บทที่ ๖

บทสรุปและเสนอแนะ

คำนิยาม

สืบเนื่องจากความสนใจที่จะหาคำนิยามที่ชัดเจนของคำว่า"แฮกเกอร์" ผู้เขียนพบว่าการให้คำนิยามของแฮกเกอร์ สามารถแบ่งได้เป็น ๓ กลุ่มคือ กลุ่มแรกคือกลุ่มที่กำหนดคำนิยามโดยอาศัยความเห็นส่วนตัว กลุ่มที่สองคือกลุ่มที่กำหนดคำนิยามโดยอาศัยเจตนาของการกระทำและกลุ่มสุดท้ายคือกลุ่มที่กำหนดคำนิยามโดยอาศัยลักษณะการกระทำ ซึ่งเมื่อพิจารณาความเหมาะสมระหว่างกลุ่มของคำนิยามเพื่อผลในด้านนิติศาสตร์ สมควรกำหนดคำนิยามตามกลุ่มที่อาศัยลักษณะการกระทำเป็นหลัก กล่าวคือกำหนดความหมายของ"แฮกเกอร์"ว่าหมายถึง "ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต"

เหตุผลในการบัญญัติให้การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิด

เนื่องจากผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตได้รับความสนใจและกล่าวถึงในปัจจุบัน ไม่ว่าจะเป็นเพราะการเจาะระบบคอมพิวเตอร์มีผลกระทบต่อความสงบเรียบร้อยของสังคมหรือต่อความหวาดกลัวต่อกระแสการคาดการณ์ถึงผลเสียหายในอนาคต เป็นสาเหตุให้ผู้เขียนต้องการหาเหตุผลเพื่อสนับสนุนในการกำหนดให้การกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา ซึ่งการที่จะกำหนดให้การกระทำใดเป็นความผิดอาญาจะต้องได้ความว่าการกระทำนั้นกระทบต่อความสงบเรียบร้อยและศีลธรรมอันดีของสังคม สำหรับผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตนั้น เมื่อศึกษาจากพฤติกรรมและเหตุการณ์ที่เกิดขึ้นอันเนื่องมาจากการกระทำของผู้เจาะระบบคอมพิวเตอร์ในบทที่ ๓ จะเห็นได้ว่ามีเหตุผลเพียงพอที่จะกำหนดให้การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดเพราะมีการกระทำที่กระทบต่อประชาชนโดยทั่วไป นอกจากนี้ผู้เขียนได้แสดงเหตุผลโต้แย้งในปัญหา ๔ หัวข้อดังต่อไปนี้คือ

๑. เมื่อมีการกำหนดความรับผิดทางอาญาต่อผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจะกระทบต่อความก้าวหน้าทางเทคโนโลยีในประเทศไทยหรือไม่

๒. การนำกฎหมายอาญามารองรับการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจะเป็นการใช้กฎหมายอาญาเฟ้อหรือไม่

๓. การนำความรับผิดทางแพ่งมารองรับการกระทำของผู้เจาะระบบคอมพิวเตอร์จะเพียงพอหรือไม่ และ

๔. การนำหลักทางจริยธรรมมาเป็นแนวทางในการกำหนดความประพฤติของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจะเพียงพอหรือไม่

นโยบายทางอาญาต่อผู้เจาะระบบคอมพิวเตอร์

วิธีการศึกษานโยบายทางอาญาเป็นแนวทางที่ผู้เขียนนำมาใช้ในการศึกษาความรับผิดทางอาญาของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เพราะเป็นการศึกษาเกี่ยวกับการกำหนด เป้าหมายในการกำหนดความผิด กำหนดโทษ การบัญญัติกฎหมาย และวิธีการลงโทษ ซึ่งได้แก่วิธีการดังต่อไปนี้ คือ

๑. วิธีการป้องกันมิให้เกิดการกระทำความผิดโดยกำจัดมูลเหตุที่ศึกษามาจากอาชญาวิทยา

จากการศึกษาพบว่าผู้เจาะระบบคอมพิวเตอร์มีแรงจูงใจในการเจาะระบบคอมพิวเตอร์แตกต่างกัน ซึ่งแบ่งออกได้เป็น ๕ ประเภทคือ แรงจูงใจทางสังคม แรงจูงใจทางเทคนิค แรงจูงใจทางการเมือง แรงจูงใจทางการเงินและแรงจูงใจทางรัฐบาล และเมื่อพิจารณาแรงจูงใจทั้ง ๕ ประการประกอบกับทฤษฎีทางอาชญาวิทยา พบว่าแรงจูงใจทั้งห้าประการมีแนวโน้มที่จะนำไปสู่การกระทำผิดได้ทั้งสิ้น ดังนั้น การป้องกันไม่ให้มีการเจาะระบบคอมพิวเตอร์ จึงศึกษาได้จากแรงจูงใจประกอบกับการกำจัดมูลเหตุแห่งการกระทำความผิดตามทฤษฎีอาชญาวิทยา ซึ่งผู้เขียนสรุปได้เป็น ๓ แนวทาง คือ

ก. ให้ความสำคัญกับสถาบันครอบครัวในการปลูกฝังความคิดที่ถูกต้อง สำหรับการป้องกันการกระทำที่เกิดจากแรงจูงใจทางสังคม แรงจูงใจทางเทคนิคและแรงจูงใจทางการเมือง

ข. ให้ความสำคัญต่อความเป็นอยู่และสวัสดิการของประชาชน สำหรับการป้องกันการกระทำความผิดที่เกิดจากแรงจูงใจทางการเงิน

ค. ให้ความสำคัญกับความสัมพันธ์ระหว่างประเทศและวิถีทางทางการทูตเพื่อลดปัญหาความขัดแย้งระหว่างรัฐ สำหรับป้องกันการกระทำความผิดที่เกิดจากแรงจูงใจทางรัฐบาล

๒. วิธีทางนิติบัญญัติเพื่อจะได้ผลในทางป้องกันและปราบปรามการกระทำความผิด

การให้ความสนใจหรือให้ความสำคัญกับตัวบทกฎหมายคือสิ่งแรกเมื่อพบการกระทำความผิด เช่นเดียวกับการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตแต่จากการศึกษาพบว่าประมวลกฎหมายอาญาในปัจจุบันไม่สามารถปรับใช้กับความผิดที่เกิดจากการเจาะระบบคอมพิวเตอร์ได้ และเพื่อทราบถึงปัญหาในการปรับใช้ประมวลกฎหมายได้อย่างชัดเจน ผู้เขียนได้แยกปัญหาการกระทำของผู้เจาะระบบคอมพิวเตอร์ตามทฤษฎีกฎหมายอาญาว่าด้วยลำดับการเริ่มต้นของการกระทำความผิดเป็น ๓ ขั้นตอน คือ

- <u>ขั้นตอนที่ ๑</u> ปัญหาการปรับบทกฎหมายกับการกระทำต่อข้อมูลและระบบคอมพิวเตอร์ ที่เกิดขึ้นภายหลังจากเจาะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตได้แล้ว

- <u>ขั้นตอนที่ ๒</u> ปัญหาการปรับบทกฎหมายกับการกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์

- <u>ขั้นตอนที่ ๓</u> ปัญหาการปรับบทกฎหมายกับการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ปัญหาการปรับใช้กฎหมายอาญาทั้ง ๓ ขั้นตอนผู้เขียนได้เสนอแนวทางในการแก้ปัญหาโดยอาศัยวิธีทางนิติบัญญัติแยกพิจารณาตามปัญหาดังนี้คือ

- สำหรับขั้นตอนที่ ๑ รัฐควรเลือกที่จะบัญญัติกฎหมายว่าด้วยการกระทำต่อข้อมูลในระบบคอมพิวเตอร์ขึ้นใหม่ เพื่อแก้ไขปัญหาในเรื่องสถานะทางกฎหมายของ "ข้อมูล" ในระบบคอมพิวเตอร์

- สำหรับขั้นตอนที่ ๒ เมื่อพิจารณาหลักทฤษฎีทางกฎหมายอาญาในการพิจารณาว่าการกระทำใดควรลงโทษในขั้นตระเตรียมหรือพยายามกระทำความผิด อีกทั้งเมื่อจารณาถึงความห่างไกลต่อความเสียหายที่จะเกิดขึ้นจากการเจาะระบบคอมพิวเตอร์ ไม่สมควรกำหนดให้การกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา

- สำหรับขั้นตอนที่ ๓ การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นขั้นตอนที่ผู้เขียนเสนอขึ้นใหม่และเห็นว่าสมควรนำมาพัฒนาและบัญญัติเป็นความผิดได้ โดยให้**เป็นความผิดตั้งแต่เมื่ออยู่ในสถานะแรกของการเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต** ซึ่งนอกจากได้แนะนำให้รัฐบัญญัติกฎหมายขึ้นใหม่เป็นพิเศษ ผู้เขียนได้เสนอแนวทางในการกำหนดองค์ประกอบความผิดของบทบัญญัติว่าด้วยการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตไว้ด้วย สำหรับปัญหาว่าเมื่อใดจึงถือว่าเป็นการลงมือเจาะระบบคอมพิวเตอร์นั้น พบว่าการต่อโทรศัพท์หรือการเชื่อมต่อสำเร็จระหว่างเครื่องคอมพิวเตอร์ด้วยกันยังไม่ถือว่าเป็นการลงมือเจาะระบบคอมพิวเตอร์จนกว่าจะ**ได้กรอกข้อความ ตัวเลขหรือรหัสเพื่อแสดงตนในการเข้าสู่ระบบคอมพิวเตอร์**

๓. วิธีการบังคับเพื่อจะให้ได้ผลในทางป้องกันอาชญากรรม

ทฤษฎีที่กล่าวถึงวัตถุประสงค์ของการลงโทษมีด้วยกัน ๕ ทฤษฎี แบ่งวัตถุประสงค์ของการลงโทษเป็น ๕ ทฤษฎี ซึ่งแต่ละทฤษฎีมีความสัมพันธ์กับการกระทำความผิดในลักษณะต่างๆ เช่น ในความผิดฐานทำร้ายร่างกายหรือความผิดฐานฆ่าคนตาย รัฐจะลงโทษในสถานหนักเพราะต้องการข่มขู่ ไม่ให้มีการกระทำความผิดอีกและไม่ให้ผู้อื่นเอาเยี่ยงอย่าง

สำหรับผู้เจาะระบบคอมพิวเตอร์นั้น พบว่าเมื่อการเจาะระบบคอมพิวเตอร์เกิดจากแรงจูงใจที่ต่างกัน ฉะนั้นการลงโทษจึงควรพิจารณาพื้นฐานของการกรทำผิดตามลักษณะแรงจูงใจประกอบกับประเภทของโทษที่มีในกฎหมายอาญา ซึ่งสรุปได้ว่าผู้ที่มีแรงจูงใจทางสังคมและทางเทคนิค การลงโทษสมควรที่จะมุ่งเพื่อฟื้นฟูผู้เจาะระบบคอมพิวเตอร์ อันได้แก่การใช้มาตรการคุมประพฤติ ขณะที่ผู้ที่มีแรงจูงใจทางการเงิน การเมืองและทางรัฐบาลควรลงโทษโดยมีจุดประสงค์เพื่อข่มขู่ไม่ให้มีการเจาะระบบคอมพิวเตอร์อีก อันได้แก่การลงโทษจำคุกและกักขัง

๔. การประสานงานระหว่างสถาบันให้ดำเนินไปสู่จุดมุ่งหมายเดียวกัน

จากการศึกษาพบว่าในประเทศไทยมีหน่วยงานในกระบวนการยุติธรรมเพียงหน่วยงานเดียวที่ดูแลด้านอาชญากรรมคอมพิวเตอร์ คือตำรวจ ซึ่งไม่เพียงพอที่จะรองรับการกระทำความผิดทางคอมพิวเตอร์ได้ในอนาคต ผู้เขียนจึงเห็นว่าเป็นการสมควรที่ก่อตั้งหน่วยงานย่อยขึ้นมาเป็นพิเศษหรือก่อตั้งองค์กรใหม่เพื่อเป็นหน่วยงานที่ช่วยเสริมหรือร่วมลงมือในการสืบสวน สอบสวน พร้อมกับให้คำปรึกษาทางเทคนิคเกี่ยวกับคอมพิวเตอร์แก่พนักงานตำรวจ อย่างไรก็ตามหน่วยงานในกระบวนการยุติธรรมที่เหลือซึ่งมีความสัมพันธ์กันแบบเชื่อมโยงจำเป็นต้องพัฒนาศักยภาพบุคลากรของตนให้เข้าใจการเปลี่ยนแปลงทางเทคโนโลยี เพื่อประสิทธิภาพในการป้องกันและปราบปรามการกระทำผิดเช่นกัน

แนวทางในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา

สืบเนื่องจากการศึกษานโยบายทางอาญาโดยวิธีทางนิติบัญญัติ ที่ผู้เขียนได้เสนอแนวคิดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิด ซึ่งผู้เขียนจึงได้พัฒนาแนวคิดดังกล่าวเพื่อให้สามารถบัญญัติเป็นความผิดทางอาญาได้ชัดเจนยิ่งขึ้น อีกทั้งแสดงให้เห็นว่าแม้การแรกเข้าไปในระบบคอมพิวเตอร์จะไม่ปรากฏความเสียหายอย่างชัดเจนดังเช่นการกระทำความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ก็ตาม แต่สามารถก่อให้เกิดความเสียหายต่อสิทธิความเป็นส่วนตัว (privacy) และสิทธิในทรัพย์สิน ซึ่งเป็นสิทธิของเจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์ได้เช่นกัน และสำหรับในส่วนของรูปแบบของบทบัญญัตินั้น พบว่าควรเป็นบทบัญญัติที่กำหนดว่าการกระทำอย่างไรเป็น **ความผิด** มากกว่าเป็นบทบัญญัติที่**บังคับให้กระทำหรือห้ามมิให้กระทำ** เพราะการพัฒนาแนวคิดนี้เป็นสิ่งที่บุคคลทั่วไปไม่ทราบว่าสมควรเป็นความผิดซึ่งจะต่างกับการกระทำที่เห็นได้ชัดว่าเป็นความผิดดังเช่นความผิดฐานลักทรัพย์หรือทำร้ายร่างกาย

นอกจากนี้ผู้เขียนพบว่าแนวคิดในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์เป็นความผิดมีแนวคิดดังเช่นความผิดฐานบุกรุก ผู้เขียนจึงอาศัยองค์ประกอบความผิดฐานบุกรุกเพื่อเป็นแนวทางในการกำหนดองค์ประกอบความผิดของการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้

รับอนุญาต โดยแยกองค์ประกอบความผิดเป็น ๔ ส่วนคือ ส่วนการเข้าไป ส่วนทรัพย์สิน ส่วนการอนุญาต และส่วนเจตนา ซึ่งโดยสรุปได้ความว่า

๑. การ "เข้าไป" หมายความรวมถึง การเข้าไปโดยใช้สัญญาณทางอิเล็กทรอนิกส์ สำหรับการพิจารณาว่า*เมื่อใดเป็นการ "แรกเข้า"ไปในระบบคอมพิวเตอร์จะพิจารณาจากสถานะแรกเมื่อเข้าสู่ระบบคอมพิวเตอร์ได้แล้ว*

๒. ระบบคอมพิวเตอร์ หรือองค์ประกอบทางคอมพิวเตอร์ซึ่งทำงานประสานกัน ต้องเป็นระบบคอมพิวเตอร์ของผู้อื่นหรืออยู่ในความครอบครองผู้อื่น ไม่รวมถึงระบบคอมพิวเตอร์ของตนเอง

๓. "โดยไม่ได้รับอนุญาต" หมายถึงการเข้าไปในระบบคอมพิวเตอร์โดยไม่มีสิทธิโดยชอบหรือไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิครอบครอง

๔. ต้องมีเจตนาในการ "เข้าไป" ในระบบคอมพิวเตอร์ แต่ไม่สมควรลงโทษผู้เข้าสู่ระบบคอมพิวเตอร์โดยประมาท

การศึกษาองค์ประกอบความผิดดังกล่าวมีวัตถุประสงค์เพื่อแสดงให้เห็นว่ามีความเป็นไปได้ตามหลักเกณฑ์ของกฎหมายอาญาที่จะกำหนดบทบัญญัติตามแนวความคิดดังกล่าว มิใช่ประสงค์ให้นำบทบัญญัติว่าด้วยความผิดฐานบุกรุกมาใช้กับแนวคิดดังกล่าว อีกทั้งผู้เขียนได้ยกตัวอย่างกฎหมายในต่างประเทศ ที่กล่าวถึงการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorize access) ไว้ประกอบการพิจารณา ซึ่งแม้ว่าจะไม่ตรงกับแนวคิดของผู้เขียนแต่จากการศึกษาพบว่าในต่างประเทศให้ความสำคัญกับการป้องกันการเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตเช่นกัน ซึ่งตรงตามจุดประสงค์ตามแนวความคิดของผู้เขียน

ข้อเสนอแนะ

ทุกๆกลุ่มในสังคม มีความพยามยามที่จะสร้างความมั่นใจให้ได้ว่าสมาชิกในสังคมมีความประพฤติที่คาดหวังได้รวมไปถึงความคาดหวังที่ว่าสมาชิกในสังคมให้ความเคารพซึ่งกันและกัน ซึ่งความพยายามนี้เป็นหัวใจของการควบคุมโดยสังคม(social control) การควบคุมโดยสังคมปรากฏขึ้นในลักษณะต่างๆ แตกต่างกัน เช่นทางใบหน้า ท่าทาง ภาษา การซุบซิบนินทา การตลกขบขัน การตัดออกจากวงสังคม และอาจจะเขียนเป็นลายลักษณ์อักษร หรืออาจจะไม่ได้เขียนเป็นลายลักษณ์อักษร แต่เป็นการส่งต่อกันโดยปากต่อปาก ลักษณะต่างๆที่กล่าวมาจะก่อให้เกิดความรู้สึกผิด ละอาย และสามารถพัฒนาไปสู่การควบคุมภายในของตนเอง

กฎหมายเป็นเพียงรูปแบบของการควบคุมสังคม และเป็นตัวอย่างของสิ่งที่เราเรียกว่าระเบียบการควบคุมสังคม แต่ไม่จำเป็นว่าเมื่อมีการกระทำความผิดแล้วต้องมีการบัญญัติกฎหมายเสมอไป แต่ที่จำเป็นต้องมีกฎหมายเพราะบางทีการควบคุมโดยการแสดงท่าทาง หรือการซุบซิบนินทาอาจไม่แน่นอน กฎหมายจึงเกิดขึ้นเพื่อสร้างความแน่นอนในการควบคุมการกระทำ

การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นการกระทำที่กระทบต่อสิทธิส่วนตัว สิทธิในทรัพย์สินและก่อให้เกิดความเสียหาย ดังนั้นเพื่อสร้างความแน่นอนในการควบคุมการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจึง**สมควรบัญญัติกฎหมายขึ้นโดยเฉพาะเพื่อกำหนดความรับผิดทางอาญาสำหรับผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต**

นอกจากการบัญญัติกฎหมายขึ้นโดยเฉพาะแล้ว การสร้างแนวความคิดเป็นสิ่งที่มีความสำคัญเพราะเป็นการเสนอแนวทางในการแก้ไขปัญหาต่างๆ **ดังนั้นการสนับสนุนให้มีการเสนอแนวคิดทางกฎหมายเพื่อรับมือกับวิวัฒนาการใหม่ๆและนำมาแก้ไขปัญหาทางสังคมคือสิ่งที่ควรสนับสนุน** ดังเช่นที่ผู้เขียนได้เสนอให้การแรกเข้าไปในระบบคอมพิวเตอร์เป็นความผิด ซึ่งแม้ไม่อาจคาดหมายได้ว่าแนวคิดที่เสนอขึ้นมานั้นจะได้ผลในทางปฏิบัติหรือไม่ แต่อย่างน้อยที่สุดก็เป็นการพัฒนาให้นักกฎหมายมีความคิดใหม่ๆ เพื่อเป็นทางเลือกสำหรับรัฐในการที่จะใช้พิจารณาความเหมาะสมในการบัญญัติกฎหมาย มากกว่าที่เดินตามอย่างไม่สร้างสรรค์ และก้าวไม่ทันกับเทคโนโลยี