไซเบอร์ที่สามารถระบุเป้าหมายโดยเฉพาะเจาะจงมีความเสียหายที่เกิดขึ้นเฉพาะต่อเครื่องคัดแยกยูเรเนี่ยมเท่านั้น มัลแวร์ Stuxnet ซึ่งใช้ในการโจมตีโรงงานผลิตยูเรเนี่ยมที่เมืองนาธานซ์ถูกออกแบบมาเพื่อทำงานกับเครื่องมือคัดแยกยูเรเนี่ยมโดยมุ่งประสงค์ให้ใบพัดแยกยูเรเนียมทำงานผิดปกติและเสื่อมสภาพเร็วซึ่งช่วยชะลอการผลิตนิวเคลียร์ของอิหร่านให้ช้าลงไปด้วย การโจมตีทางไซเบอร์ในปฏิบัติการ Stuxnet จึงเป็นการกระทำที่สอดคล้องต่อหลักการแยกแยะและความระมัดระวังล่วงหน้าก่อนการโจมตี คำถามที่น่าสนใจคือการโจมตีทางไซเบอร์ในกรณี Stuxnet เป็นการละเมิดต่อหลักความได้สัดส่วนหรือไม่เนื่องจากความเสียหายที่เกิดกับโรงงานผลิตยูเรเนี่ยมอาจนำไปสู่ความเสียหายต่อสาธารณะ

ประเด็นเรื่องความเสียหายต่อโรงงานผลิตยูเรเนี่ยมนาธานซ์นี้น่าสนใจตรงที่โดยลักษณะของโรงงานแล้วไม่ได้เป็นการนำยูเรเนี่ยมมาใช้ประโยชน์สร้างเป็นอาวุธหรือพลังงานไฟฟ้าโดยตรง แต่เป็น

---

[810] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," pp. 4-5.

[811] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, (Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018), p. 86.

การคัดแยกยูเรเนี่ยมเพื่อให้ได้เฉพาะยูเรเนี่ยมมาตรฐานที่สามารถผลิตอาวุธได้หรือผลิตกระแสไฟฟ้าได้ไปใช้ในขั้นตอนต่อไป การโจมตีที่เกิดขึ้นจึงก่อให้เกิดความเสียหายต่ออุปกรณ์คัดแยกยูเรเนี่ยมเท่านั้นโดยไม่มีหลักฐานพิสูจน์ว่าจะนำไปสู่ความเสียหายต่อชีวิตและร่างกายของพลเรือนแต่อย่างใด เมื่อคำนึงถึงปัจจัยแวดล้อมอื่นๆ เช่น สถานที่ตั้งของโรงงานซึ่งอยู่ห่างไกลจากชุมชนเนื่องจากโรงงานตั้งอยู่ในทะเลทราย ยูเรเนี่ยมที่คัดแยกออกมาได้ยังไม่อยู่ในลักษณะของการนำไปสร้างปฏิกิริยาฟิวชั่น ความตั้งใจของผู้ออกแบบโปรแกรมมัลแวร์ต้องการให้ Stuxnet ทำหน้าที่ชะลอการผลิตยูเรเนี่ยมซึ่งอาจนำไปสู่การผลิตอาวุธนิวเคลียร์ของอิหร่าน จึงมีเหตุผลอธิบายได้ว่าปฏิบัติการ Stuxnet เป็นการกระทำที่สอดคล้องต่อทั้งหลักการแยกแยะ ความได้สัดส่วนและความระมัดระวังล่วงหน้าก่อนการโจมตี

ปฏิบัติการโจมตีทางไซเบอร์ด้วยวิธีการ DDoS มีลักษณะเป็นการกระทำที่อาจไม่สอดคล้องต่อหลักความระมัดระวังล่วงหน้าก่อนการโจมตีเมื่อพิจารณาจากสถานการณ์ที่เกิดขึ้นในปัจจุบันไม่ว่าจะเป็นเหตุการณ์ที่เกิดขึ้นที่ประเทศจอร์เจีย ประเทศเอสโตเนียและประเทศยูเครนพบว่าการโจมตีด้วยวิธีการ DDoS เท่าที่ปรากฏเป็นการสร้างความเสียหายต่อเว็บไซต์ของรัฐบาลซึ่งเป็นทรัพยากรณ์ที่ใช้ร่วมกันระหว่างทหารและพลเรือน การโจมตีที่เกิดขึ้นจึงไม่สอดคล้องต่อวิธีการโจมตีที่จะต้องคำนึงถึงผลเสียหายต่อพลเรือนซึ่งเป็นองค์ประกอบของความระมัดระวังล่วงหน้าก่อนการโจมตี แม้การโจมตีด้วยวิธีการ DDoS มีลักษณะของการกระทำที่ไม่ได้คำนึงถึงความเสียหายต่อพลเรือนแต่น่าสนใจว่าความเสียหายที่เกิดขึ้นนั้นเป็นผลต่อระบบสื่อสารทางอินเทอร์เน็ตเป็นหลักแต่ไม่ได้ก่อให้เกิดความเสียหายทางกายภาพคือไม่มีผลต่อชีวิตและร่างกายของบุคคล[812] และอาจไม่ทำให้ทรัพย์สินเสียหายด้วย กรณีนี้จะยังถือว่าเป็นความเสียหายที่ไม่สอดคล้องต่อหลักความระวัดระวังล่วงหน้าหรือไม่

หลักความระมัดระวังล่วงหน้านี้มีวัตถุประสงค์เพื่อคุ้มครองผลกระทบที่อาจเกิดขึ้นแก่พลเรือน ในปฏิบัติการทางทหารตามแบบดั้งเดิมในสงครามมีความมุ่งประสงค์ให้เกิดความเสียหายทางกายภาพเป็นสำคัญแต่เมื่อโลกเข้าสู่ยุคดิจิทัล ความเสียหายที่เป็นรูปธรรมทางกายภาพอาจไม่เกิดขึ้นเช่นเดิมแล้วจะยังถือว่าเป็นความเสียหายแบบเดิมอยู่หรือไม่ เพียงใด

ประเด็นเรื่องการใช้อาวุธอิสระนั้นมีข้อเสนอจากนักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายคนต้องการให้นำหลักการ Human-Center Approach มากับการพิจารณาความรับผิด

---

[812] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

ของบุคคลต่อระบบอาวุธอิสระ แนวคิดพื้นฐานคือการมองว่าระบบอาวุธอิสระมีลักษณะการทำงานแบบปัญญาประดิษฐ์ การพิจารณาว่าปัญญาประดิษฐ์ทำงานได้น่าเชื่อถือหรือไม่จะต้องนำความสัมพันธ์ของมนุษย์ในการสั่งการ ควบคุมหรือยุติการทำงานมาพิจารณาด้วย โดยความเห็นหลักมองว่าระบบอาวุธอิสระหรือปัญญาประดิษฐ์จะทำงานโดยตนเองทั้งหมดไม่ได้ เพราะหากมีความเสียหายเกิดขึ้นจากความผิดพลาดของปัญญาประดิษฐ์ก็จะไม่มีความรับผิดในตัวประดิษฐ์เกิดขึ้น มนุษย์ผู้มีความรับผิดชอบตามกฎหมายจึงต้องเข้ามามีส่วนเกี่ยวข้องกับการควบคุมปัญญาประดิษฐ์ด้วย หากไม่มีมนุษย์ควบคุมก็อาจเชื่อได้ว่าเป็นปฏิบัติการที่ไม่คำนึงถึงความระมัดระวังล่วงหน้าก่อนการโจมตี

การขัดขวางหรือการโจมตีสัญญาณดาวเทียม เช่นกรณีที่เกิดขึ้นในความขัดแย้งระหว่างประเทศยูเครนและรัสเซียมีข้อพิจารณาว่าเป็นการกระทำที่สอดคล้องกับหลักความระมัดระวังล่วงหน้าก่อนการโจมตีหรือไม่ หากพิจารณาแล้วจะพบว่ามีประเด็นที่น่าสงสัยว่าจะเป็นการกระทำที่ละเมิดต่อหลักความระมัดระวังล่วงหน้าได้แก่ การเลือกเป้าหมายในการโจมตีที่กระทำต่อสัญญาณดาวเทียมจะถือได้ว่าเป็นการกระทำที่จะไม่ส่งผลกระทบต่อพลเรือนได้อย่างไรเมื่อสัญญาณสื่อสารผ่านดาวเทียมเป็นสัญญาณที่แยกการใช้งานของทหารและพลเรือนค่อนข้างยาก นอกจากนั้นหากพิจารณาว่าการกระทำจะต้องไม่ก่อให้เกิดความเสียหายแก่พลเรือนโดยคาดหมายได้ยิ่งมีความเสี่ยงว่าการโจมตีสัญญาณดาวเทียมจะมีลักษณะเป็นการคาดหมายได้ว่าย่อมเกิดผลกระทบต่อพลเรือน เมื่อพิจารณาลักษณะ 2 ประการนี้จึงมีน้ำหนักไปในทางที่พิสูจน์ได้ว่าการโจมตีสัญญาณดาวเทียมเป็นการกระทำที่ขัดต่อหลักความระมัดระวังล่วงหน้าก่อนการโจมตี ปัญหาที่เหลืออยู่ประการเดียวคือผลกระทบต่อพลเรือนในสงครามแบบดั้งเดิมคือผลกระทบทางกายภาพแต่การโจมตีสัญญาณดาวเทียมเท่าที่ปรากฏในปัจจุบันยังไม่พบความเสียหายทางกายภาพจะถือว่าความเสียหายดังกล่าวเทียบเท่าความเสียหายที่เกิดขึ้นจากสงครามตามแบบได้หรือไม่[813]

อากาศยานไร้คนขับซึ่งมีการนำมาใช้ในการขัดกันทางอาวุธโดยทั่วไปมักเป็นระบบการควบคุมทางไกลโดยมีมนุษย์มีส่วนเกี่ยวข้องกับทั้งระบบควบคุมทิศทาง การคัดเลือกเป้าหมายและการตัดสินใจทำลายเป้าหมาย การใช้อากาศยานไร้คนขับลักษณะการควบคุมทางไกลนี้จึงยังสามารถปรับใช้หลักความระมัดระวังล่วงหน้าก่อนการโจมตีกับผู้ควบคุมอากาศยานได้ ปัญหาจะเกิดขึ้นกับอากาศ

[813] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

ยานไร้คนขับที่สามารถตัดสินใจได้ด้วยตัวเองซึ่งปัจจุบันยังไม่พบการใช้งานจริงหากมีการใช้งานอากาศยานไร้คนขับที่สามารถตัดสินใจได้ด้วยตัวเองย่อมเกิดข้อพิจารณาแบบเดียวกับระบบอาวุธอิสระ

3.3.3 หลักการคุ้มครองทรัพย์สิ่งของพลเรือนและสถานที่คุ้มครองพิเศษ

ในกรณีที่หลักการพื้นฐานในการจำกัดวิธีการและปัจจัยในการขัดกันทางอาวุธ การแยกแยะเป้าหมายในการโจมตี ความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตีอาจไม่สามารถนำมาปรับใช้ได้หรือในกรณีที่การกระทำอย่างหนึ่งอย่างใดเป็นการละเมิดต่อข้อกฎหมายมนุษยธรรมระหว่างประเทศดังต่อไปนี้ การกระทำดังกล่าวย่อมถือเป็นการละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศ

3.3.3.1 การคุ้มครองทรัพย์สิ่งของที่จำเป็นต่อการดำรงชีพของพลเรือน[814]

การโจมตีทางไซเบอร์ด้วยวิธีการ DDoS นั้นอาจนำมาซึ่งข้อพิจารณาหลายประการทั้งเรื่องการแยกแยะเป้าหมายการโจมตี การกระทำที่สอดคล้องต่อหลักความได้สัดส่วนและปัญหาการพิจารณาความระมัดระวังล่วงหน้าก่อนการโจมตี แต่หากพิจารณาว่าสิ่งที่เกี่ยวข้องกับระบบไซเบอร์เช่นอินเทอร์เน็ต คอมพิวเตอร์ ระบบการสื่อสารและข้อมูลในระบบไซเบอร์เป็นทรัพย์สิ่งของพลเรือนที่จำเป็นต่อการดำรงชีพก็อาจนำไปสู่การตอบปัญหาว่าเหตุใดการโจมตีทางไซเบอร์ที่กระทำต่อเครือข่ายการติดต่อสื่อสารจึงเป็นการกระทำที่ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศได้

อย่างไรก็ดีการจะกำหนดให้ทรัพยากรที่เกี่ยวข้องกับระบบไซเบอร์เป็นทรัพย์สิ่งของที่จำเป็นต่อพลเรือนทั้งหมดคงเป็นไปไม่ได้ การจำกัดเฉพาะทรัพยากรที่ใช้ร่วมกันของพลเรือนจึงอาจมีความเหมาะสมกว่า เช่นระบบไซเบอร์ที่เกี่ยวข้องกับโรงพยาบาลซึ่งอาจส่งผลเสียหายต่อระบบสาธารณสุขของพลเมืองส่วนรวม หรือระบบไซเบอร์ที่เกี่ยวข้องกับระบบสาธารณูปโภคไฟฟ้า ประปา ฯลฯ การกำหนดขอบเขตของทรัพย์สิ่งของพลเรือนทางไซเบอร์ที่เกี่ยวข้องกับสาธารณะจะทำให้เกิดความชัดเจนต่อการพิจารณาการโจมตีทางไซเบอร์ที่กระทบต่อทรัพย์สิ่งของพลเรือนมากขึ้น

---

[814] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 54.

3.3.3.2 การคุ้มครองสิ่งแวดล้อมทางธรรมชาติ[815]

ในอดีตมีการใช้ปฏิบัติการ Orange Agent หรือฝนเหลืองในสงครามเวียดนามจึงก่อให้เกิดแนวทางในการห้ามการใช้เทคโนโลยีเพื่อก่อให้เกิดการเปลี่ยนแปลงทางสิ่งแวดล้อมทางธรรมชาติ ในปัจจุบันอาจมีการตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้เทคโนโลยีนาโนเพื่อการเปลี่ยนแปลงสิ่งแวดล้อมทางธรรมชาติเพื่อเป็นอาวุธในการทำลาย ทางปฏิบัติแล้วยังไม่พบการใช้เทคโนโลยีนาโนเพื่อเปลี่ยนแปลงสิ่งแวดล้อมทางธรรมชาติแต่หากเกิดกรณีดังกล่าวขึ้นหลักการคุ้มครองสิ่งแวดล้อมทางธรรมชาติย่อมสามารถนำมาปรับใช้กับเทคโนโลยีนาโนดังกล่าวได้

3.3.3.3 การคุ้มครองสิ่งติดตั้งพลังงานอันตราย[816]

การโจมตีทางไซเบอร์ในปฏิบัติการ Stuxnet ต่อโรงงานนาธานซ์ (Natanz) ที่ประเทศอิหร่านเป็นสถานการณ์ที่ใกล้เคียงกับการโจมตีสิ่งติดตั้งพลังงานอันตรายมากที่สุดเท่าที่ปรากฏเนื่องจากเกี่ยวข้องกับการบวนการคัดแยกยูเรเนี่ยมซึ่งสามารถนำมาใช้ในการผลิตอาวุธนิวเคลียร์และผลิตไฟฟ้าพลังนิวเคลียร์ได้ สิ่งที่น่าสนใจคือยูเรเนี่ยมที่คัดแยกได้จากโรงงานนาธานซ์นี้ยังไม่เข้าสู่กระบวนการสร้างพลังงานนิวเคลียร์แต่เป็นกระบวนการคัดแยกวัตถุดิบจะถือว่าเป็นสิ่งติดตั้งพลังงานอันตรายหรือไม่

ในกรณีที่เป็นการโจมตีทางไซเบอร์ต่อโรงไฟฟ้าพลังงานนิวเคลียร์ เตาปฏิกรณ์นิวเคลียร์ โรงงานผลิตอาวุธนิวเคลียร์ หรือการโจมตีทางไซเบอร์ต่อเขื่อนเก็บน้ำ ฯลฯ ย่อมเป็นการขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศในการคุ้มครองสิ่งติดตั้งพลังงานอันตรายโดยตรง แต่สถานการณ์ที่กล่าวมานี้ยังไม่เกิดขึ้นในการขัดกันทางอาวุธแต่อย่างใด

3.4 กฎหมายระหว่างประเทศอื่นที่มีบทบาทต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

กฎหมายระหว่างประเทศอื่นที่มีบทบาทต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศได้แก่ กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธ (Disarmament) กฎหมายระหว่างประเทศเกี่ยวกับเทคโนโลยีอวกาศและกฎหมายเกี่ยวกับการควบคุมการส่งออกสินค้าที่ใช้ได้สองทาง แม้

---

[815] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 55.

[816] Ibid., Article 56.

กฎหมายเหล่านี้ไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศโดยตรง แต่การใช้กฎหมายเหล่านี้ก่อให้เกิดการควบคุมเทคโนโลยีนอกสถานการณ์การขัดกันทางอาวุธและนำไปสู่การจำกัดการใช้เทคโนโลยีในการขัดกันทางอาวุธ ซึ่งอาจอธิบายได้ดังนี้

3.4.1 กฎหมายเกี่ยวกับการลดอาวุธ

กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธได้รับอิทธิพลไม่มากก็น้อยจากแนวคิดในการจำกัดความเสียหายที่เกิดจากการใช้อาวุธในการขัดกันทางอาวุธ โดยเริ่มต้นจากกฎหมายห้ามใช้อาวุธในการรบ เช่น ปฏิญญาเซ็นต์ปีเตอร์สเบิร์กว่าด้วยการห้ามใช้กระสุนปืนที่มีน้ำหนักต่ำกว่า 400 กรัม ค.ศ.1868 อนุสัญญากรุงเฮก ค.ศ. 1899 ซึ่งมีปฏิญญาประกอบ 3 ฉบับ ฉบับที่ 1 ว่าด้วยเรื่องการห้ามใช้กระสุนและวัตถุระเบิดที่ปล่อยจากบอลลูน ฉบับที่ 2 ว่าด้วยเรื่องการห้ามใช้กระสุนแก๊สพิษ ฉบับที่ 3 ว่าด้วยเรื่องการห้ามใช้กระสุนที่แตกกระจายเมื่อเข้าสู่ร่างกายมนุษย์ พิธีสารเจนีวาว่าด้วยเรื่องการห้ามใช้แก๊สพิษและแบคทีเรียในการทำสงคราม ค.ศ.1925 อนุสัญญาแห่งสหประชาชาติว่าด้วยการห้ามใช้อาวุธตามแบบที่อาจก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น ค.ศ.1980 ซึ่งมีพิธีสารเพิ่มเติม 5 ฉบับ อันได้แก่ พิธีสารฉบับที่ 1 ว่าด้วยเรื่องการห้ามใช้วัตถุที่แตกกระจายในร่างกายมนุษย์และไม่สามารถตรวจพบได้ด้วยรังสีเอ็กซ์ ค.ศ.1980 พิธีสารฉบับที่ 2 ว่าด้วยการห้ามและจำกัดการใช้ทุ่นระเบิดสังหารบุคคล ค.ศ.1980 พิธีสารฉบับที่ 3 ว่าด้วยการห้ามและจำกัดการใช้อาวุธเพลิง ค.ศ.1980 พิธีสารฉบับที่ 4 ว่าด้วยการห้ามใช้อาวุธเลเซอร์ ค.ศ.1995 พิธีสารฉบับที่ 5 ว่าด้วยเรื่องวัตถุระเบิดที่เหลือจากการสงคราม ค.ศ.2003 เป็นต้น

องค์การสหประชาชาติมีบทบาทอย่างมากในการพัฒนากฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธในยุคหลังสงครามโลกครั้งที่ 2 ซึ่งเป็นเป็นตามวัตถุประสงค์การจัดตั้งองค์การสหประชาชาติเพื่อการรักษาสันติภาพระหว่างประเทศ ในขณะที่กฎหมายมนุษยธรรมระหว่างประเทศมีขอบเขตการปรับใช้ในสถานการณ์การขัดกันทางอาวุธอยู่แล้ว กฎหมายระหว่างประเทศเกี่ยวกับการลดอาวุธของสหประชาชาติจึงถูกสร้างขึ้นมาเพื่อการการลดอาวุธที่จะก่อให้เกิดความเสียหายเกินขนาดหรือความเสียหายที่ไม่สามารถจำกัดขอบเขตได้ ซึ่งมาตรการที่เกี่ยวข้องกับการลดอาวุธย่อมรวมถึงการควบคุมการพัฒนา การควบคุมการผลิต และการควบคุมการแพร่กระจายอาวุธ[817] มาตรการเหล่านี้ไม่เกี่ยวข้องกับขอบเขตการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศโดยตรงแต่

[817] Alyn Ware, eds., Assuring our Common Future: A guide to parliamentary action in support of disarmament for security and sustainable development, (New York: United Nations Secretary general, 2020), p.10.

เป็นมาตรการที่เสริมประสิทธิผลการการใช้กฎหมายมนุษยธรรมระหว่างประเทศในสองลักษณะคือ การป้องกันไม่ให้มีการพัฒนาและผลิตอาวุธที่จะนำมาใช้ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศและการทำลายอาวุธภายหลังจากที่สถานการณ์ขัดกันทางอาวุธสิ้นสุดลง

3.4.2 กฎหมายระหว่างประเทศเกี่ยวกับเทคโนโลยีอวกาศ

กฎหมายระหว่างประเทศหลักที่เกี่ยวข้องกับกิจกรรมในอวกาศ ได้แก่ สนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศ รวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ. 1967 (1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies) ข้อตกลงระหว่างประเทศว่าด้วยเรื่องการช่วยเหลือนักบินอวกาศ การส่งกลับนักบินอวกาศ และวัตถุอวกาศที่ถูกส่งเข้าสู่อวกาศ ค.ศ.1968 (1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space) อนุสัญญาความรับผิดชอบระหว่างประเทศต่อความเสียหายเนื่องจากวัตถุอวกาศ ค.ศ.1972 (1972 Convention on International Liability for Damage Caused by Space Objects) อนุสัญญาจดทะเบียนวัตถุที่ถูกส่งเข้าสู่อวกาศ ค.ศ.1975 (1975 Convention on Registration of Objects Launched into Outer Space) ข้อตกลงว่าด้วยกิจกรรมของรัฐบนดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ. 1979 (1979 Agreement Governing the Activities of States on the Moon and other Celestial Bodies)

องค์การสหประชาชาติมีบทบาทหลักในการดูแลกิจกรรมที่เกิดขึ้นในอวกาศตามกรอบของปฏิญญาหลักกฎหมายเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศภายนอก (Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, GA Res 1962 (XVIII) 13 December 1963) และมีคณะกรรมการว่าด้วยเรื่องการใช้อวกาศภายนอกเพื่อสันติ (Committee on the Peaceful Uses of Outer Space: COPUOS) ดูแลเรื่องกิจกรรมในอวกาศ โดยคณะกรรมการชุดนี้จัดตั้งขึ้นมาตั้งแต่ปี ค.ศ. 1957 ในช่วงเวลาที่มีการส่งยานสปุตนิก (Sputnik) ขึ้นสู่อวกาศและเริ่มมีการใช้งานขีปนาวุธระยะไกลแบบข้ามทวีป[818]

[818] Duncan Blake, "The Law Applicable to Military Strategic Use of Outer Space," in Hitoshi Nasu and Robert McLaughlin, editors., New Technologies and the Law of Armed Conflict. (The Hague: T.M.C. Asser Press, 2014) p. 117.

จากหลักฐานที่ปรากฏ จะเห็นได้ชัดเจนว่ากฎหมายระหว่างประเทศที่เกี่ยวกับการควบคุมกิจกรรมในอวกาศนั้นเกิดขึ้นจากการแข่งขันทางอวกาศระหว่างประเทศสหรัฐอเมริกาและอดีตประเทศสหภาพโซเวียตในช่วงเวลาหนึ่ง โดยในขณะนั้นไม่มีกฎหมายระหว่างประเทศที่เกี่ยวข้องกับเทคโนโลยีทางอวกาศอยู่เลย จึงก่อให้เกิดความเคลื่อนไหวของสังคมระหว่างประเทศในการสร้างกฎหมายเฉพาะในเรื่องดังกล่าวขึ้นมา[819] กฎหมายระหว่างประเทศที่เกี่ยวข้องกับกิจการอวกาศมีผลเกี่ยวกับเรื่องการใช้อาวุธในบางกรณีดังต่อไปนี้

สนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศ รวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ.1967 ได้กำหนดหลักการในการห้ามติดตั้งอาวุธนิวเคลียร์และอาวุธที่มีอานุภาพทำลายล้างสูง[820]

กฎหมายระหว่างประเทศที่เกี่ยวข้องกับการใช้อาวุธในอวกาศ ได้แก่ สนธิสัญญาห้ามการทดสอบอาวุธนิวเคลียร์ในชั้นบรรยากาศ อวกาศภายนอก และใต้น้ำ ค.ศ. 1963 (1963 Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space, and Under Water, Nuclear Test-Ban Treaty: NTBT, Partial Test-Ban Treaty: PTBT) และสนธิสัญญาห้ามการทดสอบอาวุธนิวเคลียร์ ค.ศ. 1996 (1996 The Comprehensive Nuclear-Test-Ban Treaty: CTBT)

สนธิสัญญาห้ามการทดสอบอาวุธนิวเคลียร์ ค.ศ. 1996 กำหนดพันธกรณีของรัฐภาคีในการทดสอบการระเบิดอาวุธนิวเคลียร์และวัตถุระเบิดที่เกี่ยวกับนิวเคลียร์ โดยจะต้องห้ามและป้องกันการระเบิดของนิวเคลียร์ในเขตอำนาจของรัฐตนด้วย นอกจากนั้น ยังห้ามรัฐดำเนินการโดยประการใดๆ เพื่อให้มีการกระทำ สนับสนุน หรือมีส่วนร่วมในการดำเนินการทดสอบการระเบิดของอาวุธนิวเคลียร์หรือวัตถุระเบิดที่เกี่ยวข้องกับนิวเคลียร์[821]

ส่วนการห้ามใช้อาวุธนิวเคลียร์นั้นมีสนธิสัญญาว่าด้วยการห้ามอาวุธนิวเคลียร์ ค.ศ. 2017 (2017 Treaty on the Prohibition of Nuclear Weapons) มีผลบังคับใช้ตั้งแต่วันที่ 22 มกราคม ค.ศ.2021 (พ.ศ.2564)[822] ซึ่งห้ามรัฐพัฒนา ทดสอบ สร้าง ผลิต ทำให้ได้มา ครอบครอง หรือสะสม

---

[819] Duncan Blake, “The Law Applicable to Military Strategic Use of Outer Space,” p. 118.

[820] 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Art. IV.

[821] 1996 Comprehensive Nuclear Test-Ban Treaty, United Nations General Assembly Resolution 50/245, 17 September 1996, A/RES/50/245. Art. 1.

[822] สถานะเมื่อวันที่ 31 พฤษภาคม พ.ศ.2565 มีประเทศลงนามแล้ว 86 ประเทศ และมีประเทศสมาชิกแล้ว 61 ประเทศ

อาวุธนิวเคลียร์หรือวัตถุที่เกี่ยวข้องกับอาวุธนิวเคลียร์[823] ห้ามรัฐใช้หรือขู่ว่าจะใช้อาวุธนิวเคลียร์หรือระเบิดนิวเคลียร์[824]

แม้สนธิสัญญาที่เกี่ยวข้องกับการห้ามการทดสอบอาวุธนิวเคลียร์และสนธิสัญญาห้ามใช้อาวุธนิวเคลียร์จะมิได้มีการกำหนดขอบเขตการบังคับใช้กฎหมายในอวกาศ แต่หากรัฐภาคีปฏิบัติตามสนธิสัญญาอย่างเคร่งครัดการทดสอบอาวุธนิวเคลียร์ย่อมไม่เกิดขึ้นทั้งในโลกและห้วงอวกาศเช่นกัน

มีข้อสังเกตประการหนึ่งที่เกิดขึ้นคืออาวุธทั่วไปไม่ต้องห้ามตามสนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศ รวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ. 1967 นอกจากนั้นการที่กฎหมายกำหนดการห้ามติดตั้งอาวุธที่มีอานุภาพทำลายล้างสูงในสถานีอวกาศหรือดาวเทียมในอวกาศนั้น ใช้บังคับเฉพาะกับสิ่งที่อยู่ในวงโคจร สิ่งที่ยังไม่ถึงวงโคจรย่อมได้รับประโยชน์จากช่องว่างทางกฎหมายดังกล่าว[825]

ข้อตกลงว่าด้วยกิจกรรมของรัฐบนดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ.1979 ข้อ 1 ได้ขยายขอบเขตในการบังคับใช้กฎหมายให้ไกลกว่า “วงโคจร” (orbit) โดยให้รวมถึง “วิถี” (trajectories) รอบดวงจันทร์ด้วย ซึ่งการขยายพื้นที่ให้รวมถึงวิถีรอบดวงจันทร์นี้จะส่งผลอย่างมากต่อการใช้ขีปนาวุธแบบทิ้งตัวที่เดินทางออกไปนอกชั้นบรรยากาศได้ ในขณะที่ข้อ 3 มีการห้ามการกระทำที่เป็นการคุกคามหรือการกระทำที่เป็นปรปักษ์ในพื้นที่ดวงจันทร์หรือใช้ดวงจันทร์เป็นสถานที่เกี่ยวข้องกับข้อพิพาท โดยห้ามการใช้อาวุธที่มีอานุภาพทำลายล้างสูงบนดวงจันทร์ ในวงโคจรของดวงจันทร์ และวิถีการคมนาคมทางอากาศที่เกี่ยวข้องกับดวงจันทร์[826]

อนุสัญญาว่าด้วยการห้ามการทหารหรือการใช้งานใดๆ ที่ไม่เป็นมิตรด้วยการใช้เทคนิคในการปรับเปลี่ยนสิ่งแวดล้อม ค.ศ.1978 (1978 Convention on The Prohibition of Military or Any Other Hostile Use of Environmental Modification Technique: ENMOD) มีหลักการในข้อ 1 ซึ่งห้ามรัฐภาคีใช้เทคนิคการดัดแปลงสิ่งแวดล้อมเพื่อวัตถุประสงค์ทางทหารหรือการกระทำที่ไม่เป็น

---

[823] 2017 Treaty on the Prohibition of Nuclear Weapons, 7 July 2017, United Nations General Assembly Resolution, A/CONF.229/2017/8, Art. 1 (a)

[824] Ibid., Art. 1 (d)

[825] Bin Cheng, “Properly speaking, only celestial bodies have been reserved for use exclusively for peaceful (non-military) purposes, but not outer void space,” In Michael N. Schmitt (ed) International law across the spectrum of conflict: essays in honour of Professor L.C. Green on the occasion of his eightieth birthday. US Naval War College International Law Studies, Vol. 75, Naval War College, Newport, Rhode Island (2000), pp 98-99.

[826] Duncan Blake, “The Law Applicable to Military Strategic Use of Outer Space,” in Hitoshi Nasu and Robert McLaughlin, eds., New Technologies and the Law of Armed Conflict, p. 123.

มิตรอื่นๆ ซึ่งมีผลในวงกว้าง ยาวนานหรือรุนแรง ในการเป็นปัจจัยเพื่อการทำลายล้าง สร้างความเสียหาย หรือสร้างความบาดเจ็บต่อสมาชิกของรัฐภาคีอื่น โดยขอบเขตของกฎหมายดังกล่าวกว้างขวางเพียงพอที่จะบังคับใช้กับพื้นที่ทางอวกาศได้

นอกจากนั้นสนธิสัญญาต่อต้านการใช้ขีปนาวุธแบบทิ้งตัว ค.ศ. 1972 (1972 The Anti-Ballistic Missile Treaty) ยังอาจนำมาใช้ในการอุดช่องว่างของการใช้ระบบขีปนาวุธแบบทิ้งตัวที่ยิงผ่านชั้นบรรยากาศ และไม่สามารถใช้อนุสัญญาหรือสนธิสัญญาอื่นๆ เพื่อบังคับกับการกระทำดังกล่าวได้ ทั้งนี้เนื่องจากการใช้งานขีปนาวุธแบบทิ้งตัวโดยทั่วไปก็มีลักษณะคล้ายคลึงกับการใช้งานขีปนาวุธทำลายดาวเทียม เพียงแต่อาจมีข้อจำกัดเฉพาะส่วนที่ไม่เกินขอบเขตของชั้นบรรยากาศ[827] นอกจากนี้ยังมีกรอบของแนวปฏิบัติเฮกว่าด้วยเรื่องการต่อต้านการแพร่กระจายขีปนาวุธแบบทิ้งตัว (Hague Code of Conduct against Ballistic Missile Proliferation) ซึ่งเป็นแนวปฏิบัติที่มีผลทางการเมืองเท่านั้น ไม่มีผลผูกพันทางกฎหมาย ซึ่งเป็นแนวทางในการห้ามการพัฒนาและการแพร่กระจายขีปนาวุธแบบทิ้งตัว ซึ่งจะช่วยเสริมการบังคับใช้กฎหมายที่เกี่ยวข้องกับการห้ามใช้ขีปนาวุธแบบทิ้งตัวในชั้นอวกาศต่อไป[828]

บทบาทของคณะมนตรีความมั่นคงแห่งสหประชาชาติในการจัดการกับการใช้อาวุธในเขตพื้นที่อวกาศ ได้แก่ มติคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 2087 ซึ่งเน้นย้ำเรื่องการรักษาสันติภาพและความมั่นคงระหว่างประเทศในกิจกรรมที่เกิดขึ้นในชั้นอวกาศ ในขณะที่สมัชชาใหญ่แห่งสหประชาชาติมีมติว่าด้วยเรื่องการป้องกันการแข่งขันทางอาวุธในห้วงอวกาศภายนอก (Resolutions on the Prevention of an Arms Race in Outer Space: PAROS) ซึ่งยอมรับว่าในปัจจุบันยังขาดกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการห้ามการแข่งขันทางอาวุธในอวกาศ จึงมีความจำเป็นอย่างเร่งด่วนในการสร้างกฎหมายระหว่างประเทศเพื่อป้องกันการแข่งขันทางอาวุธในห้วงอวกาศ อย่างไรก็ดี สมัชชาใหญ่แห่งสหประชาชาติยังคงไม่สามารถดำเนินการอย่างเป็นรูปธรรมในการสร้างกฎหมายระหว่างประเทศในประเด็นดังกล่าวขึ้นมาได้ แม้มีความพยายามตั้งคณะผู้เชี่ยวชาญระดับรัฐบาลขึ้นมาเพื่อศึกษาแนวทางในการสร้างการตรวจสอบและการสร้างความเชื่อมั่นเพื่อสันติภาพในอวกาศ แต่กลับพบว่าในการประชุมที่ผ่านมาทั้งในปี ค.ศ.2010 และปี ค.ศ.2012 ยังไม่สามารถสร้างแนวทางใดๆ ได้เลย

---

[827] Ibid., p. 125.

[828] Ibid.

อย่างไรก็ดี จากการทำงานของกลุ่มผู้เชี่ยวชาญก่อให้เกิดแนวทาง 2 ประการต่อการพัฒนากฎหมายระหว่างประเทศ ได้แก่

1) ร่างสนธิสัญญาระหว่างประเทศว่าด้วยการป้องกันการติดตั้งอาวุธ ค.ศ. 2008 (The Draft Prevention of the Placement of Weapons Treaty: PPWT) ซึ่งมีใจความสำคัญที่ ข้อ 2 ซึ่งกำหนดหน้าที่ของรัฐภาคีในการห้ามนำระบบอาวุธใดๆ เข้าสู่วงโคจรของโลก และห้ามติดตั้งอาวุธในเทหวัตถุห้วงอวกาศ รวมถึงการห้ามข่มขู่หรือคุกคามว่าจะใช้อาวุธเพื่อต่อต้านสิ่งติดตั้งในห้วงอวกาศ และจะไม่มีการช่วยเหลือหรือสนับสนุนรัฐอื่น กลุ่ม หรือองค์การระหว่างประเทศในกิจกรรมที่เป็นการต้องห้ามตามสนธิสัญญาฉบับนี้[829]

อย่างไรก็ดี ขอบเขตตามร่างสนธิสัญญานี้ไม่ครอบคลุมถึงอาวุธที่ยิงจากโลกสู่อวกาศ (weapons 'to' space) แต่คำว่า "placement" ตามสนธิสัญญาฉบับนี้มีการให้ความหมายที่กว้างกว่าการติดตั้งกับดาวเทียมหรือเทหวัตถุในห้วงอวกาศ โดยรวมถึงการนำเข้าสู่วงโคจรหรือเป็นส่วนหนึ่งของวงโคจรด้วย[830] และคำว่าห้วงอวกาศภายนอกตามนิยามของร่างสนธิสัญญาฉบับนี้หมายถึงระยะความสูง 100 เมตรเหนือระดับน้ำทะเล[831] นอกจากนั้นการใช้ประโยชน์จากห้วงอวกาศภายนอกของรัฐนั้นจะต้องเป็นไปเพื่อสันติตามกรอบของสนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศ รวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ.1967 ทั้งนี้ยังคงรับรองสิทธิของรัฐในการป้องกันตนเองตามข้อ 51 ของกฎบัตรสหประชาชาติ[832] อย่างไรก็ดี ร่างสนธิสัญญานี้ยังมีช่องว่างที่ไม่มีข้อกำหนดเกี่ยวกับเรื่องการตรวจตราการปฏิบัติตามกฎหมาย ทำให้หลายประเทศไม่ให้การรับรอง นอกจากนั้น ปัญหาที่หลายฝ่ายยังคงวิตกกังวลคือการนิยามคำว่า "อาวุธอวกาศ" ควรจะต้องหมายถึงสิ่งใดบ้างและจะใช้เกณฑ์จำแนกอย่างไร เพราะในเชิงเทคโนโลยีในปัจจุบันที่พัฒนาอย่างรวดเร็ว การกำหนดนิยามดังกล่าวอาจเป็นเรื่องที่ค่อนข้างยาก[833]

---

[829] 2008 The Draft Prevention of the Placement of Weapons Treaty, Art. 2. [online] April 10, 2020. Available from: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/200802/t20080212_599554.html

[830] Ibid., Art. 1 (d).

[831] Ibid., Art. 1 (a).

[832] Ibid., Art. 4.

[833] Duncan Blake, "The Law Applicable to Military Strategic Use of Outer Space," in Hitoshi Nasu and Robert McLaughlin, eds., New Technologies and the Law of Armed Conflict, p. 127.

2) แนวปฏิบัติเกี่ยวกับกิจกรรมในห้วงอวกาศภายนอก (Code of Conduct for Outer Space Activities) ซึ่งร่างขึ้นมาโดยสหภาพยุโรปในปี ค.ศ.2008 และได้รับการรับรองจากหลายประเทศ รวมถึงประเทศนอกสหภาพยุโรปด้วย เช่น สหรัฐอเมริกา และออสเตรเลีย ร่างแนวปฏิบัติเกี่ยวกับกิจกรรมในห้วงอวกาศภายนอกนี้ต่อมาได้รับการพัฒนาเป็นแนวปฏิบัติระหว่างประเทศเกี่ยวกับกิจกรรมในห้วงอวกาศภายนอก (International Code of Conduct for Outer Space Activities: ICOC)

ปัญหาที่ตามมาจากแนวปฏิบัตินี้คือหลายรัฐเห็นว่าการจะสร้างความโปร่งใสในการตรวจสอบกิจกรรมที่เกิดขึ้นในห้วงอวกาศภายนอกของรัฐภาคีนั้นยังเป็นเรื่องที่ยาก เพราะจะต้องเผชิญกับปัญหาหลายประการ เช่น ความสามารถในการใช้ประโยชน์จากอวกาศของแต่ละรัฐไม่เท่ากัน แต่การใช้ประโยชน์จากอวกาศอยู่บนพื้นฐานที่ทุกรัฐสามารถใช้ประโยชน์ได้อย่างเสรีเท่ากัน การสร้างกฎหมายภายในที่เป็นมาตรฐานเดียวกันและสอดคล้องต่อแนวปฏิบัติระหว่างประเทศดังกล่าวก็จะทำได้ยาก[834] โดยรัฐที่ไม่สามารถใช้ประโยชน์จากอวกาศได้ก็อาจสร้างกฎหมายที่เข้มงวดต่อการใช้ประโยชน์ในอวกาศ แต่รัฐที่สามารถใช้ประโยชน์จากห้วงอวกาศภายนอกได้มากกว่าก็อาจออกกฎหมายที่เอื้อประโยชน์ต่อรัฐตนมากกว่าในการใช้ประโยชน์จากอวกาศ

มาตรการสำคัญประการต่อมาที่ไม่ใช่แนวทางกฎหมายคือมาตรการในการแลกเปลี่ยนข้อมูลเกี่ยวกับการเฝ้าระวังสถานการณ์ในอวกาศตามกรอบของอนุสัญญาจดทะเบียนวัตถุที่ถูกส่งเข้าสู่อวกาศ ค.ศ.1975 ของสหประชาชาติ ซึ่งการแลกเปลี่ยนข้อมูลระหว่างรัฐที่มีกิจกรรมในห้วงอวกาศและรัฐอื่นๆ จะเป็นการเสริมสร้างมาตรการตรวจตราการปฏิบัติตามกฎหมาย โดยในปัจจุบันสหรัฐอเมริกาได้ร่วมกับฝรั่งเศส แคนาดาและออสเตรเลียลงนามในแถลงการณ์เพื่อความร่วมมือในการเฝ้าระวังสถานการณ์ในอวกาศ (Situational Awareness Partnership Statements of Principles)[835]

การใช้ประโยชน์จากอวกาศมักเกี่ยวข้องกับเรื่องการใช้คลื่นความถี่หรือสัญญาณในการสื่อสารเป็นสำคัญ การพิจารณาว่าการใช้การคุกคามต่อสันติภาพและบูรณภาพแห่งดินแดนหมายถึงกรณีใดบ้างจึงควรมีขอบเขตถึงเรื่องการขัดขวางสัญญาณโดเมนของเครือข่ายไซเบอร์ดังที่ปรากฏใน

[834] Ibid., p. 128.

[835] Ibid.

คู่มือทาลินน์ด้วย[836] นอกจากนั้น การใช้อุปกรณ์ในอวกาศที่จะถือได้ว่าเป็นการใช้กำลังทางอาวุธได้นั้นจะต้องเป็นกรณีที่เทียบได้กับสัดส่วนและผลกระทบที่เกิดจากการใช้อาวุธในกรณีปกติด้วย[837]

ขณะที่การป้องกันตัวของรัฐนั้นยังเป็นสิ่งที่ยอมรับตามกฎหมายระหว่างประเทศ ทุกรัฐจึงมีสิทธิในการป้องกันตนเองจากการใช้กำลังทางอวกาศได้ ปัญหาที่ยังคงเป็นข้อสงสัยในเชิงวิชาการคือแนวทางดังกล่าวนี้จะสามารถบังคับใช้กับองค์กรที่ไม่ใช่รัฐได้อย่างไร และปัญหาที่ยังไม่เกิดขึ้นในปัจจุบันคือหากมีการโจมตีทางอวกาศด้วยอาวุธจากอวกาศสู่พื้นโลกกฎหมายระหว่างประเทศที่มีอยู่จะเพียงพอต่อการบังคับใช้หรือไม่[838]

กฎหมายมนุษยธรรมระหว่างประเทศใช้ในกรณีที่เกิดการขัดกันทางอาวุธในสงครามบนพื้นโลก ซึ่งมีปัจจัยทางด้านภูมิศาสตร์เข้ามาเกี่ยวข้อง ปัญหาเกิดขึ้นว่าการใช้กำลังทางอวกาศจะถือว่าอยู่ในขอบเขตที่กฎหมายมนุษยธรรมระหว่างประเทศสามารถปรับใช้ได้หรือไม่ คำถามดังกล่าวสามารถตอบได้ว่าโดยหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศนั้นไม่ได้มีข้อจำกัดเรื่องปัจจัยทางภูมิศาสตร์ทางกายภาพแต่อย่างใด หากพิจารณาจากหลักการแยกแยะ หลักความได้สัดส่วน หลักความจำเป็นทางการทหาร รวมถึงหลักการกระทำที่ไม่ก่อให้เกิดความทุกข์ทรมานโดยไม่จำเป็น[839] หลักการเหล่านี้ให้ความสำคัญกับการสร้างความสมดุลสองประการคือความจำเป็นทางการทหารกับการปฏิบัติอย่างมีมนุษยธรรม สาระสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศจึงมีเน้นการควบคุมการกระทำและผลของการกระทำที่เกิดขึ้นมากกว่าการพิจารณาว่าการกระทำเกิดขึ้นที่ใด

สาระสำคัญตามข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 และข้อ 1 ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ.1977 ไม่ได้สร้างข้อจำกัดเรื่องพื้นที่ในการบังคับใช้กฎหมาย ดังสังเกตได้จากการกำหนดเงื่อนไขในการใช้บังคับกฎหมายว่ากฎหมายนี้ใช้บังคับกับกรณีการขัดกันทางอาวุธของอัครภาคีสองประเทศหรือมากกว่านั้นไม่ว่าสงครามนั้นจะมีการประกาศหรือไม่ ปัญหาว่าข้อ 49 ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ.1977 ที่มีการอ้างถึงสงครามที่เกิดขึ้นในพื้นดินหรือทะเล จะถือเป็นการจำกัดขอบเขตการบังคับใช้กฎหมายหรือไม่ หากพิจารณารายละเอียดของกฎหมายข้อนี้แล้วจะพบว่าข้อ 49 นี้มีเป้าหมายในการคุ้มครองผลที่เกิดขึ้นแก่พลเรือนหรือทรัพย์สินของพลเรือนที่อยู่บนแผ่นดินและทะเล นอกจากนั้น ในข้อ 35 (3) ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ.1977 ยังมีการกำหนดห้ามการ

---

[836] Michael N. Schmitt, eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, (Cambridge: Cambridge University Press, 2013), p.43.

[837] Duncan Blake, "The Law Applicable to Military Strategic Use of Outer Space," p. 131.

[838] Ibid., p. 132.

[839] Ibid., p. 133.

กระทำที่ก่อให้เกิดผลกระทบอย่างกว้างขวางต่อสิ่งแวดล้อมทางธรรมชาติ (โดยสอดคล้องกับ ENMOD convention) ข้อกฎหมายเหล่านี้จึงสอดคล้องไปในทิศทางเดียวกัน และแสดงให้เห็นว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่ได้ต้องการสร้างข้อจำกัดในการบังคับใช้กฎหมาย[840]

การคุ้มครองทรัพย์สินสิ่งของทางอวกาศกับทรัพย์สินสิ่งของในโลกจากการขัดกันทางอาวุธเป็นประเด็นหนึ่งที่สำคัญด้วยเหตุที่การคุ้มครองทรัพย์สินสิ่งของสองประเภทนี้มีความแตกต่างกัน โดยในการขัดกันทางอาวุธรูปแบบปกตินั้นย่อมจำแนกการคุ้มครองทรัพย์สินสิ่งของของพลเรือนได้ง่ายกว่า แต่การคุ้มครองทรัพย์สินสิ่งของในอวกาศจะต้องคำนึงถึงประเด็นเรื่องยานอวกาศลำใด สถานีอวกาศใด และดาวเทียมใด เป็นทรัพย์สิ่งของที่ใช้เพื่อพลเรือนหรือเพื่อการทหาร และจะถือว่านักบินอวกาศเป็นทหารหรือไม่ก็เป็นประเด็นที่จะต้องพิจารณาก่อนการโจมตีด้วย[841]

ประเด็นสำคัญในเรื่องการจำแนกทรัพย์สินสิ่งของทางการทหารและพลเรือนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นแก่พลเรือนนั้นเป็นไปตามข้อ 52 (2) และข้อ 57 (2) (a) (ii) ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ.1977 ซึ่งกำหนดให้เป้าหมายการโจมตีจะต้องจำกัดเฉพาะทรัพย์สิ่งของซึ่งโดยลักษณะ สถานที่ตั้ง และวัตถุประสงค์ หรือการใช้งานจะก่อให้เกิดประสิทธิผลในปฏิบัติการทางทหาร โดยทรัพย์สิ่งของในอวกาศนั้นมีปัญหาว่าจะจำแนกอย่างไรระหว่างสิ่งของที่ใช้เพื่อการทหารหรือใช้เพื่อพลเรือน หรือทรัพย์สิ่งของใดใช้เพื่อวัตถุประสงค์ทั้งสองทาง เป็นประเด็นที่ยากและท้าทายต่อการปรับใช้กฎหมาย อย่างไรก็ดี ตามหลักกฎหมายมนุษยธรรมระหว่างประเทศการโจมตีเป้าหมายทางการทหารก็ยังคงต้องคำนึงถึงผลกระทบที่อาจเกิดขึ้นกับพลเรือนด้วย การจะทำลายอวกาศยาน ดาวเทียม หรือสถานีอวกาศต่างๆ ก็จะต้องคำนึงถึงผลกระทบต่อพลเรือนที่อาจเกิดขึ้นก่อนการโจมตีด้วย

ตามคู่มือกฎการใช้กำลัง (Rules of Engagement Handbook) ซานเรโมของสถาบันกฎหมายมนุษยธรรมระหว่างประเทศ ภาคผนวก A คำแนะนำในการวางแผนและการพิจารณาของฝ่ายอำนวยการ อนุภาคผนวก 2 ข้อแนะนำสภาพแวดล้อม 2.5 การปฏิบัติการไซเบอร์สเปซ

มีการพิจารณาลักษณะของไซเบอร์สเปซว่าเป็นสภาพแวดล้อมที่แตกต่างจากสภาพแวดล้อมทางกายภาพทั่วไป มีลักษณะไม่อยู่ในอำนาจอธิปไตยของรัฐใดๆ และมีลักษณะของการเป็นสิ่งไม่เคลื่อนไหว (non-kinetic) ทำให้การพิจารณาลักษณะการกระทำที่เป็นปรปักษ์ยาก เช่นเดียวกับการ

---

[840] Duncan Blake, “The Law Applicable to Military Strategic Use of Outer Space,”, p. 133.

[841] Ibid.

พิจารณาเจตนาของการกระทำที่เป็นปรปักษ์ก็ยากเช่นกัน[842] ในข้อ b. มีข้อพิจารณาด้านกฎหมายเกี่ยวกับการร่างกฎการใช้กำลังในปฏิบัติการทางไซเบอร์สเปซ ว่าข้อกฎหมายที่เกี่ยวข้องในการร่างกฎการใช้กำลังได้แก่

1) ความแตกต่างของหลักการเรื่องปฏิบัติการทางระบบเครือข่ายคอมพิวเตอร์ซึ่งกำหนดไว้ในกฎหมายแพ่งและกฎหมายอาญาภายในของแต่ละประเทศ รวมถึงกฎหมายระหว่างประเทศและนโยบายแห่งชาติ นอกจากนั้นยังรวมถึงการพิจารณาผลกระทบที่เกิดขึ้นจากอนุสัญญาระหว่างประเทศที่เกี่ยวข้องกับการสื่อสาร

2) การพิจารณาลักษณะการกระทำที่เป็นปฏิปักษ์ของปฏิบัติการทางไซเบอร์ซึ่งแม้จะไม่มีลักษณะของการเคลื่อนไหว แต่ให้พิจารณาจากความรุนแรง ความเฉียบพลัน การมุ่งตรง และผลกระทบของปฏิบัติการ

โดยในกฎการใช้กำลังของปฏิบัติการทางไซเบอร์จะต้องพิจารณากฎดังต่อไปนี้

1) การปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ (หมวด 131)

2) การเชื่อมต่อกับระบบสื่อสารผ่านดาวเทียม (หมวด 140)

3) การทำลายหรือทำให้ดาวเทียมหมดสภาพ (หมวด 141)

ในขณะที่ปฏิบัติการทางด้านสารสนเทศ (Information Operations) หมายถึง การผสานการใช้ขีดความสามารถหลักด้านสงครามอิเล็กทรอนิกส์ การปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ การปฏิบัติการจิตวิทยา การลวง และการรักษาความปลอดภัยในการปฏิบัติการทางทหาร โดยสอดคล้องกับขีดความสามารถ การสนับสนุนเฉพาะ และความสามารถอื่นๆ ที่เกี่ยวข้อง เพื่อที่จะโน้มน้าว ทำให้สับสน ฉ้อฉล หรือการแย่งชิงคนและการตัดสินใจอัตโนมัติของฝ่ายตรงข้าม ขณะที่ป้องกันฝ่ายตนเองด้วย (IO)[843]

การแสดงเจตนาอันเป็นปรปักษ์ ได้แก่[844]

1) การเล็งหรือชี้อาวุธ

2) การตั้งท่าลักษณะเข้าโจมตี

---

[842] San Remo Manual on International Law Applicable to Armed Conflicts at Sea 1995, Sub-Appendix 2, art 2.5 (a) [online] Accessed: April 10, 2020. Available from: https://www.icrc.org/en/doc/resources/documents/article/other/57jmsu.htm

[843] Ibid., Art. 69.

[844] San Remo Manual on International Law Applicable to Armed Conflicts at Sea 1995, Sub-Appendix 4, and Appendix a.

3) การเข้ามาใกล้ในพิสัยปล่อยอาวุธ

4) การชี้ด้วยเครื่องกำหนด เช่น เรดาร์หรือเลเซอร์

5) การส่งข้อมูลการกำหนดเป้าหมาย

6) การวางหรือเตรียมที่จะวางทุ่นระเบิดเรือ

7) การไม่ตอบสนองต่อมาตรการดังต่อไปนี้[845] เมื่อมีการสอบถามด้วยวาจา เมื่อมีการเตือนด้วยวาจา เมื่อมีทัศนสัญญาณ เมื่อมีสัญญาณเสียง เมื่อมีฉากขัดขวางกายภาพ เมื่อมีการเปลี่ยนเส้นทางและความเร็วเพื่อพิจารณาว่ายังคงตั้งท่าลักษณะเข้าโจมตีหรือไม่ เมื่อชี้เป้าด้วยเรดาร์ควบคุมการยิง หรือเมื่อการยิงเตือน

สนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศรวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ.1967 มีเจตนารมณ์เพื่อให้การใช้ประโยชน์จากอวกาศและดาวเทียมเป็นไปเพื่อวัตถุประสงค์เชิงสันติ แม้สนธิสัญญานี้จะไม่เกี่ยวข้องโดยตรงกับการขัดกันทางอาวุธและไม่เกี่ยวข้องกับกฎหมายมนุษยธรรมระหว่างประเทศเนื่องจากการบังคับใช้สนธิสัญญาฉบับนี้จะมีผลต่อการป้องกันการกระทำที่จะเป็นการคุกคามต่อสันติภาพตามกฎบัตรสหประชาชาติ (Jus ad Bellum) เป็นสำคัญ แต่การควบคุมกิจกรรมทางอวกาศนี้มีผลเกี่ยวเนื่องไปถึงการจำกัดการใช้งานดาวเทียมในอวกาศในสถานการณ์การขัดกันทางอาวุธด้วย สนธิสัญญาฉบับนี้จึงเป็นส่วนเพิ่มเติมทำให้การใช้เทคโนโลยีอาวุธอวกาศในการขัดกันทางอาวุธย่อมเป็นไปได้ยากขึ้น เพราะหากมีการเตรียมการก่อนการขัดกันทางอาวุธย่อมขัดกับสนธิสัญญาว่าด้วยหลักการเกี่ยวกับกิจกรรมของรัฐในการสำรวจและใช้ประโยชน์จากอวกาศรวมทั้งดวงจันทร์และเทหฟากฟ้าอื่น ค.ศ.1967 หากสามารถจำกัดกิจกรรมที่จะนำไปสู่การคุกคามระหว่างประเทศได้ก็ย่อมไม่มีการใช้อาวุธในสงครามและจะไม่นำไปสู่การกระทำที่ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศ

3.4.3 กฎหมายระหว่างประเทศเกี่ยวกับการห้ามส่งออกสินค้าที่ใช้ได้สองทาง

กฎหมายระหว่างประเทศเกี่ยวกับเรื่องการห้ามส่งออกสินค้าที่ใช้ได้สองทางเป็นมาตรการตามอนุสัญญาระหว่างประเทศว่าด้วยการห้ามใช้อาวุธตามแบบบางชนิด ค.ศ. 1980 (1980 Convention on Certain Conventional Weapons) ที่มุ่งจำกัดการแพร่กระจายอาวุธที่มีอานุภาพทำลายล้างสูงซึ่งสหภาพยุโรปได้ออกกฎระเบียบว่าด้วยการส่งออก นายหน้า การให้ความช่วยเหลือทางเทคนิค การผ่านแดนและการขนส่งสินค้าที่สามารถใช้ได้สองทาง (Council Regulation No

[845] Ibid., Sub-Appendix 4, and Appendix a.

428/2009 แก้ไขใหม่ปี ค.ศ.2021/821) มีจุดมุ่งหมายในการควบคุมการส่งออกและการข้ามแดนของสินค้ารวมตลอดถึงโปรแกรมคอมพิวเตอร์ที่อาจนำไปใช้ในการผลิตอาวุธที่มีอานุภาพทำลายล้างสูง

กฎระเบียบของสหภาพยุโรปดังกล่าวมีผลอย่างมากต่อการค้าระหว่างประเทศ หากจะมีการนำเข้าสินค้าไปยังสหภาพยุโรปก็จะมีการตรวจสอบแหล่งที่มาว่าประเทศส่งออกนั้นมีการปฏิบัติที่สอดคล้องกับกฎระเบียบการส่งออกสินค้าของสหภาพยุโรปหรือไม่ ในขณะที่การส่งออกสินค้าจากประเทศสมาชิกสหภาพยุโรปจะต้องปฏิบัติตามกฎระเบียบดังกล่าวนี้ด้วย แม้กฎระเบียบการควบคุมการส่งออกสินค้าที่อาจใช้ได้สองทางนี้ไม่มีเป้าหมายในการควบคุมการใช้อาวุธในการขัดกันทางอาวุธ เนื่องจากมาตรการควบคุมอาวุธที่มีอานุภาพทำลายล้างสูงที่เกี่ยวข้องกับการส่งออก นายหน้า การให้ความช่วยเหลือทางเทคนิค การผ่านแดนและการขนส่งสินค้าเป็นมาตรการควบคุมอาวุธในกรอบของการลดอาวุธหรือการปลดอาวุธ (Disarmament) ซึ่งอยู่นอกสถานการณ์การขัดกันทางอาวุธ แต่ก็ปฏิเสธไม่ได้ว่ากรอบการลดอาวุธหรือการปลดอาวุธนี้ย่อมส่งผลกระทบต่อการใช้อาวุธในการขัดกันทางอาวุธด้วยในลักษณะการป้องกันไม่ให้มีการถ่ายโอนหรือซื้อขายเทคโนโลยีที่อาจนำไปใช้เป็นวิธีการหรือปัจจัยในการขัดกันทางอาวุธอีกทั้งยังเป็นการป้องกันการนำเทคโนโลยีไปใช้เพื่อการก่อการร้ายได้ มาตรการควบคุมสินค้าที่อาจนำไปใช้ได้สองทางนี้จึงเป็นส่วนเพิ่มเติมการควบคุมสินค้าที่เกี่ยวข้องกับเทคโนโลยีใหม่ไม่ว่าจะเป็นการควบคุมวัสดุที่อาจนำไปใช้ผลิตอาวุธที่มีอานุภาพทำลายล้างสูงได้ การควบคุมอากาศยานไร้คนขับที่อาจนำไปใช้ทางการทหารและรวมถึงการควบคุมโปรแกรมคอมพิวเตอร์ที่อาจนำไปสู่การผลิตอาวุธที่มีอานุภาพทำลายล้างสูงได้

ส่วนที่อาจเป็นช่องว่างสำหรับการนำหลักการควบคุมการส่งออกสินค้าที่อาจนำไปผลิตอาวุธที่มีอานุภาพทำลายล้างสูงนั้นคือขอบเขตของการควบคุมสินค้าที่ใช้ได้สองทางเป็นไปเพื่อควบคุมสิ่งที่เกี่ยวข้องกับอาวุธนิวเคลียร์ อาวุธเคมีและอาวุธชีวภาพ แต่ขอบเขตของเทคโนโลยีใหม่ที่ใช้ในการขัดกันทางอาวุธกว้างขวางกว่านั้นมาก เช่นเทคโนโลยีไซเบอร์ที่ไม่เกี่ยวข้องกับการนำไปผลิตอาวุธที่มีอานุภาพทำลายล้างสูงแต่สามารถใช้ในการโจมตีทางไซเบอร์ได้ย่อมไม่อยู่ในขอบเขตการควบคุมสินค้าที่ใช้ได้สองทาง โปรแกรมคอมพิวเตอร์ที่ใช้เพื่อการประมวลผลร่วมกับระบบปัญญาประดิษฐ์ไม่อยู่ในขอบเขตของสิ่งที่นำไปผลิตอาวุธที่มีอานุภาพทำลายล้างสูงแต่สามารถนำไปใช้กับระบบอาวุธอิสระได้เป็นต้น

จากการศึกษาวิเคราะห์ในบทที่ 3 พบว่าหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมีการวางข้อกำหนดไว้เป็นการทั่วไปโดยไม่มีลักษณะเป็นข้อกฎหมายเฉพาะเรื่องในการควบคุมการกระทำในการขัดกันทางอาวุธ หลักเกณฑ์ส่วนใหญ่จึงไม่มีลักษณะเป็นการควบคุมอาวุธ

เฉพาะอย่างแต่เป็นหลักการทั่วไปที่สามารถนำไปปรับใช้ได้กับทั้งการใช้อาวุธและการใช้วิธีการในการรบ โดยพื้นฐานหลักการเหล่านี้จึงมีความยืดหยุ่นในระดับหนึ่งต่อการนำมาปรับใช้กับเทคโนโลยีใหม่ในการขัดกันทางอาวุธ นอกจากนั้น การพิจารณาคดีของศาลระหว่างประเทศหลายคดีและความเห็นของนักวิชาการในสังคมระหว่างประเทศยังมีบทบาทประการสำคัญในการสะท้อนให้เห็นพัฒนาการและความสามารถในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศในสถานการณ์ที่เปลี่ยนแปลงไปได้ในระดับหนึ่ง

อย่างไรก็ดี กฎหมายมนุษยธรรมระหว่างประเทศมีบทบาทในการควบคุมการกระทำในการขัดกันทางอาวุธ การควบคุมดังกล่าวหมายถึงการห้ามการกระทำการในบางลักษณะที่จะเป็นการละเมิดต่อบุคคลและทรัพย์สินที่กฎหมายมุ่งคุ้มครองแต่กฎหมายมนุษยธรรมระหว่างประเทศไม่ได้มุ่งควบคุมสิ่งที่จะนำมาใช้ในการขัดกันทางอาวุธเฉพาะอย่าง การควบคุมอาวุธเฉพาะอย่างนั้นอยู่ในกรอบของกฎหมายว่าด้วยการลดอาวุธ (Disarmament) ซึ่งว่าด้วยการลดอาวุธนี้ไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศในตัวเองแต่เป็นกฎหมายที่เสริมให้อาวุธบางลักษณะเป็นสิ่งต้องห้ามตามกฎหมายเฉพาะแม้จะยังไม่มีการนำมาใช้ในการขัดกันทางอาวุธ ปัญหาจึงมีว่าหากให้กฎหมายมนุษยธรรมระหว่างประเทศเพียงลำพังกับเทคโนโลยีใหม่อาจไม่เพียงพอในบางกรณีที่เทคโนโลยีดังกล่าวไม่ใช่อาวุธโดยสภาพแต่สามารถนำไปใช้งานเยี่ยงอาวุธและอาจก่อให้เกิดความเสียหายที่ไม่สามารถคาดการณ์ได้

บทที่ 4

ข้อท้าทายและแนวทางของกฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ

ข้อท้าทายของเทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายมนุษยธรรมระหว่างประเทศ คือความไม่เพียงพอของกฎหมายมนุษยธรรมระหว่างประเทศในบางกรณีที่จะปรับใช้กับสถานการณ์ที่เปลี่ยนแปลงไป โดยข้อท้าทายปรากฏในปัจจุบัน ได้แก่

1) ข้อท้าทายต่อการพิจารณาการใช้เทคโนโลยีไซเบอร์เพื่อเกิดการขัดกันทางอาวุธที่ปัจจุบันเป็นการใช้ทฤษฎีสัดส่วนความรุนแรงและผลกระทบ (Scale and Effect) ซึ่งเป็นข้อเสนอของ Schmitt ผู้เชี่ยวชาญด้านกฎหมายมนุษยธรรมระหว่างประเทศ[846] โดยยังมีข้อโต้แย้งในทางวิชาการอยู่หลายประการและไม่แน่ชัดว่าในการปรับใช้ทฤษฎีดังกล่าวกับข้อเท็จจริงจะสามารถแก้ไขปัญหาได้อย่างเหมาะสมหรือไม่ เนื่องจากยังไม่มีตัวอย่างการพิจารณาคดีของศาลยุติธรรมระหว่างประเทศจากกรณีการโจมตีทางไซเบอร์ปรากฏ

2) ข้อท้าทายต่อหลักการแยกแยะในกฎหมายมนุษยธรรมระหว่างประเทศซึ่งมีวัตถุประสงค์ในการคุ้มครองพลเรือน ทรัพย์สิ่งของพลเรือนและผู้ที่ไม่มีส่วนเกี่ยวข้องในการรบ เนื่องจากการใช้เทคโนโลยีใหม่หลายชนิด เช่น เทคโนโลยีไซเบอร์ เทคโนโลยีอากาศยานไร้คนขับ และเทคโนโลยีที่เกี่ยวข้องกับปัญญาประดิษฐ์มักอยู่บนสภาพแวดล้อมที่พลเรือนและทหารใช้งานร่วมกัน[847] โดยเฉพาะอย่างยิ่งพื้นที่ทางดิจิทัลของเทคโนโลยีไซเบอร์ที่สถานการณ์การโจมตีทางไซเบอร์นั้นมักไม่มีการแยกแยะเป้าหมายการโจมตีอย่างชัดเจน[848]

3) ข้อท้าทายต่อหลักความได้สัดส่วนทั้งจากการใช้เทคโนโลยีไซเบอร์เพื่อการโจมตี การใช้อากาศยานไร้คนขับและการใช้เทคโนโลยีระบบอาวุธอิสระ ซึ่งปรากฏว่าในการโจมตีทางไซเบอร์หลายกรณีก่อให้เกิดผลกระทบที่หลากหลาย ขณะที่บางกรณีไม่สามารถคาดการณ์ได้ว่าผลที่เกิดขึ้นจะได้สัดส่วนต่อความจำเป็นทางการทหารหรือไม่

---

[846] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, p. 43.

[847] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018, p. 96.

[848] Ibid., p.86.

4) ข้อท้าทายต่อหลักความระมัดระวังล่วงหน้าในการโจมตีซึ่งในปฏิบัติการทางทหารแต่ละครั้งจะต้องมีการเลือกวิธีการที่ก่อให้เกิดความเสียหายต่อพลเรือนและเป้าหมายที่ได้รับความคุ้มครองตามกฎหมายอย่างน้อยที่สุด แต่ในการโจมตีทางไซเบอร์ซึ่งอาจเกิดผลระทบที่หลากหลายนั้น ควรจะเลือกวิธีการอย่างไรจึงจะสอดคล้องต่อความระมัดระวังล่วงหน้า หรือในกรณีการใช้ระบบอาวุธอิสระซึ่งมีส่วนประกอบของการทำงานปัญญาประดิษฐ์ก็มีปัญหาว่าในกรณีที่ระบบอาวุธอิสระจะต้องตัดสินใจโจมตีโดยอยู่นอกเหนือจากข้อมูลพื้นฐานที่ผู้ออกแบบบันทึกข้อมูลไว้ จะคาดการณ์ได้เพียงใดว่าการปฏิบัติการนั้นจะยังคงสอดคล้องต่อหลักความระมัดระวังล่วงหน้าในการโจมตี เป็นต้น

ลักษณะการใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธที่สร้างข้อท้าทายหลายประการเป็นผลมากจากพื้นฐานของเทคโนโลยีซึ่งเป็นการนำเอาสิ่งที่ไม่ใช่อาวุธมาใช้ประโยชน์ในการขัดกันทางอาวุธทำให้เกิดลักษณะบางประการที่นำไปสู่ข้อพิจารณาต่างๆ ในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ อันได้แก่ 1) ลักษณะของความเป็นสิ่งของที่ใช้ได้สองทาง (Dual-use) คือใช้ได้ทั้งทางเพื่อวัตถุประสงค์พลเรือนและวัตถุประสงค์ทางการทหาร 2) ปัญหาการพิสูจน์ความสัมพันธ์ระหว่างผู้ใช้เทคโนโลยีกับผลที่เกิดขึ้นซึ่งในบางกรณีสร้างลักษณะความเป็นนิรนาม (Anonymity) คือตรวจสอบตัวตนของผู้ใช้งานได้ยาก[849] 3) เทคโนโลยีทำหน้าที่เป็นสื่อกลางหรือพาหะที่แสดงบทบาทของตัวเองได้ โดยเทคโนโลยีทำหน้าที่ระหว่างมนุษย์ผู้ใช้งานกับอาวุธหรือวิธีการโจมตีซึ่งอาจคาดหมายได้หรือคาดหมายไม่ได้ว่าจะเกิดผลเช่นไร และ 4) เทคโนโลยีที่มีพื้นฐานการทำงานแบบดิจิทัลมีองค์ประกอบของการทำงานที่ไม่แสดงผลทางกายภาพซึ่งนำไปสู่ปัญหาการพิจารณาลักษณะการปฏิบัติการและผลที่อาจเกิดขึ้นจากปฏิบัติการ

ความซ้อนทับกันของพื้นที่การใช้งานเทคโนโลยีระหว่างทหารและพลเรือนก่อให้เกิดประเด็นพิจารณาหลายประการทั้งข้อพิจารณาหลักการแยกแยะเป้าหมายในการโจมตีตามกฎหมายมนุษยธรรมระหว่างประเทศ ข้อพิจารณาต่อความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนโจมตี ขณะที่การพิสูจน์ความสัมพันธ์ระหว่างผู้ใช้เทคโนโลยีกับผลที่เกิดขึ้นจากการใช้งานเทคโนโลยีซึ่งทำได้ยากก็นำมาสู่ข้อพิจารณาความได้สัดส่วนในการโจมตีและการตอบโต้ ลักษณะความเป็นสื่อกลางหรือพาหะที่แสดงบทบาทได้ด้วยตัวเองของเทคโนโลยีก่อให้เกิดข้อพิจารณาต่อการปรับใช้หลักความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตี และพื้นฐานของการที่เทคโนโลยีหลายชนิดทำงานในระบบดิจิทัลที่มีปฏิบัติการบางส่วนไม่แสดงผลทางกายภาพก่อให้เกิด

---

[849] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018, p. 96.

ข้อพิจารณาทั้งต่อหลักการกำลังที่จะนำไปสู่การขัดกันทางอาวุธ ข้อพิจารณาการปฏิบัติการทางดิจิทัลที่เทียบเท่ากับการโจมตี ข้อพิจารณาต่อหลักความได้สัดส่วนในการโจมตีและข้อพิจารณาต่อหลักความระมัดระวังล่วงหน้าก่อนการโจมตี

การใช้งานเทคโนโลยีของทหารและพลเรือนมีทั้งเรื่องเชิงกายภาพ ในกรณีที่อุปกรณ์เดียวกันอาจใช้งานได้ทั้งทางทหารและพลเรือน เช่น อากาศยานไร้คนขับ อุปกรณ์เกี่ยวกับคอมพิวเตอร์ที่ใช้งานเพื่อปฏิบัติการทางไซเบอร์ ระบบการสื่อสารที่เกี่ยวข้องกับการกำหนดตำแหน่งบนพื้นโลก (GPS) ระบบเรดาร์ ฯลฯ ขณะที่เทคโนโลยีบางลักษณะเป็นสิ่งที่ไม่มีสถานะทางกายภาพแต่เป็นความรู้ ซอฟท์แวร์หรือโปรแกรมทางคอมพิวเตอร์ ระบบการทำงานของอุปกรณ์ เช่น การประมวลผลแบบอัลกอริทึ่ม การทำงานของปัญญาประดิษฐ์ สัญญาณที่เกี่ยวข้องกับการกำหนดตำแหน่งบนพื้นโลก (GPS) พื้นที่ทางไซเบอร์ซึ่งเกี่ยวข้องกับการทำงานเชื่อมต่อกันของคอมพิวเตอร์กับคอมพิวเตอร์และอุปกรณ์ต่างๆ[850] เป็นต้น

ลักษณะการใช้งานเทคโนโลยีดังกล่าวเป็นสิ่งที่แตกต่างจากการใช้งานอาวุธและวิธีการในการขัดกันทางอาวุธทางการทหารที่มีมาในอดีตซึ่งมักเน้นการสร้างอาวุธในการทำลายฝ่ายตรงข้ามในสงครามให้ได้มากที่สุดและจะนำไปสู่ความได้เปรียบในการชนะสงครามของฝ่ายตนเอง การใช้งานเทคโนโลยีใหม่ในสงครามปัจจุบันแม้จะมีเป้าหมายในการสร้างความได้เปรียบทางการทหารโดยการทำลายขีดความสามารถของกองทัพฝ่ายตรงข้ามเช่นเดียวกับการทำสงครามในอดีตแต่มีความเปลี่ยนแปลงลักษณะการใช้งานอาวุธที่เน้นการทำลายได้มากเป็นอาวุธที่ทำลายได้อย่างแม่นยำโดยมีการพัฒนาเอาองค์ความรู้ทางวิทยาศาสตร์และพัฒนาการทางเทคโนโลยีในโลกยุคปัจจุบันเข้าไปประกอบรวมกับการใช้อาวุธมากขึ้น[851] ทำให้เทคโนโลยีใหม่ที่มีการนำมาใช้ในการขัดกันทางอาวุธนี้มี 2 ลักษณะพร้อมกันคือ 1) การใช้งานตามปกติเทคโนโลยีดังกล่าวจะเป็นประโยชน์ต่อการดำรงชีวิต 2) การใช้งานเพื่อก่อให้เกิดความเสียหายเทคโนโลยีดังกล่าวจะเป็นโทษอย่างมาก การนำกฎหมายมาปรับใช้ต่อเทคโนโลยีจึงต้องพิจารณาจากลักษณะการใช้งาน การมุ่งจำกัดที่ตัวเทคโนโลยีโดยตรงอาจเกิดขึ้นได้แต่เฉพาะกรณีที่เทคโนโลยีนั้นถูกพัฒนาและสร้างขึ้นมาโดยมีวัตถุประสงค์เพื่อการก่อความเสียหายเท่านั้น

---

[850] Robert S. Gutzwiller, Sunny Fugate, Benjamin D. Sawyer, and P. A. Hancock, "The Human Factors of Cyber Network Defense," Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting – 2015, p. 322.

[851] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, (2019), p. 26.

อย่างไรก็ดี ตามกฎหมายมนุษยธรรมระหว่างประเทศไม่ว่าจะเป็นอนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติม รวมตลอดถึงหลักเกณฑ์ของกรุงเฮกและกฎหมายระหว่างประเทศที่เกี่ยวข้องกับอาวุธ ยังสามารถนำมาปรับใช้กับเทคโนโลยีใหม่ได้หลายประเภท โดยปัจจัยสำคัญที่จะทำให้กฎหมายมนุษยธรรมระหว่างประเทศซึ่งสร้างมาอย่างยาวนานแล้วมีผลครอบคลุมถึงเทคโนโลยีใหม่ได้คือ 1) การพิจารณาลักษณะการใช้งานเทคโนโลยีดังกล่าวว่าเป็นปัจจัยหรือเป็นวิธีการในการขัดกันทางอาวุธหรือไม่ อย่างไร เนื่องจากลักษณะสำคัญของเทคโนโลยีใหม่อยู่ที่การใช้งานค่อนข้างมาก 2) การใช้งานเทคโนโลยีใหม่ในฐานะเป็นปัจจัยหรือวิธีการในการขัดกันทางอาวุธนั้นสอดคล้องกับกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ อย่างไร ทั้งนี้จะต้องไม่จำแนกตั้งแต่ตอนต้นว่าเทคโนโลยีใหม่เป็นสิ่งต้องห้ามในการขัดกันทางอาวุธทุกกรณี เนื่องจากบางกรณีการใช้งานเทคโนโลยีใหม่อาจเป็นไปเพื่อการป้องกันประเทศหรือการคุ้มครองทางมนุษยธรรมได้ ดังนั้นจึงต้องแยกระหว่างการใช้งานเทคโนโลยีใหม่โดยชอบด้วยกฎหมายกับการห้ามการใช้งานที่ก่อให้เกิดการละเมิดต่อหลักกฎหมายมนุษยธรรมระหว่างประเทศ

ทั้งนี้ในประเด็นปลีกย่อยเช่นการปรับใช้หลักการกระทำที่เป็นปฏิปักษ์ (Conduct of Hostilities) อันได้แก่ การสร้างลักษณะการขัดกันทางอาวุธของเทคโนโลยีใหม่เป็นไปได้เพียงใด ข้อท้าทายของเทคโนโลยีใหม่ต่อหลักการแยกแยะเป้าหมาย หลักความได้สัดส่วน และหลักความระมัดระวังล่วงหน้าก่อนการโจมตี รวมตลอดถึงข้อท้าทายที่จะเกิดขึ้นจากลักษณะเฉพาะบางประการของเทคโนโลยีบางลักษณะ ซึ่งอาจนำไปสู่แนวทางในการพัฒนากฎหมายมนุษยธรรมระหว่างประเทศนั้น จะได้มีการอธิบายในเนื้อหาบทที่ 4 ดังต่อไปนี้

4.1 ข้อท้าทายเกี่ยวกับการเกิดการขัดกันทางอาวุธ

กฎหมายมนุษยธรรมระหว่างประเทศจะมีผลบังคับเมื่อเกิดการขัดกันทางอาวุธ จึงนำไปสู่ข้อพิจารณาว่าเทคโนโลยีใหม่ซึ่งถูกนำมาใช้เป็นอาวุธ ปัจจัยหรือวิธีการในการขัดกันทางอาวุธนั้นจะก่อให้เกิดปัญหาทางกฎหมายอย่างไรและมีกรณีใดหรือไม่ที่อาจนำไปสู่ความไม่เพียงพอของกฎหมายระหว่างประเทศในการปรับใช้กับเทคโนโลยีบางชนิดเนื่องจากลักษณะการทำงานที่เปลี่ยนแปลงไป จากการวิเคราะห์การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธในบทที่ 3 มีบางกรณีที่กฎหมายมนุษยธรรมระหว่างประเทศอาจไม่เพียงพอต่อการปรับใช้ในบางกรณีดังต่อไปนี้

4.1.1 ข้อท้าทายเกี่ยวกับการใช้เทคโนโลยีใหม่กับการเกิดการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ

ข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ทั้ง 4 ฉบับมีใจความสำคัญว่า "...Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.

The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."[852]

ประเด็นสำคัญสำหรับการพิจารณาการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธจึงอยู่ที่ 2 เรื่องคือ เทคโนโลยีใหม่จะทำให้เกิดการขัดกันทางอาวุธได้อย่างไรและเทคโนโลยีใหม่จะสามารถนำมาใช้ในการยึดครองดินแดนได้หรือไม่ โดยจากการศึกษาวิจัยพบว่าเทคโนโลยีไซเบอร์จะก่อให้เกิดปัญหาและข้อท้าทายเกี่ยวกับการเกิดการขัดกันทางอาวุธมากที่สุด เนื่องจากลักษณะของเทคโนโลยีไซเบอร์เกี่ยวข้องกับปฏิบัติการในพื้นที่อิเล็กทรอนิกส์เป็นสำคัญและอาจนำไปสู่ผลเสียหายทางกายภาพหรือผลเสียหายที่ไม่ใช่ทางกายภาพก็ได้ จึงน่าพิจารณาว่าการใช้ไซเบอร์เพื่อทำให้เกิดการขัดกันทางอาวุธจะเป็นไปได้เพียงไร โดยมีข้อพิจารณาดังต่อไปนี้

4.1.1.1 ปฏิบัติการทางไซเบอร์กับการเกิดการขัดกันทางอาวุธ

สาระสำคัญของการเกิดการขัดกันทางอาวุธคือจะต้องมีการใช้กำลังทางอาวุธเกิดขึ้น ปัญหาคือการกระทำในลักษณะใดจึงจะถือว่าเป็นการขัดกันทางอาวุธในกฎหมายระหว่างประเทศ การขัดกันทางอาวุธหมายความว่าจะต้องมีการใช้อาวุธต่อสู้กันใช่หรือไม่ ในกรณีนี้ อาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวีย (The International Criminal Tribunal for the Former Yugoslavia: ICTY) ในคดี Prosecutor v. Dusko Tadic ศาลอธิบายว่า "...an armed conflict exists whenever there is a resort to armed force between States..."[853] หรืออาจแปลได้ว่า

---

[852] Geneva Convention 1949, Common Article 2.

[853] The Prosecutor v. Dusko Tadic, The Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, The Appeal Chamber (ICTY) 2 October 1995 para.70.

การขัดกันทางอาวุธมีอยู่เมื่อใดก็ตามที่มีการใช้กำลังทางทหารระหว่างรัฐ ข้อความดังกล่าวย่อมอนุมานได้ว่าการใช้กำลังทางทหารในกรณีปกติย่อมดำเนินไปพร้อมกับวิธีการในการต่อสู้และการใช้อาวุธ การใช้ปฏิบัติการทางไซเบอร์ที่มีลักษณะเป็นการใช้กำลังทางทหารระหว่างรัฐก็ย่อมเป็นการขัดกันทางอาวุธได้ ในขณะที่ปฏิบัติการทางไซเบอร์ซึ่งกระทำในนามของรัฐหรือเป็นไปตามเงื่อนไขของกฎหมายมนุษยธรรมระหว่างประเทศในขณะที่เกิดการขัดกันทางอาวุธกรณีปกติ ย่อมถือว่าเป็นการกระทำที่อยู่ในขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศเช่นกัน

ปัญหาประการสำคัญจึงเกิดขึ้นว่าการใช้ไซเบอร์เพื่อการโจมตีนั้นจะถือเป็นการใช้กำลังทางทหารระหว่างรัฐได้หรือไม่ การพิจารณาปัญหาดังกล่าวจะต้องคำนึงถึงองค์ประกอบ 2 ประการ คือ 1) ปฏิบัติการทางไซเบอร์เพื่อการโจมตีนั้นเกิดขึ้นโดยเป็นปฏิบัติการของรัฐหรือไม่ และ 2) ปฏิบัติการทางไซเบอร์นั้นเทียบเท่ากับ “การใช้กำลังทางทหาร” อย่างไร

(ก) การปฏิบัติการของรัฐ

ปฏิบัติการใดเป็นปฏิบัติการของรัฐหรือไม่ย่อมต้องพิจารณาจากผู้ที่มีส่วนเกี่ยวข้องกับปฏิบัติการนั้นว่าเป็นการกระทำของรัฐหรือไม่ ซึ่งตามกฎหมายมนุษยธรรมระหว่างประเทศนั้นการกระทำดังกล่าวจะต้องเป็นการกระทำของทหารซึ่งสังกัดในกองทัพของรัฐหรือบุคลากรในลักษณะที่เป็นพลรบ แต่เนื่องด้วยลักษณะการทำงานของระบบไซเบอร์ซึ่งอยู่ในพื้นที่อิเล็กทรอนิกส์ที่พลเรือนและทหารต่างใช้ร่วมกัน ปัญหาของการใช้ปฏิบัติการทางไซเบอร์จึงเป็นเรื่องการพิสูจน์ว่าผู้ปฏิบัติการนั้นเป็นทหารของรัฐหรือเป็นพลเรือน[854] ในทางปฏิบัตินั้นอาจมีการพิสูจน์ต้นทางการปฏิบัติการในเครือข่ายไซเบอร์ได้ โดยพิสูจน์จาก IP address ของคอมพิวเตอร์เครื่องนั้นว่ามาจากที่ใด แต่ปัญหาก็จะเกิดขึ้นอีกว่า หากพลเรือนแอบเข้าไปใช้งานระบบคอมพิวเตอร์ทางทหารหรือทหารใช้คอมพิวเตอร์พลเรือนเพื่อปฏิบัติการโจมตี ผู้ใดหรือวิธีการใดจึงจะสามารถพิสูจน์ได้ว่าผู้ปฏิบัติการที่แท้จริงคือใคร[855] เป็นต้น

(ข) ปฏิบัติการทางไซเบอร์ที่เทียบเท่าปฏิบัติการทางทหาร

ปัญหาว่าการใช้กำลังทางทหารมีขอบเขตเพียงใด ศาลอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวียให้ความเห็นเพิ่มเติมว่า “Other cases also prove that private

---

[854] Mehmet Emin Erendor and Gurkan Tamer. “The New Face of The War: Cyber Warfare,” p. 65 - 67.

[855] International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts*, 32th International Conference of the Red Cross and Red Crescent, December 8-10, 2015. p. 44.

individuals acting within the framework of, or in connection with, armed forces, or in collusion with State authorities may be regarded as de facto State organs. In these cases it follows that the acts of such individuals are attributed to the State, as far as State responsibility is concerned, and may also generate individual criminal responsibility."[856] หรืออาจแปลความได้ว่านอกจากปฏิบัติการที่กระทำโดยทหารแล้ว ปัจเจกชนที่กระทำการภายในขอบเขตเกี่ยวกับกองกำลังทหารหรือสมรู้ร่วมคิดกับหน่วยงานของรัฐ อาจจัดว่าเป็นองค์กรของรัฐโดยพฤตินัยได้ ดังนั้นขอบเขตการกระทำที่ถือว่าเป็นการใช้กำลังทางทหารย่อมรวมถึงทั้งทหารและพลเรือนที่ทำหน้าที่แทนกองกำลังทางทหารด้วย[857]

การพิจารณาย้อนกลับไปสู่ปัญหาซึ่งเกิดขึ้นในองค์ประกอบที่ 1 ว่าจะตรวจสอบอย่างไรว่าการกระทำของพลเรือนนั้นเป็นการทำหน้าที่แทนกองกำลังทหารของรัฐ หากมีการปฏิเสธของรัฐว่าไม่เกี่ยวข้องกับปฏิบัติการของพลเรือนดังกล่าว หรือไม่สามารถหาหลักฐานพิสูจน์ถึงความสัมพันธ์ระหว่างปฏิบัติการของพลเรือนกับรัฐได้ การโจมตีทางไซเบอร์นั้นย่อมไม่ก่อให้เกิดลักษณะของการขัดกันทางอาวุธได้เช่นกัน เช่น กรณีการโจมตีทางไซเบอร์ซึ่งเกิดขึ้นที่เมืองทาลลินน์ ประเทศเอสโตเนีย พิสูจน์ได้เพียงว่าเป็นปฏิบัติการของกลุ่มแฮคเกอร์ที่ชาวรัสเซีย แต่ไม่สามารถเชื่อมโยงถึงการสั่งการหรือกระทำการแทนรัฐได้ จึงไม่อาจระบุได้ว่าเป็นการสร้างลักษณะการขัดกันทางอาวุธ คงเป็นได้เพียงการโจมตีทางไซเบอร์ปกติของพลเรือนเท่านั้น

คำอธิบายของคณะกรรมการกาชาดระหว่างประเทศให้ความสำคัญกับเงื่อนไขการใช้กำลังทางทหารในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ แต่ในคำพิพากษาศาลยุติธรรมระหว่างประเทศคดี Tadic มีความเห็นว่า "... legal conditions armed forces fighting in a prima facie internal armed conflict may be regarded as acting on behalf of a foreign Power and (ii) whether in the instant case the factual conditions which are required by law were satisfied."[858] หรือการใช้กำลังทางทหารนั้นถือเป็นเงื่อนไขสำคัญของทั้งการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศและการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ สิ่งที่แตกต่าง

---

[856] Prosecutor v. Dusko Tadic, (Appeal Judgement), Case it-94-1-A, 15 July 1999, para 144.

[857] อุบลวรรณ ภีระเป็ง, การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ: ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, (2558), หน้า 90.

[858] Prosecutor v. Dusko Tadic, (Appeal Judgement), Case it-94-1-A, 15 July 1999, para 81. คำพิพากษาคดี Tadic พิจารณาว่าการใช้กำลังทางทหารเป็นลักษณะโดยปกติของการขัดกันทางอาวุธทั้งที่มีลักษณะระหว่างประเทศและไม่มีลักษณะระหว่างประเทศ โดยการอ้างอิงถึงเหตุการณ์ที่เกิดขึ้นในบอลข่าน (Balkans)

กันคือในการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศนั้นจะไม่มีการพิจารณาถึงความรุนแรงของการขัดกันทางอาวุธ ในขณะที่การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะมีการพิจารณาเรื่องความรุนแรงของการขัดกันทางอาวุธประกอบด้วย ทั้งนี้ก็เนื่องมาจาก ลักษณะของการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศนั้นจะไม่ใช้กับกรณีความไม่สงบเรียบร้อยภายในประเทศ (Internal Disturbances) และความตึงเครียดภายในประเทศ (Internal Tensions) เช่น กรณีการประท้วงภายในประเทศ[859] เฉพาะการต่อสู้ที่รุนแรงเกินกว่าความไม่สงบเรียบร้อยภายในเท่านั้นจึงจะเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้

มุมมองของผู้เชี่ยวชาญซึ่งมีส่วนร่วมในการจัดทำคู่มือทาลลินน์ว่าด้วยกฎหมายระหว่างประเทศซึ่งปรับใช้สงครามทางไซเบอร์เห็นว่าการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธย่อมอยู่ในบังคับของกฎหมายมนุษยธรรมระหว่างประเทศโดยในข้อ 20 วรรค 1 ของคู่มือทาลลินน์กำหนดว่า “Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict”[860] หรือกฎหมายว่าด้วยการขัดกันทางอาวุธสามารถปรับใช้ได้กับปฏิบัติการทางไซเบอร์ซึ่งดำเนินอยู่ภายในบริบทการขัดกันทางอาวุธ โดยคำอธิบายหลักการดังกล่าวระบุว่า “...situation involving hostilities, including those conducted using cyber means.”[861] หรือในบริบทการขัดกันทางอาวุธนั้นหมายถึงการกระทำที่เป็นปฏิปักษ์รวมถึงการใช้ปฏิบัติการทางไซเบอร์ด้วย การกระทำที่เป็นปฏิปักษ์ตามกฎหมายมนุษยธรรมระหว่างประเทศจะเกิดขึ้นได้ก็แต่โดยเป็นการปฏิบัติการทางทหารที่ชอบธรรมเท่านั้น (legitimate military action)[862] ซึ่งหากพิจารณาจากข้อ 20 นี้แล้วจะพบว่าหลักการนี้เพียงยืนยันว่าปฏิบัติการทางไซเบอร์มีผลเสมือนเป็นวิธีหรือปัจจัยในการขัดกันทางอาวุธได้ หากทหารเป็นผู้ใช้ปฏิบัติการทางไซเบอร์ก็มีผลเท่ากับเป็นส่วนหนึ่งของการขัดกันทางอาวุธ

ในยุทธวิธีการรบมักจะต้องมีกระบวนการการสอดแนมและการลาดตระเวนเพื่อให้กองทหารทราบว่าศัตรูอยู่ตำแหน่งใดจึงจะสามารถทำการโจมตีหรือป้องกันตัวได้อย่างเหมาะสม

---

[859] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977. Art. 1 (2).

[860] Michael N. Schmitt eds., Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 20 Applicability of the Law of Armed Conflict

[861] Ibid.

[862] International Committee of the Red Cross, “International Law on the Conduct of Hostilities: Overview,” International Committee of the Red Cross (October 29, 2012) [online] accessed May 10, 2021. Available from: https://www.icrc.org/en/document/conduct-hostilities

ปัญหาว่าปฏิบัติการที่มีความรุนแรงในระดับใดจึงจะถือว่าเป็นปฏิบัติการทางทหาร ประเด็นนี้ Schmitt ให้ความเห็นว่าการจำกัดเฉพาะปฏิบัติการทางทหารที่มีระดับรุนแรงถึงขนาดเท่ากับการใช้อาวุธทำลายในการขัดกันทางอาวุธอาจเป็นแนวทางที่แคบเกินไปสำหรับการพิจารณารูปแบบปฏิบัติการทางทหารในปัจจุบัน ปฏิบัติการทางทหารจึงควรหมายรวมถึงการที่รัฐจะต้องกระทำโดยความจำเป็นเพื่อนำไปสู่การใช้กำลังทางทหารด้วย เช่น การสอดแนมและการลาดตระเวน เพื่อให้การพิจารณาเกณฑ์ของการใช้กำลังทางทหารมีความเหมาะสมต่อลักษณะการปฏิบัติที่เป็นอยู่ในปัจจุบันมากขึ้น[863]

สิ่งที่น่าสนใจคือผู้เชี่ยวชาญที่มีบทบาทสำคัญในการจัดทำคู่มือทาลลินน์ Schmitt เคยเขียนบทความเรื่องหนึ่งชื่อ “Wired Warfare: Computer Network Attack and Jus in Bello” ในบทความนี้ Schmitt มีความเห็นว่าเฉพาะกรณีการโจมตีทางไซเบอร์ที่ก่อให้เกิดผลทางกายภาพเท่านั้นจึงจะถือว่าเทียบเท่ากับปฏิบัติการทางทหารได้ โดยให้พิจารณาจากความเสียหายที่เกิดขึ้นซึ่งกระทบต่อชีวิต ร่างกาย หรือทรัพย์สิน (Scale and Effect)[864] แนวคิดนี้ของ Schmitt น่าจะมีผลไม่น้อยต่อการเขียนหลักการข้อ 20 ของคู่มือทาลลินน์ คือไม่ได้กำหนดให้ชัดเจนว่าปฏิบัติการทางไซเบอร์ที่เทียบเท่ากับปฏิบัติการทางทหารนี้จะนำไปสู่การเกิดการขัดกันทางอาวุธหรือไม่ เพราะผลที่เกิดจากปฏิบัติการทางไซเบอร์อาจมีได้ค่อนข้างหลากหลาย ในขณะที่ปฏิบัติการทางไซเบอร์โดยทหารซึ่งเกิดขึ้นขณะที่มีการขัดกันทางอาวุธสามารถยอมรับว่าเป็นส่วนหนึ่งในปฏิบัติการทางทหารได้ง่ายกว่า เพราะอย่างน้อยที่สุดปฏิบัติการทางไซเบอร์ย่อมเป็นวิธีการในการขัดกันทางอาวุธได้

โดยทั่วไปการใช้กำลังทางทหารนั้นค่อนข้างเป็นที่ยอมรับว่าหมายรวมถึงทั้งรูปแบบการใช้กำลังโดยตรงและการใช้รูปแบบอื่นทางอ้อม เช่น การสนับสนุนการใช้กำลังทางทหารด้วย[865] ดังนั้นการปฏิบัติการทางไซเบอร์ไม่ว่าโดยทางตรงหรือทางอ้อม หากเป็นผลให้เกิดความบาดเจ็บหรือการเสียชีวิต หรือก่อให้เกิดความเสียหายแก่ทรัพย์สินก็ย่อมเทียบเท่ากับการใช้กำลังทางทหาร ทั้งนี้ความเห็นของนักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศหลายคนค่อนข้างสอดคล้องกับแนวคิดของ Schmitt คือยอมรับการปฏิบัติการทางไซเบอร์ว่าจะเป็นการใช้กำลังทางทหารได้ต่อเมื่อความเสียหายที่เกิดขึ้นจะต้องมีลักษณะทางกายภาพด้วย มิเช่นนั้นย่อมจะเป็นการพิสูจน์ได้ยากว่าปฏิบัติการทางไซเบอร์ดังกล่าวส่งผลกระทบต่อบุคคลที่กฎหมายคุ้มครองอย่างไร[866]

---

[863] Michael N. Schmitt, “Wired Warfare: Computer Network Attack and Jus in Bello,”: 372.

[864] Ibid., p. 397.

[865] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 123.

[866] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 123.

ในคำอธิบาย (Commentary) อนุสัญญาเจนีวาของคณะกรรมการกาชาดระหว่างประเทศได้อธิบายข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 ว่า "...Armed conflicts...occur when one or more States have recourse to armed force against another State, regardless of the reasons for or the intensity of the confrontation."[867] หรือการขัดกันทางอาวุธเกิดขึ้นเมื่อรัฐตั้งแต่หนึ่งรัฐกำลังทางอาวุธต่อรัฐอื่นโดยคำนึงถึงความรุนแรงของการเผชิญหน้า จากข้อกฎหมายดังกล่าวย่อมสื่อความหมายในลักษณะว่าใช้กำลังทางทหารเป็นเงื่อนไขประการสำคัญของการขัดกันทางอาวุธ ซึ่งจะนำมาสู่ประเด็นพิจารณาเกี่ยวกับการขัดกันทางอาวุธในปัจจุบันได้แก่

ประเด็นที่ 1 การแยกแยะระหว่างการใช้กำลังทางทหารกับพลเรือนในปัจจุบันทำได้ยากขึ้น เนื่องจากทรัพยากรที่เกี่ยวข้องกับการใช้งานเทคโนโลยีนั้นสัมพันธ์กับทั้งการใช้งานของทหารและพลเรือน เช่น การโจมตีทางไซเบอร์ประเทศจอร์เจียซึ่งเกิดขึ้นในสถานการณ์การขัดกันทางอาวุธ โดยเหตุการณ์เกิดขึ้นในเดือนสิงหาคม ค.ศ.2008 เมื่อกลุ่มเซาท์ออสเซเทีย (South Ossetia) ต้องการแบ่งแยกดินแดนออกจากประเทศจอร์เจีย ความขัดแย้งมีมาอย่างยาวนานตั้งแต่ ค.ศ. 1991 ในความขัดแย้งดังกล่าวได้มีการตั้งกองกำลังรักษาสันติภาพขึ้นในปี ค.ศ.1992 โดยมติขององค์กรว่าด้วยความมั่นคงและความร่วมมือในยุโรป (OSCE) กองกำลังดังกล่าวประกอบด้วยกองกำลังรัสเซีย กองกำลังจอร์เจีย และกองกำลังเซาท์ออสเซเทีย[868]

ในวันที่ 20 กรกฎาคม ค.ศ.2008 มีการโจมตีทางไซเบอร์ต่อเว็บไซต์ของรัฐบาลจอร์เจียด้วยปฏิบัติการ DDoS ทำให้เว็ตไซต์ไม่สามารถทำงานได้ 24 ชั่วโมง[869] และการโจมตีทางไซเบอร์พร้อมการโจมตีด้วยกองกำลังทหารเกิดขึ้นอีกครั้งในวันที่ 8 สิงหาคม ค.ศ.2008 ในสถานการณ์ที่รัสเซียทำการโจมตีกองกำลังจอร์เจียเพื่อตอบโต้ปฏิบัติการโจมตีทางทหารของกองทัพจอร์เจียที่กระทำต่อเมือง Tskhinvali ในเขตพื้นที่เซาท์ออสเซเทียหนึ่งวันก่อนหน้า[870] ผลเสียหายจากการโจมตีทางไซเบอร์ดังกล่าวทำให้รัฐบาลจอร์เจียต้องใช้เวลาหลายวันในการแก้ไขให้เว็บไซต์ของรัฐบาลกลับมาใช้ได้เหมือนเดิม

[867] International Committee of the Red Cross, Commentary of the 1949 Geneva Convention, para 218.

[868] Kadri Kaska Eneken Tikk, Liis Vihul, International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Center of Exxellence Report (CCD COE) (2012): 68.

[869] Williams C. Ashmore, "Impact of Alleged Russian Cyber Attacks," Baltic Security and Defense Review, Vol. 11, (2009): 10.

[870] Ibid.

แม้ว่าเจ้าหน้าที่รัฐบาลจอร์เจียจะได้ทำการสอบสวนกรณีดังกล่าวและมีการกล่าวหารัฐบาลรัสเซียว่าอยู่เบื้องหลังการโจมตีทางไซเบอร์ แต่รัฐบาลรัสเซียก็ปฏิเสธว่าการกระทำดังกล่าวไม่ใช่ปฏิบัติการของกองทัพรัสเซียแต่เป็นไปได้ว่าจะเป็นปฏิบัติการของพลเรือนรัสเซียซึ่งอาจปฏิบัติการในประเทศรัสเซียหรือที่สถานที่อื่น[871] ขณะที่ผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์ยืนยันว่ากลุ่มปฏิบัติการโจมตีทางไซเบอร์ของรัสเซียนั้นรู้จักกันในชื่อกลุ่มเครือข่ายธุรกิจรัสเซีย (Russian Business Network) ซึ่งมีความเป็นไปได้สูงว่าจะเชื่อมโยงไปถึงรัฐบาลรัสเซีย[872]

ปรากฏการณ์ดังกล่าวชี้ให้เห็นว่าปฏิบัติการโจมตีทางไซเบอร์นั้นสร้างปัญหาต่อการแยกแยะปฏิบัติการทางทหารและการกระทำของพลเรือนอย่างมาก แม้จะพบว่ามีการโจมตีทางไซเบอร์ควบคู่ไปกับการขัดกันทางอาวุธตามแบบปกติ และสามารถเชื่อมโยงความสัมพันธ์ระหว่างปฏิบัติการทางไซเบอร์กับที่มาของปฏิบัติการนั้น แต่ก็ยังเป็นการยากที่จะระบุความชัดเจนของผู้กระทำการว่าเป็นทหารหรือพลเรือน ในขณะที่ผลเสียหายจากการโจมตีทางไซเบอร์นั้นปรากฏเด่นชัดว่าเป็นความเสียหายต่อสาธารณูปโภคด้านข้อมูลข่าวสาร (การเข้าถึงเว็บไซต์ของรัฐบาล) ซึ่งใช้ร่วมกันระหว่างทหารและพลเรือน และอาจเป็นการกระทำที่กระทบต่อพลเรือนมากกว่าความจำเป็นทางการทหารเสียด้วย ซึ่งอาจเป็นการละเมิดต่อข้อ 51 (5) (b) ของพิธีสารเพิ่มเติมฉบับที่ 1 ที่กำหนดว่าการโจมตีที่ไม่เลือกปฏิบัติหมายถึง "...an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[873] หรือการโจมตีซึ่งอาจคาดได้ว่าจะยังผลให้เกิดการสูญเสียชีวิตของพลเรือน การบาดเจ็บของพลเรือน ความเสียหายต่อทรัพย์สิ่งของพลเรือนหรือความเสียหายดังกล่าวรวมกัน ซึ่งทั้งนี้เป็นการสูญเสียที่มากเกินกว่าความได้เปรียบทางการทหารที่มีลักษณะเป็นรูปธรรมและโดยตรงอันคาดหมายได้

การใช้งานเว็บไซต์ที่ทุกคนสามารถเข้าถึงข้อมูลข่าวสารได้มีความสัมพันธ์กับปฏิบัติการทางทหารน้อยมาก ในขณะที่การโจมตีข้อมูลข่าวสารที่จะส่งผลต่อปฏิบัติการทางทหารโดยตรงหรือเกี่ยวข้องกับการทหารมากกว่าพลเรือนนั้นเป็นไปได้ค่อนข้างยาก เพราะระบบไซเบอร์อยู่

---

[871] John Markoff, "Before the Gunfire, Cyber Attacks," The New York Times, August 12, 2008, [online] Accessed: September 10, 2020. Available from: https://www.nytimes.com/2008 /08/13/technology/13cyber.html

[872] Siobhan Gorman, "Georgia States Computers hit by Cyberattack," The Wall Streat Journal, August 12, 2008, [online] Accessed: September 10, 2020. Available from: https://www.wsj.com/articles/SB121850756472932159

[873] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 51 (5) (b).

ในพื้นที่ทางอิเล็กทรอนิกส์หรือคลื่นไฟฟ้าที่ใช้ร่วมกันของทั้งทหารและพลเรือน การจะโจมตีระบบไซเบอร์ทางการทหารจึงต้องปรากฏชัดแจ้งว่าเป็นการทำลายระบบการสั่งการอาวุธหรือการสั่งการกองทัพซึ่งจะส่งผลต่อความแพ้-ชนะในสงครามได้ ซึ่งขณะปัจจุบันยังไม่พบรายงานว่ามีการใช้ปฏิบัติการทางไซเบอร์ในลักษณะดังกล่าว คงปรากฏเฉพาะการโจมตีสาธารณูปโภคที่ใช้ร่วมกันระหว่างพลเรือนและทหารเท่านั้น

ประเด็นที่ 2 การระบุตัวตนผู้ใช้เทคโนโลยีทำได้ยากขึ้น

ในกรณีการใช้เทคโนโลยีอื่นๆ ก็พบว่ามีการใช้งานอุปกรณ์ที่มีลักษณะร่วมกันของทหารและพลเรือนมากขึ้น โดยผู้ใช้งานเทคโนโลยีก็เป็นกลุ่มที่มีความหลาหหลายมากขึ้น โดยเฉพาะอย่างยิ่งการใช้อากาศยานไร้คนขับเพื่อการโจมตี มีหลายกรณีที่อากาศยานไร้คนขับถูกใช้โดยกลุ่มที่ไม่ใช่รัฐ ตัวอย่างเช่น กรณีเหตุการณ์วันที่ 13 มกราคม ค.ศ.2006 มีรายงานว่าหน่วยข่าวกรองของสหรัฐอเมริกา (The United States Central Intelligence Agency) ได้ใช้อากาศยานสังหารแบบไร้คนขับ (Predator Drone) ยิงขีปนาวุธโจมตีเป้าหมายซึ่งคาดว่าเป็นกลุ่มผู้ก่อการร้ายในเขตพื้นที่เมืองดามาโดลา (Damadola) ของประเทศปากีสถานใกล้เขตพรมแดนประเทศอัฟกานิสถาน[874] โดยก่อนการโจมตีนั้นได้มีการระบุว่าเป้าหมายดังกล่าวเป็นที่อยู่ของเป้าหมายระดับสูงของ Al Qaeda แต่ปรากฏว่าข้อมูลผิดพลาด ภารกิจทำลายเป้าหมายจึงล้มเหลว แต่การโจมตีดังกล่าวเป็นผลให้ประชาชนเสียชีวิตราว 18 คน โดยกองทัพสหรัฐอเมริกาได้ปฏิเสธความเกี่ยวข้องกับปฏิบัติการดังกล่าว[875]

ในสถานการณ์การใช้อากาศยานไร้คนขับเพื่อการโจมตีนี้ค่อนข้างแตกต่างจากปฏิบัติการทางไซเบอร์เพื่อการโจมตีอยู่ค่อนข้างมาก เพราะการระบุตัวตนผู้ปฏิบัติการทางไซเบอร์เป็นเรื่องที่ค่อนข้างยาก แต่การควบคุมอากาศยานไร้คนขับนั้นแม้จะมีระยะห่างระหว่างผู้ควบคุมอากาศยานและตัวอากาศยานก็ตาม แต่การพิสูจน์ความสัมพันธ์ระหว่างอากาศยานไร้คนขับกับผู้ควบคุมหรือผู้ที่เกี่ยวข้องกับอากาศยานนั้นอาจกระทำได้ง่ายกว่า ทั้งนี้อยู่ในเงื่อนไขว่าจะต้องทำลายอากาศยานหรือควบคุมอากาศยานไร้คนขับนั้นได้ก่อน ประเด็นการปฏิบัติการของหน่วยข่าวกรองสหรัฐอเมริกาซึ่งโจมตีเป้าหมายในประเทศปากีสถานนั้นไม่มีการทำลายอากาศยานไร้คนขับโดยฝ่ายที่ถูกโจมตีจึงไม่สามารถระบุความสัมพันธ์ระหว่างอากาศยานไร้คนขับกับหน่วยงานใดได้ แต่เรื่องนี้ก็ไม่ได้แตกต่างจาก

---

[874] Dafna Linzer and Griff Witte, “U.S. Airstrike Targets Al Qaeda’s Zawahiri”, Washington Post, 14 January 2006.

[875] Ibid.

กรณีการโจมตีด้วยอาวุธทั่วไป เช่น การวางระเบิดเพื่อการก่อการร้าย ที่เมื่อมีการกล่าวหาผู้กระทำความผิดก็มักจะมีการปฏิเสธความรับผิดชอบเสมอ การพิสูจน์ความสัมพันธ์ระหว่างการใช้อากาศยานไร้คนขับจึงแตกต่างจากปฏิบัติการทางไซเบอร์อยู่ค่อนข้างมาก

นอกจากการใช้งานอากาศยานไร้คนขับโดยกลุ่มกองกำลังของรัฐแล้วยังพบว่ากลุ่มก่อการร้ายก็นิยมการใช้อากาศยานไร้คนขับเพื่อการโจมตีเช่นกัน เช่น เหตุการณ์ใน ค.ศ. 1994 กลุ่มโอมชินริเคียว (Aum Shinrikyo) ในประเทศญี่ปุ่นใช้เฮลิคอปเตอร์บังคับวิทยุทำการปล่อยแก๊สซารินในที่สาธารณะแต่ภารกิจไม่สำเร็จเนื่องจากเฮลิคอปเตอร์ดังกล่าวประสบอุบัติเหตุตก[876] เหตุการณ์ใน ค.ศ.2013 กลุ่มฮามาสในปาเลสไตน์ได้ควบคุมอากาศยานไร้คนขับบรรทุกวัตถุระเบิดบินเข้าไปในเขตของอิสราเอลแต่ถูกสกัดเอาไว้ได้ก่อน[877] และเหตุการณ์ใน ค.ศ.2014 กลุ่ม Islamic State: IS ใช้อากาศยานไร้คนขับเชิงพาณิชย์และอากาศยานไร้คนขับประดิษฐ์เอง เพื่อปฏิบัติการทางทหารในประเทศอิรักและซีเรีย[878] เป็นต้น

เหตุการณ์ทั้งหลายที่เกิดขึ้นนี้อาจมิได้เกิดขึ้นในสถานการณ์การขัดกันทางอาวุธเสมอไป แต่สะท้อนให้เห็นถึงบทบาทของเทคโนโลยีหลายประการในความขัดแย้งปัจจุบัน การใช้เทคโนโลยีอาจเป็นการกระทำของตัวแทนรัฐ ในขณะที่กลุ่มกองกำลังที่ไม่ใช่รัฐก็สามารถใช้เทคโนโลยีในแบบเดียวกันต่อสู้ได้ และกลุ่มก่อการร้ายก็นิยมใช้เทคโนโลยีมากขึ้นในการก่อความไม่สงบเรียบร้อยในขณะที่การต่อต้านการก่อการร้ายนอกสถานการณ์การขัดกันทางอาวุธก็นิยมใช้เทคโนโลยีใหม่ปฏิบัติการด้วยเช่นกัน

ในกรณีการใช้หุ่นยนต์สังหารที่สามารถปฏิบัติการได้โดยการประมวลผลและตัดสินใจด้วยตัวเอง หากพิจารณาลักษณะการทำงานของหุ่นยนต์สังหารอิสระจะพบว่าผลของการปฏิบัติการนั้นมีลักษณะเชิงกายภาพมากกว่าปฏิบัติการทางไซเบอร์อย่างชัดเจน การโจมตีด้วยหุ่นยนต์สังหารจึงมีผลไม่ต่างจากการใช้อาวุธโดยทั่วไป ส่วนประเด็นว่าเป็นการกระทำของรัฐหรือไม่ก็ต้องไปพิสูจน์ความสัมพันธ์ของหุ่นยนต์กับกองกำลังทางทหารของรัฐในลำดับต่อไปซึ่งอาจนำไปสู่ปัญหาว่าจะสามารถกระทำได้เพียงใด ทั้งนี้หากสังเกตจากกรณีการใช้งานอากาศยานไร้คนขับในกรณีความขัดแย้งระหว่างยูเครนและรัสเซีย ซึ่งรัสเซียได้มีการใช้งานอากาศยานไร้คนขับเชิงพาณิชย์เพื่อบรรทุกวัตถุระเบิดเข้าสู่พื้นที่ยูเครนแต่ไม่มีการยืนยันจากฝ่ายรัสเซียว่าเป็นของรัสเซีย ในขณะที่การโจมตีทางไซ

---

[876] Robert j. Bunker, Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications. Carlisle, p. 7.

[877] Ibid., p. 11.

[878] Joby Warrick, “Use of Weaponized Drones by Isis Spurs Terrorism Fears,” Washington Post, 21 February 2017.

เบอร์หลายครั้งก็ไม่ปรากฏการแสดงความรับผิดชอบว่าเกิดจากการกระทำของฝ่ายใด เช่น การโจมตีทางไซเบอร์ต่อประเทศจอร์เจียและประเทศเอสโตเนียซึ่งมีหลักฐานพิสูจน์ได้ว่าเป็นการปฏิบัติการที่มีต้นทางจากประเทศรัสเซียแต่รัฐบาลรัสเซียก็ปฏิเสธความรับผิดชอบ หรือปฏิบัติการ Stuxnet ซึ่งเป็นการโจมตีทางไซเบอร์ต่อโรงงานเพิ่มประสิทธิภาพยูเรเนียมที่เมือง Natanz ของประเทศอิหร่าน แม้จะพบว่ามีความสัมพันธ์กับประเทศสหรัฐอเมริกาแต่ก็ไม่พบการแสดงความรับผิดชอบจากประเทศสหรัฐอเมริกาแต่อย่างใด[879]

4.1.1.2 ข้อท้าทายเรื่องการยึดครองดินแดน

เนื่องจากอนุสัญญาเจนีวา ค.ศ.1949 ข้อ 2 กำหนดว่าอนุสัญญาจะใช้กับกรณี “...all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.”[880] หรือขอบเขตการบังคับใช้กฎหมายให้รวมถึงกรณีที่เกิดการยึดครองอาณาเขตบางส่วนของรัฐแม้จะไม่มีการต่อต้านด้วยอาวุธก็ตาม ซึ่งเมื่อพิจารณาจากถ้อยคำและแนวปฏิบัติในการขัดกันทางอาวุธที่ผ่านมาจะหมายถึงการยึดครองดินแดนในลักษณะทางกายภาพ ปัญหาเกิดขึ้นมาว่าในสถานการณ์ที่กองทัพผู้ใช้ปฏิบัติการทางไซเบอร์สามารถควบคุมพื้นที่ทางไซเบอร์ของรัฐฝ่ายตรงข้ามได้จะถือว่าเป็นการยึดครองได้หรือไม่

ประเด็นเรื่องการยึดครองพื้นที่ทางไซเบอร์นี้เป็นเรื่องที่กองทัพหลายรัฐให้ความสำคัญโดยมองว่าพื้นที่ทางไซเบอร์ถือเป็นพื้นที่ทางยุทธศาสตร์หนึ่งด้วย ถึงขนาดที่หลายกองทัพสร้างความร่วมมือเพื่อเพิ่มขอบเขตการเชื่อมต่อยุทธวิธีการรบทางบก เรือ อากาศ อวกาศ และทางไซเบอร์[881] พื้นที่ทางไซเบอร์มีความแตกต่างจากพื้นที่รูปแบบอื่นๆ เนื่องจากไม่มีสถานะทางกายภาพ ปัญหานี้เป็นเรื่องที่ยังไม่มีการพิจารณาในเชิงกฎหมาย ซึ่งอาจเป็นไปได้ว่าเนื่องด้วยปฏิบัติการทางไซเบอร์ที่เข้าลักษณะการโจมตีซึ่งกระทำโดยรัฐและถือว่าเป็นปฏิบัติการทางทหารได้แล้วนั้น ย่อมถือว่าอยู่ในขอบเขตที่กฎหมายมนุษยธรรมระหว่างประเทศสามารถบังคับใช้ได้ การจะมาพิจารณาเรื่อง

---

[879] David Albright, Paul Brannan, and Christina Walrond, “Stuxnet Malware and Natanz: update of ISIS December 2010,” p.4.

[880] Common Article 2, Geneva Convention 1949

[881] Defence Review Asia Staff, “International industry partner announce collaboration agreement for GCAP advanced electronics,” Defence Review Asia, March 21, 2023, [online] Accessed March 22, 2023. Available from: https://defencereviewasia.com/international-industry-partners-announce-collaboration-agreement-for-gcap-advanced-electronics/

ลักษณะของการยึดครองอาณาเขตจึงไม่น่าจะมีความสำคัญอีก ทั้งนี้ก็น่าสังเกตว่าในการปฏิบัติการทางไซเบอร์เพื่อยึดครองพื้นที่สารสนเทศแตกต่างจากการยึดครองดินแดนตรงที่การยึดครองดินแดนมีการเคลื่อนกองกำลังทางทหารเข้าไปในพื้นที่ของรัฐอื่น ในขณะที่ปฏิบัติการทางไซเบอร์อาจไม่ได้มีการเคลื่อนที่ทางกายภาพแต่ในการยึดครองพื้นที่สารสนเทศได้นั้นจะต้องมีการใช้วิธีการเพื่อเข้าถึงระบบไซเบอร์ของเป้าหมาย เปลี่ยนแปลงข้อมูลบางอย่าง หรือมีการกระทำบางอย่างที่จะต้องมีผลกระทบต่อระบบสารสนเทศของเป้าหมายด้วย หากปฏิบัติการดังกล่าวกระทำโดยรัฐด้วยการปฏิบัติการทางทหารแล้วก็ควรจะถือเป็นปฏิบัติการทางทหารที่ก่อให้เกิดการขัดกันทางอาวุธได้

นอกจากนี้ตามหลักกฎหมายระหว่างประเทศซึ่งเกี่ยวข้องกับอำนาจอธิปไตยทางดินแดนของรัฐอาจนำไปสู่ปัญหาในการพิจารณาว่าในพื้นที่ทางไซเบอร์นั้นจะกำหนดเขตอำนาจรัฐทางดินแดนอย่างไร เนื่องจากการแบ่งแยกพื้นที่ทางไซเบอร์โดยอาศัยหลักดินแดนนั้นเป็นไปได้ยากมาก หากไม่สามารถแยกพื้นที่ทางไซเบอร์เช่นเดียวกับหลักเขตอำนาจรัฐทางดินแดนได้ก็น่าคิดว่าการยึดครองพื้นที่ทางไซเบอร์ที่เทียบเท่าการยึดครองดินแดนจะเกิดขึ้นได้อย่างไร อย่างไรก็ดี แม้การยึดครองพื้นที่ทางไซเบอร์จะอธิบายได้ค่อนข้างยากแต่หากเทียบเคียงว่าปฏิบัติการทางไซเบอร์ใดส่งผลกระทบต่อการใช้งานระบบไซเบอร์ในรัฐใด (ในลักษณะของการควบคุม) ในระดับที่กว้างขวางอาจเทียบเท่ากับการยึดครองพื้นที่ทางกายภาพหรือไม่ สิ่งนี้เป็นประเด็นที่น่าพิจารณาต่อไป

4.1.2 ข้อท้าทายเกี่ยวกับเทคโนโลยีใหม่กับการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ

การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศเป็นไปตามเงื่อนไขของข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 กำหนดว่า “In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply…”[882] หรืออนุสัญญาเจนีวาสามารถปรับใช้กับการขัดกันทางอาวุธที่เกิดขึ้นในดินแดนของรัฐใดรัฐหนึ่งโดยไม่มีลักษณะระหว่างประเทศ ในขณะที่ข้อ 1 ของพิธีสารเพิ่มเติมฉบับที่ 2 แห่งอนุสัญญาเจนีวา ค.ศ.1977 กำหนดว่าพิธีสารจะใช้ในกรณี “…shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949 … which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other

[882] Common Article 3 of Geneva Convention 1949.

organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations..."[883] หรือการเผชิญหน้าทางอาวุธของกลุ่มติดอาวุธในดินแดนหนึ่งกลุ่มหรือมากกว่าหนึ่งกลุ่มในดินแดนของรัฐที่มีการจัดตั้งอย่างเป็นระบบ มีการปฏิบัติการภายใต้การบังคับบัญชาและมีความรับผิดชอบ ทำการควบคุมดินแดนบางส่วนของรัฐได้และสามารถปฏิบัติการทางทหารได้

ประเด็นสำคัญในการพิจารณาการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธสำหรับการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศมีดังนี้

4.1.2.1 สถานะของกลุ่มติดอาวุธที่สู้รบในลักษณะเป็นองค์กร

พิธีสารฉบับที่ 2 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา ค.ศ.1949 เกี่ยวกับการคุ้มครองผู้ประสบภัยจากการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศกำหนดให้พิธีสารฉบับนี้มีผลบังคับกับการขัดกันทางอาวุธที่มิได้อยู่ภายใต้ข้อ 1 ของพิธีสารฉบับที่ 1 กล่าวคือพิธีสารฉบับที่ 2 นี้ใช้บังคับกับการขัดกันทางอาวุธที่เกิดขึ้นในอาณาเขตของรัฐภาคีระหว่างกองกำลังของตนและกองกำลังของฝ่ายต่อต้านหรือกลุ่มกองกำลังที่ได้มีการจัดตั้งอื่นๆ ซึ่งอยู่ภายใต้อำนาจการบังคับบัญชาที่รับผิดชอบและสามารถควบคุมอาณาเขตส่วนหนึ่งของรัฐภาคีนั้น จนทำให้กองกำลังดังกล่าวสามารถปฏิบัติการทางทหารได้อย่างต่อเนื่องและพร้อมเพรียง[884] สาระสำคัญของหลักการนี้มีองค์ประกอบในเรื่องกองกำลังที่ได้มีการจัดตั้งขึ้น

ในคดี Akayesu มีการพิจารณาว่ากลุ่มกองกำลังต่อต้านรัฐจะต้องมีลักษณะ "... under responsible command, which entails a degree of organization within the armed group or dissident armed forces...enable the armed group or dissident forces to plan and carry out concerted military operations, and to impose discipline ...these armed forces must be able to dominate a sufficient part of the territory so as to maintain sustained and concerted military operations...the operations must be continuous and planned. The territory in their control is usually that which has eluded the control of

[883] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 1 — Material field of application

[884] Ibid.

the government forces."[885] หรือกองกำลังที่จะต่อสู้กับกองกำลังของรัฐจนถึงขนาดเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้นั้นจะต้องเป็นกลุ่มกองกำลังที่มีแผนในการปฏิบัติการและสามารถปฏิบัติการได้เช่นเดียวกับทหาร โดยจะต้องมีการสั่งการและบังคับบัญชาอย่างเป็นระบบ การพิจารณาของศาลในคดีนี้เป็นการอธิบายลักษณะของการเป็นกองกำลังที่ได้มีการจัดตั้ง (organized armed groups)

กรณีการปฏิบัติการทางไซเบอร์เพื่อโจมตีระบบอินเทอร์เน็ตของประเทศเอสโตเนียและประเทศจอร์เจียนั้นไม่ชัดเจนว่าอยู่ในลักษณะของกลุ่มที่มีแผนปฏิบัติการ มีการสั่งการและมีการบังคับบัญชาอย่างเป็นระบบหรือไม่ เพียงแต่มีลักษณะของการปฏิบัติงานเป็นเครือข่ายเท่านั้น โดยปฏิบัติการดังกล่าวมีเป้าหมายเพียงการโจมตีระบบเครือข่ายคอมพิวเตอร์ซึ่งควบคุมระบบสาธารณูปโภคของทั้งสองประเทศดังกล่าวผ่านผู้ให้บริการเว็บไซต์ helpisraelwin.com และเว็บไซต์อื่นๆ จึงยากที่จะเข้าสู่เงื่อนไขของการเป็นปฏิบัติการของกลุ่มกองกำลังที่มีแผนปฏิบัติการอยู่ภายใต้คำสั่งและการบังคับบัญชาอย่างเป็นระบบ[886] ขณะที่ Doswald-Beck ให้ความเห็นว่า การโจมตีเครือข่ายคอมพิวเตอร์ดังกล่าวของกลุ่มผู้ปฏิบัติการ (ซึ่งแม้ว่าจะมีการจัดตั้งมาเป็นอย่างดีก็ตาม) ย่อมเป็นเพียงการกระทำความผิดทางอาญาเท่านั้น จะพิจารณาว่าเป็นการกระทำของกลุ่มกองกำลังไม่ได้ เพราะกลุ่มปฏิบัติการดังกล่าวเป็นตัวตนอื่นๆ ซึ่งอยู่ไกลจากสถานะความเป็นทหารหรือกองกำลังอยู่พอสมควร แม้การกระทำดังกล่าวจะก่อให้เกิดความเสียหายเป็นวงกว้างก็ตาม[887]

อย่างไรก็ดี การจะกล่าวว่าทุกปฏิบัติการของกลุ่มย่อยจะไม่เป็นการกระทำเยี่ยงกองกำลังก็อาจจะไม่ถูกต้องเสมอไป เพราะปัจจุบันนี้ค่อนข้างเป็นที่ยอมรับในทางวิชาการว่าการโจมตีโดยกลุ่มผู้ก่อการร้ายซึ่งอาจนำไปสู่การใช้กำลังทางทหารย่อมถือเป็นการใช้กำลังที่นำไปสู่การขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศได้เช่นกัน เช่น กรณีการโจมตีประเทศสหรัฐอเมริกาในเหตุการณ์ 911 เมื่อเดือนกันยายน ค.ศ.2001 แต่ทั้งนี้จะต้องพิจารณาการโจมตีของกลุ่มก่อการร้ายเป็นรายกรณีไปด้วย โดยจะต้องคำนึงถึงความรุนแรงของปฏิบัติการแต่ละกรณี จะถือว่าการกระทำของกลุ่มก่อการร้ายทุกกลุ่มเป็นการโจมตีด้วยกองกำลังซึ่งจะนำไปสู่การขัดกันทางอาวุธไม่ได้เสมอไป[888]

---

[885] Prosecutor v. Jean-Paul Akayesu (1998) Case No. ICTR-96-4-T. International Criminal Tribunal for Rwanda, para. 626.

[886] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 125.

[887] Louise Doswald-Beck, "Some Thoughts on Computer Network Attack and the International Law of Armed Conflict" in Michael N. Schmitt and Brian T. O'Donnell (eds.), Computer Network Attack and International Law (Naval War College, Newport. RI, 2002), p. 165.

[888] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 125.

การก่อการร้ายนั้นย่อมนำไปสู่เงื่อนไขของการเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศก็แต่โดยเป็นไปตามข้อ 3 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 และพิธีสารเพิ่มเติมฉบับที่ 2 ค.ศ.1977 หากกลุ่มก่อการร้ายดังกล่าวมีการจัดตั้ง และสามารถปฏิบัติการได้เท่าเทียมกับกองกำลังทางทหาร[889] ดังนั้น ในทางกลับกัน หากกลุ่มก่อการร้ายใดไม่เข้าเงื่อนไขของการเป็นกลุ่มที่จัดตั้งอย่างเป็นรูปแบบ มีการบังคับบัญชาอย่างเป็นระบบและปฏิบัติการเยี่ยงทหารได้ การกระทำของกลุ่มก่อการร้ายดังกล่าวย่อมเป็นเพียงการกระทำความผิดทางอาญาเท่านั้น ซึ่งจะต้องตกอยู่ภายใต้บังคับของกฎหมายอาญาภายในประเทศที่การกระทำนั้นเกิดขึ้น

การพิจารณาว่าการกระทำโดยใช้เทคโนโลยีใหม่เป็นวิธีและปัจจัยในการขัดกันทางอาวุธจะต้องกระทำโดยกลุ่มติดอาวุธที่มีลักษณะเป็นองค์กร หากการกระทำของผู้ปฏิบัติการไม่ใช่องค์กร เช่น การโจมตีระบบไซเบอร์ของประเทศเอสโตเนียเป็นเพียงการกระทำของกลุ่มแฮกเกอร์ที่ไม่ได้จัดตั้งเป็นองค์กร การโจมตีทางไซเบอร์ดังกล่าวย่อมไม่อยู่ในขอบเขตของการบังคับใช้พิธีสารฉบับที่ 2 นี้ เช่นเดียวกับการใช้เทคโนโลยีอื่นๆ เพื่อการขัดกันทางอาวุธ ดังนั้นหากกลุ่มกองกำลังติดอาวุธมีการใช้เทคโนโลยี เช่น ไซเบอร์ หรือหุ่นยนต์สังหารประกอบการต่อสู้ในดินแดนของรัฐ ย่อมอยู่ในขอบเขตการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศตามพิธีสารฉบับที่ 2

4.1.2.2 ระดับความรุนแรงของการสู้รบ

ข้อ 1 (2) ของพิธีสารเพิ่มเติมฉบับที่ 2 แห่งอนุสัญญาเจนีวากำหนดว่าพิธีสารนี้จะไม่ใช้กับ “...internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.”[890]

ข้อความดังกล่าวทำให้เข้าใจได้ว่าระดับความรุนแรงที่ถือว่าเป็นการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจะต้องมีระดับมากกว่าความไม่สงบภายในประเทศ (internal disturbance) หรือความตึงเครียดภายในประเทศ (internal tension) โดยไม่ใช่เป็นเพียงการจราจล (riots) หรือความรุนแรงเป็นครั้งคราว (isolated and sporadic acts of violence) และการสู้รบนั้นจะต้องมีลักษณะของความยืดเยื้อ (protracted) ด้วย[891] ปัญหาว่าความยืดเยื้อโดยใช้เทคโนโลยีใหม่

---

[889] Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War, p.157.

[890] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Art. 1 (2).

[891] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 1.

ในการขัดกันทางอาวุธจึงยังเป็นเรื่องที่ยังไม่อาจสรุปได้ว่าจะต้องกระทำการในลักษณะใด เนื่องจากยังไม่มีสถานการณ์ดังกล่าวเกิดขึ้นในความเป็นจริง

อย่างไรก็ดีหากการสู้รบตามรูปแบบเกิดขึ้นแล้วและมีการนำเอาเทคโนโลยีไปใช้เป็นอาวุธหรือวิธีการในการสู้รบ เทคโนโลยีดังกล่าวย่อมอยู่ในบังคับของกฎหมายมนุษยธรรมระหว่างประเทศด้วยเช่นเดียวกัน

กรณีการปฏิบัติการทางไซเบอร์ที่จะถือได้ว่าเป็นการกระทำเทียบเท่ากับการโจมตีได้นั้น ยังมีความเห็นในสองทาง คือ กลุ่มที่เห็นว่าปฏิบัติการทางไซเบอร์เพื่อการโจมตีนั้นเทียบเท่ากับการโจมตีด้วยกำลังอาวุธ และกลุ่มที่ไม่เห็นด้วย

Shulman เห็นว่าการโจมตีทางไซเบอร์นั้นอยู่ภายใต้บังคับของกฎหมายว่าด้วยการขัดกันทางอาวุธและหลักความได้สัดส่วนในการโจมตี โดยไม่จำเป็นที่จะต้องพิจารณาว่าเป็นการกระทำผ่านระบบสารสนเทศและไม่ต้องพิจารณาว่าเป็นอาวุธหรือไม่ เพราะไม่สามารถนำแนวคิดของการขัดกันทางอาวุธแบบเดิมมาใช้โดยตรงได้[892] ในขณะที่ Aldrich ไม่เห็นด้วยกับแนวคิดดังกล่าว โดยอธิบายว่าการโจมตีทางไซเบอร์ที่จะถือว่าเป็นการใช้กำลังทางอาวุธได้นั้นจะต้องมีลักษณะความเสียหายทางกายภาพเกิดขึ้นด้วย[893] Haslam มิได้วิจารณ์แนวคิดของทั้ง Shulman และ Aldrich แต่กล่าวว่าทั้งสองท่านนี้ได้แสดงทัศนะต่อปฏิบัติการทางไซเบอร์กับปฏิบัติการทางข้อมูลสารสนเทศรูปแบบอื่นๆ ในบรรทัดฐานเดียวกัน โดยสิ่งที่สองท่านนี้มิได้พิจารณาคือการทดสอบหลักการทางกฎหมายว่าด้วยการขัดกันทางอาวุธกับปฏิบัติการทางไซเบอร์ ว่าปฏิบัติการทางสารสนเทศในการสงครามแบบใดจึงจะเท่าเทียมกับการใช้กำลังในการขัดกันทางอาวุธ เช่น การพิจารณาการใช้ปฏิบัติการสารสนเทศเป็นปัจจัยในการสงครามและผลที่สืบเนื่องจากการใช้ปัจจัยดังกล่าว[894]

นอกเหนือจากนี้ยังมีแนวคิดที่แตกต่างของนักวิชาการท่านอื่นๆ เช่น Hanseman เห็นว่าการโจมตีทางไซเบอร์ที่จะถือว่าเป็นปฏิบัติการที่เทียบเท่ากับการใช้กำลังได้ก็ต่อเมื่อผลสืบเนื่องจากการโจมตีทางไซเบอร์นั้นจะต้องเท่าเทียมกับความเสียหายด้วยอาวุธตามรูปแบบปกติตามทฤษฎี

---

[892] Mark Shulman, Legal Constraints on Information Warfare, Center for Strategy and Technology, Air War Center, Occasional Paper No.7 (1999). P. 13.

[893] Richard W. Aldrich, "The International Legal Implications of Information Warfare," Airpower, Vol. 99, (1996): 102.

[894] Emily Haslam, "Information Warfare: Technological Changes and International Law", Journal of Conflict & Security Law. Vol.5 No.2 (December 2000): 167.

สัดส่วนความรุนแรงและผลกระทบ (Scale & Effect)[895] ในขณะที่ Scott มองว่ากฎหมายว่าด้วยการขัดกันทางอาวุธย่อมสามารถปรับใช้กับการโจมตีทางไซเบอร์ได้ เพราะเป้าหมายของกฎหมายว่าด้วยการขัดกันทางอาวุธให้ความสำคัญกับผลของการโจมตีมากกว่าการพิจารณาความหลากหลายของการโจมตี[896] ไม่ว่าจะเป็นหลักการแยกแยะเป้าหมายซึ่งเป็นการป้องกันผลที่จะเกิดขึ้นกับบุคคลและทรัพย์สินที่กฎหมายมนุษยธรรมระหว่างประเทศมุ่งคุ้มครอง หากแยกแยะเป้าหมายได้ยากการโจมตีนั้นก็จะต้องไม่ก่อให้เกิดความเสียหายที่เกินสัดส่วนรวมตลอดถึงความจำเป็นที่จะต้องมีการประเมินวิธีการก่อนการโจมตีตามหลักความระมัดระวังล่วงหน้าก่อนการโจมตี ซึ่งหลักการทั้งหมดนี้ล้วนแล้วแต่เป็นการคุ้มครองเป้าหมายที่ไม่เกี่ยวข้องกับปฏิบัติการทางทหารในการขัดกันทางอาวุธ

การพิสูจน์การโจมตีทางไซเบอร์ว่าเป็นไปเพื่อประกอบกับการโจมตีด้วยอาวุธตามแบบเป็นเรื่องที่ค่อนข้างละเอียดอ่อนและอาจนำไปสู่ปัญหาบางประการ เช่น หากรัฐอ้างว่าระบบเรดาร์ของตนถูกโจมตีจึงเป็นเหตุให้การสั่งการทิ้งระเบิดจากอากาศยานเกิดความผิดพลาด หรือการอ้างว่าระบบนำวิถีของขีปนาวุธถูกรบกวนจึงทำให้การโจมตีเป้าหมายคลาดเคลื่อน[897] ข้ออ้างดังกล่าวจะรับฟังได้เพียงใด เนื่องจากการพิสูจน์ให้ทันท่วงทีอาจทำได้ยาก นอกจากนั้นการพิสูจน์ที่ล่าช้ายังอาจส่งผลต่อการตัดสินใจในการโต้ตอบของกองกำลังฝ่ายตรงข้ามซึ่งอาจทำให้การปฏิบัติตามหลักความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตีได้รับผลกระทบ

4.1.2.3 การควบคุมดินแดนของรัฐ

ขอบเขตการบังคับใช้พิธีสารฉบับที่ 2 เพื่อเพิ่มเติมอนุสัญญาเจนีวานั้นมีองค์ประกอบที่ 3 เรื่อง “...control over a part of its territory...”[898] หรือการควบคุมส่วนหนึ่งส่วนใดของรัฐซึ่งองค์ประกอบนี้แตกต่างจากขอบเขตการบังคับใช้พิธีสารฉบับที่ 1 เพื่อเพิ่มเติมอนุสัญญาเจนีวา โดยในพิธีสารฉบับที่ 1 ซึ่งว่าด้วยเรื่องการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศนั้นอาศัยองค์ประกอบ

---

[895] Robert G. Hanseman, “The Realities and Legalities of Information Warfare” AFL Review, Vol.42, No.173, (1997): 184.

[896] Roger D. Scott, “Legal Aspects of Information Warfare: Military Disruption of Telecommunications”, Naval Law Review, Vol. 45, (1998): 59.

[897] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 134.

[898] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 1 para 1.

เดียวกับข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 มีขอบเขตบังคับใช้กับสถานการณ์ที่กองทัพของรัฐหนึ่งทำการ “occupy” หรือยึดครองพื้นที่ส่วนใดส่วนหนึ่งของรัฐอื่นแม้ไม่มีการต่อต้านด้วยอาวุธ

การควบคุมดินแดนส่วนหนึ่งส่วนใดของรัฐโดยกลุ่มกองกำลังอื่นที่ไม่ใช่รัฐนี้เป็นเงื่อนไขที่ทำให้กองกำลังนั้นสามารถปฏิบัติการทางทหารได้ในลักษณะ “sustained and concerted military operations”[899] หรืออย่างต่อเนื่องและพร้อมเพรียง

ข้อพิจารณาจากคำวินิจฉัยของศาลอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวีย (International Tribunal for the Former Yugoslavia) ในคดี Kunarac ได้อธิบายว่า “ ...There is no necessary correlation between the area where the actual fighting is taking place and the geographical reach of the laws of war. The laws of war apply in the whole territory of the warring states or, in the case of internal armed conflicts, the whole territory under the control of a party to the conflict, whether or not actual combat takes place there, and continue to apply until a general conclusion of peace or, in the case of internal armed conflicts, until a peaceful settlement is achieved ...”[900] หมายความว่าดินแดนที่ถูกควบคุมกับดินแดนที่เกิดการสู้รบกันนั้นไม่จำเป็นต้องเป็นดินแดนเดียวกัน เพราะกฎหมายมนุษยธรรมระหว่างประเทศสามารถปรับใช้ได้กับดินแดนทั้งหมดของรัฐในกรณีการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ ขึ้นอยู่กับว่าการต่อสู้จะเกิดขึ้นบริเวณใดของดินแดน ดังนั้นการกระทำที่เป็นการละเมิดกฎหมายมนุษยธรรมระหว่างประเทศสามารถเกิดขึ้นได้แม้แต่ในพื้นที่ที่ซึ่งมิได้ถูกควบคุม

กรณีดังกล่าวนี้จะต้องพิจารณาแยกจากการกระทำผิดตามกฎหมายอาญาปกติ ซึ่งไม่ต้องอาศัยลักษณะการขัดกันทางอาวุธ การกระทำผิดทางอาญาที่เกิดขึ้นระหว่างการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศจึงอาจเกิดขึ้น ณ พื้นที่ใดของรัฐก็ได้ ต่างจากการกระทำที่ละเมิดกฎหมายมนุษยธรรมระหว่างประเทศที่ไม่ควรจะแยกออกไปจากพื้นที่ซึ่งเกิดการขัดกันมากจนเกินไป[901]

สิ่งที่ต้องตระหนักคือคำอธิบายดังกล่าวไม่ใช่คำอธิบายสำหรับการใช้งานเทคโนโลยีหรือการโจมตีทางไซเบอร์ เพียงแต่เป็นการอธิบายเรื่องความสัมพันธ์ระหว่างการขัดกันทางอาวุธกับดินแดน

---

[899] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 1 para 1.

[900] *Prosecutor v. Dragoljub Kunarac et al*. (2002) Case No.IT-96-23 and 23/1, International Criminal Tribunal for the Former Yugoslavia, para 57.

[901] Ibid.

ของรัฐเท่านั้นหากพิจารณาในบริบทดังกล่าวการใช้งานระบบไซเบอร์เพื่อการโจมตีของกลุ่มกองกำลังภายในรัฐไม่ว่าจะกระทำในพื้นที่ใดของรัฐ หากมีความสัมพันธ์กับการขัดกันทางอาวุธแล้วย่อมสามารถปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการใช้งานระบบไซเบอร์เพื่อการโจมตีดังกล่าวได้

นอกจากนี้การพิจารณาองค์ประกอบเรื่องการครอบครองดินแดนของกลุ่มกองกำลัง เพื่อปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศตามข้อ 1 ของพิธีสารเพิ่มเติม ฉบับที่ 2 อาจต้องพิจารณาในขอบเขตที่กว้างขวางขึ้น เพราะการพิจารณาแต่เพียงการครอบครองพื้นที่ตามความเป็นจริงทางกายภาพย่อมไม่สามารถใช้ได้กับกรณีการโจมตีทางไซเบอร์ในยุคข้อมูลสารสนเทศได้ เพราะกลุ่มกองกำลังที่ต่อสู้กับรัฐย่อมสามารถใช้งานระบบไซเบอร์เพื่อการโจมตีได้โดยไม่จำเป็นต้องมีการครอบครองพื้นที่ใดๆ ของรัฐเลยก็ได้[902]

4.2 ข้อท้าทายเกี่ยวกับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ

เมื่อการขัดกันทางอาวุธเกิดขึ้นแล้วไม่ว่าจะเป็นการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศหรือการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ การกระทำใดๆ ที่เกิดขึ้นในระหว่างการขัดกันทางอาวุธในลักษณะตอบโต้กันของฝ่ายคู่พิพาทยังต้องเคารพต่อหลักความจำเป็นทางการทหารและการคุ้มครองหลักความมีมนุษยธรรมอันเป็นหัวใจหลักของกฎหมายมนุษยธรรมระหว่างประเทศด้วย การปฏิบัติตอบโต้ระหว่างคู่พิพาทในการขัดกันทางอาวุธนี้คือการกระทำอันเป็นปฏิปักษ์ซึ่งเป็นหลักการพื้นฐานของกฎหมายว่าด้วยการขัดกันทางอาวุธ และจะนำไปสู่การพิจารณาความชอบด้วยกฎหมายของการใช้วิธีการและปัจจัยในการขัดกันทางอาวุธในแต่ละกรณีด้วย ข้อพิจารณาเกี่ยวกับหลักการกระทำอันเป็นปฏิปักษ์ในการใช้เทคโนโลยีใหม่กับการขัดกันทางอาวุธมีดังนี้

4.2.1 ข้อท้าทายเรื่องการโจมตีด้วยปฏิบัติการทางไซเบอร์

ข้อ 2 ร่วมของอนุสัญญาเจนีวา ค.ศ.1949 และในพิธีสารฉบับที่ 1 ค.ศ.1977 เพื่อเพิ่มเติมอนุสัญญาเจนีวา มีการกำหนดของเขตการบังคับใช้กฎหมายต่อกรณีการโจมตีที่เกิดขึ้น โดยในข้อ 48 พิธีสารฉบับที่ 1 ค.ศ.1977 ได้กำหนดหลักในการ “โจมตี” ว่าจะจะต้องมีการจำแนกประชากร พลเรือนออกจากพลรบ และทรัพย์สิ่งของพลเรือนออกจากเป้าหมายทางการทหารอยู่ตลอดเวลา ซึ่งความหมายของการ “โจมตี” นั้นอยู่ที่ข้อ 49 ของพิธีสารฉบับนี้ โดยมีการนิยามคำว่า “...Attacks

[902] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 136.

means acts of violence against the adversary, whether in offence or in defence…" [903] หรือการโจมตีหมายถึงการกระทำในลักษณะรุนแรงต่อฝ่ายปฏิปักษ์ ไม่ว่าจะเป็นในเชิงรุกหรือเชิงรับ

นักกฎหมายบางส่วนเห็นว่าเมื่อพิจารณาในคำอธิบายพิธีสารเพิ่มเติมฉบับที่ 1 แล้วพบว่าการกระทำด้วยความรุนแรงมีความหมายค่อนข้างโน้มไปทางการทำลายในเชิงกายภาพแม้คำอธิบายจะเขียนเอาไว้กว้างๆ ก็ตาม เช่น การอธิบายว่าการโจมตี (attack) หมายถึง การต่อสู้ (combat action) เพื่อเป้าหมายในการทำลายศัตรู (offensive act aimed at destroying enemy forces and gaining ground)[904] แต่ขอบเขตของการโจมตีนี้ไม่มีข้อกำหนดในเรื่องความรุนแรง ดังนั้น การใช้กำลังทางกายภาพแม้เพียงเล็กน้อยก็ถือเป็นการโจมตีได้ เช่น การยิงปืนเพียงนัดเดียวต่อฝ่ายศัตรู[905] ปัญหาอาจเกิดขึ้นในกรณีที่มีการโจมตีด้วยการเผยแพร่ข่าวชวนเชื่อ (propaganda) การคุกคามด้วยวิธีการทางจิตวิทยา หรือการเมือง[906]

ในขณะที่นักวิชาการบางกลุ่มเห็นว่าเกณฑ์เรื่องความเสียหายทางกายภาพไม่ควรเป็นสิ่งเดียวที่ใช้ชี้วัดว่าการโจมตีเกิดขึ้นหรือไม่เพราะการโจมตี "เป้าหมายทางการทหาร" ซึ่งปรากฏตามข้อ 52 (2) ของพิธีสารเพิ่มเติม ฉบับที่ 1 กำหนดว่า "Attacks shall be limited strictly to military objectives…., military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." มีคำสำคัญเรื่องการทำลายไม่ว่าทั้งหมดหรือบางส่วน การยึด หรือการทำให้หมดสมรรถภาพของทรัพย์สิ่งของนั้น จะก่อให้เกิดความเสียหายทางการทหารอย่างชัดเจน โดยคำว่า "Neutralization" ย่อมหมายรวมถึง การทำให้วัตถุอย่างใดอย่างหนึ่งใช้การไม่ได้ เช่น การระงับระบบไฟฟ้าสาธารณะโดยไม่มีการทำลายระบบโครงสร้างทาง

---

[903] "acts of violence against the adversary, whether in offence or defence" Article 49 of Additional Protocol I

[904] Commentary of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 49.

[905] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 141.

[906] Michael Bothe, Karl Josef Partsch, Waldemar A Solf and Eaton Martin, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949, 2nd ed. (Leiden: Martinus Nijhoff, 2013), P. 289, [online] Accessed: June 10, 2020, Available from: https://doi.org/10.1163/9789004254718.

กายภาพ ก็ถือเป็นลักษณะหนึ่งของการกระทำ “การโจมตี” ด้วย[907] ทั้งนี้อาจมีข้อพิจารณาที่เกิดขึ้นจากการทำให้หมดสมรรถสภาพว่าการทำให้หมดสมรรถภาพตามข้อ 52 (2) ของพิธีสารเพิ่มเติมฉบับที่ 1 นี้ หมายความถึงปัญหาการโจมตีเป้าหมายทางการทหารเท่านั้นหรือไม่[908] เพราะผลของการกระทำจะต้องนำไปสู่ความได้เปรียบทางทหารอย่างชัดเจน

ศาลอาญาระหว่างประเทศเพื่อพิจารณาอดีตประเทศยูโกสลาเวียได้พิจารณาความหมายของการโจมตีในคดี Jokic ว่า “...Additional Protocols I (art. 53) and II (art. 16) ...reiterate the obligation to protect cultural property and expand the scope of the prohibition by...any acts of hostility directed against the historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples...whether or not the attacks result in actual damage. This immunity is clearly additional to the protection attached to civilian objects...”[909] หมายความว่าการโจมตีที่กระทำต่ออนุสรณ์สถาน สถานที่ทางศิลปวัฒนธรรม สถานที่ทางศาสนาไม่ว่าจะก่อให้เกิดผลทางกายภาพหรือไม่ ก็ถือว่าเป็นการต้องห้ามตามกฎหมาย ในทำนองเดียวกันคดี Kordic and Cerkez ในชั้นอุทธรณ์ของศาลอาญาระหว่างประเทศเพื่อพิจารณาอดีตประเทศยูโกสลาเวียก็วินิจฉัยในลักษณะใกล้เคียงกับคดี Jokic ว่า “...attacks in violation of Articles 51 and 52 of Additional Protocol I are clearly unlawful even without causing serious harm as provided for in Article 85 of Additional Protocol I...their criminalisation as a matter of international law depends on the practice of the Contracting States under Article 85 of Additional Protocol I...”[910] การโจมตีที่เป็นการละเมิดต่อข้อ 51 และข้อ 52 ของพิธีสารฉบับที่ 1 นั้นแม้จะไม่ปรากฏความเสียหายที่รุนแรงก็ถือเป็นการกระทำที่ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศเช่นกัน สังเกตได้จากการใช้คำว่า “...clearly unlawful even without causing serious harm...”

---

[907] Knut Dormann, “Applicability of the Additional Protocols to Computer Network Attacks,” Paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004, pp. 142-143.

[908] Ibid.

[909] *Prosecutor v. Miodrag Jokic (Sentencing Judgement)* (2004) Case No. IT-01-42/1-S, International Criminal Tribunal for the Former Yugoslavia – Trial Chamber I, para. 50.

[910] *Prosecutor v. Dario Kordic and Mario Cerkez (Appeal)* (2004) Case No.IT-95-14/2-A, International Criminal Tribunal for Former Yugoslavia, Appeals Chamber, para 65.

ประเด็นปัญหาของการโจมตีทางไซเบอร์มีความแตกต่างจากการโจมตีทางกายภาพอย่างชัดเจน เพราะข้อมูลดิจิทัลในระบบไซเบอร์นั้นสามารถกู้คืนได้เสมอไม่ว่าจะถูกทำซ้ำ แก้ไขหรือเปลี่ยนแปลงอย่างไรก็ตาม แต่การฟื้นฟูระบบและกู้คืนข้อมูลนั้นเป็นเรื่องที่ต้องใช้เวลาและทรัพยากร ซึ่งหากใช้หลักการเรื่องการละเมิดอย่างรุนแรงตามพิธีสารฉบับที่ 1 คงไม่สามารถปรับใช้ได้ แต่หากเทียบกับลักษณะของการให้ความคุ้มครองแก่อนุสรณ์สถาน หรือสิ่งที่คุณค่าทางจิตใจของประชาชนแล้วจะพบว่าการคุ้มครองทรัพย์สินและสถานที่เหล่านั้นไม่ได้อาศัยปัจจัยด้านความเสียหายทางกายภาพเป็นหลัก แต่อาศัยปัจจัยด้านความรู้สึกร่วมกันของคน หากจะนำเอาแนวคิดดังกล่าวมาใช้เพื่อคุ้มครองทรัพยากรทางไซเบอร์ก็อาจทำได้ โดยอาจเทียบกับกรณีของกฎหมายภายในประเทศที่เกี่ยวกับอาชญากรรมทางไซเบอร์หรือกฎหมายความมั่นคงทางไซเบอร์ที่ไม่ได้อาศัยเงื่อนไขความเสียหายในเชิงรูปธรรมเป็นหลัก แต่เป็นการคุ้มครองสิทธิของปัจจักเจกทางด้านข้อมูลข่าวสารและกำหนดเป็นฐานความผิดพร้อมทั้งกำหนดโทษทางอาญาได้[911]

อย่างไรก็ดีเมื่อไม่มีคำอธิบายที่ชัดเจนเกี่ยวกับแนวคิดในเรื่องการทำให้หมดสมรรถภาพของผู้ร่างกฎหมาย แต่น่าจะอนุมานจากบริบทแวดล้อมได้ว่าการทำให้หมดสมรรถภาพเป็นวิธีคิดเกี่ยวกับการโจมตีตามรูปแบบปกติ ซึ่งย่อมนำมาสู่ผลคือความตาย ความบาดเจ็บ หรือการทำลาย การตีความให้การเสื่อมสมรรถภาพให้มีความหมายแตกต่างไปจากการทำให้เกิดความตาย ความบาดเจ็บ หรือการทำลาย จึงไม่น่าจะทำให้ความหมายของการโจมตีมีความชัดเจนมากขึ้นแต่อย่างใด[912]

ในขณะที่นักวิชาการบางฝ่าย เช่น Schmitt มีความเห็นว่า “ปฏิบัติการทางทหาร” ในข้อ 48 นั้นจะต้องแยกพิจารณาออกจากข้อกฎหมายอื่นๆ โดยในคำอธิบายข้อ 48 นั้นให้ความสำคัญกับคำว่า “ปฏิบัติการ” มากกว่า “การโจมตี” ซึ่งข้อ 48 มีวัตถุประสงค์ในการปรับใช้กับการปฏิบัติการทางทหารในระหว่างเวลาที่มีการกระทำในลักษณะรุนแรงเกิดขึ้น กรณีการใช้งานระบบปฏิบัติการทางคอมพิวเตอร์ซึ่งมิได้ถูกออกแบบมาเพื่อการก่อให้เกิดความตาย ความบาดเจ็บหรือแม้กระทั่งความเสียหาย ย่อมไม่อยู่ในขอบเขตของคำว่า “การโจมตี” แต่อยู่ในขอบเขตของ “การปฏิบัติการ” ได้ และปฏิบัติการทางระบบคอมพิวเตอร์นั้นย่อมเกี่ยวข้องโดยตรงกับองค์ประกอบสำคัญของการปฏิบัติการ หลักการแยกแยะเป้าหมายดังที่ปรากฏในข้อ 48 จึงต้องสามารถปรับใช้แก่

---

[911] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 253.

[912] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 198.

ปฏิบัติการทางคอมพิวเตอร์ด้วย แม้จะไม่อยู่ในลักษณะ “การโจมตี” ที่จะก่อให้เกิดความตาย ความบาดเจ็บ หรือความเสียหายก็ตาม[913]

Schmitt ให้ความเห็นว่า ข้อ 51 นั้น มีเนื้อหาที่เกี่ยวข้องกับเรื่องการให้ความคุ้มครองพลเรือน ในขณะที่ ข้อ 57 นั้น มีเนื้อหาเกี่ยวข้องกับความระมัดระวังล่วงหน้าก่อนการโจมตี ดังนั้น คำว่า “ปฏิบัติการทางทหาร” (Military operation) ในข้อ 51 และข้อ 57 มีความหมายที่แตกต่างกัน คือ ในข้อ 51 ปฏิบัติการทางทหาร หมายถึง การกระทำการใดๆ ของกองทัพที่เกี่ยวเนื่องกับการกระทำอันเป็นปฏิปักษ์[914] ส่วนข้อ 57 นั้น ทำให้เข้าใจไปในทางว่า “ปฏิบัติการทางทหาร” หมายถึง ปัจจัย การเคลื่อนไหว กิจกรรมใดๆ ซึ่งกระทำโดยกองทัพในลักษณะของการต่อสู้[915] ดังนั้น การกระทำใดๆ ที่อยู่ในขอบเขตของการกระทำอันเป็นปฏิปักษ์ย่อมถือเป็นการกระทำที่มีวัตถุประสงค์ทางการทหาร

เมื่อพิจารณาจากลักษณะของ “ปฏิบัติการทางทหาร” แล้ว การโจมตีทางไซเบอร์ย่อมเกิดขึ้นได้หากเป็นไปร่วมกับการโจมตีทางกายภาพ โดยการโจมตีทางไซเบอร์ดังกล่าวนั้นไม่จำเป็นต้องก่อให้เกิดความเสียหายในลักษณะรุนแรงก็ได้

ในคดี Kupreskic ใน Appeals Chamber ของศาลอาญาระหว่างประเทศเพื่อพิจารณาคดีอดีตประเทศยูโกสลาเวีย (ICTY) ยืนยันหลักการว่า Martens Clause จะต้องนำมาใช้ในการตีความข้อ 57 และ 58 โดยจะต้องใช้เพื่อการคุ้มครองพลเรือนและจำกัดการโจมตี ศาลพิจารณาว่า “... Martens Clause...now become part of customary international law. True, this Clause may not be taken to mean that the “principles of humanity” and the “dictates of public conscience” have been elevated to the rank of independent sources of international law... this Clause enjoins, as a minimum, reference to those principles and dictates any time a rule of international humanitarian law is not sufficiently rigorous or precise: in those instances the scope and purport of the rule must be

---

[913] Michael N. Schmitt, “Wired Warfare: Computer Network Attack and Jus in Bello,”: 194.

[914] Claude Pilloud, Jean de Preux, Bruno Zimmermann, Philippe Eberlin, Hans-Peter Gasser and Claude Wenger, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, (Geneva: International Committee of the Red Cross, 1987), p. 677-690.

[915] Ibid., para. 2191.

defined with reference to those principles and dictates...to expand the protection accorded to civilians."[916]

ความหมายที่ศาลในคดีนี้ต้องการกล่าวถึงคือหลักทั่วไปของกฎหมายว่าด้วยการขัดกันทางอาวุธหรือ Martens Clause ซึ่งอยู่นอกเหนือจากอนุสัญญาเจนีวาและพิธีสารเพิ่มเติม จะต้องได้รับความคุ้มครองเสมอ หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศที่พัฒนามาจาก Martens Clause เช่น การรบจะต้องเป็นไปเพื่อความจำเป็นทางการทหารโดยจะต้องแยกแยะเป้าหมายพลเรือนออกจากเป้าหมายทางทหาร และปฏิบัติการทางทหารจะต้องไม่ส่งผลกระทบต่อพลเรือนโดยตรงหรือส่งผลกระทบต่อพลเรือนมากเกินความจำเป็น เป็นต้น หลักการ Martens Clause นี้จะต้องคำนึงถูกนำมาใช้เสมอหากกฎหมายมนุษยธรรมระหว่างประเทศที่เป็นลายลักษณ์อักษรไม่สามารถปรับใช้ได้อย่างเพียงพอ

กล่าวโดยสรุป การใช้ระบบไซเบอร์อาจนำมาซึ่งการขัดกันทางอาวุธได้ โดยเหตุที่ระบบไซเบอร์เองสามารถใช้เป็นปัจจัยในการขัดกันทางอาวุธได้ การใช้ระบบไซเบอร์ในการโจมตีเครือข่ายการทำงานของคอมพิวเตอร์ทางการทหาร และการสั่งการเพื่อทำลายสาธารณูปโภคที่จำเป็นทางการทหารที่เป็นการกระทำของกองกำลังทางทหารของรัฐหรือที่เทียบเท่าจึงเป็นที่มาของการขัดกันทางอาวุธได้ แต่ทั้งนี้จะต้องอาศัยแนวทางการปฏิบัติของรัฐต่อไปในอนาคตว่าจะเกิดกรณีใดที่ศาลระหว่างประเทศจะสร้างบรรทัดฐานรับรองแนวคิดนี้หรือไม่ อย่างไร[917]

ดังที่ได้กล่าวในตอนต้นว่าปัญหาย่อมอาจเกิดขึ้นกับการโจมตีระบบไซเบอร์โดยกลุ่มที่ไม่ใช่รัฐในการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ เพราะการระบุตัวตนของกลุ่มที่ไม่ใช่รัฐนั้นอาจเป็นปัญหาที่ทำได้ยากขึ้น ในขณะที่การพิจารณาองค์ประกอบของการเริ่มต้นการขัดกันทางอาวุธที่ไม่ได้เกิดจากการใช้กำลังปะทะกัน แต่เป็นการใช้กำลังทางทหารเข้าครอบครองดินแดนย่อมเป็นเรื่องที่พิจารณาได้ยากขึ้นไปอีก เพราะการครอบครองดินแดนโดยการใช้ปฏิบัติการทางไซเบอร์จะกระทำได้อย่างไร เนื่องจากปฏิบัติการทางไซเบอร์ไม่มีลักษณะทางกายภาพ โดยการครอบครองดินแดนนั้นโดยปกติจะเป็นการดำเนินการทางกายภาพเป็นสำคัญ

เหตุที่ระบบไซเบอร์อาจถูกใช้ทั้งเป็นวิธีและปัจจัยในการขัดกันทางอาวุธ จึงอยู่ในขอบเขตของกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งนี้ปัญหาที่อาจเกิดแก่การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศกับการโจมตีทางไซเบอร์นั้นอาจเกิดขึ้นได้หลายประการอันได้แก่ ปัญหา

---

[916] Prosecutor v Kuprekic (2000) case No. IT-95-16-T, International Criminal Tribunal for the Former Yugoslavia, para. 525.

[917] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 219.

เรื่องการแบ่งแยกระหว่างพลเรือนและพลรบจากลักษณะการใช้งานร่วมกันของพลเรือนและพลรบ ผลกระทบที่อาจเกิดขึ้นในลักษณะ Knock-on หรือผลกระทบต่อเนื่องจากการโจมตีทางการทหารที่อาจส่งผลต่อการใช้ชีวิตของพลเรือน และย่อมรวมถึงการคำนึงถึงความได้สัดส่วนในการโจมตีซึ่งจะกระทำได้ยากขึ้น[918] เนื่องจากการตัดสินใจในการโจมตีทางระบบไซเบอร์ทุกครั้งจะต้องคำนึงถึงผลกระทบที่อาจเกิดขึ้นหรือมีตามมาอย่างชัดเจนด้วย จึงหลีกเลี่ยงไม่ได้ที่จะต้องคำนึงถึงหลักความระมัดระวังล่วงหน้าก่อนการโจมตีเพิ่มเติม ว่าการตอบโต้หรือการโจมตีโดยผ่านระบบไซเบอร์นั้นจะต้องกระทำบนพื้นฐานการพิจารณาหลักเกณฑ์มากเพียงใด อย่างไรก็ดีหลักเกณฑ์พื้นฐานเหล่านี้ย่อมสามารถบังคับใช้ได้เสมอ

ปัญหาประการสำคัญคงอยู่ที่เรื่องการแยกแยะเป้าหมายการโจมตีผ่านระบบไซเบอร์ว่าจะกระทำได้ยากง่ายเพียงใด ด้วยเหตุที่ระบบไซเบอร์ก่อให้เกิดปัญหาความยุ่งยากในการระบุตัวตนผู้กระทำและความยากในการแบ่งแยกเป้าหมายการโจมตี ลักษณะการทำงานในโลกเสมือนจึงสร้างประเด็นพิจารณาหลายประการต่อกฎหมายมนุษยธรรมระหว่างประเทศในรูปแบบเดิมซึ่งมีพัฒนาการจากการขัดกันทางอาวุธในอดีตที่การกระทำต่างๆ ปรากฏเป็นรูปธรรมเห็นได้ชัดเจน

4.2.2 ข้อท้าทายเกี่ยวกับการใช้เทคโนโลยีรูปแบบอื่นเพื่อการโจมตี

การใช้เทคโนโลยีอื่นนอกเหนือจากปฏิบัติการทางไซเบอร์ในฐานะเป็นอาวุธเพื่อการโจมตี ได้แก่ การใช้ระบบอาวุธที่อิสระ การใช้อากาศยานไร้คนขับ ฯลฯ นั้น มีลักษณะทางกายภาพอย่างชัดเจนเมื่อเทียบกับปฏิบัติการทางไซเบอร์ที่เป็นการทำงานในระบบอิเล็กทรอนิกส์ ปัญหาความไม่ชัดเจนเรื่องการโจมตีจึงเกิดขึ้นได้ค่อนข้างน้อย แต่ประเด็นที่ไม่แตกต่างจากการปฏิบัติการทางไซเบอร์คือปัญหาเกี่ยวกับการพิจารณาลักษณะการใช้งานเทคโนโลยีที่สอดคล้องกับนิยามของการโจมตีซึ่งหมายถึงการกระทำในลักษณะรุนแรงต่อฝ่ายปฏิปักษ์ ไม่ว่าจะเป็นในเชิงรุกหรือเชิงรับ ว่าเทคโนโลยีเหล่านี้ก่อให้เกิดประเด็นพิจารณาอย่างไรบ้าง

การใช้อากาศยานไร้คนขับในปฏิบัติการทางทหารเมื่อเกิดการขัดกันทางอาวุธนั้นเป็นสิ่งที่เกิดขึ้นอย่างแพร่หลายในปัจจุบัน และนำมาซึ่งประเด็นทางกฎหมายหลายประการ แต่ประเด็นทางกฎหมายเหล่านี้เกิดขึ้นจากความคิดของนักกฎหมายและสังคมระหว่างประเทศ ซึ่งไม่มีกรณีใดที่เป็นข้อพิพาทสู่ศาลระหว่างประเทศ จึงไม่มีกรณีการพิจารณาทั้งความชอบด้วยกฎหมายของการใช้งานและสถานะของอากาศยานไร้คนขับโดยศาลระหว่างประเทศ อย่างไรก็ดีจากการศึกษาวิจัย

---

[918] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 205-208.

ของนักวิชาการและองค์การระหว่างประเทศต่างๆ มีแนวคิดที่เห็นว่าจะอากาศยานไร้คนขับนำไปสู่ประเด็นปัญหาทางกฎหมายหลายประการ

ปัญหาเรื่องการใช้งานอากาศยานไร้คนขับที่กระทบต่อหลักการป้องกันตัวนั้น เป็นประเด็นที่นักวิชาการเสนอโดยมีความคล้ายคลึงกับปัญหาของการโจมตีทางไซเบอร์ ประเด็นการโจมตีทางไซเบอร์ก่อให้เกิดปัญหาทางกฎหมายตั้งแต่ก่อนเกิดการขัดกันทางอาวุธ เช่น จะถือว่าเป็นการใช้กำลังทางอาวุธหรือไม่ และจะนำไปสู่การป้องกันตัวอย่างไร เนื่องจากการป้องกันตัวจะเกิดขึ้นได้ก็ต่อเมื่อมีการคุกคามต่อบูรณภาพแห่งดินแดน ลักษณะแนวคิดเช่นเดียวกันนี้มีการนำมาพิจารณากับลักษณะการใช้งานอากาศยานไร้คนขับเพื่อการโจมตี

งานศึกษาของ Hitaj เรื่อง Use of Drones and Global Security: Implications under International Law เสนอว่าการใช้อากาศยานไร้คนขับจะก่อให้เกิดปัญหาอย่างน้อย 2 ประการ ได้แก่[919]ปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับจะก่อให้เกิดการโจมตีนอกเขตพื้นที่การสู้รบ[920] และการใช้อากาศยานไร้คนขับจะนำไปสู่ปัญหาทางกฎหมายเกี่ยวกับการป้องกันตัวตามกฎบัตรสหประชาชาติ[921]

ข้อพิจารณาเรื่องปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับจะนำไปสู่การโจมตีนอกพื้นที่การสู้รบนั้น Hitaj เห็นว่าการรบตามแบบปกติจะต้องเกิดขึ้นในเขตพื้นที่การสู้รบ (battle field) เท่านั้น การใช้อากาศยานไร้คนขับซึ่งสามารถเดินทางไปยังพื้นที่ต่างๆ นอกเขตการสู้รบเพื่อการทำลายเป้าหมายที่ไม่ได้อยู่ในสนามรบจะเป็นการเปลี่ยนรูปแบบในการทำสงครามและจะทำให้เกิดปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองบุคคลในการขัดกันทางอาวุธเกิดขึ้น ประเด็นพิจารณาเกี่ยวกับการใช้อากาศยานไร้คนขับนอกพื้นที่ขัดกันทางอาวุธมีดังต่อไปนี้

การใช้อากาศยานไร้คนขับเพื่อปฏิบัติการโจมตีนอกเขตพื้นที่การสู้รบมีประเทศที่เกี่ยวข้องกับเรื่องขอบเขตของสนามรบ วัตถุประสงค์ของปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับและกฎหมายที่จะบังคับใช้กับปฏิบัติการและอากาศยานไร้คนขับดังกล่าวก่อให้เกิดประเด็นพิจารณาได้แก่

---

[919] Erjan Hitaj, “Use of Drones and Global Security: Implications under International Law,” Koreuropa, Rivista elettronica del Centro di Documentazione Europea dell’Università Kore di Enna, pp. 1-14. [online] Accessed: April 10, 2020. Available from: https://www.academia.edu/27011103/Use_of_Drones_and_Global_Security_Implications_Under_International_Law

[920] Ibid.

[921] Ibid.

ประเด็นพิจารณาที่ 1 ประเด็นเรื่องการโจมตีนอกพื้นที่การสู้รบนี้เป็นเรื่องที่มีการถกเถียงทางวิชาการด้านกฎหมายมนุษยธรรมอย่างมาก โดยเฉพาะอย่างยิ่งเรื่องการใช้สิทธินอกอาณาเขตของรัฐเพื่อการลอบสังหาร เช่น ในขณะที่มีการขัดกันทางอาวุธระหว่างรัฐ A กับรัฐ B หากรัฐ A ใช้อากาศยานไร้คนขับเข้าไปปฏิบัติการค้นหาและสังหารผู้บัญชาการกองทัพทหารของรัฐ B จะถือว่าปฏิบัติการดังกล่าวเป็นไปโดยชอบด้วยกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ หรือในกรณีการต่อต้านการก่อการร้ายของสหรัฐอเมริกาซึ่งมีการใช้อากาศยานไร้คนขับในดินแดนปากีสถานเพื่อค้นหาและสังหารผู้นำระดับสูงของกลุ่ม Al Qaeda จะถือว่าเป็นการกระทำที่ชอบด้วยกฎหมายว่าด้วยการขัดกันทางอาวุธหรือไม่

ประเด็นเรื่องการลอบสังหาร (Assassination) นั้นมีพลวัตที่น่าสนใจคือหลักการสงครามยุคเดิม ยอมรับว่าการฆาตกรรมศัตรูรวมตลอดถึงผู้นำของฝ่ายศัตรูสามารถกระทำนอกสมรภูมิได้ ไม่ว่าจะอยู่ไกลเท่าไรก็ตาม ในศตวรรษที่ 13 นักบุญโธมัส อไควนัส (St. Thomas Aquinas) กล่าวว่าการฆาตกรรมกษัตริย์ของศัตรูนั้น หากเป็นไปเพื่อประโยชน์ส่วนรวมถือว่ามีความชอบธรรมเสมอ ในขณะที่ในศตวรรษที่ 16 เซอร์โธมัส มอร์ (Sir Thomas More) ผู้ประพันธ์หนังสือเรื่อง Utopia ได้เขียนแนวคิดเขาไว้ในผลงานชิ้นนี้ว่า ในช่วงเวลาแห่งสงครามนั้นมีรางวัลที่ยิ่งใหญ่รอผู้สังหารเจ้าชายแห่งฝ่ายศัตรู แนวคิดเดียวกันนี้ยังมีการอ้างอิงโดยฮูโก โกรเชียส (Hugo Grotius) ผู้ที่ได้รับการยกย่องให้เป็นบิดาแห่งกฎหมายระหว่างประเทศยุคใหม่ โกรเชียสเขียนแนวคิดของเขาเอาไว้ในงานประพันธ์คลาสสิกเรื่อง “On the Law of War and Peace” ว่า “Not merely by the law of nature but also by the law of nations ... it is in fact permissible to kill an enemy in any place whatsoever; and it does not matter how many there are that do the deed, or who suffer.”[922] หรือทั้งกฎธรรมชาติและกฎของประชาชาติ...อนุญาตให้ฆ่าศัตรูได้ไม่ว่าที่ใดก็ตาม และไม่สำคัญว่าผู้กระทำมีกี่คนและใครเดือดร้อน

ต่อมาในศตวรรษที่ 18 แนวคิดเกี่ยวกับการลอบสังหารเริ่มเปลี่ยนแปลงไป โดยเอเมริค เดอ วาตเตล (Emmerich de Vattel) ในงานเขียนชื่อ The Law of Nations นั้น วาตเตลพยายามแยกการลอบสังหารออกจากการฆาตกรรมโดยชอบด้วยกฎหมายในยามสงคราม โดยอ้างว่าการลอบสังหารนั้นมีประเด็นละเอียดอ่อนเกี่ยวกับการกระทำเพื่อความชอบธรรมกับการทรยศ ปัญหาที่จะเกิดขึ้นจากการลอบสังหารคือผู้กระทำอาจเป็นใครก็ได้ไม่ว่าจะเป็นคนที่อยู่ในดินแดนนั้นเอง คน

[922] Michael N. Schmitt, “Assassination in the Law of War,” Lieber Institute West Point, October 15, 2021, [online] Accessed: February 10, 2022. Available from: https://lieber.westpoint.edu/assassination-law-of-war/

ในดินแดนศัตรู หรือเขาอาจเข้ามาในดินแดนในฐานผู้ลี้ภัย การกระทำนั้นจึงน่าละอายและน่ารังเกียจแก่ทั้งตัวผู้กระทำการและผู้สั่งการ[923] หลังจากนั้นแนวคิดในศตวรรษที่ 19 จึงเริ่มก่อตัวขึ้นมาในรูปแบบใหม่

หลักกฎหมายว่าด้วยการขัดกันทางอาวุธใน ค.ศ.1863 ซึ่งเป็นจุดเริ่มต้นของหลักการสงครามในยุคใหม่คือประมวลลีเบอร์ (Lieber Code) ได้กำหนดเอาไว้ในข้อ 148 ว่า “The law of war does not allow proclaiming either an individual belonging to the hostile army, or a citizen, or a subject of the hostile government, an outlaw, who may be slain without trial by any captor, any more than the modern law of peace allows such intentional outlawry; on the contrary, it abhors such outrage. The sternest retaliation should follow the murder committed in consequence of such proclamation, made by whatever authority. Civilized nations look with horror upon offers of rewards for the assassination of enemies as relapses into barbarism.”[924] หรือกฎหมายสงครามไม่อนุญาตให้บุคคลที่อยู่ในกองทัพศัตรู หรือพลเมือง หรือผู้อยู่ในบังคับบัญชาของรัฐที่เป็นศัตรูกระทำการนอกกฎหมาย รวมถึงการห้ามตอบโต้บุคคลดังกล่าวด้วยการฆาตกรรมโดยปราศจากการพิจารณาคดีเมื่อบุคคลดังกล่าวถูกจับได้ อารยประเทศเห็นว่าเรื่องดังกล่าวน่าสยดสยองหากจะมีการมอบรางวัลให้กับการลอบสังหารศัตรูเพราะจะนำเอาความป่าเถื่อนมาสู่สังคม

นอกจากนั้น ในข้อ 37 ของพิธีสารฉบับที่ 1 เพื่อเพิ่มเติมอนุสัญญาเจนีวากำหนดว่า “It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are examples of perfidy” โดยการกระทำที่อยู่ในลักษณะการล่อลวง (Perfidy) ได้แก่ a) the feigning of an intent to negotiate under a flag of truce or of a surrender; b) the feigning of an incapacitation by wounds or sickness; c) the feigning of civilian, non-combatant

---

[923] Emmerich de Vattel, The Law of Nations, Knud Haakonssen edit. (Indianapolis: Liberty Fund, 2008), p. 559.

[924] Instructions for the Government of Armies of the United States in the Field (Lieber Code). 24 April 1863, Article 148.

status; and d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict."[925]

ซึ่งอาจแปลความได้ว่าห้ามมิให้ประหาร ทำให้บาดเจ็บ หรือควบคุมตัวฝ่ายปฏิปักษ์โดยการล่อลวงฝ่ายตรงข้ามว่าตนเองเป็นผู้ได้รับการปกป้องตามพันธกรณีของกฎหมายมนุษยธรรมระหว่างประเทศ และการล่อลวงที่ว่าเป็นไปเพื่อนำไปสู่การหักหลัง การล่อลวงเช่นว่าหมายถึง

1) การแสร้งว่ามีเจตนาที่จะเจรจาภายใต้ธงอันแสดงถึงการพักรบหรือการยอมจำนน

2) การแสร้งว่าไร้ความสามารถ เพราะได้รับบาดเจ็บหรือป่วย

3) การแสร้งว่ามีสถานภาพเป็นพลเรือนหรือไม่ใช่พลรบ และ

4) การแสร้งว่ามีสถานภาพของผู้ได้รับความคุ้มครอง โดยการใช้สัญญาณเครื่องหมาย หรือเครื่องแบบขององค์การสหประชาชาติหรือของรัฐที่เป็นกลางหรือของรัฐอื่นซึ่งมิได้เป็นภาคีคู่พิพาท

แนวทางของกฎหมายว่าด้วยการขัดกันทางอาวุธในสมัยใหม่จึงไม่มีทัศนะในการยอมรับการลอบสังหารบางกรณีเช่นประมวลลีเบอร์ว่าด้วยการขัดกันทางอาวุธมีทัศนะรังเกียจการลอบสังหารอย่างชัดเจน เพราะเป็นการกระทำที่ไม่เป็นธรรมต่อฝ่ายผู้ถูกกระทำ ในขณะที่กฎหมายว่าด้วยการขัดกันซึ่งปรากฏในพิธีสารฉบับที่ 1 นั้นไม่ยอมรับการลอบสังหารซึ่งมีลักษณะเป็นการล่อลวงซึ่งคล้ายกับข้อเสนอของวาตเตล (Vattel) ที่เคยกล่าวว่าผู้ลอบสังหารอาจเข้ามาในฐานะเป็นใครก็ได้ทั้งคนในรัฐ คนต่างด้าว แม้กระทั่งผู้ลี้ภัย การลอบสังหารโดยอาศัยความได้เปรียบด้วยการแสดงสถานะเป็นผู้ไม่มีพิษภัยถือเป็นสิ่งที่ไม่ควรเกิดขึ้นในการทำสงคราม แตกต่างจากการปฏิบัติในการขัดกันทางอาวุธที่อาจมีการลอบสังหารด้วยพลซุ่มยิง (Sniper) ได้ เพราะการซุ่มยิงนั้นไม่มีลักษณะของการก่อให้เกิดความเข้าใจผิดว่าผู้กระทำเป็นบุคคลที่ได้รับความคุ้มครอง แต่เป็นการใช้เครื่องอำพรางการปฏิบัติการจึงไม่ต้องห้ามตามข้อ 37 วรรค 2 ของพิธีสารเพิ่มเติมฉบับที่ 1

หากปรับใช้พิธีสารฉบับที่ 1 กับกรณีการใช้อากาศยานไร้คนขับเพื่อการลอบสังหารจะก่อให้เกิดประเด็นน่าพิจารณาว่าการใช้อากาศยานไร้คนขับเพื่อการลอบสังหารบุคคลที่อยู่นอกพื้นที่การรบหรือนอกสมรภูมิจะเป็นการละเมิดต่อข้อ 37 ของพิธีสารฉบับที่ 1 นี้หรือไม่ น่าคิดว่าหากใช้อากาศยานดังกล่าวเสมือนการส่งทหารเข้าไปในดินแดนเพื่อการลอบสังหารย่อมไม่เป็นการละเมิดต่อข้อ 37 ของพิธีสารฉบับที่ 1 นี้ แต่หากอำพรางอากาศยานดังกล่าวด้วยการดัดแปลงใช้อากาศยาน

[925] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 37.

ไร้คนขับเชิงพาณิชย์ติดตั้งอาวุธยิงหรือวัตถุระเบิดเพื่อก่อวินาศกรรมหรือลอบฆาตกรรมย่อมถือว่าเป็นการสร้างความเข้าใจผิดแก่ผู้ถูกโจมตีว่าอากาศยานไร้คนขับดังกล่าวเป็นของพลเรือน

ประเด็นพิจารณาที่ 2 ขอบเขตของสนามรบ แม้สนามรบมีความหมายเป็นพื้นที่ในการสู้รบ แต่กฎหมายมนุษยธรรมระหว่างประเทศก็ไม่ได้มีเป้าหมายในการจำกัดพื้นที่ในการใช้กฎหมายให้อยู่เฉพาะในสนามรบเท่านั้น หากพิจารณาอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3 ข้อที่ 4 เรื่องประเด็นเรื่องกรณีที่พลเรือนรวมตัวกันใช้อาวุธเพื่อต่อสู้ (Levee en Masse) นั้นจะพบว่ากลุ่มพลเรือนที่สามารถกระทำการ Levee en Masse ได้จะต้องเป็นพลเรือนที่อยู่นอกเขตพื้นที่การสู้รบ หมายความว่าอนุสัญญาเจนีวาเองก็ไม่ได้จำกัดว่าการสู้รบจะต้องเกิดขึ้นแต่ในพื้นที่สนามรบที่กระทำการขณะนั้น แม้การกระทำจะเกิดขึ้นในพื้นที่อื่นๆ แต่มีความสัมพันธ์โดยตรงกับการสู้รบก็ย่อมถือว่าอยู่ในขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศเช่นเดียวกัน

นอกจากนั้น ในการพิจารณาลักษณะการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศตามอนุสัญญาเจนีวา ค.ศ.1949 ข้อ 2 ยังระบุว่า “...even if the said occupation meets with no armed resistance...”[926] หมายความว่าการขัดกันทางอาวุธเกิดขึ้นได้ในกรณีที่มีการยึดครองพื้นที่ส่วนหนึ่งของรัฐแม้ไม่มีการตอบโต้ด้วยอาวุธ กรณีเช่นนี้จะถือว่าพื้นที่ดังกล่าวเป็นพื้นที่สนามรบด้วยได้หรือไม่ก็มิได้มีคำอธิบายใดๆ ไว้ แต่เมื่อพิจารณาจากทั้งเงื่อนไขการขัดกันทางอาวุธที่มีลักษณะระหว่างประเทศ ตั้งแต่กรณีการพิพาทกันด้วยอาวุธระหว่างสองรัฐขึ้นไปและการครอบครองพื้นที่ส่วนใดส่วนหนึ่งของรัฐ การขัดกันทางอาวุธตามกฎหมายมนุษยธรรมระหว่างประเทศนี้ย่อมสื่อไปในทางให้ความหมายว่าหมายถึงสถานการณ์ที่อาจเกี่ยวข้องหรือไม่เกี่ยวข้องกับดินแดนทางกายภาพก็ได้ จริงอยู่ว่าการพิพาทกันด้วยอาวุธระหว่างรัฐย่อมต้องมีองค์ประกอบเรื่องดินแดนที่เป็นส่วนหนึ่งของรัฐเข้ามาเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้ แต่การต่อสู้หรือการโจมตีอาจไม่จำกัดเพียงการสู้กันในพื้นที่รัฐใดรัฐหนึ่ง การต่อสู้นั้นอาจเกิดขึ้นที่ดินแดนของรัฐที่ 3 หรืออาจเกิดขึ้นในบริเวณพรมแดนระหว่างสองประเทศโดยไม่มีการข้ามแดนก็ได้ ส่วนกรณีการครอบครองดินแดนที่ถือว่าเป็นการขัดกันทางอาวุธได้ตามกฎหมายนั้น ชี้ให้เห็นว่าการขัดกันทางอาวุธอาจไม่ต้องมีการใช้กำลังต่อสู้กันด้วยอาวุธจริงๆ ก็ได้ แต่ลักษณะของการกระทำของรัฐก่อให้เกิดความได้เปรียบทางการทหารในการที่จะเข้าไปควบคุมหรือครอบครองดินแดนของรัฐนั้นๆ แล้ว

[926] Geneva Conventions of 12 August 1949, Common Article 2.

เมื่อพิจารณาประเด็นทางกฎหมายดังกล่าวย่อมเห็นได้ชัดเจนว่ากฎหมายมนุษยธรรมระหว่างประเทศมีแนวทางที่จะบังคับใช้กฎหมายแก่กรณีของ “สถานการณ์” ที่เกิดขึ้นและก่อให้เกิดความเสียหายต่อรัฐ โดยมีองค์ประกอบเรื่องดินแดนทางกายภาพเป็นส่วนหนึ่งเท่านั้น และแม้องค์ประกอบของความเป็นดินแดนทางกายภาพอาจไม่ปรากฏในบางกรณีกฎหมายมนุษยธรรมระหว่างประเทศก็ยังคงมีผลบังคับใช้อยู่เช่นเดียวกัน ข้อกล่าวอ้างเรื่องการใช้อากาศยานไร้คนขับจะก่อให้เกิดประเด็นทางกฎหมายเกี่ยวกับการต่อสู้นอกพื้นที่สนามรบจึงไม่ใช่ปัญหาทางกฎหมายมนุษยธรรมระหว่าประเทศแต่อย่างใด หากปฏิบัติการใช้อากาศยานไร้คนขับดังกล่าวมีความเกี่ยวข้องกับสถานการณ์การขัดกันทางอาวุธโดยตรง

ประเด็นพิจารณาที่ 3 กฎหมายที่จะบังคับใช้ เมื่อเกิดการขัดกันทางอาวุธขึ้นก็มิได้หมายความว่ากฎหมายอื่นๆ จะหยุดใช้งาน หมายความว่าแม้จะไม่สามารถใช้อนุสัญญาเจนีวาได้ในการกระทำที่เกิดขึ้นทั้งในและนอกสนามรบ แต่กฎหมายระหว่างประเทศอื่นๆ และกฎหมายภายในของรัฐก็ยังคงสามารถบังคับใช้ได้ ดังนั้นหากมีการใช้อากาศยานไร้คนขับนอกพื้นที่การสู้รบ หรือแม้กระทั่งนอกสถานการณ์การขัดกันทางอาวุธ ย่อมมีกฎหมายรูปแบบอื่นๆ ใช้บังคับอยู่ เช่น หากเป็นกรณีปกติที่มิได้เกิดการขัดกันทางอาวุธ รัฐต่างๆ ก็ย่อมมีกฎหมายควบคุมการส่งออก นำเข้าสินค้าที่ใช้ได้สองทาง กฎหมายอาญาที่บังคับใช้กับการกระทำที่มีความผิดทางอาญา และกฎหมายที่ควบคุมการใช้งานอากาศยานไร้คนขับ ให้ผู้ใช้งานจะต้องมีใบอนุญาตและได้รับอนุญาตก่อนบินอากาศยานดังกล่าว แม้ในกฎหมายระหว่างประเทศจะไม่มีกฎหมายเฉพาะก็ตาม

กฎหมายที่จะใช้บังคับกับการกระทำที่เกิดขึ้นในการขัดกันทางอาวุธและการกระทำที่ไม่อยู่ในขอบเขตของการขัดกันทางอาวุธจึงได้แก่กฎหมายภายใน กฎหมายระหว่างประเทศ และกฎหมายสิทธิมนุษยชน[927] ปัญหาว่ากรณีการใช้งานอากาศยานไร้คนขับนอกพื้นที่สนามรบจะใช้กฎหมายใดพิจารณานั้น Erjan มองว่าน่าจะเป็นกฎหมายสิทธิมนุษยชนระหว่างประเทศทั่วไปก็ครอบคลุมต่อการคุ้มครองบุคคลแล้ว[928]

พึงสังเกตว่าการบังคับใช้กฎหมายเกี่ยวกับการควบคุมอากาศยานไร้คนขับนั้นเกิดผลอย่างเป็นรูปธรรมจากการบังคับใช้กฎหมายภายในเป็นหลัก เพราะกฎหมายภายในสามารถควบคุมต้นทาง กลางทาง และปลายทางของการนำเข้า ส่งออก ผลิต หรือถ่ายโอนเทคโนโลยีได้ ในขณะที่กฎหมายระหว่างประเทศอาจทำได้เพียงสร้างมาตรฐานหรือแนวทางปฏิบัติระหว่างรัฐเท่านั้น ใน

---

[927] Erjan Hitaj, “Use of Drones and Global Security: Implications under International Law,”: 10.

[928] Ibid., 11.

สถานการณ์จริงรัฐจึงสามารถควบคุมการงานเทคโนโลยีอากาศยานไร้คนขับด้วยกฎหมายของรัฐเองได้ง่ายกว่า

ในสถานการณ์การขัดกันทางอาวุธอาจมีประเด็นการบังคับใช้กฎหมายที่แตกต่างออกไป ได้แก่ กรณีสถานการณ์การใช้อากาศยานไร้คนขับของประเทศยูเครนในการขัดกันทางอาวุธกับประเทศรัสเซียนั้น ยูเครนย่อมนำเข้าอากาศยานไร้คนขับเพื่อการโจมตีกองทัพรัสเซียตามที่ประเทศต่างๆ ให้การสนับสนุน กฎหมายภายในที่ควบคุมการนำเข้า ส่งออก หรือถ่ายโอนเทคโนโลยีอากาศยานไร้คนขับย่อมไม่ถูกใช้บังคับ ในทัศนะว่าเป็นการให้ความช่วยเหลือทางมนุษยธรรม เมื่อยูเครนและประเทศต่างๆ ในยุโรปไม่ใช้หลักกฎหมายควบคุมการส่งออกสินค้าดังกล่าว การใช้อาวุธอากาศยานไร้คนขับของกองทัพยูเครนย่อมทำได้อย่างไร้ข้อจำกัด ปัญหาย่อมตกไปสู่ผู้ที่ต้องรับผลของการโจมตีด้วยอากาศยานไร้คนขับนั้นคือกองทัพรัสเซีย ในกรณีนี้มีนักวิชาการให้ความเห็นว่าปัญหาของกฎหมายภายในคือการพิจารณาสถานะของอากาศยานไร้คนขับในการขัดกันทางอาวุธนั้นย่อมเป็นไปตามกฎการปะทะ (Rule of engagement) ของแต่ละรัฐซึ่งอาจมีความแตกต่างกัน และการพิจารณาเป็นเรื่องภายในของรัฐ

กล่าวโดยสรุป ประเด็นเรื่องการปฏิบัติการนอกดินแดนของรัฐ (Extraterritorial) ที่นักวิชาการด้านกฎหมายมนุษยธรรมระหว่างประเทศถกเถียงกันอย่างมากว่าเป็นปรากฏการณ์ที่เกิดขึ้นในสังคมระหว่างประเทศในปัจจุบัน เหตุการณ์ที่มักถูกอ้างถึงเสมอคือปฏิบัติการของกองทัพสหรัฐอเมริกาที่มักกระทำในพื้นที่ของรัฐอื่น อันที่จริงปัญหานี้ไม่ได้เกิดขึ้นเฉพาะกับเรื่องการใช้อากาศยานไร้คนขับเท่านั้น ในปฏิบัติการทางทหารของอเมริกาโดยปกติก็มักมีลักษณะของการใช้กองกำลังทางทหารข้ามแดน ดังนั้นการใช้อากาศยานไร้คนขับนอกอาณาเขตของรัฐ ก็จะต้องไปพิจารณาปัญหาว่าปฏิบัติการดังกล่าวเกี่ยวข้องกับการขัดกันทางอาวุธหรือไม่ หากเกี่ยวกับปฏิบัติการทางทหารในการขัดกันทางอาวุธก็ถือเป็นการโจมตีตามปกติ แต่ถ้าหากเป็นปฏิบัติการที่นอกเหนือจากการขัดกันทางอาวุธแล้วย่อมไม่อยู่ในขอบเขตการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ รัฐเจ้าของอาณาเขตมีสิทธิใช้กฎหมายภายในเพื่อการจัดการกับอากาศยานไร้คนขับนั้นได้หากมองว่าเป็นการคุกคามต่อดินแดนหรือเป็นการขัดต่อหลักการเดินอากาศ

ปัญหาทางกฎหมายที่จะเกิดขึ้นจากการใช้อากาศยานไร้คนขับคือผู้ถูกโจมตีจะทำการป้องกันตัวอย่างไร การตอบโต้จะกระทำได้ทันทีเมื่อตรวจพบอากาศยานไร้คนขับหรือไม่ ความ

ได้เปรียบ-เสียเปรียบของผู้ใช้อากาศยานไร้คนขับกับผู้ถูกโจมตีเป็นไปโดยชอบด้วยกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่[929]

การใช้อากาศยานไร้คนขับเพื่อการโจมตีในการขัดกันทางอาวุธคือเรื่องการกำหนดเป้าหมายในการโจมตี ว่าจะแยกแยะเป้าหมายอย่างไรระหว่างพลเรือนและทหาร และจะสอดคล้องต่อหลักความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตีอย่างไร[930] นอกจากนั้นปัญหาจะยิ่งเกิดมากขึ้นในกรณีการขัดกันทางอาวุธที่ไม่มีลักษณะระหว่างประเทศ เช่น การใช้งานอากาศยานไร้คนขับของกลุ่มกองกำลังที่มิใช่รัฐเพราะการระบุสถานะการใช้งานเทคโนโลยีอากาศยานไร้คนขับว่าเป็นของกลุ่มกองกำลังที่ไม่ใช่รัฐเป็นเรื่องที่ยาก ยิ่งไปกว่านั้น ยังต้องพิจารณาสถานะของกลุ่มกองกำลังนั้นว่าเป็นกลุ่มกองกำลังที่ต่อสู้กับรัฐได้หรือไม่ด้วย[931]

ในการโจมตีพลเรือนด้วยการใช้อากาศยานไร้คนขับก็จะต้องอยู่ภายใต้ขอบเขตของกฎหมายมนุษยธรรมระหว่างประเทศเช่นกัน คือพลเรือนที่จะถูกโจมตีได้จะต้องเป็นพลเรือนที่มีส่วนร่วมด้วยโดยตรงในการสู้รบ (Direct participation in hostilities) เท่านั้น[932]

ปัญหาประการสำคัญคือการใช้งานอากาศยานไร้คนขับก่อให้เกิดลักษณะของความได้เปรียบ-เสียเปรียบแตกต่างกันอย่างมากระหว่างผู้โจมตีและผู้ถูกโจมตี ลักษณะดังกล่าวเป็นที่มาของคำว่าสงครามอสมมาตร (Asymmetric warfare) คือผู้โจมตีได้เปรียบผู้ถูกโจมตีในเรื่องความเสียหาย กล่าวคือผู้โจมตีมีความเสียหายน้อยกว่าผู้ถูกโจมตีในแง่การสูญเสียกำลังพล ซึ่งความได้เปรียบเสียปรียบดังกล่าวส่งผลต่อหลักความได้สัดส่วนในการโจมตีอย่างมีนัยสำคัญ แม้ว่าการใช้อากาศยานไร้คนขับดังกล่าวจะช่วยลดความสูญเสียทางด้านกำลังพลก็ตาม แต่เป็นการลดความสุญเสียทางด้านกำลังพลฝ่ายเดียวของผู้โจมตี แต่ผู้ถูกโจมตีที่ไม่สามารถเข้าถึงเทคโนโลยีดังกล่าวได้ หรือไม่สามารถเข้าถึงเทคโนโลยีการป้องกันตัวจากเทคโนโลยีดังกล่าวได้ย่อมมีความเสี่ยงต่อการสูญเสียทั้งกำลังพล พลเรือนและวัตถุสิ่งของ รวมถึงสถานที่

หลักความได้สัดส่วนที่มีการกล่าวถึงในสังคมระหว่างประเทศและนักวิชาการหลายฝ่าย มองว่าตามข้อ 51 ของพิธีสารฉบับที่ 1 เพิ่มเติมอนุสัญญาเจนีวาที่กำหนดว่า “The civilian … shall enjoy general protection against dangers arising from military operations. To give

[929] Erjan Hitaj, “Use of Drones and Global Security: Implications under International Law,”: 11.

[930] Ibid., p. 7.

[931] Ibid., p. 8.

[932] Nils Mezler, Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, (Geneva: ICRC, 2009) pp. 42-43

effect to this protection..."[933] การใช้กำลังทางทหารจึงต้องเป็นไปโดยหลักความจำเป็นและเกิดผลกระทบน้อยที่สุดต่อพลเรือน แต่หลายฝ่ายเห็นว่าการใช้อากาศยานไร้คนขับนั้นเป็นการควบคุมทางไกล มองผ่านกล้องที่ติดตั้งในอากาศยาน เปรียบเสมือนการเล่นเกมส์ ทำให้ความรู้สึกของผู้ปฏิบัติการโจมตีต่อความเสียหายที่เกิดขึ้นแตกต่างจากการสู้รบตามแบบปกติอย่างมาก คือรู้สึกถึงความเสียหายน้อยลง และจะทำให้โจมตีเกิดมากขึ้น แม้อาจเกิดปัญหาดังกล่าวแต่สังคมระหว่างประเทศยังมองว่าไม่ใช่เรื่องสำคัญ สิ่งสำคัญมากกว่าคือความรับผิดชอบตามกฎหมายของผู้ปฏิบัติการโจมตีด้วยอากาศยานไร้คนขับ[934]

นอกเหนือจากปัญหาสำคัญ 2 ประการที่กล่าวมาแล้ว การใช้อากาศยานไร้คนขับยังมีปัญหาทางกฎหมายเรื่องการแยกแยะเป้าหมาย เนื่องจากพบว่าในหลายกรณีที่มีการโจมตีด้วยอากาศยานไร้คนขับนั้น มักเกิดความเสียหายเกินขอบเขตเป้าหมายทางการทหาร มีความเสียหายเกิดขึ้นกับพลเรือนในปริมาณมาก การปฏิบัติการดังกล่าวจึงมีลักษณะของการไม่แยกแยะเป้าหมายซึ่งขัดต่อหลักสิทธิมนุษยชน[935]

ข้อท้าทายเกี่ยวกับการโจมตีด้วยอากาศยานไร้คนขับประการหนึ่งที่น่าสนใจคือลักษณะของความเป็น Anonymous ของการใช้งานอากาศยานตัวอย่างของกรณีที่อากาศยานไร้คนขับกว่า 20 ลำเข้าโจมตีอาคารพลเรือนในเมืองเคียฟ ประเทศยูเครนในความขัดแย้งระหว่างยูเครนและรัสเซียเมื่อวันที่ 31 พฤษภาคม พ.ศ. 2566 เป็นเหตุให้มีผู้เสียชีวิต 1 รายและบาดเจ็บ 3 ราย แม้จะปรากฏว่าเป็นการโจมตีด้วยอากาศยานไร้คนขับแบบพลีชีพ (Kamikaze Drone) ร่วมกับการใช้ขีปนาวุธแบบทิ้งตัว (Ballistic Missiles) ซึ่งเป็นการโจมตีตามแบบปกติ[936] แต่การใช้ขีปนาวุธนั้นย่อมถูกจำแนกว่าเป็นการใช้กำลังของกองทัพทหารได้ง่ายกว่าเนื่องจากการใช้งานขีปนาวุธโดยพลเรือนเป็นไปไม่ได้ ในขณะที่อากาศยานไร้คนขับนั้นพลเรือนอาจเป็นผู้ใช้งานได้ การปฏิเสธความรับผิดชอบโดยกองกำลังทหารหรือรัฐบาลอาจเกิดขึ้นได้จากลักษณะการใช้งานเทคโนโลยีร่วมกันทั้งทหารและพลเรือนดังกล่าว

กฎหมายมนุษยธรรมระหว่างประเทศจะถูกนำมาปรับใช้เมื่อเกิดการขัดกันทางอาวุธ ซึ่งช่วงเวลาดังกล่าวกฎหมายสิทธิมนุษยชนบางประการอาจไม่สามารถใช้เพื่อคุ้มครองบุคคลได้หรืออาจ

---

[933] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 51 (1).

[934] Report of the Special Rapporteur, para 84.

[935] Erjan Hitaj, "Use of Drones and Global Security: Implications under International Law," 12.

[936] Jaroslav Lukiv, "Ukraine war: Russian air strikes target Kyiv for third night running," BBC News, (May 31, 2023) Accessed June 2, 2023. Available from: https://www.bbc.com/news/world-europe-65750745

ถูกจำกัด[937] หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศจึงเกิดขึ้นเพื่อสร้างดุลภาพแก่แนวคิดสองประการ คือ การคุ้มครองความเป็นมนุษย์ (Humanity) และความจำเป็นทางการทหาร (Military Necessity) ในการขัดกันทางอาวุธที่จะต้องอยู่ภายใต้ข้อจำกัด[938] เพื่อไม่ให้การขัดกันทางอาวุธก่อให้เกิดความเสียหายมากเกินความจำเป็น หลักการนี้ปรากฏในกฎเกณฑ์พื้นฐานข้อ 35 ของพิธีสารเพิ่มเติมฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ. 1949 โดยกำหนดให้คู่พิพาทในการขัดกันทางอาวุธจะต้องจำกัดวิธีการ (Methods) และปัจจัย (Means) ในการทำสงคราม[939] ภายใต้หลักการดังกล่าวการใช้กำลังในการขัดกันทางอาวุธย่อมทำได้หากเป็นไปโดยสอดคล้องกับหลักเกณฑ์ดังต่อไปนี้

4.2.3 ข้อท้าทายต่อหลักการแยกแยะเป้าหมายทางทหารและพลเรือน

ข้อ 51 ของพิธีสารฉบับที่ 1 เพื่อเพิ่มเติมอนุสัญญาเจนีวาระบุว่า “The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations...”[940] ดังนั้นในปฏิบัติการทางทหารเพื่อการรบจึงต้องแยกพลเรือนออกจากเป้าหมายการโจมตีด้วย

กฎหมายมนุษยธรรมระหว่างประเทศแบ่งบุคคลในการสู้รบออกเป็น 2 กลุ่ม คือ พลเรือนและพลรบ โดยพลรบเท่านั้นที่จะตกเป็นเป้าหมายหลักในการโจมตี แต่พลเรือนย่อมได้รับความคุ้มครองตามกฎหมาย อย่างไรก็ดี ข้อยกเว้นอาจเกิดขึ้นในบางกรณีที่การจำแนกระหว่างพลเรือนและพลรบอาจทำได้ยากขึ้น เช่นการโจมตีค่ายทหารซึ่งอยู่ใกล้กับพื้นที่ชุมชนหรือการทำลายสาธารณูปโภคทางการทหารที่อาจส่งผลต่อพลเรือน ดังนั้นประเด็นในการพิจารณาการใช้เทคโนโลยีใหม่เพื่อการขัดกันทางอาวุธจึงได้แก่สาระสำคัญดังต่อไปนี้

---

[937] Jean Pictet, Humanitarian Law and the Protection of War Victims, p.15.

[938] Ibid, p. 28.

[939] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 35, “1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.”

[940] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 51 (1).

4.2.3.1 การแยกแยะสถานะพลรบ

การพิจารณาสถานะพลรบซึ่งเกิดจากการใช้เทคโนโลยีใหม่จะเกิดขึ้นกับกรณีการใช้งานระบบไซเบอร์ซึ่งไม่สามารถใช้หลักการพื้นฐานของกฎหมายว่าด้วยการขัดกันทางอาวุธได้ เนื่องจากในขณะปฏิบัติการนั้นจะไม่พบการสวมเครื่องแบบและการถืออาวุธของผู้ปฏิบัติการณ์ กิจกรรมทั้งหมดจะอยู่บนเครือข่ายการทำงานของคอมพิวเตอร์ การพิจารณาสถานะพลรบเพื่อการโจมตีตอบโต้จึงอาจกระทำได้โดยการตรวจสอบข้อมูลว่าการสั่งการดังกล่าวมาจากคอมพิวเตอร์ของหน่วยงานทหารหรือกองกำลังอื่นหรือไม่ ซึ่งส่งผลต่อการตอบโต้อย่างทันท่วงทีที่ไม่สามารถดำเนินได้[941]

นอกจากนั้นระบบการทำงานของเทคโนโลยีไซเบอร์ซึ่งอยู่บนพื้นฐานของทรัพยากรที่ใช้ร่วมกันระหว่างทหารและพลเรือนยังเป็นการยากต่อการจำแนกเป้าหมายในการโจมตี แม้ว่าทางเทคนิคนั้นการโจมตีทางไซเบอร์เป็นการเฉพาะอาจกระทำได้ก็ตามแต่เป็นเรื่องที่ค่อนข้างยาก ในสถานการณ์การโจมตีทางไซเบอร์หลายครั้งจึงเกิดผลกระทบต่อทั้งทรัพยากรและข้อมูลของทหารและพลเรือนไปพร้อมกัน

4.2.3.2 ข้อท้าทายลักษณะการมีส่วนร่วมของพลเรือนในการสู้รบ

การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นย่อมก่อให้เกิดปัญหาว่าจะพิจารณาการเข้าร่วมการสู้รบของพลเรือนอย่างไรด้วย เช่น การใช้ระบบไซเบอร์เพื่อการโจมตี หากเกิดจากการกระทำของพลเรือนที่รักชาติและต้องการสู้เพื่อประเทศตนโดยไม่สังกัดกองทัพ จะถือว่าพลเรือนรายดังกล่าวตกอยู่ในสถานะใด และจะจำแนกอย่างไรในขณะกระทำการ หากมีการจับกุมพลเรือนซึ่งกระทำการดังกล่าวได้โดยรัฐฝ่ายตรงข้าม พลเรือนนั้นจะอยู่ในสถานะเชลยศึกหรือไม่[942]

ปัญหาดังกล่าวนี้ย่อมจะเป็นประเด็นเมื่อพลเรือนทำการบังคับหุ่นยนต์สังหารหรืออากาศยานไร้คนขับเพื่อทำการต่อสู้กับรัฐคู่พิพาทเช่นเดียวกัน แม้ว่าการควบคุมจักรกลจะมีสภาพทางกายภาพที่ชัดเจนกว่าการใช้งานระบบไซเบอร์ แต่การตอบโต้กลับของรัฐคู่พิพาทย่อมกระทำได้ยากขึ้น และเมื่อมีการจับกุมพลเรือนที่ใช้เทคโนโลยีดังกล่าวย่อมนำมาซึ่งปัญหาในการจำแนกสถานะพลเรือนดังกล่าวเช่นเดียวกัน

---

[941] Jean Pictet, Humanitarian Law and the Protection of War Victims, p.15.

[942] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

4.2.3.3 ปัญหาการพิจารณาตัวตนของผู้มีส่วนร่วมโดยตรงในการสู้รบ

เทคโนโลยีใหม่ที่ใช้ในการขัดกันทางอาวุธในปัจจุบันที่จะก่อให้เกิดปัญหาในการพิจารณาตัวตนของผู้กระทำในการสงครามคือการใช้ระบบปฏิบัติการไซเบอร์ และการใช้งานของระบบอัลกอริที่มของซอฟท์แวร์ที่สามารถตัดสินใจด้วยตนเองได้ โดยการมีการใช้งานระบบอัลกอริที่มทั้งผ่านการทำงานของปฏิบัติการทางไซเบอร์หรือผ่านระบบอาวุธที่ตัดสินใจได้ด้วยตนเอง การกระทำการจะมิใช่การกระทำการของพลรบซึ่งเป็นมนุษย์ต่อพลรบซึ่งเป็นมนุษย์ แต่อาจเป็นการตัดสินใจของระบบประมวลผลต่อมนุษย์ หรือระบบประมวลผลต่อระบบประมวลผล เช่น หากมีการโจมตีทางไซเบอร์ต่อระบบปฏิบัติการทางไซเบอร์ของคู่กรณีในการขัดกันทางอาวุธโดยระบบตอบโต้อัตโนมัติ ซึ่งการโจมตีดังกล่าวไม่เกี่ยวข้องกับปฏิบัติการของมนุษย์เลย หรือการใช้ระบบอาวุธที่ตัดสินใจได้ด้วยตนเองโจมตีระบบอาวุธที่ตัดสินใจได้ด้วยตนเองของคู่กรณีในการขัดกันทางอาวุธ ปัญหาในการพิจารณาการมีส่วนร่วมโดยตรงในการสู้รบย่อมเกิดขึ้น โดยหากการปฏิบัติการนั้นเกิดขึ้นโดยเทคโนโลยีเองซึ่งไม่ต้องอาศัยการสั่งงานจากมนุษย์ จะถือว่าเทคโนโลยีดังกล่าวเป็นผู้มีส่วนร่วมโดยตรงในการสู้รบ หรือจะต้องคำนึงถึงบุคคลที่เป็นมนุษย์ผู้มีส่วนร่วมกับการใช้ ออกแบบ หรือประดิษฐ์เทคโนโลยีดังกล่าวหรือไม่ อย่างไร[943]

การปฏิบัติต่อเป้าหมายกับเทคโนโลยีใหม่เป็นการพิจารณาหลักการกระทำที่เป็นปฏิปักษ์ (Conduct of Hostilities) ซึ่งเป็นปฏิบัติการทางทหารกับปัญหาที่อาจเกิดขึ้นจากการใช้เทคโนโลยีใหม่ โดยมีพื้นฐานสำคัญของกฎเกณฑ์ว่าด้วยการขัดกันทางอาวุธที่จะต้องเคารพได้แก่ หลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการโจมตี และหลักความระมัดระวังในการโจมตี[944] ซึ่งปรากฏรายละเอียดการศึกษาวิเคราะห์ดังนี้

หลักการแยกแยะเป้าหมายได้มีการบัญญัติเอาไว้ในข้อ 48 ข้อ 51 (4), (5) และข้อ 52 (2) ของพิธีสารฉบับที่ 1 ค.ศ. 1977 แห่งอนุสัญญาเจนีวา ค.ศ. 1949 โดยเป็นข้อห้ามการใช้กำลังทางทหารเพื่อโจมตีพลเรือนโดยตรง และหลักเกณฑ์ข้อนี้สอดคล้องกับหลักเกณฑ์ ข้อ 8 (2) (b) (ii) “...War crime of intentionally directing attacks against the civilian objects...” ของธรรมนูญศาลยุติธรรมระหว่างประเทศกล่าวคือการกระทำโดยเจตนาเพื่อโจมตีต่อพลเรือนโดยตรง โดยมิใช่เป้าหมายทางการทหาร การกระทำนั้นย่อมเป็นความผิดฐานอาชญากรรมสงคราม[945] หลักการนี้ได้มี

---

[943] International Committee of the Red Cross. “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.” International Committee of the Red Cross. Paper, June 6, 2019, p. 6.

[944] Jean Pictet, Humanitarian Law and the Protection of War Victims, p.15.

[945] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.25.

การกล่าวอ้างถึงในคดีสำคัญ เช่น คดี 1996 Legality of the Threats or Use of Nuclear Weapons โดยในความเห็นเชิงแนะนำของศาลยุติธรรมระหว่างประเทศให้ทัศนะว่า เป็นหลักจารีตประเพณีระหว่างประเทศที่จะล่วงละเมิดมิได้ (intransgressible principles of international law)[946] ทั้งนี้ เป้าหมายทางการทหารย่อมหมายถึง เป้าหมายซึ่งโดยสภาพ ที่ตั้ง วัตถุประสงค์ หรือการใช้งานเป็นไปเพื่อประสิทธิภาพในการปฏิบัติงานทางทหาร ซึ่งจะต้องถูกแยกออกมาเป็นลักษณะเฉพาะเพื่อประโยชน์ทางการทหารเท่านั้น[947]

นอกเหนือจากการกำหนดเรื่องการคุ้มครองเป้าหมายที่เกี่ยวกับทรัพย์สินพลเรือนแล้ว การคุ้มครองร่างกายพลเรือนยังแสดงผ่านหลักการแยกพลรบออกจากพลเรือนตามอนุสัญญาเจนีวา ค.ศ.1949 3 ฉบับแรก โดยพลรบที่แบ่งแยกจากพลเรือนได้จะต้องมีเครื่องหมายกำหนดไว้เด่นชัดและเห็นได้ในระยะไกล ถืออาวุธโดยเปิดเผย และปฏิบัติการรบตามกฎและประเพณีสงคราม[948] ทั้งนี้เพื่อให้พลเรือนมีลักษณะแตกต่างจากพลรบ และพลเรือนจะไม่ตกเป็นเป้าหมายของการโจมตีนั่นเอง หลักเกณฑ์นี้ยังสอดคล้องกับข้อ 1 ของ 1907 Hague Regulation ด้วยเช่นกัน

หลักการแยกแยะเป้าหมายเป็นหลักการพื้นฐานสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศ โดยเป็นส่วนหนึ่งของหลักการกระทำอันเป็นปรปักษ์ซึ่งรวมถึงการใช้วิธี (methods) และปัจจัย (means) ในการขัดกันทางอาวุธ[949] ทั้งนี้ ปัจจัยย่อมหมายรวมถึงอาวุธที่ใช้ในการขัดกันทางอาวุธ และอุปกรณ์ที่เกี่ยวข้องกับการใช้งานอาวุธเหล่านั้น ส่วนวิธีการย่อมหมายความถึงการใช้อาวุธ และวิธีการในการใช้กำลังเพื่อการขัดกันทางอาวุธ[950] โดยนัยนี้ การกระทำไม่ว่าจะเป็นการใช้วิธีการหรือการใช้อาวุธใดๆ หากเป็นไปเพื่อประโยชน์ในการขัดกันทางอาวุธ และผู้ใช้วิธีการหรืออาวุธนั้นสังกัดอยู่ในกองทัพหรืออาจจำแนกได้ว่าเป็นผู้มีส่วนร่วมโดยตรงในการสู้รบ ย่อมถือว่าการกระทำนั้นๆ อยู่ในบังคับของกฎหมายมนุษยธรรมระหว่างประเทศด้วย

ปัญหาที่เกิดขึ้นในปัจจุบันคือการใช้งานสาธารณูปโภคขั้นพื้นฐาน เช่น การสื่อสารและการคมนาคมขนส่ง ทั้งทางการทหารและทางพลเรือนมักจะมีการใช้งานร่วมกัน (Dual-use facilities) จึงเกิดประเด็นว่า เป้าหมายทางการทหารมีความหมายครอบคลุมถึงพื้นที่ หรือการใช้งาน

---

[946] ICJ, 1996 Legality of the Threats or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, p.35.

[947] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.29.

[948] ปรากฏในข้อ 13 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 และฉบับที่ 2 และข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3

[949] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 1.

[950] Ibid.

ในลักษณะใด พบว่าในทางปฏิบัตินั้น คู่มือในการปฏิบัติการทางทหารของหลายประเทศได้ทำการจำแนกเป้าหมายทางการทหารโดยพิจารณาจากรูปแบบการใช้งานว่าเป็นไปเพื่อการทหารมากน้อยเพียงไรเป็นสำคัญ หากมีการใช้งานการสื่อสาร หรือช่องทางการคมนาคมใดเพื่อประโยชน์ทางการทหารเป็นสำคัญ ย่อมอาจจำแนกได้ว่าพื้นที่ หรือช่องทางดังกล่าวคือเป้าหมายทางการทหารด้วยเช่นกัน[951]

ในปัจจุบันปรากฏการใช้เทคโนโลยีเพื่อประโยชน์ในการขัดกันทางอาวุธมากขึ้น โดยเฉพาะอย่างยิ่งการใช้ระบบไซเบอร์เพื่อการโจมตี การใช้ระบบสื่อสารผ่านดาวเทียมเพื่อประโยชน์ในการระบุตำแหน่งเป้าหมายการโจมตี และการใช้ระบบประมวลผลของอาวุธที่สามารถตัดสินใจทำลายเป้าหมายได้ด้วยตนเอง ซึ่งนำไปสู่ข้อพิจารณาถึงการนำกฎหมายมนุษยธรรมระหว่างประเทศในส่วนที่เกี่ยวข้องกับการพิจารณาการกระทำอันเป็นปรปักษ์ โดยเฉพาะเรื่องการแยกแยะเป้าหมายในการโจมตีว่ากฎหมายมนุษยธรรมระหว่างประเทศจะสามารถคุ้มครองบุคคลที่ไม่มีส่วนเกี่ยวข้องโดยตรงกับการสู้รบได้อย่างไร เนื่องจากเทคโนโลยีที่มีการใช้ในปัจจุบันนี้ปรากฏในลักษณะการใช้งานทั้งทางการทหารและเพื่อวัตถุประสงค์ของพลเรือน จึงจำเป็นต้องมีการพิจารณาถึงเงื่อนไขในการปรับใช้กฎหมายในกรณีต่างๆ อย่างชัดเจนมากขึ้น

ขณะที่เป้าหมายพลเรือน หมายถึง พื้นที่ทั่วไปที่พลเรือนใช้ประโยชน์ เมือง หมู่บ้าน ที่พักอาศัย อาคาร บ้าน โรงเรียน โรงพยาบาล ศาสนสถาน อนุสาวรีย์ รวมถึงทรัพย์สินทางวัฒนธรรมและสิ่งแวดล้อมทางธรรมชาติ[952] อย่างไรก็ดี หากเป้าหมายพลเรือนถูกนำไปใช้เพื่อประโยชน์ทางการทหารเพื่อการขัดกันทางอาวุธ เป้าหมายพลเรือนดังกล่าวย่อมไม่ได้รับความคุ้มครองตามหลักการนี้อีกต่อไป เว้นเสียแต่ในกรณีที่เกิดความไม่ชัดเจนว่าสถานที่ของพลเรือนนั้นถูกใช้เพื่อประโยชน์ทางการทหารหรือไม่ พื้นที่ดังกล่าวจะได้รับความคุ้มครองตามหลักบทสันนิษฐานว่าเป็นเป้าหมายทางพลเรือน[953] จึงยังคงได้รับความคุ้มครองตามกฎหมาย

นอกเหนือจากการกำหนดเรื่องการคุ้มครองเป้าหมายที่เกี่ยวกับทรัพย์สินพลเรือนแล้ว การคุ้มครองร่างกายพลเรือนยังแสดงผ่านหลักการแยกพลรบออกจากพลเรือนตามอนุสัญญาเจนีวา ค.ศ.1949 3 ฉบับแรก โดยพลรบที่แบ่งแยกจากพลเรือนได้จะต้องมีเครื่องหมายกำหนดไว้เด่นชัด

---

[951] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 32.

[952] Ibid., p.34.

[953] Ibid., p.35

และเห็นได้ในระยะไกล ถืออาวุธโดยเปิดเผย และปฏิบัติการรบตามกฎและประเพณีสงคราม[954] ทั้งนี้เพื่อให้พลเรือนมีลักษณะแตกต่างจากพลรบ และพลเรือนจะไม่ตกเป็นเป้าหมายของการโจมตีนั่นเอง นอกจากนี้หลักเกณฑ์การแยกแยะนี้ยังสอดคล้องกับข้อ 1 ของ Hague Regulation ค.ศ. 1907 ด้วยเช่นกัน

หลักการแยกแยะตามกฎหมายมนุษยธรรมระหว่างประเทศซึ่งปรับใช้แก่การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธอาจเกิดขึ้นได้ในทั้ง 2 มิติ คือ ทั้งในแง่ของการจำกัดปัจจัยและวิธีการในการสู้รบ โดยอาจแบ่งพิจารณาได้ดังนี้

1) การจำกัดปัจจัยในการสู้รบ ข้อพิจารณาเบื้องต้นคือปัจจัยในการสู้รบซึ่งรวมถึงอาวุธนี้ ตามหลักกฎหมายมนุษยธรรมระหว่างประเทศอาจจำแนกได้เป็น 2 รูปแบบ คือ อาวุธทั่วไปที่ถูกนำไปใช้ทำลายเป้าหมายโดยไม่จำกัด (ขึ้นอยู่กับการใช้งานของผู้ใช้) และอาวุธที่โดยสภาพนั้นเป็นการออกแบบมาเพื่อการทำลายเป้าหมายอย่างแบ่งแยกไม่ได้ ซึ่งอาวุธที่ต้องห้ามใช้ คืออาวุธที่ถูกออกแบบมาโดยไม่สามารถจำกัดการทำลายเป้าหมายได้[955] หรืออาวุธที่ไม่ชอบด้วยกฎหมายโดยสภาพ (Unlawful per se)[956] เท่านั้น ไม่รวมไปถึงอาวุธที่เกิดจากการใช้งานโดยไม่จำกัดเป้าหมายโดยตัวผู้ใช้งานเอง

เทคโนโลยีใหม่ซึ่งถูกนำมาใช้ในการขัดกันทางอาวุธบางประการไม่สามารถจำกัดเป้าหมายการโจมตีได้ ในขณะที่บางเทคโนโลยีสามารถจำกัดเป้าหมายได้ ตัวอย่างเทคโนโลยีทางไซเบอร์ที่ใช้เป็นอาวุธ เช่น สตักซ์เน็ต (Stuxnet) ซึ่งถูกออกแบบมาเพื่อการทำลายระบบปฏิบัติการของโรงงานคัดแยกยูเรเนียมทั้งนี้แม้สตักเน็ตจะสามารถแพร่กระจายสู่ระบบไซเบอร์ของพลเรือนได้ แต่ก็ไม่สร้างความเสียหายแก่พลเรือน จึงถือว่าเป็นอาวุธที่แบ่งแยกเป้าหมายได้โดยสภาพ แต่หากเป็นการใช้มัลแวร์ เช่น ไวรัส โทรจัน หรือหนอนคอมพิวเตอร์ ซึ่งสามารถสร้างความเสียหายให้กับระบบปฏิบัติการคอมพิวเตอร์ทุกระบบ ย่อมถือว่าเป็นอาวุธที่ถูกออกแบบมาให้ไม่สามารถแยกแยะเป้าหมายในการโจมตีได้[957]

---

[954] ปรากฏในข้อ 13 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 1 และฉบับที่ 2 และข้อ 4 ของอนุสัญญาเจนีวา ค.ศ.1949 ฉบับที่ 3

[955] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p 62.

[956] Dissenting Opinion of Judge Higgins in ICJ, (1996), Advisory Opinion on the Legality of Threat or Use of Nuclear Weapons, p. 588-9.

[957] อุบลวรรณ ภีระเป็ง, การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ: ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2558, หน้า 151.

ระบบปฏิบัติการทางไซเบอร์นี้บางครั้งก็มีสถานะเป็นทั้งวิธีการและปัจจัยในตัวเอง เช่น การใช้วิธีการ DDOS (Distributed Denial of Service)[958] ซึ่งผู้ใช้วิธีการ DDOS นี้จะทำการส่งโทรจันซึ่งอยู่ในโปรแกรมคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ต่างๆ โดยเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมที่มีโทรจันนี้โดยไม่รู้ตัวจะตกอยู่ในสภาวะของการเป็นเครื่องคอมพิวเตอร์ซอมบี้ เพื่อรอการสั่งงานจากผู้ออกคำสั่ง เมื่อถึงเวลาหรือเงื่อนไขที่โทรจันถูกกำหนดไว้ เครื่องคอมพิวเตอร์ทุกเครื่องที่ถูกฝังการทำงานของโทรจันจะทำหน้าที่ในการโจมตีระบบการสื่อสารของเป้าหมายพร้อมกันทันที วิธีการ DDOS ในส่วนของการติดตั้งโทรจันในคอมพิวเตอร์ไม่มีการแยกแยะระหว่างเป้าหมายพลเรือนและเป้าหมายทหาร แต่เมื่อมีการสั่งการโจมตีอาจระบุเป้าหมายในการโจมตีได้

นอกเหนือจากการใช้ระบบไซเบอร์เพื่อการโจมตีแล้ว การใช้ระบบอาวุธที่สามารถตัดสินใจได้ด้วยตนเอง (Autonomous Weapons System) ยังถือเป็นการใช้อาวุธซึ่งจะต้องตกอยู่ภายใต้หลักเกณฑ์การแยกแยะด้วย เช่น การใช้หุ่นยนต์สังหารอัตโนมัติที่สามารถค้นหาเป้าหมายเพื่อการทำลาย หรือการใช้ระบบปฏิบัติการตอบโต้การโจมตีทางขีปนาวุธ ฯลฯ จะต้องใช้กับเป้าหมายทางการทหารเท่านั้น

2) การจำกัดวิธีการในการสู้รบ - เทคโนโลยีใหม่ที่ถูกนำมาใช้เป็นวิธีการในการสู้รบปรากฏในหลายรูปแบบด้วยกัน เช่น การใช้ระบบการกำหนดพิกัดบนพื้นโลก (Global Positioning System: GPS) เพื่อประกอบกับการใช้ขีปนาวุธโจมตี หรือการใช้ประกอบยานพาหนะไร้คนขับ (Unmanned Vehicle System)[959] ข้อพิจารณาสำคัญคือการใช้ระบบกำหนดพิกัดบนพื้นโลกนี้จะส่งผลกระทบต่อพลเรือนอย่างไร หรือไม่ หากการใช้เทคโนโลยีดังกล่าวมีเป้าหมายทางการทหารแต่ปฏิบัติการจะต้องเกิดขึ้นกับเครือข่ายการสื่อสารของพลเรือน โดยไม่ก่อให้เกิดผลกระทบต่อพลเรือนย่อมไม่เป็นการขัดต่อหลักกฎหมายมนุษยธรรมระหว่างประเทศ หากการใช้ระบบดังกล่าวส่งผลกระทบต่อข้อมูลข่าวสาร และการสื่อสารของพลเรือน ซึ่งเป็นผลกระทบต่อสาธารณูปโภคขั้นพื้นฐานย่อมเป็นการขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศ

เทคโนโลยีนาโน เช่น เทคโนโลยี Stealth (เทคโนโลยีที่ลดโอกาสที่ศัตรูจะมองเห็นโดยการใช้วัสดุที่ตรวจจับไม่ได้จากรังสี คลื่นความร้อน หรือเรดาร์) ทั้งนี้รวมตลอดถึงการใช้

[958] William Boothby, “Some legal challenges posed by remote attack,” International Humanitarian Law and the protection of civilians,” International Review of the Red Cross, Volume 94 Number 886, (2012), p. 580.

[959] Duncan Blake, “The Law Applicable to Military Strategic Use of Outer Space,” p. 105.

เครื่องหมายพรางตา (camouflage)[960] ได้รับการพัฒนามาถึงระดับที่สามารถใช้ในการออกแบบยานพาหนะได้ เช่น เครื่องบินรบ และโดรนลาดตระเวน โดยในปัจจุบันมีความพยายามในการออกแบบเครื่องแบบทหารที่พรางตาจนไม่สามารถมองเห็นได้ และอาวุธที่ถูกพรางจนล่องหนได้ (Cloaked weapons)[961] ซึ่งประเด็นที่น่าสนใจคือปัญหาเกี่ยวกับการจำแนกระหว่างพลเรือนและพลรบในกรณีที่มีการใช้เครื่องแบบพรางตาล่องหน หรืออาวุธล่องหนว่าจะมีผลกระทบทางกฎหมายอย่างไรหรือไม่ เนื่องด้วยธรรมเนียมการทำสู้รบที่จะต้องสวมเครื่องแบบทหารและการถืออาวุธอย่างเปิดเผย เป็นเกณฑ์พื้นฐานในการแยกแยะระหว่างพลเรือนและพลรบ เพื่อไม่ให้พลเรือนตกเป็นเป้าหมายของการโจมตี การใช้เทคโนโลยีการพรางตัวดังกล่าวย่อมจะต้องสอดคล้องกับหลักการแยกแยะนี้ด้วย อย่างไรก็ดี อาจพิจารณาได้ว่าการพรางเครื่องแบบย่อมไม่ถือเป็นการขัดต่อกฎหมายมนุษยธรรมระหว่างประเทศ เพราะประเด็นสำคัญในเรื่องเครื่องแบบคือการมีไว้เพื่อแบ่งระหว่างพลเรือนและพลรบระหว่างการสู้รบ แต่ไม่มีข้อกฎหมายระบุว่าจะพลรบจะต้องเปิดเผยตัวชัดเจน[962] จึงปรากฏการใช้เครื่องแบบทหารที่มีลายพราง ดังนั้น หากการพรางเครื่องแบบจะทำให้ทหารล่องหนได้ก็ย่อมไม่ขัดต่อหลักกฎหมายว่าด้วยการขัดกันทางอาวุธ หากเครื่องแบบดังกล่าวมิได้ก่อให้เกิดความสับสนระหว่างพลเรือนและพลรบ หรือการใส่เครื่องแบบนั้นไม่ได้ทำให้ทหารกลายเป็นพลเรือน ย่อมไม่ถือเป็นการขัดต่อหลักกฎหมาย ในขณะที่การพรางอาวุธเป็นประเด็นที่น่าพิจารณาว่าจะส่งผลต่อหลักการพื้นฐานนี้หรือไม่ เพราะการไม่ปรากฏอาวุธในมือพลรบย่อมนำไปสู่ความเข้าใจผิดแก่ทหารฝ่ายตรงข้ามซึ่งจะไม่ทำการโจมตีเพราะไม่เห็นว่าศัตรูตนมีอาวุธ อาจนำไปสู่ความเสียเปรียบทางการรบที่ทหารฝ่ายไม่โจมตีนั้นจะถูกโจมตีเสียเอง อนึ่ง การพิจารณาเรื่องการถืออาวุธโดยเปิดเผยนี้จะต้องขึ้นอยู่กับลักษณะโดยสภาพของอาวุธและภาวะแวดล้อมขณะที่มีการสู้รบนั้นด้วย[963] เช่น การใช้อาวุธประจำกายที่เป็นปืนสั้นอาจไม่เห็นอย่างชัดเจนในการรบด้วยลักษณะของขนาดอาวุธเอง ในขณะที่การรบในเวลากลางคืนนั้นย่อมเป็นการยากที่จะสังเกตอาวุธประจำกายแม้จะเป็นปืนเล็กยาวประจำกายพลรบก็ตาม การถืออาวุธโดยเปิดเผยจึงมิได้หมายถึงการถืออาวุธตลอดเวลา แต่การถืออาวุธที่ทำให้ไม่สามารถเห็นได้โดยการใช้เทคโนโลยีออกแบบอาวุธนั้น ย่อมไม่สอดคล้องกับบริบททั้งสองที่ได้กล่าวมา

[960] Hitoshi Nasu, "Nanotechnology and the law of armed conflict," in Hitoshi Nasu and Robert McLaughlin, eds., New Technologies and the Law of Armed Conflict, p. 152.

[961] Ibid., p. 154.

[962] Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict, p. 44.

[963] Ibid., p. 45.

อย่างไรก็ดี ข้อกฎหมายที่น่าพิจารณาในกรณีการพรางอาวุธประจำกายของทหารนี้ คือตามข้อ 37 ของพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ.1977 ของอนุสัญญาเจนีวา ในเรื่องการห้ามล่อลวงจะสามารถนำมาปรับใช้แก่กรณีนี้เพียงใด สาระสำคัญของกฎหมายข้อนี้ต้องการแยกแยะระหว่างบุคคลที่ได้รับความคุ้มครองตามกฎหมายและพลรบที่ทำหน้าที่ตามกฎหมายซึ่งตกเป็นเป้าหมายในการโจมตีได้ โดยสังเกตได้จากข้อกฎหมายที่กำหนดว่า "...Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence..."[964] หรือการกระทำที่ชักชวนให้ฝ่ายปฏิปักษ์เกิดความวางใจอันชักนำไปสู่ความเชื่อว่าตนมีสิทธิได้รับหรือมีพันธกรณีที่ต้องให้ความคุ้มครองภายใต้กฎหมายระหว่างประเทศว่าด้วยการขัดกันทางอาวุธ หากการพรางอาวุธไม่ทำให้ฝ่ายปฏิปักษ์เข้าใจว่าทหารที่พรางอาวุธนั้นเป็นบุคคลที่ได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ การพรางอาวุธเช่นว่าย่อมไม่เป็นการกระทำที่ละเมิดต่อหลักการห้ามล่อลวง (Perfidy) เพราะการที่ทหารไม่ถืออาวุธไม่ได้ทำให้ทหารคนดังกล่าวเปลี่ยนสถานะเป็นพลเรือนแต่อย่างใด

ข้อท้าทายบางประการต่อหลักการแยกแยะตามกฎหมายมนุษยธรรมระหว่างประเทศจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธอาจเกิดขึ้นด้วยเหตุที่การพัฒนาทางด้านเทคโนโลยีทางการทหารมีการพัฒนาอยู่เสมอและหลากหลายรูปแบบ การระบุถึงข้อพิจารณาหรือข้อท้าทายที่จะครอบคลุมในทุกกรณีจึงไม่สามารถทำได้ ข้อท้าทายของการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธจึงอาจนำเสนอได้ในบางประการ ดังต่อไปนี้

1) ข้อท้าทายต่อการแยกแยะระหว่างพลเรือนและพลรบและการมีส่วนร่วมโดยตรงในการสู้รบ

จากหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศซึ่งยอมรับให้เป้าหมายทางการทหารถือว่าเป็นเป้าหมายที่ชอบด้วยกฎหมาย[965] ส่วนเป้าหมายที่เป็นพลเรือนหรือทรัพย์สินสิ่งของของพลเรือนนั้นจะได้รับความคุ้มครองเสมอ เว้นเสียแต่ว่าพลเรือนดังกล่าวจะมีส่วนร่วมในการสู้รบโดยตรง (Direct participation) ปัญหาที่ท้าทายอย่างยิ่งคือการใช้งานระบบไซเบอร์ที่พลเรือนและทหารสามารถเข้าถึงข้อมูลข่าวสารต่างๆ ได้ในช่องทางเดียวกัน การแยกแยะระหว่าง

---

[964] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 37.

[965] Gabriella Blum and Philip Heymann, "Law and Policy of Targeted Killing", Harvard National Security Journal, Vol. 1 June 27, 2010: 146.

ปฏิบัติการทางทหารและการกระทำเฉพาะตัวของพลเรือนในการขัดกันทางอาวุธ แม้จะสามารถกระทำได้แต่จะก่อให้เกิดความยุ่งยากมากขึ้นในการโจมตีตอบโต้ เช่นหากพลเรือนที่ไม่ได้สังกัดในกองทัพ และไม่มีความเกี่ยวข้องใดๆ กับกองทัพเลย ต้องการช่วยเหลือกองทัพชาติตนโดยการเข้าสู่ระบบปฏิบัติการทางคอมพิวเตอร์ของประเทศคู่พิพาทและทำการโจมตีฐานข้อมูลทางการทหารให้เกิดความเสียหาย กองทัพของรัฐที่ถูกโจมตีจะดำเนินการตามหลักการระมัดระวังล่วงหน้า (Precautionary) ในการตอบโต้กลับอย่างไร และกรณีเช่นนี้จะถือว่าพลเรือนดังกล่าวมีส่วนร่วมในการสู้รบโดยตรงหรือไม่ ความคลุมเครือดังกล่าวเป็นสิ่งที่จะต้องมีการพัฒนาแนวทางในการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อไปในอนาคต

เทคโนโลยีประการอื่นนั้นไม่อาจระบุได้ชัดเจนถึงปัญหาที่อาจเกิดขึ้นจากความคลุมเครือในการแยกแยะระหว่างการใช้งานของพลเรือนและพลรบ เพราะโดรนหรือหุ่นยนต์สังหารในทางการทหารนั้นมีความแตกต่างจากอุปกรณ์ชนิดเดียวกันที่พลเรือนใช้อยู่อย่างชัดเจน ทั้งโดยการออกแบบและลักษณะการใช้งาน ปัญหาการแยกแยะการใช้งานและการมีส่วนร่วมในการสู้รบโดยตรงจึงเกิดขึ้นกับระบบไซเบอร์เป็นสำคัญ

2) ข้อท้าทายต่อการแยกแยะเป้าหมายในการโจมตี

เนื่องจากเทคโนโลยีที่มีการนำมาใช้ในปัจจุบันมีลักษณะการใช้ที่คาบเกี่ยวกับพลเรือนและการทหาร คือมีลักษณะการใช้งานในสองทาง (Dual use) โดยเฉพาะอย่างยิ่งเทคโนโลยีสารสนเทศ ระบบการกำหนดตำแหน่งบนพื้นโลก[966] ทำให้เกิดข้อท้าทายหลายประการในการปรับใช้หลักการแยกแยะเป้าหมาย เป็นต้นว่า การโจมตีทางไซเบอร์นั้นจะไม่นำไปสู่ความเสียหายแก่ทรัพย์สินอื่นๆ ของพลเรือนคนอื่นซึ่งไม่มีส่วนเกี่ยวข้องในการสู้รบได้อย่างไร นอกจากนั้นปัญหาทางเทคนิคในการค้นหาและยืนยันเครื่องคอมพิวเตอร์ที่มีการสั่งการโจมตีในบางกรณียังอาจไม่สามารถกระทำได้โดยง่าย หากมีการสั่งงานผ่านเครือข่ายเครื่องคอมพิวเตอร์หลายเครื่องเช่น กรณีการใช้ปฏิบัติการ DDOS แม้ว่าในความเป็นจริงจะสามารถกระทำได้ก็ตาม

นอกจากนี้การใช้งานเครือข่ายไซเบอร์เพื่อการโจมตีนั้นอาจกระทบต่อโครงสร้างโดยรวมของทั้งพลเรือนและกองทัพ ปัญหาจึงเกิดขึ้นกับหลักการแบ่งแยกเป้าหมายในการโจมตีหากเกิดการใช้ระบบไซเบอร์เพื่อการปฏิบัติการทางทหาร ว่ารัฐจะสร้างมาตรการในการคุ้มครองสาธารณูปโภคขั้นพื้นฐานของพลเรือนอย่างไร ทั้งนี้รวมไปถึงเรื่องการให้ความคุ้มครองต่อฐานข้อมูล

[966] William Boothby, Weapons and the Law of Armed Conflict, p. 356.

ของพลเรือน ผลกระทบที่อาจเกิดสืบเนื่องจากความเสียหายของโครงสร้างพื้นฐานที่ถูกโจมตี เป็นต้น[967]

3) ข้อท้าทายต่อการควบคุมเทคโนโลยีใหม่ในฐานะเป็นวิธีการและปัจจัยใหม่ในการทำสงคราม

ภายใต้บทบัญญัติข้อ 36 แห่งพิธีสารเพิ่มเติมฉบับที่ 1 ของอนุสัญญาเจนีวา ได้กำหนดให้เป็นพันธกรณีของรัฐภาคีในการตัดสินว่าการใช้อาวุธหรือวิธีการหรือปัจจัยใหม่นั้น ในบางกรณีหรือทุกพฤติการณ์ จะถูกห้ามโดยพิธีสารฉบับนี้หรือกฎแห่งกฎหมายระหว่างประเทศอื่นๆ หรือไม่[968] ปรากฏว่าการปฏิบัติการให้เป็นไปตามพันธกรณีข้อนี้ยังเป็นเรื่องที่ทำได้ค่อนข้างยาก[969] โดยพบการสร้างระบบการทบทวนกฎหมายที่เกี่ยวข้องกับการพัฒนาอาวุธในบางประเทศเท่านั้น เช่น ประเทศออสเตรเลีย เบลเยี่ยม เนเธอร์แลนด์ สวีเดน นอร์เวย์ สหรัฐอเมริกา ฝรั่งเศส และสหราชอาณาจักร[970] อย่างไรก็ดี ในกรอบของกฎหมายระหว่างประเทศเกี่ยวกับการควบคุมอาวุธที่มีอานุภาพทำลายล้างสูงได้ก่อให้เกิดความร่วมมือในการควบคุมการนำเข้าส่งออกสินค้าที่อาจนำไปใช้ในการผลิตอาวุธที่มีอานุภาพทำลายล้างสูงได้ (Dual-use Item) ภายใต้กฎเกณฑ์ของสหภาพยุโรป ซึ่งมีผลต่อการค้าระหว่างประเทศต่างๆ ที่เชื่อมโยงกับภูมิภาคยุโรป และนำไปสู่การสร้างมาตรการในการควบคุมการนำเข้าส่งออกสินค้าตามกฎหมายภายในประเทศต่างๆ ต่อไป

4.2.3.4 ข้อท้าทายเรื่องการกระทำที่เป็นลักษณะ Levée en Masse

---

[967] International Committee of the Red Cross, International Humanitarian Law and the challenges of contemporary armed conflicts, (Geneva: International Committee of the Red Cross, 2015), p. 42-43.

[968] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 36 "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party"

[969] William Boothby, Weapons and the Law of Armed Conflict, p. 341.

[970] International Committee of the Red Cross, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, Measures to Implement Article 36 of Additional Protocol 1 of 1977, (Geneva: ICRC), January 2006. Note 8, p. 5.

การที่พลเรือนเข้าไปมีส่วนร่วมในการโจมตีทางไซเบอร์จะถือว่าเป็นการ “ลุกขึ้นสู้” Levée en Masse หรือไม่ และจะถือว่าพลเรือนดังกล่าวมีส่วนร่วมโดยตรงกับการรบหรือไม่ ประเด็นนี้มีผู้ศึกษาวิจัยเอาไว้คือ Buchan และ Tsagourias[971]

การพิจารณาเรื่องการมีส่วนร่วมในการรบเป็นเรื่องจำเป็นตามกฎหมายมนุษยธรรมระหว่างประเทศ เนื่องจากหากกองกำลัง “IT Army” ของยูเครนจัดเป็นพลรบ ก็จะเป็นผู้ที่มีส่วนร่วมโดยด้วยกฎหมายในการขัดกันทางอาวุธ (Lawfully participate in Armed Conflict) คือสามารถใช้อาวุธได้ ตกเป็นเป้าหมายในการโจมตีได้ และหากถูกจับตัวโดยฝ่ายตรงข้ามย่อมได้รับความคุ้มครองในสถานะเชลยศึก แต่หากจำแนกว่ากองทัพดังกล่าวเป็นพลเรือน ย่อมได้รับความคุ้มครองตราบเท่าที่ไม่ได้มีส่วนร่วมโดยตรงในการขัดกันทางอาวุธ ตามข้อ 51 (3) ของพิธีสารฉบับที่ 1 ดังนั้นหากถูกจับตัวไปโดยฝ่ายตรงข้าม ย่อมไม่ได้รับสถานเชลยศึก แต่อาจอยู่ในสถานะของอาชญากร และจะต้องถูกดำเนินคดีอาญาทั้งโดยกฎหมายภายในและกฎหมายระหว่างประเทศ โดยฝ่ายตรงข้ามสามารถกักขังไว้ได้ (ข้อ 5 อนุสัญญาเจนีวาฉบับที่ 4) ทั้งนี้เนื่องจากพลเรือนจะได้รับการปฏิบัติที่แตกต่างจากพลรบ (ข้อ 5 อนุสัญญาเจนีวาฉบับที่ 3)

หากพิจารณาข้อ 4 (A) ของอนุสัญญาเจนีวาฉบับที่ 3 ประกอบกับข้อ 43 และข้อ 44 ของพิธีสารฉบับที่ 1 พลรบที่จะตกอยู่ในสถานะ “เชลยศึก” ได้ ย่อมหมายถึง ผู้สังกัดในกองทัพของภาคีคู่พิพาท รวมทั้งผู้สังกัดในมิลิเชียหรือหน่วยอาสาสมัครซึ่งเป็นส่วนของกองทัพเหล่านี้ ข้อ 4 (A) (1) อนุสัญญาฉบับที่ 3 ผู้สังกัดในมิลิเชีย ผู้สังกัดในหน่วยอาสาสมัครอื่นใด รวมทั้งผู้สังกัดในขบวนต่อต้านที่ได้จัดตั้งขึ้นโดยมีระเบียบ ซึ่งเป็นของภาคีคู่พิพาทและปฏิบัติการอยู่ภายในหรือภายนอกอาณาเขตของตนเอง แม้ว่าอาณาเขตนั้นจะถูกยึดครองอยู่ก็ตาม หากว่าหน่วยมิลิเชียหรืออาสาสมัครรวมทั้งขบวนต่อต้านที่ได้จัดตั้งขึ้นโดยมีระเบียบเหล่านี้ได้ปฏิบัติตามเงื่อนไขอันได้แก่ มีผู้บัญชาการสั่งการ มีเครื่องหมายเด่นชัดเห็นได้ในระยะไกล ถืออาวุธโดยเปิดเผย และปฏิบัติการรบตามกฎและประเพณีการสงคราม ข้อ 4 (A) (2) และ ข้อ 4 (A) (6) พลเมืองในอาณาเขตที่มิได้ถูกยึดครอง ซึ่งเมื่อศัตรูประชิดเข้ามาได้สมัครใจเข้าจับอาวุธต่อต้านกองทหารที่บุกเข้ามานั้น โดยไม่มีเวลาจัดรวมกันเข้าเป็นหน่วยกองทหารประจำ หากว่าบุคคลเหล่านี้ถืออาวุธโดยเปิดเผย และเคารพต่อกฎและประเพณีการสงคราม

[971] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

หากพิจารณาตามเงื่อนไขที่กล่าวมาจะเห็นได้ว่า IT Army มีส่วนผสมทั้งพลเรือนและพลรบ การพิจารณาสถานะของบุคคลที่เกี่ยวข้องในลักษณะ Levée en Masse ใน IT Army จึงหมายถึงกลุ่มพลเรือนที่เข้ามามีส่วนร่วมโดยตรงในการขัดกันทางอาวุธและได้รับการจำแนกให้เป็นบุคคลที่ตกอยู่ในสถานะเชลยศึกได้ (หมายถึงบุคคลที่ได้รับการปฏิบัติเช่นเดียวกับพลรบโดยผลของข้อ 4 อนุสัญญาเจนีวาฉบับที่ 3 นี้ ทั้งที่มิได้มีการจัดตั้งหรือเป็นสมาชิกตามกฎหมายของกลุ่มกองกำลังใดๆ รวมตลอดถึงการเชื่อมโยงทางปฏิบัติต่อคู่ภาคีในการขัดกันทางอาวุธ[972]

ตามข้อ 4 (A) (6) ของอนุสัญญาเจนีวาฉบับที่ 3 ผู้มีส่วนร่วมใน Levée en Masse หมายถึง พลเมืองในอาณาเขตที่มิได้ถูกยึดครอง ซึ่งเมื่อศัตรูประชิดเข้ามาได้สมัครใจเข้าจับอาวุธต่อต้านกองทหารที่บุกเข้ามานั้น โดยไม่มีเวลาจัดรวมกันเข้าเป็นหน่วยกองทหารประจำ หากว่าบุคคลเหล่านี้ถืออาวุธโดยเปิดเผย และเคารพต่อกฎและประเพณีการสงคราม

หากเราแยกองค์ประกอบของการเป็น Levée en Masse ย่อมมีรายละเอียดดังต่อไปนี้

ประการที่หนึ่ง การตอบโต้อย่างทันที นั่นหมายความว่าผู้ที่มีส่วนร่วมใน Levée en Masse จะต้องทำการตอบโต้อย่างฉับพลันต่อกองทหารที่บุกเข้ามานั้น มีผู้วิพากษ์ว่า การมีส่วนร่วมใน Levée en Masse จะต้องมิได้เกิดจากการริเริ่มของกองทัพฝ่ายที่ถูกโจมตี[973] การริเริ่มหรือการยุยงนี้มีความใกล้ชิดกับการบังคับให้เข้าร่วม ซึ่งจะแตกต่างจากการเชื้อเชิญให้เข้าร่วมในกองทัพ หรือการสนับสนุนให้ก่อตั้งกองทัพ เนื่องจากการสนับสนุนหรือการเชื้อเชิญไม่มีผลในลักษณะของการบังคับและการโน้มน้าว ซึ่งเมื่อพิจารณาเทียบกับคำอธิบายอนุสัญญาเจนีวา ฉบับที่ 3 ข้อ 4 จะพบว่าการทำ Levée en Masse นั้นกระทำได้แม้ว่าจะเป็นการฝ่าฝืนต่อคำสั่งของรัฐตนเองก็ได้ เช่น แม้กองทัพยูเครนจะไม่สนับสนุนให้มีการจัดตั้ง IT Army หรือมีคำสั่งห้าม แต่พลเรือนทำการรวมตัวกันเพื่อทำ Levée en Masse ก็ย่อมเป็นองค์ประกอบที่ชอบด้วยกฎหมายเช่นกัน[974]

---

[972] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

[973] Emily Crawford, “Armed Ukraine Citizens: Direct Participation in Hostilities, Levee en Masse, or Something Else?” European Journal of International Law, (March 1, 2022) [online] Accessed: April 9, 2022. Available from: https://www.ejiltalk.org/armed-ukrainian-citizens-direct-participation-in-hostilities-levee-en-masse-or-something-else/

[974] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

หากวิเคราะห์ในมุมมองของ Buchan มองว่าข้อมูลที่มีในปฏิบัติการของกลุ่ม IT Army ค่อนข้างน้อยเกินกว่าที่จะพิจารณาว่าเป็นการเชื้อเชิญ การสนับสนุน หรือการออกคำสั่งของรัฐบาลยูเครนหรือไม่ แต่หากจะเป็นกรณีดังกล่าวผู้เขียนก็บังคงมองว่าไม่อาจจัดให้เข้าเกณฑ์ของการจัดการอย่างเป็นระบบแต่อย่างใด

ประการที่สอง ผู้ที่มีส่วนในการเป็น Levée en Masse จะต้องเป็นพลเมืองในอาณาเขตที่มิได้ถูกยึดครอง ปัญหาสำคัญคือ พลเมืองดังกล่าวหมายถึงคนที่มีสัญชาติหรือเป็นประชากรของรัฐที่ถูกยึดครอง หรือหมายถึงคนทุกคนที่อยู่ในอาณาเขตที่มิได้ถูกยึดครอง เพราะคำว่า “Inhabitant” ไม่ได้จำแนกว่าเป็นบุคคลประเภทใด อย่างไรก็ดีหากพิจารณาข้อกฎหมายนี้ตามตัวอักษร ย่อมตีความได้ว่า หมายถึงบุคคลที่มีส่วนสัมพันธ์กับยูเครนในลักษณะถาวร ไม่ว่าจะเป็นพลเมืองหรือเป็นผู้มีสัญชาติยูเครนก็ตาม ดังนั้น ผู้ที่เป็นคนยูเครน และไม่ใช่คนยูเครนที่อยู่ในดินแดนที่ถูกยึดครองก็จะเข้าร่วมกับ Levée en Masse ไม่ได้ เช่นเดียวกับคนยูเครนและพลเมืองที่อยู่ในต่างประเทศ[975]

ในขณะที่ผู้ที่มิได้อาศัยอยู่ในยูเครนหากเข้ามามีส่วนร่วมในกองทัพ IT Army ย่อมไม่มีลักษณะของการเป็นผู้อาศัยอยู่ถาวรเช่นกัน หากจำแนกว่าการใช้ทรัพยากรทางไซเบ อร์ของยูเครนถือเป็นดินแดนของยูเครน เพราะปฏิบัติการดังกล่าวคงทำได้เพียงชั่วคราว ไม่มีลักษณะเป็นการถาวรแต่ประการใด

ประการที่สาม ขอบเขตทางภูมิศาสตร์ของ Levée en Masse จะต้องเกิดขึ้นนอกดินแดนที่รัสเซียยึดครอง และการตอบโต้ของกองทัพ IT Army จะต้องกระทำนอกดินแดนที่รัสเซียยึดครอง ไม่ว่าการยึดครองนั้นจะกระทำโดยกองทัพรัสเซียหรือโดยรัฐบาลยูเครนภายใต้การใช้อำนาจของรัสเซีย (ข้อ 42 อนุสัญญาเจนีวาฉบับที่ 4) กรณีสถานการณ์ที่เกิดขึ้นในประเทศยูเครนนั้น กองทัพรัสเซียได้ยึดครองพื้นที่ Kherson ของประเทศยูเครน ในขณะที่พื้นที่ส่วนใหญ่ของประเทศยูเครนมิได้ถูกกองทัพรัสเซียยึดครอง ประชาชนที่อยู่ในพื้นที่อื่นๆ ซึ่งมิได้ถูกยึดครองนั้นจึงสามารถเข้าร่วมกับ IT Army และถือเป็น Levée en Masse ได้ ทั้งนี้ รวมตลอดถึงกรณีที่รัสเซีย สูญเสียอำนาจการยึดครองพื้นที่ดังกล่าวไป และพยายามเข้าสู่การยึดครองพื้นที่ดังกล่าวอีกครั้ง ก็มิได้ทำให้ลักษณะของขบวนการ Levée en Masse ที่เกิดขึ้นแล้วนั้นเสียไปแต่อย่างใด[976]

คำถามประการต่อมาคือหากการโจมตีทางไซเบอร์เกิดขึ้นบนดินแดนรัสเซียจะถือว่าเข้าลักษณะของการเป็น Levée en Masse หรือไม่ ตามหลักการแล้วการโจมตีดังกล่าวไม่ถือว่าเป็น

---

[975] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

[976] Ibid.

ลักษณะของ Levée en Masse เนื่องจาก การกระทำที่จะเข้าลักษณะการเป็น Levée en Masse ตามรูปแบบปกตินั้นจะต้องเป็นการต่อต้านการรุกรานของฝ่ายตรงข้ามในลักษณะการเผชิญหน้ากันที่แนวพรมแดน

สิ่งที่น่าพิจารณาอย่างมากคือการทำ Levée en Masse โดยการโจมตีทางไซเบอร์นั้นจะต้องกระทำบนพื้นฐานของเครือข่ายและทรัพยากรในพื้นที่ทางไซเบอร์ (เครือข่ายคอมพิวเตอร์) และกระทำโดยตรงต่อทรัพยากรทางไซเบอร์ของฝ่ายตรงข้าม โดยการโจมตีทางไซเบอร์นั้นจะต้องกระทำบนดินแดนซึ่งถูกโจมตีเท่านั้น โดยกระทำการต่อต้านการรุกรานซึ่งทำลายทรัพยากรทางไซเบอร์ของฝ่ายป้องกัน และผลจะต้องเกิดขึ้นบนดินแดนหรือทรัพยากรทางไซเบอร์ในดินแดนของฝ่ายป้องกันเท่านั้น หรืออาจกล่าวในทางตรงข้ามได้ว่า หากยูเครนจะทำการโจมตีทรัพยากรทางไซเบอร์ของประเทศเบลารุส เพราะมองว่าเป็นประเทศที่รัสเซียใช้เป็นฐานในการเข้ารุกรานประเทศยูเครน ย่อมไม่สามารถกระทำได้ และไม่อยู่ในขอบเขตของการทำ Levée en Masse เพราะประเทศเบลารุสมิได้เกี่ยวข้องโดยตรงกับการรุกรานประเทศยูเครน[977]

ประการที่สี่ ผู้มีส่วนเข้าร่วมในการทำ Levée en Masse จะต้องทำการรบโดยการถืออาวุธอย่างเปิดเผย ประเด็นนี้นำมาซึ่งคำถามสองประการ คือ

คำถามที่หนึ่ง ผู้เข้าร่วมในกองทัพ IT Army จะใช้อุปกรณ์ทางคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ในลักษณะเป็นอาวุธได้อย่างไร

คำตอบของคำถามข้อนี้คือ อาวุธย่อมหมายถึงอุปกรณ์ใดๆ ก็ได้ที่นำมาซึ่งผลของการกระทำในลักษณะที่ร้ายแรง[978]

คำถามที่สอง อาวุธไซเบอร์จะถืออย่างเปิดเผยได้หรือไม่

เมื่อพิจารณาจากคำอธิบายอนุสัญญาเจนีวาฉบับที่ 3 ปี ค.ศ.2020 วรรคที่ 1067 ซึ่งมีการอ้างอิงคำอธิบายข้อ 4 (a) (2) (c) para 1021-1023 คำว่าเปิดเผยหมายถึงการที่พลรบจะต้องไม่ทำการปกปิดอาวุธของตนในขณะที่ทำการโจมตีหรือในระหว่างที่มีการตระเตรียมการเพื่อโจมตี เพราะจะก่อให้เกิดความสับสนกับลักษณะของพลเรือน (อย่างไรก็ดีการถืออาวุธตามที่ปรากฏในหน่วยพลรบอื่นๆ เช่น หน่วยอาสา หรือมิลิเซีย ย่อมมีความแตกต่างจากการถืออาวุธของพลเรือนที่เข้าร่วม Levée en Masse เพราะหน่วยอาสาถือเป็นพลรบ ในขณะที่ผู้เข้าร่วม Levée en Masse มิใช่พลรบ)

---

[977] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

[978] ICJ, 1996 Legality of the Threats or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, para 39

สิ่งที่น่าพิจารณาประการต่อมาคือหากเรายอมรับสถานะการเป็นอาวุธของไซเบอร์ เครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องย่อมเป็นอาวุธที่ถือโดยเปิดเผยได้ แต่ Malware จะถือว่าเป็นสิ่งที่ใช้งานโดยเปิดเผยได้อย่างไร เว้นเสียแต่ว่าอนุมาณว่า Malware เป็นส่วนหนึ่งของคอมพิวเตอร์ โทรศัพท์เคลื่อนที่ หรืออุปกรณ์สื่อสารอื่นๆ อย่างไรก็ดี การจำแนกด้วยเกณฑ์ดังนี้จะถือว่าเป็นการเพียงพอต่อการพิจารณาสถานะที่แตกต่างกันของผู้ที่มีส่วนร่วมในการรบว่าเป็นพลเรือนหรือเป็นพลรบได้หรือไม่ หากพลเรือนมีคอมพิวเตอร์หรือมีโทรศัพท์ในความครอบครอง จะถือว่าเป็นผู้ถืออาวุธโดยเปิดเผยหรือไม่ ปัญหาจึงน่าจะอยู่ที่ว่า “ลักษณะการใช้งานอาวุธไซเบอร์” นั้นเป็นอย่างไรมากกว่า

ประการที่ห้า การกระทำ Levée en Masse จะต้องเคารพต่อกฎหมายและจารีตประเพณีในการทำสงคราม ในคำอธิบายอนุสัญญาเจนีวาฉบับที่ 3 ปี ค.ศ.2020 อ้างอิงถึงข้อ 4 (a) (2) (d) ย่อหน้าที่ 1024-1028 ว่าหลักเกณฑ์ข้อนี้สัมพันธ์กับหลักการของมิลิเซียซึ่งจะต้องปฏิบัติการรบตามกฎหมายและประเพณีในการทำสงคราม อย่างไรก็ดี ข้อ 4 (a) (6) มิได้กล่าวถึงเรื่องการปฏิบัติการ คำว่าปฏิบัติการทางทหารเป็นสิ่งที่หมายรวมตั้งแต่การกระทำเพื่อการโจมตีและการกระทำในลักษณะอื่นๆ ด้วย การปฏิบัติการนั้นจะสัมพันธ์กับเรื่องการจัดการ (Organization) หากการทำ Levée en Masse มีองค์ประกอบของการ “ไม่จัดตั้ง” หรือ “ไม่จัดการ” เป็นสำคัญ ลักษณะของการรบที่เคารพต่อกฎและประเพณีในการทำสงครามย่อมมีน้ำหนักไปที่การกระทำในทางปฏิบัติมากกว่าการปฏิบัติการในเชิงการทหาร (ข้อ 49 พิธีสารฉบับที่ 1) และการโจมตีทางไซเบอร์จะเป็นการกระทำที่สมบูรณ์ตามเงื่อนไขนี้ก็ต่อเมื่อการโจมตีทางไซเบอร์นั้นก่อให้เกิดผลต่อการสูญเสียชีวิต การบาดเจ็บหรือการทำลายเท่านั้น

ในสถานการณ์การโจมตีของกองกำลัง IT Army นั้นไม่ปรากฏการรายงานถึงผลการโจมตีที่ก่อให้เกิดความเสียหายต่อชีวิต การบาดเจ็บและความเสียหายทางกายภาพ ทั้งนี้เพราะการโจมตีด้วยวิธีการ DDoS นั้นมีผลต่อการโจมตีเว็บไซต์ของรัฐบาลรัสเซียเท่านั้น และแม้ว่าจะมีรายงานว่าการโจมตีทางไซเบอร์มีผลกระทบต่อเรื่องอื่นด้วยเช่นการธนาคารหรือธุรกิจในลักษณะที่เกี่ยวข้องกับเป้าหมายในเชิง Dual Use แต่การโจมตีทางไซเบอร์ที่ปรากฏก็มิได้เป็นไปเพื่อการขับไล่ผู้รุกรานออกไปจากดินแดนแต่อย่างใด ยิ่งไปกว่านั้นหากพิจารณาลักษณะของเป้าหมายในการโจมตี ว่า

เป้าหมายใดชอบด้วยกฎหมายหรือไม่ แม้การโจมตีธนาคารจะไม่ชอบด้วยกฎหมาย แต่ลักษณะการโจมตีทางไซเบอร์ที่เกิดขึ้นก็ไม่ก่อให้เกิดลักษณะของการกระทำ Levée en Masse ได้แต่อย่างใด[979]

จากองค์ประกอบที่พิจารณาดังกล่าวจะเห็นได้ว่า IT Army ไม่เข้าองค์ประกอบของการเป็น Levée en Masse จึงไม่สามารถได้รับการคุ้มครองเช่นเดียวกัลพลรบได้ และย่อมไม่สามารถได้รับสถานะของเชลยศึกด้วยเช่นกัน

ปัญหาสำคัญประการต่อมาคือหากการเข้าร่วม IT Army ไม่เข้าลักษณะการเป็น Levée en Masse แล้วพลเรือนที่เข้าร่วมกับกองกำลัง IT Army จะถือว่าเป็นพลเรือนที่มีส่วนร่วมโดยตรงกับการรบหรือไม่

ผู้ที่เข้าร่วมกองกำลัง IT Army โดยไม่มีคุณสมบัติเป็นพลรบย่อมได้รับความคุ้มครองเช่นเดียวกับพลเรือน และไม่ตกเป็นเป้าหมายของการถูกโจมตี เว้นเสียแต่ว่าในขณะนั้นผู้เข้าร่วมได้กระทำการในลักษณะมีส่วนร่วมโดยตรงต่อการกระทำอันเป็นปฏิปักษ์ โดยพิจารณาจากองค์ประกอบ 3 ประการคือ 1) ภัยคุกคาม 2) ผลกระทบโดยตรงจากภัยคุกคามนั้น 3) ความสัมพันธ์ระหว่างการกระทำตอบโต้ต่อภัยคุกคามนั้น

จากรายงานการโจมตี พบว่ามีการโจมตีเว็บไซต์กระทรวงกลาโหมของรัสเซียให้ล่ม ซึ่งไม่เป็นไปตามเกณฑ์ข้อ 1 คือภัยคุกคามไม่ได้นำมาซึ่งความตาย ความบาดเจ็บ ความเสียหาย หรือการกระทำในลักษณะโต้กลับต่อปฏิบัติการทางการทหารของรัสเซีย ปฏิบัติการทางไซเบอร์ซึ่งมีเป้าหมายในการรวบรวมข้อมูลข่าวกรองของรัสเซีย การเปลี่ยนแปลงการสื่อสาร และการทำลายการประสานงานของเจ้าหน้าที่และอุปกรณ์ต่างๆ อาจทำให้เงื่อนไขแรกนี้เกิดขึ้นได้ หากการโจมตีลักษณะดังกล่าวก่อให้เกิดผลต่อปฏิบัติการทางทหารของกองทัพรัสเซีย

แม้จะมีรายงานว่าการโจมตีทางไซเบอร์มีผลต่อปฏิบัติการทางทหารของรัสเซียก็ตาม แต่ก็ไม่ปรากฏว่ามีผลต่อการขัดขวางการรุกรานของกองทัพรัสเซียในประเทศยูเครนแต่อย่างใด การโจมตีทางไซเบอร์ของพลเรือนอาจนำมาซึ่งความเดือดร้อนรำคาญและข้อหาทางอาญาเท่านั้น แต่ไม่ทำให้บุคคลดังกล่าวตกเป็นเป้าหมายของการโจมตีแต่อย่างใด หากพลเรือนดังกล่าวถูกจับกุมตัว ผู้จับกุมก็สามารถทำการกักขังได้เพื่อวัตถุประสงค์ความมั่นคง (ข้อ 5 อนุสัญญาเจนีวาฉบับที่ 4)

[979] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

เพียงแต่การกระทำผ่านระบบไซเบอร์นั้นมักอยู่ในลักษณะการสั่งการทางไกล ซึ่งจะทำให้โอกาสในการถูกจับตัวลดลง[980]

แล้วพลเรือนดังกล่าวจะมีสถานะทางกฎหมายอย่างไรหากไปร่วมกับกองทัพยูเครนในการปฏิบัติการ หรือได้รับการจัดตั้งอย่างเป็นระบบตามข้อ 4 (a) (2) อนุสัญญาเจนีวาฉบับที่ 3 ทั้งนี้ไม่ว่าโดยชัดแจ้งหรือโดยปริยายจากรัฐบาลยูเครน

หากเป็นกรณีดังกล่าวย่อมถือว่าพลเรือนนั้นมีส่วนร่วมโดยตรงในการกระทำอันเป็นปรปักษ์ สามารถใช้อาวุธโดยชอบด้วยกฎหมายได้ และย่อมตกเป็นเป้าหมายในการถูกโจมตีด้วยเช่นกัน ยิ่งไปกว่านั้นหากถูกจับตัวโดยฝ่ายรัสเซีย พลเรือนดังกล่าวย่อมได้รับสถานะการเป็นเชลยศึกด้วยเช่นกัน

คำถามคือสถานะดังกล่าวเป็นประโยชน์อย่างไร? หากพิจารณาลักษณะของปฏิบัติการที่พลเรือนผู้โจมตีทางไซเบอร์นั้นปฏิบัติการทางไกล โอกาสในการจะถูกจับตัวและตกอยู่ในสถานะของเชลยศึกย่อมเป็นไปได้ยากขึ้น แต่อย่างน้อยการมีส่วนร่วมโดยตรงในการปฏิบัติอันเป็นปฏิปักษ์ก็ทำให้พลเรือนดังกล่าวได้รับการจำแนกออกไปจากพลเรือนทั่วไป (กล่าวคือไม่ได้รับความคุ้มครองตามกฎหมายเช่นพลเรือนปกติ)

4.2.4 ข้อท้าทายต่อหลักความได้สัดส่วนในการโจมตี

ความได้สัดส่วนในการขัดกันทางอาวุธหมายถึงคู่พิพาทในการขัดกันทางอาวุธนั้นจะต้องไม่ก่อความรุนแรงมากไปกว่าสัดส่วนที่จำเป็นต้องใช้เพื่อวัตถุประสงค์ในการทำสงคราม คือการทำลายกองทัพฝ่ายตรงข้ามเพื่อความได้เปรียบทางการทหารเท่านั้น[981] การใช้กำลังทางทหารจึงไม่ใช่ว่าจะทำได้โดยปราศจากข้อจำกัด[982] นอกจากนั้น ในการโจมตีด้วยปฏิบัติการทางทหารจะต้องคาดหมายล่วงหน้าถึงความเสียหายที่อาจกระทบต่อชีวิตและทรัพย์สินของพลเรือนด้วย หากความเสียหายดังกล่าวเกินขอบเขตจากการทำลายเป้าหมายทางการทหารฝ่ายตรงข้ามมากเกินไปย่อมถือว่าเป็นการต้องห้ามตามกฎหมาย[983]

---

[980] Russell Buchan and Nicholas Tsagourias. “Ukranian ‘IT Army’: A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?”

[981] Jean Pictet., Humanitarian Law and the Protection of War Victims, p. 31.

[982] Ibid., p. 33.

[983] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p.46.

ปัญหาว่า ความเกี่ยวข้องต่อประโยชน์ทางการทหารโดยตรงและเป็นรูปธรรม (concrete and direct military advantage anticipate) ซึ่งเป็นสัดส่วนที่สามารถโจมตีได้นั้น เป็นอย่างไร พบว่าทางปฏิบัติโดยรัฐส่วนมากพิจารณาจากสาระสำคัญและความใกล้ชิดอย่างยิ่ง (substantial and relatively close) ว่าพื้นที่หรือปฏิบัติการใดเป็นไปเพื่อการใช้กำลังทางหทารมากที่สุดย่อมตกเป็นเป้าหมายของการโจมตีได้ แม้กระนั้นก็ตามการพิสูจน์ดังกล่าวยังเป็นเรื่องที่ค่อนข้างยาก จึงต้องอาศัยการวางแผนและการพิจารณาถึงความจำเป็นในการปฏิบัติการเพื่อการโจมตีเป้าหมายดังกล่าว ก่อนที่จะมีการตัดสินใจโจมตีด้วย[984]

ระบบอาวุธอิสระนั้นมีข้อพิจารณาเรื่องความรับผิดขอบของผู้วางแผน ผู้ตัดสินใจ ผู้ควบคุมการโจมตี หลักการนี้จะต้องนำมาปรับใช้กับทุกการโจมตี โดยคำนึงถึงปัจจัยและวิธีที่นำมาใช้ และพิจารณาความรับผิดของพลรบซึ่งเป็นบุคคลที่ต้องคำนึงถึงหลักเกณฑ์ดังกล่าว ทั้งนี้จะกล่าวอ้างความผิดที่เกิดจากจักรกล ระบบข้อมูลการประมวลผล หรือระบบการใช้อาวุธไม่ได้ จึงต้องมีการกำหนดพันธกรณีตามกฎหมายให้มีเกณฑ์ขั้นต่ำเรื่องการใช้มนุษย์ควบคุมระบบอาวุธเหล่านี้[985]

ข้อท้าทายที่น่าพิจารณาเพิ่มเติมคือเรื่องการออกแบบอาวุธที่อาจนำไปสู่ความไม่สามารถคาดการณ์ปฏิบัติการณ์ของอาวุธได้ เช่น การใช้จักรกลอัจฉริยะ (AI: Artificial Intelligence) ซึ่งใช้ชุดคำสั่งอัลกอริทึ่ม (Algorithms) ประมวลผลการระบุเป้าหมาย ซึ่งจะก่อให้เกิดปัญหาเรื่องการปรับใช้หลักกฎหมายกับระบบประมวลผลดังกล่าว รวมถึงประเด็นเรื่องจริยธรรมในการใช้อาวุธ (Ethic) คณะกรรมการกาชาดระหว่างประเทศ มองว่าประเด็นสำคัญอยู่ที่ปฏิบัติการของจักรกล และความรับผิดชอบในการตัดสินใจสังหารหรือทำลายล้าง เมื่อความรับผิดชอบในด้านจริยธรรมนี้ไม่อาจใช้กับจักรกลได้ จึงต้องมีการกำหนดประเภทและระดับการควบคุมจักรกลซึ่งต้องมีมนุษย์เข้ามาเกี่ยวข้องในการตัดสินใจในการสังหารและทำลาย เพื่อกำหนดความรับผิดของผู้ควบคุมได้ด้วย[986]

---

[984] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules ,p. 50.

[985] ICRC, Expert Meeting on Lethal Autonomous Weapons Systems, Statement, November 15, 2017. [online] Accessed: November 16, 2017. Available from: https://www.icrc.org/en/document/expert-meeting-lethal-autonomous-weapons-systems

[986] Ibid.

4.2.5 ข้อท้าทายต่อหลักความระมัดระวังในการโจมตีกับเทคโนโลยีใหม่

หลักความระมัดระวังก่อนการโจมตีจะต้องอยู่บนพื้นฐานของการพิจารณาว่าการปฏิบัติการทางทหารเพื่อการโจมตีฝ่ายตรงข้ามนั้นจะต้องคาดหมายได้ว่าจะเกิดผลกระทบต่อพลเรือนอย่างน้อยที่สุด และหลีกเลี่ยงจากการก่อความเสียหายแก่พลเรือน หรือความเสียหายดังกล่าวจะต้องเกิดน้อยที่สุดด้วย จึงต้องมีการตรวจสอบเป้าหมายทางการทหารที่ย่อมตกอยู่ภายใต้การทำลายได้เสมอ นอกจากนั้นยังต้องมีการเลือกวิธีและปัจจัยในการโจมตีที่จะไม่ก่อให้เกิดความเสียหายต่อพลเรือน หรือความเสียหายที่อาจเกิดขึ้นแก่พลเรือนจะต้องน้อยที่สุด ต้องมีการประเมินความเสียหายล่วงหน้า ปฏิบัติการจะต้องอยู่ภายใต้การควบคุมที่อาจมีการยกเลิกหรือเลื่อนการปฏิบัติการได้หากเป้าหมายดังกล่าวไม่ใช่เป้าหมายทางการทหาร ต้องมีการเตือนภัยล่วงหน้าแก่พลเรือนถึงผลกระทบที่อาจเกิดขึ้น และในกรณีที่สามารถเลือกเป้าหมายในการโจมตีได้ การโจมตีนั้นจะต้องกระทำต่อเป้าหมายที่จะเกิดความเสียหายน้อยที่สุดต่อพลเรือนด้วย ทั้งนี้ ย่อมรวมถึงกรณีจำเป็นที่อาจมีการเคลื่อนย้ายพลเรือนออกจากพื้นที่ปฏิบัติการทางทหารด้วย[987]

ปัญหาในทางปฏิบัติจึงเกิดขึ้นว่าในการปฏิบัติการทางทหารแต่ละกรณีที่จะต้องมีการพิจารณาปัจจัยหลายประการนั้นจะสามารถนำไปสู่การตอบโต้ได้รวดเร็วเพียงใด[988]

นอกเหนือจากหลักพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศซึ่งจะนำมาปรับใช้แก่กรณีวิธีและปัจจัยในการขัดกันทางอาวุธแล้ว หลักพื้นฐานเกี่ยวกับเรื่องการใช้อาวุธในการขัดกันทางอาวุธที่จะต้องพิจารณายังได้แก่กฎการห้ามใช้อาวุธที่ก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น กฎความได้สัดส่วนในการใช้อาวุธ กฎการห้ามใช้อาวุธที่ไม่สามารถจำแนกเป้าหมายได้ กฎข้อจำกัดในการใช้ปัจจัยและวิธีการในการรบ และพันธกรณีของรัฐภาคีในการทบทวนการพัฒนา การศึกษา การได้มา และการยอมรับซึ่งอาวุธใหม่[989]

ความคิดเห็นของนักวิชาการกลุ่มหนึ่ง โดยเฉพาะอย่างยิ่ง William H. Boothby มองว่าหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศนั้นได้กำหนดนิยามศัพท์ที่ค่อนข้างมีทั้งความยืดหยุ่นและปรับใช้ได้กับในหลายกรณีอยู่แล้ว แม้ว่าอาจมีข้อท้าทายบางประการเกิดขึ้นจาก

---

[987] Jean-Marie Hanckaerts and Louis Doswald-beck, Customary International Humanitarian Law: Volume I Rules, p. 51-68.

[988] Ibid., p. 64.

[989] William Boothby, Weapons and the Law of Armed Conflict, p. 348.

เทคโนโลยีซึ่งไม่อาจทราบได้ว่าจะเป็นอย่างไรในอนาคตก็ตาม ความล้าหลังของกฎหมายที่เกี่ยวกับอาวุธจึงไม่ใช่เรื่องที่น่าวิตก เพราะกฎหมายสร้างลักษณะความเป็นพลวัตในตัวเองอยู่แล้ว[990]

4.2.5.1 การตรวจสอบเป้าหมายในการโจมตี

การตรวจสอบเป้าหมายในการโจมตีเป็นประเด็นสำคัญประการหนึ่งของปฏิบัติการทางทหาร โดยปรากฏในข้อ 52 (2) ของพิธีสารเพิ่มเติมอนุสัญญาเจนีวาฉบับที่ 1 โดยระบุว่าการโจมตีจะต้องกระทำอย่างเคร่งครัดต่อเป้าหมายทางทหาร ในกรณีที่เกี่ยวกัยทรัพย์สินสิ่งของนั้น เป้าหมายทางทหารจำกัดเฉพาะทรัพย์สินสิ่งของซึ่งโดยลักษณะ สถานที่ตั้ง วัตถุประสงค์ หรือการใช้ ก่อให้เกิดประสิทธิภาพในปฏิบัติการทางทหาร และการทำลายล้างไม่ว่าทั้งหมดหรือบางส่วน การยึดหรือทำให้หมดสมรรถภาพซึ่งทรัพย์สิน สิ่งของในสภาวการณ์ที่ปฏิบัติการนั้น จะก่อให้เกิดความได้เปรียบทางทหารอย่างชัดเจน”

บทบัญญัติดังกล่าวเป็นพื้นฐานสำคัญที่จะต้องพิจารณาว่าการใช้เทคโนโลยีในการขัดกันทางอาวุธนั้นก่อให้เกิดผลกระทบต่อกฎหมายหรือไม่ โดยจะต้องคำนึงถึงสถานที่ตั้ง และความได้เปรียบทางการทหาร เช่น ระบบการสื่อสารทางไซเบอร์โดยปกติเป็นช่องทางของพลเรือน หากมีการใช้งานเพื่อเป้าหมายทางการทหารและตกอยู่ภายใต้การถูกตอบโต้ได้ จะต้องพิจารณาด้วยว่าการตอบโต้ดังกล่าวนั้นจะก่อให้เกิดความได้เปรียบทางการทหารมากกว่าผลเสียหายที่จะเกิดแก่พลเรือนหรือไม่ และการกระทำต่อระบบดังกล่าวกระทำบนพื้นฐานที่ช่องทางการสื่อสารดังกล่าวต้องมีวัตถุประสงค์หลักในปฏิบัติการทางทหารเป็นสำคัญด้วย

4.2.5.2 การเลือกปัจจัยและวิธีการในการเข้าโจมตี

การเลือกปัจจัยและวิธีการในการเข้าโจมตีเป็นกระบวนการหนึ่งซึ่งจะต้องกระทำในปฏิบัติการทางทหารเพื่อให้การโจมตีนั้นเป็นไปด้วยความได้สัดส่วนและเป็นไปเพื่อประโยชน์ในความได้เปรียบทางการทหารเท่านั้น[991] ปัญหาจึงอยู่ที่ว่าระบบอาวุธที่ตัดสินใจได้ด้วยตนเองนั้นใช้วิธีการประมวลผลแบบอัลกอริทึ่มซึ่งกระทำได้โดยไม่ผ่านการตัดสินใจของมนุษย์ หากมีความผิดพลาดเกิดขึ้นจากการตัดสินใจในการโจมตี จะเชื่อมโยงผลดังกล่าวสู่ความรับผิดชอบของผู้ใด ในขณะที่ระบบ

---

[990] William Boothby, Weapons and the Law of Armed Conflict, p. 370.

[991] Ibid., p. 348

การโจมตีทางไซเบอร์อาจเกิดได้ทั้งสองทางคือการใช้ระบบอัลกอริทึ่มประมวลและตัดสินใจโจมตีเองกับการที่ระบบไซเบอร์ทำตามเงื่อนไขที่ผู้ใช้งานกำหนดเอาไว้ กรณีที่มีมนุษย์เป็นผู้มีส่วนร่วมในการตัดสินใจจึงเป็นประเด็นที่สามารถวิเคราะห์ความรับผิดชอบได้ง่ายกว่า

4.2.5.3 การละเว้นการโจมตีที่คาดได้ว่าอาจเกิดความสูญเสียต่อพลเรือน

การเลือกเป้าหมายในการโจมตีที่จะต้องกระทำต่อเป้าหมายทางทหารเท่านั้น และจะต้องพยายามให้ความเสียหายเกิดขึ้นแก่พลเรือนน้อยที่สุด เช่นเดียวกันกับการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธที่จะต้องคำนึงถึงความเสียหายที่อาจเกิดขึ้นแก่พลเรือนทั้งต่อระบบสาธารณูปโภคขั้นพื้นฐานและปัจจัยสำคัญประการอื่นๆ ด้วย[992]

ในการพิจารณาตามปกตินั้นมนุษย์จะมีส่วนเกี่ยวข้องในการตัดสินใจเพื่อโจมตี หากเทคโนโลยีที่ใช้ในการขัดกันทางอาวุธนั้นสามารถระงับการปฏิบัติการเพื่อรอการตัดสินใจจากผู้ที่เกี่ยวข้องได้ ย่อมถือว่าเป็นการปฏิบัติตามหลักการ แต่หากระบบอาวุธนั้นตัดสินใจได้ด้วยตนเอง และมีความผิดพลาดจากการประมวลผลเกิดขึ้นปัญหาย่อมตามมาว่าจะถือเป็นการละเมิดต่อหลักกฎหมายหรือไม่ และความรับผิดชอบตกแก่ผู้ใด

4.2.5.4 ผลที่เกิดจากการโจมตีโดยทั่วไปและผลลักษณะ Knock-on

ผลกระทบที่อาจเกิดขึ้นในลักษณะ Knock-on หรือผลกระทบต่อเนื่องจากการโจมตีทางการทหารที่อาจส่งผลต่อการใช้ชีวิตของพลเรือน และย่อมรวมถึงการคำนึงถึงความได้สัดส่วนในการโจมตีซึ่งจะกระทำได้ยากขึ้น[993] เนื่องจากการตัดสินใจในการโจมตีทางระบบไซเบอร์ทุกครั้งจะต้องคำนึงถึงผลกระทบที่อาจเกิดขึ้นหรือมีตามมาอย่างชัดเจนด้วย จึงหลีกเลี่ยงไม่ได้ที่จะต้องคำนึงถึงหลักความระมัดระวังล่วงหน้าก่อนการโจมตีเพิ่มเติมว่าการตอบโต้หรือการโจมตีโดยผ่านระบบไซเบอร์นั้นจะต้องกระทำบนพื้นฐานการพิจารณาหลักเกณฑ์มากเพียงใด อย่างไรก็ดีหลักเกณฑ์พื้นฐานเหล่านี้ย่อมสามารถบังคับใช้ได้เสมอ

ในทำนองเดียวกันกับการใช้งานระบบไซเบอร์การใช้งานเทคโนโลยีในรูปแบบอื่นๆ ก็จะต้องคำนึงถึงผลกระทบต่อเนื่องที่อาจเกิดขึ้นต่อการใช้ชีวิตของพลเรือนเช่นเดียวกัน แต่ปัญหาที่

---

[992] Jean Pictet, Humanitarian Law and the Protection of War Victims. (Geneva: Henry Dunant Institute, 1975), p. 28.

[993] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p. 205-208.

จะต้องเกิดขึ้นคือหากการประมวลผลในการโจมตีนั้นเป็นของระบบอาวุธตัดสินใจเองและก่อให้เกิดผลกระทบลักษณะ Knock-on เกิดขึ้น ความผิดพลาดดังกล่าวจะเกี่ยวข้องกับผู้ใดเป็นสำคัญ และจะถือว่าเป็นปฏิบัติการที่ละเมิดต่อหลักกฎหมายมนุษยธรรมระหว่างประเทศหรือไม่ หากใช่ ใครเป็นผู้ละเมิด และใครต้องรับผิดชอบ[994]

4.3 ข้อท้าทายเกี่ยวกับการควบคุมและการใช้อาวุธ

ประเด็นเรื่องการควบคุมและการจำกัดการใช้อาวุธนั้นอยู่ในกฎหมายระหว่างประเทศใน 2 กรอบ คือ กฎหมายมนุษยธรรมระหว่างประเทศที่มีหลักการพื้นฐานในการจำกัดการใช้อาวุธและวิธีการในการรบและกฎหมายระหว่างประเทศอื่นที่ควบคุมการใช้อาวุธนอกสถานการณ์การขัดกันทางอาวุธ ซึ่งกฎหมายทั้ง 2 รูปแบบต้องเผชิญกับความเปลี่ยนแปลงของเทคโนโลยีในยุคปัจจุบันก่อให้เกิดข้อท้าทายดังต่อไปนี้

4.3.1 ข้อท้าทายต่อการจำกัดวิธีและปัจจัยที่ใช้ในการขัดกันทางอาวุธ

ข้อจำกัดการใช้วิธีและปัจจัยที่ใช้ในการขัดกันทางอาวุธนั้น ปรากฏตามข้อ 35 แห่งพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ.1977 ของอนุสัญญาเจนีวา ค.ศ.1949 ซึ่งมีเป้าหมายในการควบคุมความรุนแรงของการขัดกันทางอาวุธให้เป็นไปเท่าที่จำเป็นต่อปฏิบัติการทางทหารเท่านั้น การจำกัดวิธีและปัจจัยในการขัดกันทางอาวุธนี้มีความหมายรวมถึงอาวุธและการใช้อาวุธด้วย

คำว่า “อาวุธ” ในทางกฎหมายนั้นมีสองรูปแบบ คืออาวุธโดยสภาพกับอาวุธโดยการใช้งาน เช่น ปืนถูกออกแบบมาเพื่อการใช้งานในการทำลาย และต่อสู้เป็นสำคัญ ปืนจึงเป็นอาวุธโดยสภาพ ในขณะที่มีดอาจถูกออกแบบมาเพื่อการใช้งานครัว มีดโดยทั่วไปจึงอาจไม่ใช่อาวุธโดยสภาพ แต่อาจเป็นอาวุธโดยการใช้งาน ในขณะที่ท่อนไม้ไม่ใช่ทั้งอาวุธโดยสภาพและการออกแบบ เพราะเป็นสิ่งที่มีอยู่แล้วตามธรรมชาติ ก็อาจถูกนำมาใช้งานเพื่อให้กลายเป็นอาวุธในการต่อสู้หรือป้องกันตัวได้[995]

กฎหมายมนุษยธรรมระหว่างประเทศนั้น อาวุธ (Weapons) ที่ใช้ในการขัดกันทางอาวุธย่อมหมายถึง สิ่งที่ออกแบบมาเพื่อใช้ในการต่อสู้ต่อพลรบฝ่ายตรงข้าม หรือเพื่อการโจมตีเป้าหมายทางการทหารฝ่ายตรงข้าม[996] เช่น ปืนที่พลรบหรือทหารมีไว้ใช้ประจำกาย ย่อมเป็นสิ่งที่ออกแบบมาเพื่อการ

---

[994] William Boothby, Weapons and the Law of Armed Conflict, p. 348

[995] Ibid., p. 4.

[996] Ibid.

ต่อสู้และการป้องกันตัว ปืนประจำกายจึงเป็นอาวุธโดยสภาพ ระเบิดที่ทหารพกไว้เพื่อการรบมีเป้าหมายเพื่อใช้ในการทำลาย จึงเป็นอาวุธโดยสภาพ ในขณะที่รถหุ้มเกราะเพื่อใช้ลำเลียงทหารมิได้ถูกออกแบบมาเพื่อการทำลาย จึงไม่ใช่อาวุธโดยสภาพ แต่หากมีการติดตั้งอาวุธเข้าไปเพื่อการทำลายย่อมเป็นการนำเอายานพาหนะไปรวมเข้ากับการใช้งานอาวุธ จึงเป็นการใช้งานยานพาหนะให้เป็นสิ่งประกอบการใช้อาวุธ เครื่องมือสื่อสารทางการทหารมิใช่อาวุธ แต่มีไว้เพื่อประกอบการใช้งานสั่งการโจมตีและป้องกัน โดยนัยนี้เครื่องมือสื่อสารจึงไม่ใช่อาวุธแต่ถูกใช้งานเพื่ออำนวยประโยชน์ต่อการรบฯลฯ ดังนี้ย่อมสังเกตได้ว่าการใช้งานสิ่งต่างๆ ในการรบนั้น อาจอยู่ในหลายสถานะตั้งแต่การเป็นอาวุธโดยการออกแบบ การใช้สิ่งที่มิใช่อาวุธมาประกอบกับการใช้อาวุธ และสิ่งที่มิใช่อาวุธมาประกอบการรบ การควบคุมการใช้อาวุธจึงไม่อาจคุ้มครองบุคคลในสถานการณ์การขัดกันทางอาวุธในทุกกรณีได้ จึงมีการใช้ถ้อยคำทางกฎหมายที่ก่อให้เกิดความครอบคลุมมากขึ้น โดยปรากฏคำว่า วิธี (Methods) และปัจจัย (Means)

ปัจจัย (Means) หมายถึง อาวุธ เครื่องกระสุน ส่วนประกอบ ชิ้นส่วน และอุปกรณ์ที่ใช้ประกอบกับอาวุธนั้น โดยนัยนี้ ปัจจัยย่อมรวมถึงอาวุธทุกชนิดที่ใช้ในการสงคราม สิ่งประกอบการใช้อาวุธ แท่นยิง เครื่องกระสุน ในขณะที่วิธี (Methods) หมายถึง วิธีการใช้อาวุธต่อศัตรู หรือวิธีการในการใช้กำลังกับศัตรู[997] วิธีการจึงมีความกว้างขวางมากกว่าอาวุธ และย่อมครอบคลุมถึงพฤติกรรมในการใช้กำลังในการขัดกันทางอาวุธในหลายกรณี

4.3.1.1 การใช้เทคโนโลยีใหม่เป็นวิธีหรือปัจจัยในการขัดกันทางอาวุธ

ข้อพิจารณาประการแรกของระบบอาวุธอิสระเช่นหุ่นยนต์สังหารหรือระบบอาวุธตอบโต้อัตโนมัติโดยการตรวจจับลักษณะของสิ่งบุกรุกนั้นย่อมอยู่ในลักษณะของการออกแบบเพื่อใช้เป็นอาวุธโดยสภาพเพราะมีเป้าหมายในการใช้งานเพื่อการทำลาย จึงย่อมตกอยู่ภายใต้การบังคับของกฎหมายมนุษยธรรมระหว่างประเทศ

เนื่องจากระบบอาวุธที่ตัดสินใจได้ด้วยตนเองนั้นไม่ต้องอาศัยมนุษย์เป็นผู้ตัดสินใจในการสั่งการโจมตี ปัญหาเรื่องความรับผิดชอบในการกระทำจึงควรอยู่ในขอบเขตความรับผิดชอบของผู้ออกแบบ ผู้วางแผน ผู้ตัดสินใจ ผู้ควบคุมการโจมตี และหลักการนี้จะต้องนำมาปรับใช้กับทุกการโจมตี โดยคำนึงถึงปัจจัยและวิธีที่นำมาใช้ และพิจารณาความรับผิดของบุคคลที่ต้องคำนึงถึงหลักเกณฑ์ดังกล่าว ทั้งนี้ ความรับผิดต่อผลที่เกิดจากปฏิบัติการของระบบอาวุธที่ตัดสินใจได้ด้วย

---

[997] William Boothby, Weapons and the Law of Armed Conflict, p. 4.

ตนเองนี้จะต้องอยู่บนพื้นฐานของความรับผิดเด็ดขาด ผู้เกี่ยวข้องจะกล่าวอ้างความผิดที่เกิดจากจักรกล ระบบข้อมูลการประมวลผล หรือระบบการใช้อาวุธไม่ได้ การกำหนดพันธกรณีตามกฎหมายให้มีเกณฑ์ขั้นต่ำเรื่องการใช้มนุษย์ควบคุมระบบอาวุธเหล่านี้จึงเป็นเรื่องสำคัญ[998]

หลักกฎหมายที่จะเข้ามามีบทบาทในการปรับใช้ต่อเรื่องระบบอาวุธที่ตัดสินใจได้ด้วยตนเองคือ หลักความระมัดระวังล่วงหน้าก่อนการโจมตี โดยต้องพิจารณาจาก การคาดหมาย (Predictabilities) การแทรกแซงปฏิบัติการของระบบอาวุธดังกล่าวโดยมนุษย์สามารถกระทำได้เพียงใด (human supervision and ability to intervene) และการพิจารณาข้อจำกัดในการปฏิบัติการในประเด็นต่างๆ ดังที่ได้กล่าวไปแล้ว

ปัญหาที่อาจเกิดขึ้นได้คือ การออกแบบอาวุธที่อาจนำไปสู่ความไม่สามารถคาดการณ์ปฏิบัติการณ์ของอาวุธได้ เช่น การใช้จักรกลอัจฉริยะ (AI: Artificial Intelligence) ซึ่งใช้ชุดคำสั่งอัลกอริทึ่ม (Algorithms) ประมวลผลการระบุเป้าหมาย ซึ่งจะก่อให้เกิดปัญหาเรื่องการปรับใช้หลักกฎหมายกับระบบประมวลผลดังกล่าว เพราะระบบประมวลผลที่ซับซ้อนอาจตัดความสัมพันธ์ระหว่างบุคคลผู้ปฏิบัติการกับระบบอาวุธออกไป อย่างไรก็ดี ตามหลักความระมัดระวังก่อนการโจมตี ผู้ใช้ระบบอาวุธดังกล่าว ก็ย่อมต้องมีความรับผิดชอบเพิ่มขึ้นในการตรวจสอบประสิทธิภาพการใช้งานอาวุธดังกล่าวด้วย

ประเด็นเรื่องจริยธรรมในการใช้อาวุธ (Ethic) คณะกรรมการกาชาดระหว่างประเทศมองว่าประเด็นสำคัญอยู่ที่ปฏิบัติการของจักรกล และความรับผิดชอบในการตัดสินใจสังหารหรือทำลายล้าง เมื่อความรับผิดชอบในด้านจริยธรรมนี้ไม่อาจใช้กับจักรกลได้ จึงต้องมีการกำหนดประเภทและระดับการควบคุมจักรกลซึ่งต้องมีมนุษย์เข้ามาเกี่ยวข้องในการตัดสินใจในการสังหารและทำลายเพื่อกำหนดความรับผิดของผู้ควบคุมได้ด้วย[999]

การใช้อากาศยานไร้คนขับ (UAV) ที่สามารถตัดสินใจได้ด้วยตนเองนั้น อาจการเปลี่ยนรูปแบบของการทำสงครามได้มีแค่ประเด็นเดียวคือเรื่องการใช้ UAV แทนทหารในการรบ ซึ่งคงกระทบหลักการเดียวคือประเด็น “การจำแนกพลรบ” ที่เป็นมนุษย์ และการตอบโต้กับ UAV

---

[998] ICRC, (2017), Expert Meeting on Lethal Autonomous Weapons Systems, Statement, November 15, 2017. https://www.icrc.org/en/document/expert-meeting-lethal-autonomous-weapons-systems, Retrieved November 16, 2017.

[999] ICRC, Expert Meeting on Lethal Autonomous Weapons Systems, Statement, November 15, 2017. [online] Accessed: November 16, 2017. Available from: https://www.icrc.org/en/document/expert-meeting-lethal-autonomous-weapons-systems

ดังกล่าว อย่างไรก็ดี หากพิจารณาว่า UAV เป็นอาวุธ ก็ต้องพิจารณาว่าเป็นอาวุธที่ต้องห้ามหรือไม่ตามหลักกฎหมายมนุษยธรรมระหว่างประเทศ[1000] ทั้งนี้หลักการสำคัญคือความระมัดระวังก่อนการโจมตียังคงเป็นประเด็นที่จะต้องคำนึงถึงเสมอเมื่อมีการใช้ระบบอาวุธดังกล่าว

4.3.1.2 การใช้เทคโนโลยีใหม่ที่อาจเป็นได้ทั้งวิธีและปัจจัยในการขัดกันทางอาวุธ

การใช้ระบบไซเบอร์เพื่อการขัดกันทางอาวุธย่อมก่อให้เกิดประเด็นที่ต้องพิจารณาว่าระบบไซเบอร์จะถูกนำมาใช้ในฐานะเป็นอาวุธหรือเป็นวิธีการในการขัดกันทางอาวุธเป็นประการแรก หากจะพิจารณาว่าระบบไซเบอร์สามารถนำมาใช้เพื่อทำลายเป้าหมายหรือก่อให้เกิดความเสียหายได้ ระบบไซเบอร์ย่อมตกอยู่ในสถานะการเป็นอาวุธหรืออีกนัยหนึ่งคือเป็นปัจจัยในการขัดกันทางอาวุธ แต่หากระบบไซเบอร์เป็นเพียงวิธีการเพื่อทำให้ได้มาซึ่งความได้เปรียบทางการทหารแต่มิได้ใช้เพื่อการทำลายเป้าหมายโดยตรง ระบบไซเบอร์ย่อมเป็นเพียงวิธีในการขัดกันทางอาวุธ ปรากฏว่าในความเป็นจริงนั้นระบบไซเบอร์อาจถูกใช้ในสองลักษณะ อันได้แก่ การก่อวินาศกรรมทางไซเบอร์ (Cyber sabotage) และการจารกรรมทางไซเบอร์ (Cyber espionage)[1001]

ในกรณีของการก่อวินาศกรรมทางไซเบอร์ ย่อมหมายรวมถึงการปล่อยไวรัสทางคอมพิวเตอร์ และการใช้ระบบไซเบอร์เพื่อการโจมตีในลักษณะของ DDOS (Distributed Denial of Service)[1002] เพื่อทำลายเครือข่ายการทำงานของคอมพิวเตอร์ โดยการกระทำลักษณะดังกล่าวส่งผลประการสำคัญต่อการทำลาย และอาจนำไปสู่ความเสียหายทางกายภาพต่อทั้งคอมพิวเตอร์ และรวมถึงการทำลายอุปกรณ์หรือระบบอื่นๆ ที่เชื่อมโยงกับการทำงานของคอมพิวเตอร์ด้วย ในขณะที่การใช้ระบบไซเบอร์เพื่อการจารกรรมนั้นอาจทำให้ได้มาซึ่งข้อมูลสำคัญของคู่พิพาทฝ่ายตรงข้ามในการขัดกันทางอาวุธ รวมถึงการสร้างข้อมูลข่าวสารลวงเพื่อประโยชน์ทางการทหารของกองทัพ ย่อมไม่ใช่การใช้ระบบไซเบอร์เพื่อการโจมตีแต่สามารถใช้ประกอบการขัดกันทางอาวุธเพื่อประโยชน์ทางการทหารได้ การกระทำในลักษณะนี้จึงเป็นการใช้ไซเบอร์ในสถานะของการเป็นวิธีเพื่อการขัดกันทางอาวุธ

[1000] Matthew Larkin, Brave new warfare: Autonomy in lethal UAVS**,** Master's Thesis, Naval Postgraduate School, 2011, pp.43-53. [online] Accessed: May 10, 2020. Available from: https://core.ac.uk/download/pdf/36699485.pdf

[1001] Cordula Droege, "Get off my cloud: Cyber warfare, International Humanitarian Law and the protection of civilians," International Review of the Red Cross, Volume 94 Number 886, (2012): 533-578.

[1002] William Boothby, "Some legal challenges posed by remote attack," International Humanitarian Law and the protection of civilians," International Review of the Red Cross, Volume 94 Number 886, (2012): 580.

นอกจากการกระทำในสองลักษณะนี้แล้ว การใช้งานระบบไซเบอร์ในลักษณะของการส่งโทรจันเพื่อเข้าไปยึดครองคอมพิวเตอร์เครื่องอื่นให้ปฏิบัติตามเงื่อนไขในการทำงานตามที่ได้มีการโปรแกรมไว้เพื่อการทำลายเครือข่ายคอมพิวเตอร์อื่นๆ อาจมีลักษณะของการกระทำทั้งในลักษณะการใช้เป็นอาวุธหรือปัจจัยและการใช้เป็นวิธีการไปพร้อมๆ กัน การใช้งานระบบไซเบอร์เพื่อการขัดกันทางอาวุธจึงอาจเป็นได้ทั้งการเป็นวิธีและปัจจัยในการขัดกันทางอาวุธ ซึ่งมีความแตกต่างจากการใช้อาวุธหรือการทำสงครามตามแบบที่เคยปฏิบัติกันมา โดยลักษณะของการใช้อาวุธในอดีตนั้นจะมีลักษณะเป็นการใช้อาวุธหรือการเป็นปัจจัยแต่เพียงประการเดียว และการใช้วิธีการเช่นการจารกรรมข้อมูลก็สามารถใช้จารชนเพื่อการจารกรรมข้อมูลได้ประการเดียว จารชนหรือสายลับคงไม่สามารถเป็นอาวุธในตัวเองได้ ในขณะที่อาวุธในอดีตก็ไม่สามารถทำหน้าที่เป็นจารชนได้เช่นกัน

อย่างไรก็ดี ยังมีประเด็นวิพากษ์โดยนักวิชาการอีกจำนวนมากที่ยังไม่ยอมรับว่าระบบไซเบอร์จะถือว่าเป็นอาวุธได้ เนื่องจากระบบไซเบอร์ไม่ใช่อาวุธที่จับต้องได้และก่อให้เกิดความเสียหายทางกายภาพโดยตรง จึงอาจจำต้องมีการสร้างนิยามคำว่าอาวุธที่มีความชัดเจนเพิ่มมากขึ้น[1003]

4.3.2 ข้อท้าทายต่อการจำกัดการใช้อาวุธบางประเภทในการขัดกันทางอาวุธ

ในกรอบของกฎหมายมนุษยธรรมระหว่างประเทศนั้นมีกรอบการจำกัดการใช้อาวุธใน 2 ลักษณะ คือการจำกัดวิธีการและปัจจัยในการรบและการพันธกรณีในการพิจารณาเรื่องอาวุธใหม่ ซึ่งอาจอธิบายได้ดังนี้

4.3.2.1 ข้อท้าทายข้อ 35 ของพิธีสารเพิ่มเติม ฉบับที่ 1 ค.ศ. 1977 ของอนุสัญญาเจนีวา ค.ศ.1949

กฎเกณฑ์พื้นฐานข้อ 35 เกี่ยวกับวิธีการและปัจจัยในการทำสงคราม กำหนดว่าในการขัดกันทางอาวุธนั้นมีข้อจำกัด โดยข้อจำกัดได้แก่ การห้ามใช้อาวุธ กระสุน วัตถุ และวิธีการทำสงครามในลักษณะที่ก่อให้เกิดการบาดเจ็บเกินสมควรหรือความทุกข์ทรมานเกินความจำเป็น รวมตลอดถึงการใช้วิธีการ

[1003] Heather Harrison Dinniss, Cyber Warfare and the Laws of War, p.68-70.

หรือปัจจัยในการทำสงครามที่จะทำให้สภาพแวดล้อมทางธรรมชาติเสียหายในลักษณะขยายเป็นวงกว้าง มีระยะเวลายาวนานและมีลักษณะรุนแรง[1004]

กฎเกณฑ์ข้อ 35 นี้เป็นกฎเกณฑ์ที่มีความกว้างขวาง ครอบคลุมต่อการจำกัดทั้งการใช้อาวุธและสิ่งที่ไม่ใช่อาวุธ คือทั้งวิธีการและปัจจัยอื่นๆ ที่เกี่ยวข้องกับการทำสงคราม ดังนั้นเทคโนโลยีใหม่ซึ่งมีการนำมาใช้ในการขัดกันทางอาวุธย่อมอยู่ภายใต้บทบัญญัติข้อ 35 นี้ หากเทคโนโลยีดังกล่าวเป็นอาวุธ ถูกนำมาใช้เยี่ยงอาวุธ หรือแม้แต่การใช้เป็นวิธีการหรือปัจจัยในการสงคราม โดยหากการใช้งานเทคโนโลยีนั้นก่อให้เกิดการบาดเจ็บเกินสมควรหรือความทุกข์ทรมานเกินความจำเป็น หรือทำให้สภาพแวดล้อมทางธรรมชาติเสียหายในลักษณะขยายเป็นวงกว้าง มีระยะเวลายาวนาน และมีลักษณะรุนแรง

ด้วยเหตุที่การใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นมีลักษณะที่เปลี่ยนแปลงไปจากการใช้อาวุธ วิธีการและปัจจัยในรูปแบบเดิม ทั้งในแง่ของการใช้เทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพ และการใช้เทคโนโลยีที่ไม่ก่อให้เกิดผลอย่างร้ายแรงต่อบุคคล เช่น การใช้ปฏิบัติการทางไซเบอร์เพื่อการโจมตีนั้นอาจก่อให้เกิดผลกระทบที่ร้ายแรงต่อร่างกายของบุคคลหรือไม่ก็ได้ ในกรณีที่การโจมตีทางไซเบอร์นั้นไม่ถึงขั้นก่อให้เกิดความเสียหายในรูปแบบของความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็น หรือไม่ก่อให้เกิดผลกระทบต่อสภาพแวดล้อมทางธรรมชาติอย่างกว้างขวางแล้วย่อมไม่เป็นการขัดต่อหลักเกณฑ์ดังกล่าว เช่นเดียวกับการใช้ระบบอาวุธที่ไม่ก่อให้เกิดความร้ายแรงต่อร่างกาย (Non-lethal weapons) เช่น อาวุธยิงคลื่นแม่เหล็กไฟฟ้า (Electromagnetic weapons)

แนวโน้มความเปลี่ยนแปลงทางเทคโนโลยีใหม่ในการขัดกันทางอาวุธมักเป็นการลดความเสียหายที่อาจเกิดขึ้นแก่ทั้งตัวพลรบและพลเรือน รวมทั้งสร้างความแม่นยำในการปฏิบัติต่อเป้าหมาย[1005] ประเด็นในเรื่องการพิจารณาบทบัญญัติข้อ 35 นี้จึงอาจเกิดขึ้นกับการใช้เทคโนโลยีที่ทำให้เกิดผลกระทบต่อสภาพแวดล้อมทางธรรมชาติ เช่นหากมีการพัฒนาระบบอาวุธทางอวกาศที่สามารถก่อให้เกิดสภาวะการ

[1004] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 35 Basic Rules “

1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.

2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.

3. It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.”

[1005] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p.26.

เปลี่ยนแปลงทางภูมิอากาศได้ หรือการใช้เทคโนโลยีที่อาจก่อให้เกิดภัยพิบัติทางธรรมชาติได้ย่อมเป็นการต้องห้ามตามหลักกฎหมายในเรื่องนี้

ทั้งนี้ พึงสังเกตว่าบทบัญญัติข้อ 35 นี้เป็นการสร้างข้อจำกัดเกี่ยวกับการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามเท่าที่จำเป็นต่อปฏิบัติการทางทหารแบบกว้างเท่านั้น โดยคำนึงถึงผลที่จะเกิดจากการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามบางลักษณะ แต่หากเป็นการพิจารณาหลักเกณฑ์การกระทำที่เป็นปรปักษ์ (Conduct of Hostilities) ประการอื่นๆ เช่นการปฏิบัติต่อเป้าหมาย ความได้สัดส่วนในการใช้กำลัง การแยกแยะเป้าหมาย และการระมัดระวังในการโจมตี เช่นนี้ต้องดูบทบัญญัติเฉพาะเรื่องในส่วนนั้นไป

นอกเหนือจากการใช้ข้อ 35 กับการจำกัดการใช้อาวุธ วิธีการและปัจจัยในการทำสงครามแล้ว ยังปรากฏว่ามีความพยายามในการสร้างอนุสัญญาระหว่างประเทศอีกหลายฉบับเพื่อการจำกัดและควบคุมการใช้อาวุธเฉพาะอย่างซึ่งจะเป็นประเด็นที่ได้มีการวิเคราะห์ในหัวข้อต่อไป

4.3.2.2 ข้อท้าทายต่อการใช้อาวุธตามอนุสัญญาเกี่ยวกับการห้ามใช้อาวุธเฉพาะอย่าง

เป็นที่น่าสังเกตว่าการสร้างอนุสัญญาระหว่างประเทศเพื่อควบคุมอาวุธเฉพาะอย่างนั้นเกิดขึ้นมาอย่างต่อเนื่องนับอดีตจนถึงปัจจุบัน แต่ก็ยังเป็นที่น่าสนใจว่าอนุสัญญาระหว่างประเทศทั้งหลายที่เกิดขึ้นมานั้นมักจะมีบทบาทภายหลังจากที่การขัดกันทางอาวุธจบสิ้นไปแล้วแทบทั้งหมด โดยเฉพาะอย่างยิ่งอนุสัญญาระหว่างประเทศที่เกิดขึ้นในสมัยขององค์การสหประชาชาตินั้น แทบทั้งผมดเกิดขึ้นหลังสงครามโลกครั้งที่ 2 และอนุสัญญาระหว่างประเทศเหล่านั้นก็มีผลต่อการกำจัดและการสร้างความร่วมมือระหว่างประเทศในการควบคุมการพัฒนาและการแพร่ขยายอาวุธต่างๆ เป็นสำคัญ ในขณะที่การใช้งานอาวุธหลายชนิดที่จำเป็นในการขัดกันทางอาวุธยังคงมีอยู่เช่นเดิม

ตัวอย่างที่เห็นได้ชัดเจนเช่นกรณีของพิธีสารว่าด้วยการห้ามทุ่นระเบิดสังหารบุคคลที่ออกมาตามอนุสัญญาว่าด้วยการห้ามอาวุธตามแบบบางชนิดนั้นมีบทบาทในการจัดการปัญหาทุ่นระเบิดน้อยมากเนื่องจากมีอนุสัญญาห้ามใช้ทุ่นระเบิดสังหารบุคคลอีกฉบับหนึ่งที่อยู่นอกกรอบของอนุสัญญาว่าด้วยการห้ามอาวุธตามแบบบางชนิด ซึ่งปรากฏการณ์นี้สะท้อนให้เห็นว่าการมีกฎหมายมากก็อาจไม่ได้นำไปสู่การแก้ไขปัญหาเสมอไป[1006]

[1006] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

กรณีของเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นอาจไม่จำเป็นต้องมีการสร้างอนุสัญญาระหว่างประเทศฉบับใหม่เป็นการเฉพาะเสียทีเดียว เนื่องจากเทคโนโลยีหลายประการเป็นการนำเอาสิ่งที่ไม่ใช่อาวุธโดยสภาพมาประกอบกับการใช้งานอาวุธ การจะสร้างมาตรการการปลดอาวุธหรือการลดอาวุธที่เคยเกิดขึ้นในอดีตอาจไม่จำเป็นสำหรับกรณีการใช้เทคโนโลยีใหม่นี้ และหากพิจารณารายละเอียดของการใช้เทคโนโลยีใหม่แล้วยิงจะพบว่าเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นเป็นความพยายามในการสร้างระบบการใช้อาวุธและระบบการป้องกันที่ช่วยลดความสูญเสียมากกว่าการสร้างความเสียหายรุนแรงอย่างกว้างขวาง บริบทของการบังคับใช้กฎหมายเพื่อจำกัดการใช้เทคโนโลยีใหม่เสมือนการห้ามใช้อาวุธในรูปแบบเดิมจึงไม่น่าจะเป็นการแก้ไขปัญหาที่เหมาะสม แนวทางที่อาจเป็นประโยชน์มากกว่าคือความพยายามในการนำเอากฎหมายระหว่างประเทศที่เกี่ยวข้องกับเทคโนโลยีรูปแบบต่างๆ และรวมถึงกฎหมายภายในที่สามารถปรับใช้ได้กับเทคโนโลยีแต่ละชนิดมาบังคับใช้กับการกระทำแต่ละลักษณะที่แตกต่างกันออกไป ประกอบกับการบังคับใช้อนุสัญญาเจนีวา ค.ศ.1949 พร้อมทั้งพิธีสารเพิ่มเติม ค.ศ.1977 ก็น่าจะเพียงพอต่อสิ่งที่เกิดขึ้นในปัจจุบันแล้ว

นอกจากนั้น กฎหมายระหว่างประเทศที่ควบคุมอาวุธเฉพาะอย่างนี้โดยปกติถูกสร้างขึ้นมาบนพื้นฐานของการลดอาวุธ (Disarmament) ซึ่งต่างจากการจำกัดใช้อาวุธในการขัดกันทางอาวุธในกฎหมายมนุษยธรรมระหว่างประเทศ แม้ว่าอนุสัญญาควบคุมอาวุธเฉพาะอย่างจะสร้างขึ้นมาจากหลักการจำกัดการใช้วิธีการและปัจจัยในการขัดกันทางอาวุธที่จะก่อให้เกิดความบาดเจ็บเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นก็ตาม แต่อนุสัญญาระหว่างประเทศที่ควบคุมอาวุธเฉพาะอย่างเหล่านี้มีเป้าหมายในการห้ามการผลิต การพัฒนา การถ่ายโอน เป็นสำคัญ ลักษณะของกฎหมายว่าด้วยการควบคุมอาวุธเฉพาะอย่างในกรอบของการลดอาวุธ (Disarmament) นี้จึงเป็นกฎหมายที่ใช้นอกการขัดกันทางอาวุธแต่มีบทบาทบางประการในการทำให้อาวุธบางประเภทถูกควบคุมก่อนการนำมาใช้ในการขัดกันทางอาวุธ ซึ่งเป็นผลดีต่อการใช้กฎหมายมนุษยธรรมระหว่างประเทศ

การพัฒนาการของกฎหมายว่าด้วยการลดอาวุธซึ่งมีอยู่อย่างต่อเนื่องสะท้อนให้เห็นว่าการควบคุมอาวุธเฉพาะอย่างที่อาจก่อให้เกิดผลกระทบสำคัญนั้นสามารถทำได้ง่ายกว่าการพัฒนากฎหมายมนุษยธรรมระหว่างประเทศซึ่งมีหลักเกณฑ์ทั่วไปที่ไม่ต้องการให้จำกัดเฉพาะเพียงการควบคุมอาวุธแต่กฎหมายมนุษยธรรมระหว่างประเทศต้องการควบคุมพฤติกรรมหรือการกระทำที่เป็นการละเมิดต่อบุคคลหรือทรัพย์สินที่กฎหมายมุ่งคุ้มครอง จึงไม่สามารถสร้างหลักการเพื่อจำกัดสิ่งใดสิ่ง

หนึ่งโดยเฉพาะเจาะจงได้ อนึ่งการที่กฎหมายมนุษยธรรมระหว่างประเทศดูเหมือนจะมีพัฒนาการที่ช้า แต่ก็มิได้หมายความว่ากฎหมายมนุษยธรรมระหว่างประเทศไม่มีการพัฒนา แต่การพัฒนาจะต้องอยู่บนพื้นฐานของความเหมาะสมต่อสถานการณ์ที่เปลี่ยนแปลงไปด้วยซึ่งจำเป็นต้องใช้เวลาและย่อมมีความแตกต่างจากการควบคุมอาวุธหรือเทคโนโลยีเฉพาะอย่างที่สามารถสร้างกฎหมายได้รวดเร็วกว่า

ดังที่ได้กล่าวไปในตอนต้นว่าปัญหาของการทบทวนความเหมาะสมในการพัฒนาอาวุธ วิธีการและปัจจัยที่ใช้ในการขัดกันทางอาวุธนั้นค่อนข้างเป็นจุดอ่อนของพิธีสารเพิ่มเติมฉบับที่ 1 นี้ เช่นเดียวกับการบังคับใช้กฎหมายระหว่างประเทศโดยทั่วไป เนื่องจากการขาดองค์กรบังคับ รวมตลอดถึงการเมืองระหว่างประเทศที่เป็นอุปสรรคต่อการบังคับใช้กฎหมายระหว่างประเทศ ทำให้การรายงานเกี่ยวกับการพิจารณาความเหมาะสมในการพัฒนาอาวุธใหม่เกิดขึ้นเพียงในบางประเทศในขณะที่หลายประเทศไม่มีกระบวนการดังกล่าว ทั้งนี้การแก้ไขปัญหาดังกล่าวเป็นเรื่องที่ค่อนข้างยาก แนวทางที่สามารถทำได้จึงอาจอยู่ในลักษณะของการตรวจตราในรูปแบบการรายงานข้อเท็จจริงเกี่ยวกับพัฒนาการทางอาวุธ วิธีการและปัจจัยในการขัดกันทางอาวุธโดยเจ้าหน้าที่พิเศษที่จะต้องมีการจัดตั้งขึ้นมาในลักษณะของผู้รายงานพิเศษ ที่สามารถเข้าถึงข้อมูลต่างๆ ได้ ทั้งจากข้อเท็จจริงที่เกิดขึ้นจากสถานการณ์จริงและการพิจารณาข้อกฎหมายของรัฐต่างๆ รวมถึงรายงานจากหน่วยงานต่างๆ ซึ่งผู้รายงานนี้อาจทำงานเชื่อมต่อกับองค์กรเอกชนที่ทำงานด้านอาวุธ และหน่วยงานภาครัฐที่ยินดีให้ข้อมูล เพื่อให้ได้ข้อเท็จจริงที่เที่ยงตรงมากที่สุดเท่าที่จะทำได้ และนำไปสู่การประเมินผลการปฏิบัติตามพันธกรณีข้อ 36 นี้

การพิจารณาถึงลักษณะความเป็นอาวุธของเทคโนโลยี และการใช้เทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพเป็นสารสำคัญอีกประการหนึ่งที่ต้องพิจารณา ทั้งนี้ตามข้อ 36 นั้น ระบุหัวข้อเรื่องการพัฒนาอาวุธ แต่ในสาระของข้อ 36 นั้นได้มีการกล่าวถึงทั้งการพัฒนาอาวุธ วิธีการและปัจจัย ในรายละเอียดจึงมีเนื้อหาที่กว้างกว่าหัวข้อที่กำหนด เป้าหมายของการใช้กฎหมายข้อนี้จึงน่าจะมีความกว้างขวางกว่าการพัฒนาอาวุธ อย่างไรก็ดีการนำเอาเทคโนโลยีของพลเรือนมาใช้ในการทหารจะถือว่าเป็นประเด็นการพัฒนาอาวุธ วิธีการหรือปัจจัยใหม่หรือไม่ ยังเป็นเรื่องที่ต้องการความชัดเจน เพราะเทคโนโลยีที่พัฒนามาเพื่อการใช้งานของพลเรือนถูกนำมาใช้ทางทหารอย่างแพร่หลาย[1007]

[1007] Hitoshi Nasu, “Nanotechnology and the law of armed conflict,” in Hitoshi Nasu and Robert McLaughlin, editors., New Technologies and the Law of Armed Conflict, p. 154.

ปัญหาประการต่อมาคือหากมีการไม่ปฏิบัติตามข้อ 36 นี้จะต้องทำอย่างไร ทางแก้ไขปัญหานั้นอาจเป็นไปได้ยากที่จะมีการกำหนดโทษแก่รัฐผู้ไม่ปฏิบัติตามพันธกรณี แต่อาจทำโดยประการอื่น เช่นการสร้างมาตรการกดดันผ่านองค์กรย่อยระดับภูมิภาค หรือสร้างกลุ่มความร่วมมือระหว่างประเทศโดยเฉพาะขึ้นมา เพื่อให้ประเทศต่างๆ เกิดความตระหนักถึงปัญหาจากการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธและเกิดการตรวจสอบระหว่างกันเองมากขึ้น

อย่างไรก็ดีการทำให้ข้อ 36 บรรลุเป้าหมายได้นั้นเป็นเรื่องที่อาจไม่สามารถกระได้อย่างสมบูรณ์ แต่การสร้างความเคลื่อนไหวเพียงเล็กน้อยอาจทำให้ความเข้าใจและความรับรู้เกี่ยวกับผลกระทบจากเทคโนโลยีใหม่ได้รับความสนใจในทางระหว่างประเทศมากขึ้น

จากการศึกษาวิเคราะห์ในบทที่ 4 พบว่าข้อท้าทายประการสำคัญของเทคโนโลยีใหม่ในการขัดกันทางอาวุธต่อกฎหมายมนุษยธรรมระหว่างประเทศคือการพัฒนาการทางเทคโนโลยี นั้นเปลี่ยนแปลงรูปแบบการขัดกันทางอาวุธไปอย่างมีนัยสำคัญ ความเปลี่ยนแปลงดังกล่าวเกิดขึ้นกับสารสำคัญของการกระทำซึ่งเป็นขอบเขตที่กฎหมายมนุษยธรรมระหว่างประเทศยังมีพัฒนาการในเรื่องดังกล่าวค่อนข้างน้อย กล่าวคือเดิมนั้นกฎหมายมนุษยธรรมระหว่างประเทศมีพัฒนาการหลักในเรื่องขอบเขตการปรับใช้กฎหมายและลักษณะของสถานการณ์การขัดกันทางอาวุธซึ่งประเด็นทั้งสองนี้กฎหมายมนุษยธรรมระหว่างประเทศใช้เวลาอย่างอย่าวนานจนกระทั่งผู้สร้างกฎหมายสามารถสกัดเอาแนวคิดที่ได้จากการขัดกันทางอาวุธในอดีตมาสร้างเป็นหลักการที่ปรากฏในกฎหมายมนุษยธรรมระหว่างประเทศได้ ในขณะที่สาระสำคัญของการกระทำ เช่นการใช้สิ่งที่ไม่ใช่อาวุธมาประกอบการใช้อาวุธหรือนำสิ่งที่ไม่ใช่อาวุธมาใช้เยี่ยงอาวุธตัวอย่างของกรณีการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้น ยังเป็นขอบเขตที่กฎหมายมนุษยธรรมระหว่างประเทศยังไม่มีพัฒนาการเรื่องดังกล่าวเท่าที่ควร เมื่อกฎหมายมนุษยธรรมระหว่างประเทศต้องเผชิญหน้ากับสถานการณ์ที่เปลี่ยนแปลงทางเทคโนโลยีจึงทำให้ในบางกรณีกฎหมายมนุษยธรรมระหว่างประเทศอาจยังไม่เพียงพอต่อการแก้ไขปัญหาที่เกิดขึ้นหรืออาจเกิดขึ้นได้

อย่างไรก็ดี กรอบของกฎหมายการลดอาวุธ (Disarmament) และกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการควบคุมเทคโนโลยีบางชนิดซึ่งไม่ใช่กฎหมายมนุษยธรรมระหว่างประเทศในตัวเองยังมีบทบาทเป็นส่วนเสริมให้เทคโนโลยีบางชนิดถูกควบคุมการใช้งาน แม้ขอบเขตการควบคุมดังกล่าวอยู่นอกสถานการณ์การขัดกันทางอาวุธแต่ก็ทำให้อาวุธหรือเทคโนโลยีดังกล่าวไม่ถูกนำมาใช้ในการขัดกันทางอาวุธได้

บทที่ 5

บทสรุปและข้อเสนอแนะ

พัฒนาการทางเทคโนโลยียุคปัจจุบันที่มีลักษณะใช้งานได้ทั้งเพื่อประโยชน์พลเรือนและประโยชน์ทางทหารมีบทบาทอย่างมากต่อการขัดกันทางอาวุธ[1008] เทคโนโลยีเหล่านี้สร้างประเด็นพิจารณาหลายประการต่อกฎหมายมนุษยธรรมระหว่างประเทศเนื่องจากการใช้งานเทคโนโลยีเป็นสาระสำคัญที่เกิดขึ้นในการกระทำ ซึ่งเป็นข้อท้าทายใหม่ที่เกิดขึ้นกับกฎหมายมนุษยธรรมระหว่างประเทศ โดยกฎหมายมนุษยธรรมระหว่างประเทศที่พัฒนามาจนถึงปัจจุบันนั้นเป็นการทำให้กฎหมายมีหลักการที่ครอบคลุมขอบเขตการปรับใช้กฎหมาย (Scope of application) ต่อสถานการณ์ (Situation) และการกระทำ (ปฏิบัติการ) ของบุคคลที่เกี่ยวข้องกับการขัดกันทางอาวุธ (Conduct of Hostilities) ที่หลากหลาย ซึ่งสะท้อนผ่านหลักการจำกัดวิธีการและปัจจัยในการรบรวมตลอดถึงหลักพื้นฐานเรื่องการแยกแยะเป้าหมาย ความได้สัดส่วนในการโจมตีและความระมัดระวังล่วงหน้าก่อนการโจมตี

การใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธนั้นในปัจจุบันมีแนวโน้มที่จะเป็นการใช้งานเทคโนโลยีที่ไม่ใช่อาวุธโดยสภาพเพื่อประกอบการทำงานกับระบบอาวุธมากขึ้น แม้กรอบของการพิจารณาเรื่องเทคโนโลยีใหม่จะรวมถึงการควบคุมการใช้อาวุธใหม่ด้วยก็ตาม แต่ลักษณะการใช้งานเทคโนโลยีใหม่หลายชนิดมักอยู่ในลักษณะของการใช้เป็นวิธีการในการรบหรือเป็นปัจจัยที่เกี่ยวข้องกับการใช้อาวุธมากกว่าการเป็นอาวุธ เทคโนโลยีใหม่จึงเปลี่ยนรูปแบบการใช้อาวุธที่เกิดขึ้นมาในสงครามโลกทั้งสองครั้งที่มุ่งแข่งขันการสร้างอาวุธที่มีอานุภาพทำลายล้างสูง นอกจากนั้นการทำลายเป้าหมายด้วยเทคโนโลยีใหม่ก็เปลี่ยนแปลงไปด้วย ทั้งการใช้เทคโนโลยีระบุตำแหน่งบนพื้นโลกผ่านดาวเทียมที่ชัดเจนร่วมกับการใช้งานระบบอาวุธทำให้การโจมตีเป้าหมายมีความแม่นยำมากขึ้นและเทคโนโลยีระบุตำแหน่งบนพื้นโลกยังเป็นประโยชน์ประโยชน์ต่อการสื่อสารรวมถึงการใช้ระบบอาวุธเพื่อการป้องกันประเทศด้วย

ลักษณะของการใช้งานเทคโนโลยีไซเบอร์ที่มีลักษณะการทำงานของระบบคอมพิวเตอร์เชื่อมต่อการสื่อสารผ่านช่องทางอิเล็กทรอนิกส์ทำให้ลักษณะการกระทำในทางกายภาพหายไป[1009]

[1008] Patricia Justino, “The Conflict in Ukraine – The Role of Civilians,” UNU Wider. (February 2022) [online] Accessed: March 26, 2022. Available from: https://www.wider.unu.edu/publication/conflict-ukraine-role-civilians

[1009] Patricia Justino, “The Conflict in Ukraine – The Role of Civilians,”

การปรากฏตัวตนของผู้กระทำการและผู้ได้รับความเสียหายซึ่งอยู่ห่างด้วยระยะทางในสื่อกลางที่ระบุตัวตนได้ยากนี้ ยิ่งนำไปสู่ปัญหาหลายประการในการระบุตัวผู้ที่เกี่ยวข้องในปฏิบัติการ[1010] และเมื่อมีการนำปฏิบัติการทางไซเบอร์มาใช้ในการขัดกันทางอาวุธเพื่อร่วมกับการโจมตีตามแบบปกติก็ยิ่งทำให้ปรากฏการของการขัดกันทางอาวุธในปัจจุบันยกระดับเป็นสงครามที่ก่อให้เกิดทั้งความเสียหายทางกายภาพ ความเสียหายต่อจิตใจ และผลกระทบต่อการเข้าถึงข้อมูลข่าวสารเป็นอย่างมาก ตัวอย่างของการขัดกันทางอาวุธระหว่างประเทศยูเครนและประเทศรัสเซียเป็นภาพสะท้อนของการทำสงครามที่เปลี่ยนแปลงรูปแบบการทำสงครามในโลกยุคเดิมไปอย่างมาก

ขณะที่การโจมตีทางไซเบอร์เป็นเครื่องมือสำคัญในการโจมตีทางด้านสารสนเทศ บทบาทของอากาศยานไร้คนขับก็ทวีคูณแสดงความสำคัญในความขัดแย้งระหว่างประเทศมากยิ่งขึ้น ทั้งการใช้อากาศยานไร้คนขับเพื่อการโจมตีในการขัดกันทางอาวุธระหว่างประเทศ ไม่ว่าจะเป็นกรณีความขัดแย้งระหว่างประเทศยูเครนและประเทศรัสเซีย หรือเหตุการณ์ก่อนหน้าที่กองทัพสหรัฐอเมริกาได้ใช้อากาศยานไร้คนขับปฏิบัติการในพื้นที่ตะวันออกกลางหลายปฏิบัติการ ทั้งที่อากาศยานไร้คนขับนั้นเป็นอุปกรณ์ที่มีลักษณะการใช้งานคล้ายคลึงกับการใช้งานระบบไซเบอร์ คือทั้งพลเรือนและทหารต่างเข้าถึงเทคโนโลยีเหล่านี้ได้ ใช้งานในลักษณะเดียวกัน แต่เปลี่ยนแปลงวัตถุประสงค์การใช้งานให้เข้ากับความต้องการในปฏิบัติการที่แตกต่างกัน

นอกจากนั้นเทคโนโลยีปัญญาประดิษฐ์ การใช้งานระบบอัลกอริทึ่มในสายงานด้านวิทยาศาสตร์คอมพิวเตอร์ยังมีบทบาทอย่างมากต่อพัฒนาการทางอาวุธของทหาร ทำให้อาวุธมีความแม่นยำมากขึ้นและเป็นประโยชน์ทั้งต่อการป้องกันประเทศและการโจมตีศัตรูมากขึ้น[1011] การพัฒนาดังกล่าวสร้างความตระหนกแก่สังคมระหว่างประเทศอย่างมากต่อโอกาสที่จะเกิดหุ่นยนต์สังหารทางการทหารขึ้นในอนาคต

ปัญหาหลายประการนำไปสู่ข้อท้าทายต่อกฎหมายมนุษยธรรมระหว่างประเทศว่ากฎหมายที่มีอยู่จะเหมาะสมและพอเพียงต่อการปรับใช้อย่างไร ทั้งประเด็นเรื่องการแยกแยะพื้นที่ทางไซเบอร์ระหว่างทหารและพลเรือน และแยกเทคโนโลยีที่เกี่ยวข้องกับทหารโดยตรงและที่เกี่ยวข้องเฉพาะกับพลเรือน การโจมตีด้วยเทคโนโลยีไซเบอร์ การโจมตีด้วยอากาศยานไร้คนขับและการโจมตีด้วยอาวุธอิสระจะมีการควบคุมที่สอดคล้องต่อหลักความได้สัดส่วนอย่างเพียงพอหรือไม่ รวมตลอดถึงการ

[1010] Timothe Lopez, L'adaptabilité du droit international humanitaire aux évolutions des conflits armés contemporains, p. 86.

[1011] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

ประเมินผลกระทบที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์จะกระทำได้เพียงไร เป็นต้น ข้อท้าทายเหล่านี้นำไปสู่ความพยายามในสังคมระหว่างประเทศหลายประการ ทั้งการสร้างคู่มือทาลลินน์ว่าด้วยปฏิบัติการทางไซเบอร์ซึ่งเป็นการนำเอากฎหมายระหว่างประเทศรวมถึงกฎหมายมนุษยธรรมระหว่างประเทศมาปรับใช้กับปฏิบัติการทางไซเบอร์และการโจมตีทางไซเบอร์ในการขัดกันทางอาวุธ และความพยายามของสหประชาชาติในการสร้างกฎหมายระหว่างประเทศเกี่ยวกับระบบอาวุธอิสระ (Autonomous Weapons Systems) โดยกรณีความพยายามของสหประชาชาติในการสร้างกฎหมายระหว่างประเทศเพื่อควบคุมอาวุธเฉพาะอย่างนี้ยังมีสถานะเป็นร่างกฎหมาย ด้วยสาเหตุที่ยังอาจไม่สามารถกำหนดหลักการที่แน่นอนได้เนื่องจากการพัฒนาระบบอาวุธสังหารอิสระยังอยู่ในระหว่างการพัฒนาและไม่แน่ว่าในอนาคตจะเทคโนโลยีเหล่านี้จะเป็นอย่างไร[1012]

เทคโนโลยีการสื่อสารผ่านระบบดาวเทียมเพื่อการกำหนดตำแหน่งพื้นที่บนโลก (GPS) ที่ประชาชนใช้งานกันปกติจนเป็นสื่อกลางสาธารณะก็ไม่ได้มีบทบาทแต่เพียงการใช้งานเพื่อประโยชน์ทางพลเรือนเท่านั้นแต่ยังเป็นประโยชน์ทางการทหารอย่างมาก ปัญหาในการแบ่งแยกพื้นที่ทางการทหารและพลเรือนย่อมมีไม่น้อย หากในการขัดกันทางอาวุธมีการขัดขวางสัญญาณดาวเทียมเพื่อทำลายขีดความสามารถทางการทหารของฝ่ายศัตรูแต่ความเสียหายดังกล่าวส่งผลต่อพลเรือนในวงกว้างด้วย กฎหมายมนุษยธรรมระหว่างประเทศจะคุ้มครองพลเรือนได้อย่างไร

ปัญหาสำคัญสำหรับการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศประการหนึ่งคือการที่กฎหมายจะต้องเผชิญหน้ากับประเด็นเรื่องอำนาจอธิปไตยและการที่ไม่มีองค์กรใดมีอำนาจเหนือรัฐในการปรับใช้กฎหมายและบังคับให้การปฏิบัติเป็นไปตามกฎหมายได้ทั้งหมด เมื่อคำนึงถึงมุมมองทางการเมืองที่แตกต่างกันรวมถึงการตีความสถานการณ์ต่างๆ ที่แตกต่างกันยิ่งทำให้การปรับใช้กฎหมายเป็นไปอย่างยากขึ้น[1013] อย่างไรก็ดีคณะมนตรีความมั่งคงแห่งสหประชาชาติก็เป็นหน่วยงานในองค์การระหว่างประเทศที่สามารถชี้ได้ว่าการกระทำของรัฐใดเป็นการโจมตีหรือการคุกคามหรือไม่ภายใต้อำนาจหน้าที่ในหมวด 7 ของกฎบัตรสหประชาชาติ ในขณะที่ศาลยุติธรรมระหว่างประเทศทำ

[1012] United Nations, “Report of the 2023 session of the Group of the Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,” CCW/GGE.1/2023/2, 24 May 2023, Para 20.

[1013] Olivier Durr, “Humanitarian Law of Armed Conflict: Problems of Applicability,” Journal of Peace Research, Vol.24 No.3 (1987): 263. [online] Accessed May 20, 2022. Available form: https://journals.sagepub.com/doi/abs/10.1177/0022343387 02400306

หน้าที่ระงับข้อพิพาทระหว่างประเทศที่เกิดขึ้นได้[1014] คำพิพากษาของศาลระหว่างประเทศนี้ไม่ได้เป็นเพียงการจำกัดความแนวคิดสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศแต่ยังเป็นการขยายความสาระสำคัญของกฎหมายระหว่างประเทศด้วย[1015]

5.1 บทสรุป

เมื่อพิจารณาจากความสามารถในการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศโดยคำนึงถึงการปรับตัวของกฎหมายเพื่อแก้ไขปัญหาเฉพาะหน้าที่เกิดขึ้น ความพอเพียงเหมาะสมในการปรับตัวของกฎหมายต่อข้อเท็จจริง บทบาทของศาลระหว่างประเทศในการพัฒนาการปรับตัวของกฎหมาย และการปรับตัวของกฎหมายมนุษยธรรมระหว่างประเทศโดยไม่บิดเบือนต่อหลักการพื้นฐานองกฎหมายมนุษยธรรมระหว่างประเทศ จะพบว่าแม้กฎหมายมนุษยธรรมระหว่างประเทศจะไม่ได้มีข้อกฎหมายที่ครอบคลุมทุกเรื่องทุกสถานการณ์ แต่หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศมีลักษณะเป็นการทั่วไป และมีคุณลักษณะยืดหยุ่นเพียงพอที่จะนำมาปรับใช้กับสถานการณ์การขัดกันทางอาวุธที่เปลี่ยนแปลงไปได้ในระดับหนึ่ง แต่การพัฒนากฎหมายมนุษยธรรมระหว่างประเทศเพื่อแก้ไขปัญหาและข้อท้าทายที่เกิดขึ้นใหม่ๆ นั้นจะต้องอาศัยเวลาและโอกาสที่เหมาะสม กฎหมายมนุษยธรรมระหว่างประเทศมีความเปลี่ยนแปลงและพัฒนาการตลอดเวลา ไม่เฉพาะแต่การแก้ไขกฎหมายลายลักษณ์อักษรแต่รวมถึงการนำหลักการพื้นฐานของกฎหมายมาใช้อย่างเหมาะสมและสอดคล้องต่อสถานการณ์โดยไม่ต้องมีการแก้ไขเปลี่ยนแปลงกฎหมายด้วย

กฎหมายมนุษยธรรมระหว่างประเทศซึ่งมีผลบังคับใช้ในสถานการณ์การขัดกันทางอาวุธนั้นสามารถนำมาใช้บังคับต่อกรณีการใช้เทคโนโลยีใหม่ได้เนื่องจากเทคโนโลยีทั้งหลาย อันได้แก่ เทคโนโลยีไซเบอร์ เทคโนโลยีอากาศยานไร้คนขับ เทคโนโลยีอาวุธอิสระ เทคโนโลยีนาโน และเทคโนโลยีอวกาศ ฯลฯ ล้วนแล้วแต่ถูกนำมาใช้เป็นได้ทั้งอาวุธ ปัจจัย และวิธีการในการขัดกันทางอาวุธได้ทั้งสิ้น เมื่อเทคโนโลยีดังกล่าวเป็นอาวุธ เป็นปัจจัยหรือเป็นวิธีการในการขัดกันทางอาวุธได้ก็ย่อมถูกจำกัดวิธีการใช้งานที่จะต้องไม่ละเมิดต่อกฎหมายมนุษยธรรมระหว่างประเทศเช่นกัน

[1014] Vincent Chetail, “The Contribution of the International Court of Justice to International Humanitarian Law,” International Review of the Red Cross, Vol. 85, No. 850, (2003): 235. [online] Accessed: May 20, 2023. Available from: https://www.icrc.org/en/doc/assets/files/other/irrc_850_chetail.pdf

[1015] Michael J. Matheson et Djamchid Momtaz, Les règles et institutions du droit international humanitaire à l’épreuve des conflits armés récents, (Leiden: Martinus Nijhoff Publishers, 2010): 139.

การใช้งานเทคโนโลยีในฐานะเป็นอาวุธนั้นอาจต้องพิจารณาเงื่อนไข 2 ประการ คือ 1) ความชอบด้วยกฎหมายของการใช้อาวุธว่าเป็นอาวุธที่สามารถใช้ได้ในการขัดกันทางอาวุธเพราะไม่ละเมิดต่อหลักเกณฑ์พื้นฐานในการทำสงคราม กับ 2) เทคโนโลยีลักษณะอาวุธนั้นต้องห้ามตามอนุสัญญาเกี่ยวกับอาวุธเรื่องใดหรือไม่

ในขณะที่เทคโนโลยีที่ถูกนำมาใช้เป็นวิธีการในการขัดกันทางอาวุธนั้นจะต้องสอดคล้องต่อหลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศ คือไม่ก่อให้เกิดความเสียหายเกินขนาดหรือความทุกข์ทรมานเกินความจำเป็นด้วย

นอกจากนั้นในการพิจารณาลักษณะการใช้งานเทคโนโลยีเพื่อการโจมตีและการป้องกันตนเองในปฏิบัติการทางทหารจะต้องสอดคล้องต่อหลักเกณฑ์การปฏิบัติที่เป็นปฏิปักษ์ซึ่งเป็นหัวใจสำคัญของกฎหมายว่าด้วยการขัดกันทางอาวุธซึ่งมีที่มาแต่ยุคดั้งเดิมจนเปลี่ยนสภาพเป็นกฎหมายมนุษยธรรมระหว่างประเทศในยุคปัจจุบันด้วย

อย่างไรก็ดีการนำเทคโนโลยีใหม่มาใช้ในการขัดกันทางอาวุธก่อให้เกิดประเด็นต่างๆ ที่ต้องพิจารณารวมถึงสร้างข้อท้าทายหลายประการต่อกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งในเรื่องการกำหนดลักษณะความเป็นเทคโนโลยีใหม่ การใช้เทคโนโลยีใหม่เพื่อก่อการขัดกันทางอาวุธและหลักการที่เกี่ยวข้องกับการปฏิบัติการทางทหาร โดยเทคโนโลยีที่สร้างปัญหาต่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศมากที่สุดคือการใช้ระบบปฏิบัติการทางไซเบอร์เพื่อการโจมตี และการใช้ระบบอาวุธสังหารที่ตัดสินใจได้ด้วยตนเองซึ่งทำงานผ่านระบบประมวลผลแบบอัลกอริทึ่ม ซึ่งกระทบต่อทั้งหลักการก่อการขัดกันทางอาวุธ หลักการแยกแยะเป้าหมาย หลักความระมัดระวังล่วงหน้าในการโจมตี และหลักความได้สัดส่วน นอกจากนั้นยังมีปัญหาในเรื่องตัวตนของผู้ปฏิบัติการในการขัดกันทางอาวุธซึ่งกระทบต่อความรับผิดชอบในกรณีที่เกิดการละเมิดกฎหมายด้วย

จากข้อสรุปดังกล่าวจึงนำไปสู่ข้อเสนอแนะในการแก้ไขการปรับใช้หลักกฎหมายมนุษยธรรมระหว่างประเทศดังต่อไปนี้

5.2 ข้อเสนอแนะ

แม้กฎหมายมนุษยธรรมระหว่างประเทศจะสามารถปรับใช้กับเทคโนโลยีใหม่ได้ แต่มีประเด็นที่ต้องคำนึงถึงดังต่อไปนี้

1. การแก้ไขเพิ่มเติมกฎหมายสารบัญญัติ

1.1 การเกิดการขัดกันทางอาวุธ

สถานะปัจจุบันของเทคโนโลยีไซเบอร์สร้างปัญหาสำคัญต่อการพิจารณาการเกิดการขัดกันทางอาวุธที่จะนำไปสู่การปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศเนื่องจากลักษณะของการกระทำทางไซเบอร์ การโจมตีทางไซเบอร์มีวิธีการที่หลากหลายและอาจนำมาซึ่งผลที่หลากหลายการแก้ไขกฎหมายมนุษยธรรมระหว่างประเทศอาจเป็นเรื่องที่ยากในปัจจุบัน ยังคงจำเป็นต้องรอเวลาและโอกาสที่เหมาะสมเพื่อการพัฒนากฎหมายต่อไป

แนวโน้มในอนาคตอาจเป็นไปได้ว่าควรมีการรับรองพื้นที่ทางไซเบอร์เป็นพื้นที่หนึ่งในการรบและกำหนดลักษณะการกระทำการบนพื้นที่ทางไซเบอร์ที่ชัดเจนว่าการกระทำใดจึงถือว่าเป็นการโจมตีและก่อให้เกิดการขัดกันทางอาวุธ โดยจะต้องสร้างนิยามเฉพาะที่อาจแตกต่างจากกฎหมายมนุษยธรรมระหว่างประเทศที่มีอยู่ในปัจจุบันและอาจการทำสงครามหรือการขัดกันทางอาวุธในอนาคตอาจมหายรวมถึงการทำสงครามบนพื้นที่ไซเบอร์ด้วย ทั้งนี้จะต้องคำนึงถึงบริบทต่างๆที่เหมาะสมด้วย

1.2 หลักการพื้นฐานของกฎหมายมนุษยธรรมระหว่างประเทศ

การแยกแยะเป้าหมายในการโจมตีอาจมีประเด็นที่เกี่ยวข้องกับการใช้เทคโนโลยีไซเบอร์เพื่อการโจมตีค่อนข้างมากจำเป็นที่จะต้องพิจารณาอย่างถี่ถ้วน สิ่งที่น่าสนใจคือในกฎหมายภายในที่เกี่ยวข้องกับกิจกรรมทางอิเล็กทรอนิกส์ได้แก่กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมตลอดถึงกฎหมายเกี่ยวกับความมั่นคงทางไซเบอร์เหล่านี้ล้วนแล้วแต่มีบทสันนิษฐานเพื่อระบุตัวตนของผู้ใช้งานระบบไซเบอร์ เช่น ผู้นำเข้าข้อมูล ผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ ฯลฯ

หากจะพิจารณาว่าเป็นไปได้หรือไม่ที่จะนำเอาบทสันนิษฐานผู้ใช้งานระบบไซเบอร์ตามกฎหมายธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายอาชญากรรมทางคอมพิวเตอร์มาใช้กับกฎหมายมนุษยธรรมระหว่าประเทศนั้นน่าจะมีประเด็นที่ต้องพิจารณาปลายประการ ได้แก่ ประการที่ 1 กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายอาชญากรรมทางไซเบอร์ที่กล่าวถึงนี้เป็นกฎหมายภายใน จึงเป็นเรื่องการใช้อำนาจอธิปไตยของรัฐในการดำเนินการบังคับกับบุคคลเพื่อให้สามารถดำเนินกระบวนการยุติธรรมกับคดีที่เกี่ยวข้องกับเขตอำนาจของรัฐ แต่กฎหมายมนุษยธรรมระหว่างประเทศอยู่บนพื้นฐานของข้อตกลงระหว่างสมาชิกซึ่งต่างมีอำนาจอธิปไตยเท่าเทียมกัน หากมีบทสันนิษฐานว่าผู้ใดกระทำความผิดทางไซเบอร์อาจเป็นไปได้ค่อนข้างยากที่จะดำเนินการตามกฎหมายกับบุคคลดังกล่าวหากบุคคลนั้นอยู่ในรัฐอื่นและการดำเนินคดีจะต้องอาศัยความร่วมมือระหว่าง

ประเทศ แต่บทสันนิษฐานเรื่องผู้กระทำการนี้อาจเป็นประโยชน์ในกรณีที่รัฐผู้เสียหายจากการโจมตีทางไซเบอร์สามารถจับกุมตัวบุคคลดังกล่าวได้ ประการที่ 2 การตรวจสอบความถูกต้องแท้จริงของตัวผู้กระทำการผ่านระบบข้อมูลทางดิจิทัลตามกฎหมายภายในประเทศย่อมทำได้สะดวกกว่าการดำเนินการตามกฎหมายระหว่างประเทศ กล่าวคือแม้จะมีบทสันนิษฐานว่าผู้ใดเป็นผู้กระทำการในปฏิบัติการทางไซเบอร์ใดหรือการโจมตีทางไซเบอร์ใดในการขัดกันทางอาวุธ แต่หากรัฐผู้ผู้เสียหายไม่สามารถเข้าถึงข้อมูลการจราจรทางไซเบอร์เพราะจะต้องขออนุญาตจากรัฐเจ้าของข้อมูลดังกล่าว บทสันนิษฐานเรื่องผู้กระทำการนี้ก็อาจไม่เป็นประโยชน์ทางปฏิบัติ ต่างจากการบังคับใช้กฎหมายภายในที่เกี่ยวข้องกับรัฐเดียวในการดำเนินการสืบหาข้อมูลผู้กระทำความผิดในรัฐตน

หลักความได้สัดส่วนในการโจมตีอาจต้องมีการสร้างคำจำกัดความที่ชัดเจนขึ้นว่าการโจมตีทางไซเบอร์ที่กระทำต่อระบบไซเบอร์ลักษณะใดจึงถือว่าสอดคล้องต่อหลักความได้สัดส่วน เช่นเดียวกันกับการโจมตีโดยการใช้ระบบอาวุธอิสระว่าการโจมตีโดยระบบอาวุธอิสระในระดับใดจึงถือว่าเป็นการกระทำที่สอดคล้องต่อหลักความได้สัดส่วนในการโจมตี ประเด็นสำคัญคือการแยกทรัพยากรทางไซเบอร์ระหว่างทหารและพลเรือนจะกระทำได้อย่างไร ปัญหานี้น่าจะนำไปสู่การกำหนดให้ข้อมูลทางคอมพิวเตอร์รูปแบบใดจะต้องได้รับความคุ้มครองตามกฎหมายมนุษยธรรมระหว่างประเทศ ข้อมูลลักษณะใดเป็นของพลเรือนและข้อมูลรูปแบบใดหรือแฟลตฟอร์มใดเป็นทรัพยากรทางทหาร

อย่างไรก็ดีแม้ในปัจจุบันจะไม่มีคำจำกัดความที่ชัดเจนแต่ด้วยเหตุที่ยังไม่มีกรณีศึกษาที่เกิดขึ้นจริง จึงยังอาจสรุปไม่ได้ว่าการคาดการณ์ที่กล่าวมานี้จะเป็นสิ่งที่เหมาะสมหรือไม่

ในเรื่องหลักการระมัดระวังล่วงหน้าก่อนการโจมตีจะต้องมีการสร้างคำอธิบายเกี่ยวกับเรื่องการประเมินความเสียหายที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ การใช้ระบบอาวุธที่ตัดสินใจได้ด้วยตนเอง (Autonomous weapon system) หรือระบบการตัดสินในแบบอัตโนมัติของซอฟท์แวร์คอมพิวเตอร์แบบอัลกอริที่มว่าการปฏิบัติการในลักษณะใด ภายใต้การควบคุมของมนุษย์ในรูปแบบใดจึงจะถือว่าสอดคล้องต่อหลักการ และหากเป็นการปฏิบัติการโดยปราศจากมนุษย์ทั้งรูปแบบจะประเมินอย่างไรว่าปฏิบัติการนั้นเป็นไปโดยชอบด้วยหลักเกณฑ์ทางกฎหมาย

ทั้งนี้ กฎหมายที่ชัดเจนขึ้นไม่ได้หมายความว่าจะต้องมีความละเอียดมากขึ้น เพราะจุดเด่นสำคัญของกฎหมายมนุษยธรรมระหว่างประเทศคือลักษณะของความเป็นกลางของหลักการที่สามารถยืดหยุ่นและเพียงพอเหมาะสมต่อการปรับใช้ในสถานการณ์ที่หลากหลายได้ เพียงแต่อาจจำเป็นต้อง

สร้างนิยามที่เหมาะสมต่อเทคโนโลยีบางประการที่จะกระทบต่อหลักความระมัดระวังล่วงหน้าก่อนการโจมตี

ลักษณะการกระทำที่ถือว่าเป็น Levee en Masse

ปัญหาเรื่องการพิจารณาลักษณะการกระทำที่เป็น Levee en Masse อาจต้องมีการสร้างนิยามทางกฎหมายมนุษยธรรมระหว่างประเทศว่าปฏิบัติการทางไซเบอร์กรณีใดบ้างที่จะถือว่าสามารถปรับใช้หลัก Levee en Masse ได้บ้างดังที่ได้กล่าวมาในบทที่ 4 โดยอาจต้องสร้างนิยามของการเป็น Levee en Masse ที่เหมาะสมกับการใช้งานไซเบอร์ของพลเรือนมากขึ้นและคำนึงถึงลักษณะการใช้งานไซเบอร์ที่แตกต่างไปจากเดิม โดยอาศัยหลักการพื้นฐานเรื่องปัจจัยและวิธีในการรบการกระทำที่เป็น Levee en Masse ในปฏิบัติการทางไซเบอร์อาจต้องก้าวข้ามลักษณะการใช้อาวุธตามแบบดั้งเดิมไป และมองว่าไซเบอร์เป็นเครื่องมือของพลเรือนในการเข้ามามีส่วนร่วมในการรบได้

1.3 หลักเกี่ยวกับสถานภาพของพลรบ

(1) การสวมเครื่องแบบ

อาจมีความจำเป็นในการแก้ไขพิธีสารเพิ่มเติมฉบับที่ 1 ของอนุสัญญาเจนีวา ค.ศ. 1977 ในบทบัญญัติข้อ 44 (3) ในเรื่องการแสดงตนของพลรบที่จะต้องแตกต่างจากพลเรือนในขณะที่กำลังทำการโจมตี และการถืออาวุธโดยเปิดเผยซึ่งจะต้องคำนึงถึงปฏิบัติการโจมตีทางไซเบอร์และปฏิบัติการโจมตีโดยระบบอาวุธตัดสินใจด้วยตนเองโดยเฉพาะที่เกิดจากการประมวลผลแบบอัลกอริทึ่มให้มากขึ้น โดยจะต้องพิจารณาองค์ประกอบใหม่ของการแสดงตนของพลรบที่ไม่จำต้องสวมเครื่องแบบที่แตกต่างเสมอไป แต่จะต้องคำนึงถึงลักษณะการปฏิบัติการที่กระทำในนามของกองทัพแห่งรัฐหรือเป็นตัวแทนของกองทัพแห่งรัฐให้มากขึ้น โดยจะต้องสร้างเกณฑ์ในการพิจารณาที่ชัดเจนและเหมาะสมต่อการใช้เทคโนโลยีดังกล่าว

กรณีการใช้นาโนเทคโนโลยีเพื่อการออกแบบชุดพลรบที่สามารถล่องหนได้ หรือรอดพ้นจากการตรวจจับด้วยอุปกรณ์ตรวจจับได้นั้นจะต้องมีการเพิ่มเติมคำอธิบายว่าพลรบดังกล่าวจะตกอยู่ในสถานะใด หากอยู่ในระหว่างการปฏิบัติการโจมตีจะเป็นพลรบเช่นเดิมหรือไม่ และหากพลรบดังกล่าวกระทำการจารกรรมย่อมถือเป็นจารชนใช่หรือไม่ นอกจากนั้นยังต้องพิจารณาความเหมาะสมในการสร้างเครื่องแบบล่องหนดังกล่าวด้วยว่าเป็นการกระทำที่เกินกว่าความจำเป็นทางการทหารหรือไม่ ทั้งนี้ จะต้องแยกการอธิบายให้ชัดเจนระหว่างการสวมเครื่องแบบล่องหนที่ไม่อาจตกเป็น

เป้าหมายในการโจมตีได้ กับการใช่หุ่นยนต์แทนพลรบ ซึ่งทั้งสองรูปแบบมีเป้าหมายเดียวกันคือลดความเสียหายแก่พลรบ แต่การสวมเครื่องแบบก่อให้เกิดความได้เปรียบของพลรบมากกว่า (เนื่องจากไม่ตกเป็นเป้าหมายในการโจมตี แต่ตนเองสามารถทำการโจมตีได้) จึงควรจัดให้การสวมเครื่องแบบล่องหนมีค่าเท่ากับการแสดงตนเป็นพลเรือน (คือทำให้ตนเองไม่ตกเป็นเป้าหมายในการโจมตี)

(2) การถืออาวุธโดยเปิดเผย

ประเด็นเรื่องการถืออาวุธโดยเปิดเผยนั้นอาจต้องคำนึงถึงรูปแบบการใช้งานเทคโนโลยีใหม่ในการขัดกันทางอาวุธที่แตกต่างจากเดิม กล่าวคือพลรบไม่จำต้องถืออาวุธเสมอไป แต่จะต้องคำนึงถึงการถืออุปกรณ์ควบคุมระยะไกล การสั่งการจากศูนย์ปฏิบัติการ อีกทั้งยังอาจจำเป็นต้องมีการกำหนดสถานะพลรบให้กับระบบอาวุธที่ตัดสินใจได้ด้วยตนเองและสามารถปฏิบัติการเยี่ยงพลรบได้ (กรณีเป็นหุ่นยนต์สังหาร) ด้วยเหตุที่ระบบอาวุธดังกล่าวย่อมตกเป็นเป้าหมายในการโจมตีจากทั้งพลรบและระบบอาวุธชนิดเดียวกันได้โดยชอบด้วยกฎหมาย แต่หลักบางประการที่ใช้กับพลรบซึ่งเป็นมนุษย์ไม่จำเป็นต้องใช้กับระบบอาวุธตัดสินใจได้ด้วยตนเอง เช่นการปฏิบัติในฐานะเชลยศึกเพราะระบบอาวุธดังกล่าวมิใช่มนุษย์ที่จะต้องปฏิบัติอย่างมีมนุษยธรรมด้วย นอกจากนั้นการกำหนดสถานะของการเป็นอาชญากรให้แก่ระบบอาวุธดังกล่าวที่ปฏิบัติการเช่นเดียวกับจารชนก็ไม่มีความจำเป็น เพราะเทคโนโลยีจะตกเป็นเป้าหมายในการคุ้มครองเช่นมนุษย์ไม่ได้เช่นกัน หลักการแยกแยะสถานะพลรบของเทคโนโลยีใหม่จึงควรใช้เพื่อการตกเป็นเป้าหมายในการโจมตีโดยชอบด้วยกฎหมายเท่านั้น

(3) การมีส่วนร่วมของพลเรือนในการสู้รบ

ประเด็นเรื่องการมีส่วนร่วมของพลเรือนในการสู้รบจำเป็นต้องมีการสร้างแนวทางปฏิบัติ (Guideline) เกี่ยวกับการมีส่วนร่วมโดยตรงของพลเรือนในการสู้รบเพิ่มเติม โดยเหตุที่การใช้เทคโนโลยีในบางลักษณะอาจมีพลเรือนเข้ามาเกี่ยวข้อง อันได้แก่ การโจมตีทางไซเบอร์ หากเป็นการกระทำของพลเรือนที่ไม่มีส่วนเกี่ยวข้องกับกองทัพและไม่ใช่การกระทำในนามของกองทัพ การกระทำการของพลเรือนดังกล่าวไม่ถือเป็นการกระทำของกองทัพของรัฐที่จะทำให้เป็นการโจมตีเพื่อก่อการ

ขัดกันทางอาวุธได้ แต่ย่อมถือได้ว่าพลเรือนนั้นเข้ามามีส่วนร่วมในการสู้รบโดยตรง แต่จะต้องมีการจำแนกสถานะของพลเรือนดังกล่าวว่าจะตกเป็นพลรบที่ชอบด้วยกฎหมายหรือไม่ ทั้งนี้พลเรือนดังกล่าวจะตกเป็นเป้าหมายในการถูกโจมตีได้

ประเด็นเรื่องตัวตนของผู้กระทำการในปฏิบัติการทางทหารเป็นเรื่องสำคัญอีกหนึ่งประการที่จะต้องมีการอธิบายเพิ่มเติม ซึ่งอาจทำได้ทั้งลักษณะของการเขียนคำอธิบาย (Commentary) เพิ่มเติมให้กับพิธีสารฉบับที่ 1 ของอนุสัญญาเจนีวา และอาจทำได้ในลักษณะของการสร้างแนวทางการปฏิบัติ (Guideline) เนื่องจากปฏิบัติการของระบบไซเบอร์และระบบอาวุธตัดสินใจอัตโนมัติบนพื้นฐานของการประมวลผลแบบอัลกอริทึ่มจะทำให้เกิดการเผชิญหน้ากันระหว่างตัวตนที่ไม่ใช่มนุษย์มากขึ้น ทั้งลักษณะของการเผชิญหน้ากันของเทคโนโลยีกับเทคโนโลยี เทคโนโลยีกับมนุษย์ เทคโนโลยีกับข้อมูล จึงต้องระบุให้ชัดเจนว่าในกรณีในจะถือว่าเป็นการกระทำในลักษณะการมีส่วนร่วมโดยตรงในการสู้รบ และตัวตนใดมีส่วนร่วมโดยตรงในการสู้รบ

2. การพัฒนาระบบในการตรวจตราการปฏิบัติการตามบทบัญญัติข้อ 36 ของพิธีสารเพิ่มเติมฉบับที่ 1 แห่งอนุสัญญาเจนีวา ค.ศ.1977

ด้วยเหตุที่การรายงานผลการตรวจตราการปฏิบัติตามพันธกรณีข้อ 36 ของพิธีสารเพิ่มเติมฉบับที่ 1 แห่งอนุสัญญาเจนีวา ค.ศ.1977 เกี่ยวกับความเหมาะสมในการพัฒนาอาวุธใหม่นั้นยังประสบปัญหาที่หลายประเทศไม่มีการทบทวน หรือตรวจตราการปฏิบัติตามพันธกรณี ซึ่งจำเป็นที่ต้องมีการสร้างระบบการตรวจตราที่สามารถปฏิบัติหน้าที่ได้จริงให้มากขึ้น เช่นการจัดตั้งคณะผู้รายงานพิเศษโดยไม่จำต้องแทรกแซงกิจการของรัฐ แต่จะต้องเข้าถึงข้อมูลการพัฒนาอาวุธของแต่ละประเทศและมีการรายงานต่อคณะกรรมการกลางของคณะกรรมการกาชาดระหว่างประเทศหรือองค์กรอื่นใดในรูปแบบความร่วมมือระหว่างประเทศ เพื่อพิจารณาแนวโน้มความเปลี่ยนแปลงทางด้านอาวุธของประเทศต่างๆ และเตรียมการรับมือกับสถานการณ์ที่อาจเกิดขึ้น นอกจากนั้นอาจต้องสร้างความตระหนักแก่สังคมระหว่างประเทศให้เกิดขึ้นในประเด็นของการพิจารณาความเหมาะสมในการนำเทคโนโลยีมาใช้เพื่อการขัดกันทางอาวุธ เพื่อให้เกิดความรู้สึกร่วมกันในการเคารพต่อกฎหมาย ซึ่งแม้จะไม่สามารถทำให้ทุกประเทศปฏิบัติตามพันธกรณีข้อ 36 นี้ได้ แต่ย่อมเป็นการสร้างระบบให้แต่ละประเทศสอดส่องดูแลกันเอง และอาจรวมถึงการสร้างมาตรการตอบโต้กับประเทศที่นำเทคโนโลยีใหม่มาใช้ในทางที่ละเมิดต่อหลักการทางกฎหมายมนุษยธรรมระหว่างประเทศด้วย

3. การบูรณาการกฎหมายที่เกี่ยวข้องกับเทคโนโลยีชนิดต่างๆ เพื่อปรับใช้ร่วมกับกฎหมายมนุษยธรรมระหว่างประเทศ

เนื่องจากลักษณะของเทคโนโลยีหลายประการมีการใช้งานร่วมกันระหว่างทหารและพลเรือน การใช้งานเทคโนโลยีหลายประเภทไม่ใช่อาวุธโดยการออกแบบจึงสามารถใช้งานทั้งทหารและ พลเรือนได้ในยามสันติและในสถานการณ์การขัดกันทางอาวุธ ในขณะที่เทคโนโลยีแต่ละชิดที่ใช้นั้นอาจไม่ได้มีไว้เพื่อการทำลายเสมอไป และในสถานการณ์การขัดกันทางอาวุธก็ยังคงสามารถปรับใช้กฎหมายอื่นได้เช่นกัน การบังคับใช้กฎหมายในสถานการณ์การขัดกันทางอาวุธต่อเทคโนโลยีใหม่จึงสามารถบูรณาการนำเอากฎหมายระหว่างประเทศและกฎหมายภายในเรื่องต่างๆ เพื่อให้มีการควบคุมหรือจำกัดการใช้งานเทคโนโลยีเหล่านั้นให้เป็นไปในเชิงการใช้ประโยชน์ในทางสันติได้ เช่น

การใช้งานระบบไซเบอร์แม้จะไม่มีกฎหมายมนุษยธรรมระหว่างประเทศกำหนดหลักการห้ามใดๆ เอาไว้ แต่คู่มือทาลลินน์ก็แสดงให้เห็นว่ากฎหมายที่ควบคุมกิจกรรมทางไซเบอร์เท่าที่มีอยู่ก็เพียงพอแล้ว จึงให้มีการนำกฎหมายระหว่างประเทศส่วนที่เกี่ยวข้องกับปฏิบัติการทางไซเบอร์มาใช้ตามพฤติกรรมและสถานการณ์ที่มีการใช้งานระบบไซเบอร์ที่แตกต่างกันได้

การใช้งานอากาศยานไร้คนขับมีกฎหมายภายในและกฎหมายระหว่างประเทศที่เกี่ยวข้องอยู่แล้ว หากเป็นการใช้งานอากาศยานพลเรือนในเวลาที่เกิดการขัดกันทางอาวุธ อย่างน้อยที่สุดก็ย่อมบังคับใช้กฎหมายปกติที่เกี่ยวข้องได้ เฉพาะการใช้งานที่เกี่ยวข้องกับปฏิบัติการทางทหารจึงจะมีการนำเอาหลักการของกฎหมายมนุษยธรรมระหว่างประเทศมาบังคับ

การใช้งานระบบอาวุธอิสระต้องปรับใช้กฎหมายมนุษยธรรมอย่างเคร่งครัดและอาจนำแนวทางจริยธรรมในการใช้ปัญญาประดิษฐ์มาพิจารณาความเหมาะสมในการใช้ การพัฒนาระบบอาวุธอิสระได้ เพื่อให้การพัฒนาระบบปัญญาประดิษฐ์ในระบบอาวุธอิสระนั้นมีความครอบคลุมมากยิ่งขึ้น

ระบบเทคโนโลยีอวกาศโดยเฉพาะอย่างยิ่งเกี่ยวกับการใช้ระบบสัญญาณดาวเทียม มีกฎหมายระหว่างประเทศที่ควบคุมกิจกรรมทางอวกาศและการห้ามฝ่าฝืนหลักการใช้ประโยชน์จากทรัพยากรทางอวกาศอยู่แล้วหลักเกณฑ์ตามกฎหมายเฉพาะเรื่องต่างๆ นี้จึงสามารถนำมาบังคับใช้กับกรณีการกระทำที่เป็นการละเมิดต่อกฎหมายได้ เช่น การดัดแปลงดาวเทียมเพื่อให้เป็นอาวุธ เป็นต้น อย่างไรก็ดีในบางกรณีอาจไม่จำกัดได้เสมอไปเพราะอาจเกี่ยวข้องกับการใช้ประโยชน์ของพลเรือนด้วย เช่น ระบบอาวุธนำวิถีที่ใช้สัญญาณดาวเทียมแบบเดียวกับพลเรือนใช้ในระบบนำทาง กรณีดังกล่าว

อาจต้องให้ทั้งพลเรือนและทหารใช้ร่วมกัน โดยทางการทหารย่อมเป็นไปเพื่อประโยชน์ในการใช้งานระบบอาวุธอย่างแม่นยำ[1016]

4. การสร้างกลุ่มความร่วมมือระหว่างประเทศ

นอกเหนือจากการให้คณะกรรมการกาชาดระหว่างประเทศมีบทบาทในการขับเคลื่อนกฎหมายมนุษยธรรมระหว่างประเทศ และองค์การสหประชาชาติมีบทบาทในการลดอาวุธแล้ว การสร้างความร่วมมือระหว่างประเทศทั้งที่เกิดขึ้นแล้ว และจะเกิดขึ้นในอนาคตจะเป็นหนทางหนึ่งในการรับมือกับสถานการณ์การใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธ และเป็นการส่งเสริมให้ประเทศต่างๆ มีส่วนร่วมต่อการปฏิบัติตามกฎหมายด้วย ทั้งนี้การทำให้กฎหมายเกิดผลบังคับใช้จริงนั้น ไม่อาจพึ่งพาเฉพาะองค์การระหว่างประเทศหลักเพียงประการเดียวได้ แต่ความเข้าใจในปัญหาของแต่ละประเทศย่อมนำไปสู่แนวทางการแก้ไขได้อย่างมีประสิทธิผล

การสร้างแนวทางเพื่อการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศต่อการใช้เทคโนโลยีใหม่ในการขัดกันทางอาวุธดังที่กล่าวมาทั้งหมดนี้ ไม่ได้เป็นไปเพื่อหยุดยั้งพัฒนาการทางเทคโนโลยีแต่เป็นการสร้างสมดุลระหว่างการใช้งานในเชิงที่เป็นคุณประโยชน์และความจำเป็นในปฏิบัติการทางทหารเพื่อการขัดกันทางอาวุธ และเราย่อมปฏิเสธไม่ได้ว่าเทคโนโลยีเหล่านี้มีบทบาททั้งสองทางทั้งในด้านดีและด้านลบ การจำกัดการใช้งานในด้านลบที่ก่อให้เกิดความเสียหายย่อมเป็นเรื่องจำเป็น ในทางตรงข้าม หากการใช้งานเทคโนโลยีจะเป็นประโยชน์ต่อการทำสงครามเพื่อลดความเสียหายที่จะเกิดขึ้นจากการต่อสู้ ก็ไม่มีเหตุผลที่จะหยุดพัฒนาการทางเทคโนโลยีนั้นแต่อย่างใด

ในสถานการณ์ปัจจุบันขณะที่เทคโนโลยียังมีการพัฒนาอยู่ตลอดเวลาการจะสร้างกฎหมายเฉพาะเพื่อควบคุมเทคโนโลยีเฉพาะเรื่องอาจเป็นไปได้ยาก ความพยายามในการปรับใช้กฎหมายกฎหมายอื่นที่นอกเหนือจากกฎหมายมนุษยธรรมระหว่างประเทศ ทั้งที่อยู่ในรูปแบบของกฎหมายระหว่างประเทศและกฎหมายภายในประเทศซึ่งเกี่ยวข้องกับการควบคุมการใช้งานเทคโนโลยีอาจเป็นประโยชน์ต่อการเสริมสร้างการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ เช่น มาตรการป้องกันก่อนเกิดการขัดกันทางอาวุธด้วยการควบคุมพัฒนาการทางเทคโนโลยีที่อาจถูกนำมาใช้ในการขัดกันทางอาวุธ ผ่านกฎหมายระหว่างประเทศและกฎหมายภายในเกี่ยวกับการห้ามพัฒนาอาวุธใหม่

[1016] International Committee on the Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, Report, (2019), p. 26.

กฎหมายห้ามส่งออกสินค้าที่ใช้ได้สองทางและกฎหมายการควบคุมการกระทำทางไซเบอร์ มาตรการในการควบคุมเทคโนโลยีทั้งก่อนและหลังการใช้งานตามกรอบกฎหมายเกี่ยวกับการลดอาวุธ รวมตลอดถึงการห้ามพัฒนา การถ่ายโอน และการแพร่กระจาย กฎหมายเหล่านี้แม้จะใช่กฎหมายมนุษยธรรมระหว่างประเทศในตัวเองแต่มีบทบาทนอกสถานการณ์ขัดกันทางอาวุธอย่างมาก เป็นทั้งการป้องกันการนำเทคโนโลยีไปใช้ในการขัดกันทางอาวุธและเป็นมาตรการในการควบคุมเทคโนโลยีที่อาจถูกนำไปใช้งานเพื่อการก่อให้เกิดความเสียหาย

การใช้กฎหมายในบริบทแวดล้อมหล่านี้อาจไม่ได้นำไปสู่การแก้ไขปัญหาการปรับใช้กฎหมายมนุษยธรรมระหว่างประเทศ แต่ในมิติหนึ่งกฎหมายมนุษยธรรมระหว่างประเทศไม่ได้อยู่เป็นเอกเทศโดดเดี่ยวจากกฎหมายอื่น เพราะในการขัดกันทางอาวุธอาจเกิดการกระทำที่เกี่ยวข้องกับกฎหมายหลายเรื่องนอกจากกฎหมายมนุษยธรรมระหว่างประเทศได้

บรรณานุกรม

This entry was generated through inserting a Case citation for 1996 Legality of the Threats or Use of Nuclear Weapons Advisory Opinion of 8 July 1996. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

Alam, Imran. "First Computer Virus-Creeper." (February 4, 2022 2014). Accessed January 10, 2023. https://www.linkedin.com/pulse/first-computer-virus-creeper-imran-alam.

Albayrak, Fatma Tasdemmir and Gokhan. "The Law of Cyber Warfare in Terms of Jus Ad Bellum and Jus in Bello: Application of International Law to the Unknown." *E-journal of Law* 3, no. 2 (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092654.

Aldrich, Richard W. "The International Legal Implications of Information Warfare.". *Airpower* 99 (1996): 102.

Anderson, Cecilia. "Killer Robot-Autonomous Weapons and Their Compliance with Ihl." Master of Law Thesis, Lund University, 2014.

Ashmore, Williams C. "Impact of Alleged Russian Cyber Attacks." *Baltic Security and Defense Review* 11 (2009). https://www.baltdefcol.org/files/files/BSDR/BSDR_11_1.pdf.

Assembly, United Nations General. *Resolution on Countering the Use of Information and Communications Technologies for Criminal Purposes.* United Nations General Assembly (January 20, 2020 2020).

Association, International Law. "The Conduct of Hostilities and International Humanitarian Law." *International Law Studies* 93 (2017): 322-88. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1709&context=ils.

Bachman, Jeffrey. "The New York Times and Washington Post: Misleading the Public About Us Drone Strikes." *Journalism Studies* 18, no. 4 (2017): 470-94.

Baker, Joanne. "Forgotten Heroes of the Enigma Story." (September 3, 2018 2018). Accessed October 10, 2020. https://www.nature.com/articles /d41586-018-06149-y.

Ball, Philip. "New Lessons for Stealth Technology." *Nature Materials* 20, no. 4 (2021): 2-9.

Bamatraf, B. Pratama and M. "Tallinn Manual: Cyber Warfare in Indonesian Regulation." International Conference on Biospheric Harmony Advanced Research (ICOBAR 2020), IOP Conference Series: Earth and Environmental Science, Jakata, Indonesia. , 23-24 June 2020 2021.

Batu, Göktuğ Sönmez and Gökhan. *Iron Dome Air Defense System: Basic Characteristics, Limitations, Local and Regional Implications.* Center for Middle Eastern Studies (2021). https://orsam.org.tr/d_hbanaliz/iron-dome-air-defense-system-basic-characteristics-limitations-local-and-regional-implications.pdf.

Bedjaoui, Mohamed. "L'humanité En Quête De La Paix Et Le Développement,." *RCADI* 325 (2006).

Bettati, Mario. *Le Droit De La Guerre.* Paris: Odile Jacob, 2016.

Black, George. "The Victims of Agent Orange the U.S. Has Never Acknowledged." (March 16, 2021 2021). Accessed April 10, 2021. https://www.nytimes.com/2021/03/16/magazine/laos-agent-orange-vietnam-war.html,.

Blake, Duncan. "The Law Applicable to Military Strategic Use of Outer Space ". In *New Technologies and the Law of Armed Conflict*, edited by Hitoshi Nasu and Robert McLaughlin. The Hague: T.M.C. Asser Press, 2014.

———. "Military Strategic Use of Outer Space." In *New Technologies and the Law of Armed Conflict*, edited by Hitoshi Nasu and Robert McLaughlin. The Hague: T.M.C. Asser Press, 2014.

Boothby, William. "Some Legal Challenges Posed by Remote Attack." *International Review of the Red Cross Review* 94, International Humanitarian Law and the protection of civilians, no. 886 (2012).

———. "Space Weapons and the Law." *International Law Studies* 93 (2017).

Boothby, Williams. *Weapons and the Law of Armed Conflict.* Oxford: Oxford University Press, 2009.

"The Practical Guide to Humanitarian Law: War." Medecins sans Frontieres, accessed May 10, 2022, https://guide-humanitarian-law.org/content/article/3/war/.

Brand, George. "The Development of the International Law of War." *Tulane Law Review* 25, no. 2 (1951).

Briggs, John N. *Target Detection by Marine Radar.* London: The Institution of Electrical Engineers, 2004.

Bunker, Robert J. *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications.* Strategic Studies Institute U.S. Army War College (Pennsylvania: 2015). https://apps.dtic.mil/sti/citations/ADA623134.

Burgess, Matt. "The Bad Rabbit Malware Was Disguised as a Flash Update." (October 27, 2017 2017). Accessed January 19, 2020. https://www.wired.co.uk/article/bad-rabbit-ransomware-flash-explained.

Cadirci, Serdar. "Rf Stealth (or Low Observable) and Counter- Rf Stealth Technologies: Implications of Counter-Rf Stealth Solutions for Turkish Air Force." Master of Science in Electronic Warfare System Engineering, Naval Postgraduate School, 2009. https://core.ac.uk/download/pdf/36698589.pdf.

This entry was generated through inserting a Case citation for Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America) (Merit) Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Case Concerning the Gabcikovo-Nagymaros Project. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon V. Nigeria: Equatorial Guinea Intervening). Case references

should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Case Concerning the United States Diplomatic and Consular Staff in Tehran (United States V. Iran). Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

Cavelty, Myriam Dunn. "The Militarisation of Cyberspace: Why Less May Be Better." 4th International Conference on Cyber Conflict, Tallinn, 2012.

Chai, Westley. "Google Analytics." (April 2021 2021). Accessed Feb 15, 2022. https://www.techtarget.com/searchbusinessanalytics/definition /Google-Analytics,.

Chetail, Vincent. "The Contribution of the International Court of Justice to International Humanitarian Law." *International Review of the Red Cross Review* 85, no. 850 (2003). https://www.icrc.org/en/doc/assets/files/other/irrc_850_chetail.pdf.

Claude Pilloud, Jean de Preux, Bruno Zimmermann, Philippe Eberlin, Hans-Peter Gasser and Claude Wenger. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.* Geneva: International Committee of the Red Cross, 1987.

Cohen, Eliot A. *Gulf War Air Power Survey.* Washington, D.C.: U.S. Government Printing, 1993.

Coker, Christopher. *Waging War without Warriors?: The Changing Culture of Military Conflict.* London: Lynne Rienner Publisher, 2002.

Collier, Basil. *The Battle of the V-Weapons.* Morley: The Elm field Press, 1976.

Commission of Jurists to Consider and Report Upon the Revision of the Rules of Warfare. American Journal of International Law (1938). https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/commission-of-jurists-to-consider-and-report-upon-the-revision-of-the-rules-of-warfare-general-report1/F25B66816C13A812DE257DBB37CDFE96.

" Comprehensive Nuclear Test-Ban Treaty." In *United Nations General Assembly Resolution 50/245, A/RES/50/245*, edited by United Nations General Assembly, 17 September 1996 1996.

Constant, James. *Fundamentals of Strategic Weapons: Offense and Defense Systems.* Amsterdam: Martinus Nijhoff Publishers, 1981.

"Convention (Ii) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land." The Hague, July 29, 1899 1899. https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-ii-1899/preamble?activeTab=undefined.

"Convention (Iv) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land." The Hague, October 18, 1907 1907. https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907.

This entry was generated through inserting a Case citation for Corfu Channel Case (Uk V. Albania) (Merit). Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

Corn, Geoffrey S. "Autonomous Weapon Systems: Managing the Inevitability of "Taking the Man out of the Loop"." In *Autonomous Weapons Systems: Law Ethics, Policy*, edited by Susanne Beck Nehal Bhuta, Robin Geib, Hin-Yan Liu and Claus Kreb. Cambridge: Cambridge University Press, 2016.

Crandall, Scott Levy and Jedidiah R. "The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus." (June 20, 2020 2020). Accessed January 19, 2022. https://arxiv.org/abs/2007.15759, .

Crawford, Emily. "Armed Ukraine Citizens: Direct Participation in Hostilities, Levee En Masse, or Something Else?". *European Journal of International Law* (March 1, 2022 2022). https://www.ejiltalk.org/armed-ukrainian-citizens-direct-participation-in-hostilities-levee-en-masse-or-something-else/.

Cross, International Committee of the Red. *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach.* (June 6, 2019 2019). https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach.

———. *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Function of Weapons.* (March 15-16, 2016 2016).

https://icrcndresourcecentre.org/wp-content/uploads/2017/11/4283_002_Autonomus-Weapon-Systems_WEB.pdf.

———. *Expert Meeting on Lethal Autonomous Weapons Systems.* (November 15, 2017 2017). https://www.icrc.org/en/document/expert-meeting-lethal-autonomous-weapons-systems.

———. *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, Measures to Implement Article 36 of Additional Protocol 1 of 1977.* Geneva: International Committee of the Red Cross, January 2006, 2006.

———. "Icrc Position on Autonomous Weapon Systems ". (May 12, 2021 2021). Accessed June 10, 2021. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

———. "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts." 32th International Conference of the Red Cross and Red Crescent, December 8-10, 2015. 2015.

———. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (November 28-December 1, 2011 2011).

———. "International Law on the Conduct of Hostilities: Overview." (October 29 2012). Accessed May 10, 2021. https://www.icrc.org/en/document/conduct-hostilities.

———. *Report of the Icrc Expert Meeting on 'Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects.* (Geneva: March 26-18, 2014 2014).

Darcy, Shane. *Judges, Law and War: The Judicial Development of International Humanitarian Law.* Cambridge: Cambridge University Press, 2014.

Das, Rajatendu. "Advances in Active Radar Seeker Technology." *Defence Science Journal* 55, no. 3 ((July 2005) 2005). https://core.ac.uk/download/pdf/333720359.pdf,.

David Albright, Paul Brannan, and Christina Walrond. *Stuxnet Mulware and Natantz: Update of Isis December 2010.* Institute for Science and International Security (2011). https://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/.

David, Eric. "Le Droit International Humanitaire Face À Ces Évolutions: Un Droit Adapté Ou Adaptable?" Pertinence du Droit international humanitaire pour les acteurs

non-étatiques, Actes du Colloque de Bruges CICR et Collège d'Europe, 25-26 Octobre 2002 2003.

"Declaration (Iv,2) Concerning Asphyxiating Gases." The Hague, July 29, 1899 1899. https://ihl-databases.icrc.org/en/ihl-treaties/hague-decl-iv-2-1899/declaration?activeTab=undefined.

"Declaration (Iv,3) Concerning Expanding Bullets." The Hague, July 29, 1899 1899. https://ihl-databases.icrc.org/en/ihl-treaties/hague-decl-iv-3-1899/declaration?activeTab=undefined.

"Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight." Saint Petersburg, 29 November/11 December 1868 1868. https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868.

A Definition of Ai: Main Capabilities and Scientific Disciplines. European Commission's High-Level Expert Group on Artificial Intelligence, European Commission (Brussels: December 18, 2018 2018). https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War.* New York: Cambridge University Pres, 2012.

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict.* Cambridge: Cambridge University Press, 2004.

Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004 2004.

Doswald-beck, Jean-Marie Hanckaerts and Louis. *Customary International Humanitarian Law: Volume I Rules.* New York: Cambridge University Press, 2009.

" The Draft Prevention of the Placement of Weapons Treaty." 2008. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/200802/t20080212_599554.html.

Droege, Cordula. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians." *International Review of the Red Cross Review* 94, no. 886 (2012).

Durr, Olivier. "Humanitarian Law of Armed Conflict: Problems of Applicability." *Journal of Peace Research* 24, no. 3 (1987). https://journals.sagepub.com/doi/abs/10.1177/002234338702400306.

Eaton, Bothe Michael Karl Josef Partsch Waldemar A Solf and Martin. *New Rules for Victims of Armed Conflicts : Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949.* 2 ed. Leiden: Martinus Nijhoff, 2013. https://doi.org/10.1163/9789004254718.

Edgar, Gerald A. "Darwin: A Survival Game for Programmers." *Computer Language* 4, no. 4 (1987).

Egeland, Kjølv. "Lethal Autonomous Weapon Systems under International Humanitarian Law." *Nordic Journal of International Law* 85, no. 2 (2016).

Eilstrup-Sangiovanni, Mette. "Why the World Needs an International Cyberwar Convention." *Philosophy and Technology* 31 (2018): 379-407.

Emily B. Landau, and Azriel Bermant. "Iron Dome Protection: Missile Defense in Israel's Security Concept." In *The Lessons of Operation Protective Edge*, edited by Anat Kurz and Shlomo Brom, 37. Tel Aviv: Institute for national Security Studies, 2014.

Episkopos, Mark. "Forget the Iron Dome: This Israel Laser Is Changing Air Defense." (July 15, 2021 2021). Accessed April 19, 2022. https://nationalinterest.org/blog/reboot/forget-iron-dome-israeli-laser-changing-air-defense-189704.

Erickson, Jeff. *Algorithms.* Illinois: Illinois University Press, 2019. https://jeffe.cs.illinois.edu/teaching/algorithms/book/Algorithms-JeffE.pdf,.

Fenrick, W. J. "The Law Applicable to Targeting and Proportionality after Operation Allied Force: A View from the Outside." *Yearbook of International Humanitarian Law* 3 (2000): 53-80. https://doi.org/10.1017/S1389135900000581. https://www.cambridge.org/core/article/law-applicable-to-targeting-and-

proportionality-after-operation-allied-force-a-view-from-the-outside1/C00ADDD84DB8B6947CE66A425B394F58.

Ferran, Lee. "Intel Chair: Civilian Drone Casualties in 'Single-Digits' Year-to-Year." *ABC News*, February 7, 2013 2013. http://abcnews.go.com/blogs/headlines/2013/02/intel-chair-civilian-dronecasualties-in-single-digits-year-to-year/.

Foerster, Heinz von. *Ethics and Second-Order Cybernetics, in Understanding: Essays on Cybernetics and Cognition.* New York: Springer-Verlag, 2003.

Foltz, Andrew C. "Stuxnet Schmitt Analysis, and the Cyber 'Use of Force' Debate." *Joint Force Quarterly* 67, no. 4 (2012): 44.

Fruhlinger, Josh. "What Is a Botnet? When Infected Devices Attack." (April 5, 2022 2022). Accessed February 16, 2023. https://www.csoonline.com/article /3240364/what-is-a-botnet.html.

Gahegan, Stephen D. Weaver and Mark. "Constructing, Visualizing and Analyzing a Digital Footprint." *The Geographical Review* 97, no. 3 (2007): 328-31.

Gill, Amandeep Singh. "The Roles of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weapons Systems." *UN Chronicle* LV, no. 3&4 (December 2018 2018). https://www.un.org/en/un-chronicle/role-united-nations-addressing-emerging-technologies-area-lethal-autonomous-weapons.

Gorman, Siobhan. "Georgia States Computers Hit by Cyberattack." *The Wall Streat Journal*, August 12, 2008 2008. https://www.wsj.com/articles/SB121850756472932159.

Gray, Christine. "The Limits of Force." In *Collected Courses of the Hague Academy of International Law*, 2015.

Greig, Jonathan. "First Draft of Controversial Un Cyber Crime Treaty Slate for June." *The Record* (2023). https://therecord.media/first-draft-of-un-cybercrime-treaty-expected-in-june.

Grimes, Roger A. "9 Types of Malware and How to Recognize Them." (November 17, 2020 2020). Accessed January 10, 2022. https://www.csoonline.com/article /2615925/security-your-quick-guide-to-malware-types.html.

Guelff, Adam Roberts and Richard. *Documents on the Laws of War.* Edited by 3rd edition. Oxford: Oxford University Press, 2000.

Gulick, J. F., and J. S. Miller. *Missile Guidance: Interferometer Homing Using Body Fixed Antennas.* Maryland: Johns Hopkins University Applied Physics Laboratory, 1982.

Hagström, Martin. "Characteristics of Autonomous Weapon Systems." Expert meeting. Autonomous weapon systems: Implications of increasing autonomy in the critical function of weapons, Versoix, Switzerland, International Committee of the Red Cross, Geneva, 15–16 March 2016 2016.

Haines, Stuart Casey-Maslen and Steven. *Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict.* London: Bloomsbury Publishing, 2018.

Hanna, Katie Terrell. "Chernobyl Virus." (December 2021 2021). Accessed January 19, 2022. https://www.techtarget.com/searchsecurity /definition/Chernobyl-virus.

Hanseman, Robert G. "The Realities and Legalities of Information Warfare." *AFL Review* 42, no. 173 (1997).

Haslam, Emily. "Information Warfare: Technological Changes and International Law." *Journal of Conflict & Security Law* 5, no. 2 (2000).

Hawley, John K. *Patriot Wars: Automation and the Patriot Air and Missile Defense System.* Center for a New American Security (January 2017 2017). http://www.jstor.org/stable/resrep06103.

Heinegg, Wolff Heintschel von. "Asymmetric Warfare: How to Respond?". *International Law Studies* 87 (2011).

———. "Neutrality and Outer Space." *International Law Studies* 93 (2017).

Heymann, Gabriella Blum and Philip. "Law and Policy of Targeted Killing." *Harvard National Security Journal* 1 (2010): 145-70.

Highland, Harold Joseph. "The Brain Virus: Fact and Fantasy." *Computers and Security* 7 (1988).

Hitaj, Erjan. "Use of Drones and Global Security: Implications under International Law." *Koreuropa Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*.

https://www.academia.edu/27011103/Use_of_Drones_and_Global_Security_Implications_Under_International_Law.

Hogue, Simon. "Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observer of War." *Surveillance and Society* 20, no. 1 (2023): 108-12.

Huiskes, Katherine. "The September 11 Terrorist Attack." Accessed January 30, 2022. https://millercenter.org/remembering-september-11/september-11-terrorist-attacks,.

Husnain Ahmad, Asra Tariq, Amir Shehzad, Muhammad S. Faheem, Muhammad Shafiq, Iqra A. Rashid, Ayesha Afza, Adnan Munir, Muhammad T. Riaz, Hafiz T. Haider, Ali Afzal, Muhammad B. Qadir, and Zubair Khaliq. "Stealth Technology: Methods and Composite Materials—a Review." *Polymer Composites* (2019): 4469.

Iasiello, Emilio. "Are Cyber Weapons Effective Military Tools?". *Military and Strategic Affair* 7, no. 1 (March 2015 2015).

"Instructions for the Government of Armies of the United States in the Field (Lieber Code). ." April 24, 1863 1863. https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863.

International, Amnesty. "Forensic Methodology Report: How to Catch Nso Group's Pegasus." (July 18, 2021 2021). Accessed July 19, 2021. https://www.amnesty.org/en/latest/research /2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

———. "Will I Be Next? Us Drone Strikes in Pakistan." (2013). Accessed February 22, 2018. https://www.amnestyusa.org/files/asa330132013en.pdf.

———. *Will I Be Next?: Us Drone Strikes in Pakistan.* New York: Amnesty International, 2013. https://www.amnesty.org/en/documents/asa33/013/2013/en/.

International Committee on the Red Cross. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts.* (2019). https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts.

"International Declaration Concerning the Laws and Customs of War." Brussels, August 27, 1874 1874. https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874.

"International Law across the Spectrum of Conflict: Essays in Honour of Professor L.C. Green on the Occasion of His Eightieth Birthday." *US Naval War College International Law Studies* 75 (2000).

Joint Targeting. U.S. Army, 2013.

Justino, Patricia. "The Conflict in Ukraine – the Role of Civilians." (February 2022 2022). Accessed March 26, 2022. https://www.wider.unu.edu/publication/conflict-ukraine-role-civilians.

Kadri Kaska, Eneken Tikk and Liis Vihul. *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Center of Excellence (CCD COE), 2010. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

Kapul, Vivek. "Stealth Technology and Its Effect on Aerial Warfare." *IDSA Monograph Series* 33 (2014). https://www.idsa.in/system/files/monograph33.pdf.

Karatas, Serkan Savas and Suleyman. "Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance." *International Cybersecurity Law Review* 3 (2022).

Kennedy, David. "Modern War and Modern Law." *University of Baltimore Law Review* 36, no. 2 (2007).

———. *Reassessing International Humanitarianism: The Dark Side.* Oxford: Princeton University Press, 2004.

Knight, Will. "Russia's Killer Drone in Ukraine Raises Fears About Ai in Warfare." (March 17, 2022 2022). Accessed April 16, 2023. https://www.wired.com/story/ai-drones-russia-ukraine/.

Kunertova, Dominika. "The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game." *Bulletin of the Atomic Scientists* 79, no. 2 (2023/03/04 2023): 95-102. https://doi.org/10.1080/00963402.2023.2178180. https://doi.org/10.1080/00963402.2023.2178180.

Landler, Mark. "Civilian Deaths Due to Drones Are Not Many, Obama Says." *The New York Times*, January 30, 2012 2012. https://www.nytimes.com/2012/01/31/world/middleeast/civilian-deaths-due-to-drones-are-few-obama-says.html.

Larkin, Matthew. "Brave New Warfare: Autonomy in Lethal." Master Degree, Naval Postgraduate School, 2011. https://core.ac.uk/download/pdf/36699485.pdf.

"The Laws of War on Land, Manual Published by the Institute of International Law (Oxford Manual)." edited by Institute of International Law at Oxford, September 9, 1880 1880. http://hrlibrary.umn.edu/instree/1880a.htm.

This entry was generated through inserting a Case citation for Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

Lennane, Richard. "New Types of Weapons Need New Forms of Governance." (June 28, 2018 2018). Accessed June 10, 2021. https://blogs.icrc.org/law-and-policy/2018/06/28/weapons-governance-new-types-weapons-need-new-forms-governance/.

Letts, Hitoshi Nasu and David. "The Legal Characterization of Lethal Autonomous Maritime Systems: Warship, Torpedo, or Naval Mine?"." *International Law Studies* 96 (2020).

Liebermann, Katie Bo Lillis and Oren. "How Ukraine Became a Testbed for Western Weapons and Battlefield Innovation." *CNN*, January 16, 2023 2023. https://edition.cnn.com/2023/01/15/politics/ukraine-russia-war-weapons-lab/index.html.

Liebermann, Natasha Bertrand and Oren. "Us Assessing Potential Damage of Patriot Missile Defense System Following Russian Attack near Kyiv." *CNN.* , May 16, 2023 2023. https://edition.cnn.com/2023/05/16/politics/patriot-missile-damage-ukraine/index.html

Liivoja, Rain. "Technological Change and the Evolution of the Law of War." *International Review of the Red Cross Review* 97, The evolution of warfare, no. 900 (2015).

Linda Null, and Julia Lobur. *The Essentials of Computer Organization and Architecture.* Massachusetts: Jones & Bartlett Publishers, 2006.

Looks, Deeper. "The Future of Battlefield." (April 2021 2021). Accessed July 16, 2023. https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield.

Lopez, Timothe. "L'adaptabilité Du Droit International Humanitaire Aux Évolutions Des Conflits Armés Contemporains." Master, Université Clerment-Auvergne, 2018.

———. "L'adaptabilité Du Droit International Humanitaire Aux Évolutions Des Conflits Armés Contemporains." Master mention Droit public parcours Carrières Internationales, Université Clerment-Auvergne, 2018.

"Iron Dome; Dual- Mission Counter Rocket, Artillery and Mortar (C-Ram) and Very Short-Range Air Defense (V-Shorad) System." Rafael Advanced Defense Systems LTD., accessed May 20, 2021, https://web.archive.org/web/20120710092155/http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/0/1190.pdf.

Lukiv, Jaroslav. "Ukraine War: Russian Air Strikes Target Kyiv for Third Night Running." *BBC News*, May 31, 2023 2023. https://www.bbc.com/news/world-europe-65750745.

Lynch, Justin Roger. "The Chain Home Early Warning Radar System a Case Study in Defense Innovation." *JFQ 95* (2019). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95_100-103_Lynch.pdf,.

Mahulikar, Arvind Gangoli Rao and Shripad P. "Integrated Review of Stealth Technology and Its Role in Airpower ". *Aeronautical Journal* 106, no. 1006 (2002). https://www.researchgate.net/publication/287536552_Integrated_review_of_stealth_technology_and_its_role_in_airpower.

Markley, Rich. *Oscilloscope Basics.* Bangkok: Rohde & Schwarz, 2015.

Markoff, John. "Before the Gunfire, Cyber Attacks." *The New York Times*, August 12, 2008 2008. https://www.nytimes.com/2008 /08/13/technology/13cyber.html,.

Martin, Craig. "Target Killing, Self-Defense, and the Jus Ad Bellum Regime." In *Targeted Killings: Law & Morality in an Asymmetrical World*, edited by Jens David Ohlin Claire Finkelstein, Andrew Altman, 223. Oxford: Oxford University Press, 2012.

Masood, Scott Shane and Salman. "Drone Strike in Pakistan Kills Haqqani Commander." *The New York Times*, October 14, 2011 2011. https://www.nytimes.com/2011/10/14/world/asia/drone-attack-in-pakistan-kills-a-haqqani-leader.html.

Meikle, Hamish. *Modern Radar Systems.* London: Artech House, 2008.

Melzer, Nils. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.* Geneva: International Committee of the Red Cross, 2009. https://www.refworld.org/docid/4a670dec2.html.

Meron, Theodor. "The Hague Tribunal: Working to Clarify International Humanitarian Law." *American University International Law Review* 13, no. 6 (1998).

———. *The Humanization of International Law.* The Nethelands: Matinus Nijjhof, 2006.

———. "The Martens Clause, Principles of Humanity, and Dictates of Public Conscience." *The American Journal of International Law* 94, no. 1 (January 2000 2000).

Meurant, Jacques. "Inter Arma Caritas: Evolution and Nature of International Humanitarian Law." *Journal of Peace Research* 24, no. 3 (1987).

Mills, Ivoty. "Emergent International Humanitarian Law in the Context of Cyber Warfare." *Transmission: The Journal of Film and Media Studies* 2, no. 1 (2017).

Momtaz, Michael J. Matheson et Djamchid. *Les Règles Et Institutions Du Droit International Humanitaire À L'épreuve Des Conflits Armés Récents.* Leiden: Martinus Nijhoff Publishers, 2010.

Moore, Wilbert E. "Introduction." In *Technology and Social Change*, edited by Wilbert E. Moore. Chicago: Quadrangle Books, 1972.

Muhammad Hanifudin Al Fadli, Dadang Gunawan, Romie Oktovianus Bura, and Larasmoyo Nugroho. "Design and Implementation of Anti-Tank Guided Missile (Atgm) Control System Using Semi-Automatic Command Line of Sight (Saclos) Method Based on Digital Image Processing." *Jurnal Pertahanan* 7, no. 2 (2021). https://www.academia.edu/59048238/Design_and_Implementation_of_Anti_Tank_Guided_Missile_Atgm_Control_System_Using_Semi_Automatic_Command_Line_of_Sight_Saclos_Method_Based_on_Digital_Image_Processing.

Murphy, Peter W. "Judging War Criminals." *Texas International Law Journal* 35, no. 2 (2000).

Nasu, Hitoshi. "Nanotechnology and the Law of Armed Conflict." In *New Technologies and the Law of Armed Conflict*, edited by Hitoshi Nasu and Robert McLaughlin. The Hague: T.M.C. Asser Press, 2014.

Nations, United. *Assuring Our Common Future: A Guide to Parliamentary Action in Support of Disarmament for Security and Sustainable Development.* Edited by Alyn Ware. New York: United Nations Secretary general, 2020.

———. "Report of the 2023 Session of the Group of the Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems ", edited by United Nations, 24 May 2023 2023.

———. *Report of the Informal Meeting of Experts on Lethal Autonomous Weapons Systems (Laws).* United Nations Office for Disarmament Affairs (November 12-13, 2015 2015).

Neil Chuka, and Jean Francoise Born. *Hybrid Warfare: Implication for Caf Force Development.* Defence Research and Development Canada (August 2014 2014). https://apps.dtic.mil/sti/pdfs/AD1017608.pdf.

Neufeld, Michael J. *The Rocket and the Reich: Peenemunde and the Coming of the Ballistic Missile Era.* New York: The Free Press, 1995.

Neumann, John Von. *Theory of Self-Reproducing Automata.* Urbana and London: University of Illinois Press, 1966.

Nitesh Kumar Dixit, Lokesh Mishra, Mahendra Singh Charan and Bhabesh Kumar Dey. "The New Age of Computer Virus and Their Detection." *International Journal of Network Security & Its Applications (IJNSA)* 4, no. 3 ((May 2012) 2012).

Nunes, Afonso Seixas. "Autonomous Weapons System and Deploying States: Making Designers and Programmers Accountable." *Nacao e Defesa*, no. 161 (2022): 69-91. https://doi.org/10.47906/ND2022.161.04.

"Obama 2009 Pakistan Strikes." *The Bureau of Investigative Journalism*, August 10, 2011 2011. http://www.thebureauinvestigates.com/2011/08/10 /obama2009-strikes/.

OECD. *Scoping the Oecd Ai Principles: Deliberations of the Expert Group on Artificial Intelligence at the Oecd (Aigo).* (November 2019 2019). https://www.oecd-ilibrary.org/docserver/d62f618a-en.pdf?expires=1679043632&id=id&accname=guest&checksum=AB48031E1C037FAD29746BB78DC284D9.

Ohlin, Jens David. "The Combatant's Stance: Autonomous Weapons on the Battlefield." *International Law Studies* 92 (2016).

Okechukwu, Elizabeth Kirkham and Nneka. *Controlling the Transfer of Man-Portable Air Defence Systems: A Guide to Best Practice.* London: Saferworld, 2010. https://www.files.ethz.ch/isn/126449/MANPADS%20with%20footnotes%20REV.pdf.

Oren Liebermann, Jennifer Hansler, Haley Britzky, and Natasha Bertrand. "Russian Fighter Jet Forces Down Us Drone over Black Sea." *CNN online*, March 15, 2023 2023. https://edition.cnn.com/2023/03/14/politics/us-drone-russian-jet-black-sea/index.html.

Organization, Research and Technology. *Technologies for Future Precision Strike Missile Systems.* North Atlantic Treaty Organization (2000). https://www.sto.nato.int/publications/STO%20Educational%20Notes/RTO-EN-013/EN-013-$$ALL.PDF, .

Pagallo, Ugo. *The Laws of Robots: Crimes, Contracts and Torts.* New York: Springer, 2013.

"Raytheon Mim-104 Patriot." Directory of U.S. Military Rockets and Missiles, 2002, accessed June 12, 2022, 2022, http://www.designation-systems.net/dusrm/m-104.html,.

Patch, Nathaniel. "Kamikazes: When Japanese Planes Attacked the U.S. Submarine Devilfish." *Prologue* 46, no. 1 (2014). https://www.archives.gov/files/publications/prologue/2014/spring/kamikazes.pdf,.

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke. *On Cyber Warfare.* A Chatham House Report (November 2010 2010).

Pellet, Alain. "L'adaptation Du Droit International Aux Besoins Changeants De La Société Internationale." *RCADI* 329 (2007).

Piatkowski, Mateusz. "The Definition of the Armed Conflict in the Conditions of Cyber Warfare." *Polish Political Science Yearbook* 46, no. 1 (2017).

Pictet, Jean. "The Formation of International Humanitarian Law." *International Review of Red Cross* 244 (January-February 1985 1985).

———. *Humanitarian Law and the Protection of War Victims.* Geneva: Henry Dunant Institute, 1975.

Piper, Elizabeth. "Cyber Attack Hits 200,000 in at Least 150 Countries: Europol." *Reuters*, May 14, 2017 2017. https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX,.

Pir Zubair Shah, Sabrina Tavernise and Mark Mazzetti. "Taliban Leader in Pakistan Is Reportedly Killed." *The New York Times*, August 8, 2009 2009. https://www.nytimes.com/2009/08/08/world /asia/08pstan.html.

Pledger, Thomas G. *The Roles of Drones in Future Terrorist Attacks.* (The Association of the United States Army, February 2021 2021).

Press, Associated. "Yemen: Drone Kills Suspected Militants, Officials Say." *The New York Times*, September 1, 2012 2012. https://www.nytimes.com/2012/09/01/world/middleeast/drone-kills-suspected-militants-in-yemen-officials-say.html.

Priya, Niraj Prasad Bhatta and M. Geetha. "Radar and Its Applications." *IJCTA* 10, no. 3 (2017).

This entry was generated through inserting a Case citation for Prosecutor V Kuprekic. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Prosecutor V. Dario Kordic and Mario Cerkez (Appeal). Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Prosecutor V. Dragoljub Kunarac Et Al. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Prosecutor V. Dusko Tadic, (Appeal Judgement). Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for The Prosecutor V. Dusko Tadic, the Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, the Appeal Chamber (Icty) 2 October 1995 Para.70. Case

references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Prosecutor V. Jean-Paul Akayesu. Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

This entry was generated through inserting a Case citation for Prosecutor V. Miodrag Jokic (Sentencing Judgement) Case references should appear only in the notes. Remove field codes in the final document and then remove this entry.

"Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol Ii)." 8 June 1977 1977.

Quince, Annabelle. "Future Drone Strikes Could See Execution by Algorithm." (January 21, 2013 2013). Accessed July 24, 2020. https://www.abc.net.au/radionational/programs/rearvision/drones/4703792.

"R-27 (Aa-10 Alamo) Guided Medium Range Air-to-Air Missile." Airforce Technology, Updated December 9, 2020, 2020, accessed June 10, 2022, 2022, https://www.airforce-technology.com/projects/r-27-aa-10-alamo-guided-medium-range-air-missile/.

Rae, James DeShaw. "Remote Killing and the Ethics of Drone Warfare." In *Analyzing the Drone Debates: Targeted Killing, Remote Warfare, and Military Technology*, edited by James DeShaw Rae. New York: Palgrave Pivot, 2014.

Ramsay, Patricia Spieth. "Heinrich Hertz, the Father of Frequency." *The Neurodiagnostic Journal* 53, no. 1 (2013): 3-26. https://doi.org/10.1080/21646821.2013.11079882.

Randall, Henry A. H. Boot and John T. "Historical Notes on the Cavity Magnetron." *IEEE Transactions on Electron Devices* 23, no. 7 (July 1976 1976).

Ranum, Macus J. "Fred Cohen on Strategic Security: Start with the Assumptions." (February 2018 2018). Accessed January 19, 2020. https://www.techtarget.com/searchsecurity/opinion/Fred-Cohen-on-strategic-security-Start-with-the-assumptions,.

Rebecca Wright, Ivan Watson, Olha Konovalova, and Tom Booth. "Chinese-Made Drone, Retrofitted and Weaponized, Downed in Eastern Ukraine." *CNN online*, March 16, 2023 2023. https://edition.cnn.com/2023/03/16/europe/china-made-drone-downed-eastern-ukraine-hnk-intl/index.html.

Reddy, V. Phaninder. *Rocket and Missiles, Lecture Notes.* Telangana: Institute of Aeronautical Engineering, 2000.

Reiher, Jelena Mirkovic and Peter. "A Taxonomy of Ddos Attack and Ddos Defense Mechanisms." *ACM SIGCOMM Computer Communication Review* 34, no. 2 (April 1, 2004 2004): 40.

Rivault, Daniele Palombo and Erwan. "Ukraine War: Satellite Images Reveal Russian Defences before Major Assault." *BBC News*, May 22, 2023 2023. https://www.bbc.com/news/world-europe-65615184.

Robert S. Gutzwiller, Sunny Fugate, Benjamin D. Sawyer, and P. A. Hancock. "The Human Factors of Cyber Network Defense." Paper presented at the Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting – 2015, 2015.

Roberts, Adam. "The Equal Application of the Law of War: A Principle under Pressure." *International Review of the Red Cross Review* 90, no. 872 (December 2008 2008). https://international-review.icrc.org/sites/default/files/irrc-872-6.pdf.

Rogers, A.P.V. *Law on the Battlefield.* 2nd edition ed. Manchester: Manchester University Press, 2004.

"Rome Statute of the International Criminal Court." July 17, 1998 1998. https://ihl-databases.icrc.org/en/ihl-treaties/icc-statute-1998?activeTab=undefined.

Rouse, Margaret. "What Does Jerusalem Virus Mean?". (May 31, 2012 2012). Accessed January 19, 2020. https://www.techopedia.com/definition /27875/jerusalem-virus.

"San Remo Manual on International Law Applicable to Armed Conflicts at Sea ". 1995. https://www.icrc.org/en/doc/resources/documents/article/other/57jmsu.htm.

Sarker, Iqbal H. "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions." *SN Computer Science* 2, no. 420 (2021).

https://www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview,.

Schaper, David. "It Was Shoes on, No Boarding Pass or Id but Airport Security Forever Changed on 9/11." (September 10, 2021 2021). Accessed January10, 2022. https://www.npr.org/2021/09/10/1035131619/911-travel-timeline-tsa#:~:text=It's%20not%20 clear%20what% 20exactly, it%20wouldn't%20have%20mattered.

Schmitt, Michael N. "Assassination in the Law of War." (October 15, 2021 2021). Accessed February 10, 2022. https://lieber.westpoint.edu/assassination-law-of-war.

———. "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis." *Harvard National Security Journal* 1, no. 55 (2010).

———. "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross Review* 84, no. 846 (June 2002 2002).

Schulze, Matthias. "Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations." 12th International Conference on Cyber Conflict, 2020.

Scott, Roger D. "Legal Aspects of Information Warfare: Military Disruption of Telecommunications." *Naval Law Review* 45 (1998).

Sharkey, Noel. "Cassandra or False Prophet of Doom: Ai Robots and War." *IEEE Intelligent Systems* 23, no. 4 (July-Aug. 2008 2008).

Sharp, Jeremy M. *U.S. Foreign Aid to Israel.* Washington DC: Congress Research Service, 2015.

———. *U.S. Foreign Aid to Israel.* Washington, DC: Congressional Research Service, 2023.

Shulman, Mark. *Legal Constraints on Information Warfare.* Center for Strategy and Technology, Air War Center (1999).

Siouris, George M. *Missile Guidance and Control Systems.* New York: Springer, 2014.

Skolnik, Merrill I. *Introduction to Radar Systems.* Second edition ed. Singapore: McGraw-Hill Book Co., 1981.

Slegers, John Harris and Nathan. "Performance of Fire-and-Forget Anti-Tank Missile with a Damaged Wing." *Biomedical, Mechanical, and Civil Engineering* 7 (2009). https://digitalcommons.georgefox.edu/mece_fac/7.

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War.* Cambridge: Cambridge University Press, 2010.

Staff, Defence Review Asia. "International Industry Partner Announce Collaboration Agreement for Gcap Advanced Electronics." *Defence Review Asia* (March 21, 2023 2023). https://defencereviewasia.com/international-industry-partners-announce-collaboration-agreement-for-gcap-advanced-electronics/.

———. "What Is the Best Drone Defeat Technique?". (March 21, 2023 2023). Accessed March 22, 2023. https://defencereviewasia.com/what-is-the-best-drone-defeat-technique/

Stephens, Dale. "The International Legal Implications of Military Space Operations: Examining the Interplay between International Humanitarian Law and the Outer Space Legal Regime." *International Law Studies* 94 (2018).

Steward, Darren M. "New Technology and the Law of Armed Conflict." *International Law Studies* 87 (2011): 271-98. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1082&context=ils.

Tabansky, Lior. "Israel Defense Forces and National Cyber Defense." *Connections* 19, no. 1 (2020): 45–62. https://www.jstor.org/stable/26934535.

Tallinn Manual on the International Law Applicable to Cyber Warfare. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2013.

Tamer, Mehmet Emin Erendor and Gurkan. "The New Face of the War: Cyber Warfare." *Cyberpolitik Journal* 2, no. 4 (2018): 58-75.

Taylor, Michael Bedford. "The Evolution of Bitcoin Hardware." *Computer* 50, no. 9 (2017): 59-60.

Team, Pandora FMS. "History of Computer Viruses: Creeper and Reaper." (October 10, 2018 2018). Accessed December 18, 2020. https://pandorafms.com/blog/creeper-and-reaper/.

Thomson, Iain. "25,000 Malware-Riddled Cctv Cameras Form Network-Crashing Botnet." (28 June 2016 2016). Accessed May 20, 2022. https://www.theregister.com/2016/06/28/25000_compro mised_cctv_cameras/.

Tiwari, Sakshi. "Making History- Israel Becomes the First Country to Successfully Shoot Down Drones with Iron Beam Laser Interceptors." *The Eurasian Times*, April 15, 2022 2022. https://eurasiantimes.com/israel-successfully-shoot-down-drones-with-laser-interceptor/.

"Top 10 Military Technology Trends and Innovations for 2023." (2023). https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/.

"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies." 1967

"Treaty on the Prohibition of Nuclear Weapons." edited by United Nations General Assembly, 7 July 2017 2017

Tsagourias, Russell Buchan and Nicholas. "Ukranian 'It Army': A Cyber Levée En Masse or Civilians Directly Participating in Hostilities?". *European Journal of International Law* (2022). . https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-inhostilities/?fbclid=IwAR1IL6iWjPKOUQQ4QUvOj3G3aDWK2g7W4Bxy QumJLFoweDtP3YHpiT40wkU.

———. "Ukranian 'It Army': A Cyber Levée En Masse or Civilians Directly Participating in Hostilities?" *European Journal of International Law*. (March 9, 2022 2023). Accessed March 26, 2023. https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-inhostilities/?fbclid=IwAR1IL6iWjPKOUQQ4QUvOj3G3aDWK2g7W4Bxy QumJLFoweDtP3YHpiT40wkU.

Tsui, Chi-Hao Cheng and James. *An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques* London: River Publishers, 2021.

Turns, David. "Weapons in the Icrc Study on Customary International Law." *Journal of Conflict and Security Law* 11, no. 1 (2006). https://doi.org/10.1093/jcsl/krl010. https://academic.oup.com/jcsl/article/11/2/201/836156.

Uamduang, Piyanat. "Export Control of Dual-Use Items: A Comparative Study of Thai and Foreign Laws." Master of Laws in Business Law, Thammasat University, 2016.

Un Special Rapporteur on Extrajudicial Killing. United Nations (28 May 2010 2010).

"United Nations Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques." 1977.

Warrick, Joby. "Airstrike Kills Dozens of Insurgents." *Washington Post*, June 24, 2009 2009. http://www.washingtonpost.com.

———. "Use of Weaponized Drones by Isis Spurs Terrorism Fears." *Washington Post*, February 21, 2017 2017. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

Watch, Human Rights. *Between a Drone and Al-Qaeda: The Civilian Cost of Us Targeted Killings in Yemen.* Human Rights Watch (2013). https://www.hrw.org/sites/default/files/report_pdf/yemen1013web.pdf.

Werrell, Kenneth P. *The Evolution of the Cruise Missile.* Alabama: Air University Press, 1985.

Wiener, Norbert. *Cybernetics: Or Control and Communication in the Animal and the Machine.* Cambridge: MIT Press, 1948.

Witt, Stephen. "The Turkish Drone That Changed the Nature of Warfare." *The New Yorker*, May 16, 2022 2022. https://www.newyorker.com/magazine/annals-of-war.

Witte, Dafna Linzer and Griff. "U.S. Airstrike Targets Al Qaeda's Zawahiri." *Washington Post*, January 14, 2006 2006. https://www.washingtonpost.com/archive/politics/2006/01/14/us-airstrike-targets-al-qaedas-zawahiri/235b61c5-0c8d-477d-868c-54565c3f30fa/.

Yanushevsky, Rafael. *Modern Missile Guidance.* London: CRC Press, 2008.

Yasuaki, Onuma. "International Law in and with the International Politics: The Functions of International Law in International Society." *European Journal of International Law* 14, no. 1 (2003).

"Yemen: Reported Us Covert Action 2012." *The Bureau of Investigative Journalism*, 2012. https://www.thebureauinvestigates.com/2012/05/08/yemen-reported-us-covert-action-2012/.

Yenkin, Jonathan. "Company Tracks Down Michelangelo Computer Virus." *AP news*, January 29, 1992 1992. https://apnews.com/article/1b3d0b1803e743a0898f2c1dedd73f69.

Zarchan, Paul. *Tactical and Strategic Missile Guidance.* 6th edition ed. Virginia: American Institute of Aeronautics and Astronautics, 2012.

คณะกรรมการกาชาดระหว่างประเทศ. กฎหมายมนุษยธรรมระหว่างประเทศ ถาม-ตอบทุกคำถาม. กรุงเทพฯ: คณะกรรมการกาชาดระหว่างประเทศ, 2562.

"ความขัดแย้งระหว่างรัสเซีย-ยูเครน 2 เมื่อต่างฝ่ายยืนยันที่จะสู้เพื่อปกป้องประเทศ." (25 กุมภาพันธ์ 2565). Accessed 1 มีนาคม พ.ศ.2565. https://themomentum.co/report-russia-ukraine-fight-2/.

พีรพัฒ โชคสุวัฒนสกุลและคณะ. *Thailand Artificial Intelligence Guidelines 0.1:* แนวปฏิบัติเกี่ยวกับมาตรฐานการใช้ปัญญาประดิษฐ์. กรุงเทพ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2565.

ภูภุช กนิษฐชาติ. "Hypersonic Weapon อาวุธเหนือเสียงนวัตกรรมเปื้อนเลือดเหนือน่านฟ้าสงครามยูเครน-รัสเซีย." (24 มีนาคม 2565). Accessed 15 มกราคม 2566. https://waymagazine.org/hypersonic-weapon-in-russia-ukraine-war/.

"รัสเซียส่งโดรนพลีชีพ Kub-Bla ติดตั้งปัญญาประดิษฐ์ Ai เข้าไปปฏิบัติการในยูเครน." (21 มีนาคม 2565). Accessed 16 มกราคม 2566. https://www.tnnthailand.com/news/tech/108526/?fbclid=IwAR2fvcOgDFRHRHZQhoP3yLvHeJk5kHa6gXX25okHSNFUugI3LWo s6TMAKE.

"สบายแต่เสี่ยงโดนแฮก กล้อง Cctv ในยุคอินเทอร์เน็ตของทุกสิ่ง." (2559). Accessed 20 พฤษภาคม พ.ศ.2565. https://www.dga.or.th/document-sharing/article/35961/.

อาคม รวมสุวรรณ. "ส่องโดรนพิฆาต Bayraktar Tb-2 จนเรือเร็วตรวจฝั่งรัสเซียดิ่งทะเลดำสองลำซ้อน." (4 พฤษภาคม 2565). Accessed 10 พฤษภาคม พ.ศ.2565 https://www.thairath.co.th/news/auto/news/2383455

อุบลวรรณ ภีระเป็ง. "การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ: ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ." วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2558.

ประวัติผู้เขียน

ชื่อ-สกุล	ดามร คำไตรย์
วัน เดือน ปี เกิด	10 สิงหาคม 2521
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	นิติศาสตรบัณฑิต (เกียรตินิยมอันดับสอง) จุฬาลงกรณ์มหาวิทยาลัย นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย
ที่อยู่ปัจจุบัน	202 หมู่ 4 ต.นางแล อ.เมือง จ.เชียงราย