ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์

นายปรเมศวร์ กุมารบุญ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

The Relationship between Anonymity and Cybercrime

Mr. Poramez Kumarnboon

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2020

หัวข้อวิทยานิพนธ์	ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์
โดย	นายปรเมศวร์ กุมารบุญ
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.เอก ตั้งทรัพย์วัฒนา)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศ.พล.ต.ต.ดร.หญิงพัชรา สินลอยมา)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)

..... กรรมการ
(รองศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.เจษฎา ศิวรักษ์)

ปรเมศวร์ กุมารบุญ : ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ . (The Relationship between Anonymity and Cybercrime) อ.ที่ปรึกษาหลัก : รศ. ดร.สุมนทิพย์ จิตสว่าง

ดุษฎีนิพนธ์นี้ มีวัตถุประสงค์เพื่ออธิบายความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ด้วยทฤษฎีเกม โดยการไร้ตัวตนในดุษฎีนิพนธ์นี้หมายถึง การหลบพ้นการสืบสวนจับกุมทางดิจิทัลและการไม่สามารถรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีเอาผิดได้ เพราะอาชญากรไซเบอร์เป็นอาชญากรที่คอยมองหาโอกาสอยู่เสมอและเมื่อได้พบไซเบอร์เทคโนโลยีใดที่มีปัจจัยการไร้ตัวตนจะตัดสินใจเลือกก่ออาชญากรรมทันทีและเมื่อไซเบอร์เทคโนโลยีนั้นการไร้ตัวตนหมดสิ้นไป อาชญากรรมไซเบอร์ประเภทนั้นจะหมดไปเป็นวัฏจักร ดุษฎีนิพนธ์นี้เป็นการวิจัยแบบผสมผสานมีทั้งการวิจัยเชิงปริมาณจากสถิติคดีอาชญากรรมไซเบอร์กับการสำรวจความเห็นออนไลน์จำนวน 35 ราย และการวิจัยเชิงคุณภาพด้วยวิธีการวิจัยเอกสาร รวบรวมเนื้อหาอาชญากรรมไซเบอร์ คำสารภาพของอาชญากรไซเบอร์ คดีที่มีคำพิพากษาอาชญากรรมไซเบอร์ที่เคยเกิดขึ้นจากอดีตจนถึงปัจจุบันและการสัมภาษณ์แบบเจาะลึก 1 กรณีศึกษา จากนั้นเลือกกรณีศึกษาที่น่าสนใจขึ้นมา 17 กรณีศึกษาและใช้ทฤษฎีเกมกับทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลเป็นเครื่องมือในการวิเคราะห์ความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับการไร้ตัวตน โดยอธิบายรูปแบบความสัมพันธ์เป็น ต้นไม้การตัดสินใจ ตารางผลตอบแทน และสมการผลตอบแทน ผลการวิจัยพบว่า ทฤษฎีเกมอธิบายความสัมพันธ์ระหว่างการไร้ตัวตนและการเกิดอาชญากรรมไซเบอร์ให้ได้เข้าใจง่ายและได้มีข้อเสนอแนะให้รัฐแก้กฎหมายที่ยังมีช่องว่างและเสนอให้มีศาลชำนัญพิเศษพิจารณาอาชญากรรมไซเบอร์โดยเฉพาะต่อไป

สาขาวิชา อาชญาวิทยาและงานยุติธรรม ลายมือชื่อนิสิต .....

ปีการศึกษา 2563 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5981361024 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Cybercrime, Game theory, Anonymity

Poramez Kumarnboon : The Relationship between Anonymity and Cybercrime . Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

The aim of using Game theory in this dissertation illustrates that there is the relationship between anonymity and cybercrime in almost in every domain. Consequently, this has defined to the anonymity of cybercrime in both obstacles to digital investigations and digital evidences collection cannot be used in court. Furthermore, cybercriminals make decision to commit crime only performs the act if the opportunity occurs. In my opinion, when anonymity enables individuals to engage in activities is revealing themselves that cybercrime type is over. This dissertation is mixed method, one is quantitative researches both a few cybercrime statistics and 35 victims' online survey result. Another is qualitative research that is documentary research method and in-depth interview 1 case. The next step is collected event of cybercrimes from past until today, which is chosen interesting 17 studied cases. Purpose to understand cyber criminal's decision-making by rational choice theory that has been used Game theory as a explaination via Decision Tree, Payoff Matrix and Payoff Function. The result of this dissertation proved that the relationship between cybercrimes and anonymity are relating. The policy recommendations include developing loopholes in the judiciaries and the establishment of the specialized court is to ensure that specific or technical problems will be solved by appropriate adjudicators.

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2020	Advisor's Signature .....

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณ รศ.ดร.สุมนทิพย์ จิตสว่าง อาจารย์ที่ปรึกษาดุษฎีนิพนธ์ ที่เสียสละเวลาให้คำแนะนำอันเป็นประโยชน์จนดุษฎีนิพนธ์มีความก้าวหน้าขึ้นเรื่อยๆจนสำเร็จลุล่วงอย่างดีและในระหว่างการศึกษาข้าพเจ้าได้เห็นการทุ่มเททำงานหนักของท่านอาจารย์เสมอมา เพื่อจะให้ความรู้นิสิตและจุฬาฯ เป็นเสาหลักสำคัญในงานวิชาการด้านอาชญาวิทยาและงานยุติธรรม ข้าพเจ้าขอขอบพระคุณ ศ.พล.ต.ต.(หญิง) ดร.พัชรา สินลอยมา ประธานกรรมการสอบดุษฎีนิพนธ์ ที่เมตตาให้โอกาสทางวิชาการกับข้าพเจ้าเสมอมา ยังช่วยชี้แนะทิศทางการวิจัยจนดุษฎีนิพนธ์ฉบับนี้มีความก้าวหน้าทางวิชาการ ข้าพเจ้าขอขอบพระคุณ รศ.ดร.อุนิษา เลิศโตมรสกุล ที่ได้สั่งสอนให้ความรู้ทางวิชาการสมัยใหม่มากมายในระหว่างการศึกษาจนนำมาเป็นประโยชน์ต่อดุษฎีนิพนธ์ฉบับนี้และยังได้ช่วยชี้แนะทฤษฎีสำคัญจนพัฒนามาเป็นบทสรุปที่ลงตัวและมีข้อเสนอแนะที่ก้าวหน้าในกระบวนการยุติธรรม ข้าพเจ้าขอขอบพระคุณ ผศ.ดร.ฐิติยา เพชรมุนี ที่ได้ให้คำแนะนำมากมายที่ข้าพเจ้ามองข้ามในการวิจัย จนแก้ไขกลับมาเป็นดุษฎีนิพนธ์ที่สมบูรณ์ ข้าพเจ้าขอขอบพระคุณ ดร.เจษฎา ศิวรักษ์ กรรมการผู้ทรงคุณวุฒิภายนอก ท่านได้ให้ความรู้ใหม่เสมอมาและคำแนะนำมากมายที่กลายมาเป็นประเด็นสำคัญในบทสรุป และขอขอบพระคุณอาจารย์ ดร.นัทธี จิตสว่าง อาจารย์ต้นแบบผู้อุทิศตัววางรากฐานอาชญาวิทยาและงานยุติธรรมของจุฬาฯ ให้ก้าวหน้าเติบโตมาอย่างแข็งแกร่งจนทุกวันนี้

ปรเมศวร์ กุมารบุญ

สารบัญ

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union) หรือ ITU เป็นองค์กรชำนัญพิเศษแห่งสหประชาชาติซึ่งมีหน้าที่ในการให้คำแนะนำรัฐต่างๆ ในการกำกับดูแลกิจการสื่อสาร ได้ตีพิมพ์เอกสารทางวิชาการเรื่อง Understanding Cybercrime: Phenomena, Challenge and Legal Response (Development, 2012) ประเด็นที่น่าสนใจกล่าวว่า

"Cybercrime และ Cyber Security เป็นเรื่องที่แยกจากกันคนละประเด็น ในการประชุมสมัชชาใหญ่แห่งสหประชาชาติ พ.ศ.2553 (2010 UN General Assembly) ในเรื่อง Cyber security ได้กำหนดว่า Cybercrime เป็นภัยคุกคามสังคมสำคัญที่ต้องให้ความสนใจอย่างยิ่ง"

ITU Development (Development, 2012) ได้นิยามไว้ว่า Cyber Security เป็นเรื่องสำคัญของการพัฒนาเทคโนโลยีข้อมูลข่าวสาร (Information Technology) ที่เกี่ยวข้องกับบริการอินเทอร์เน็ต ที่จะต้องปกป้องข้อมูลข่าวสารไม่ให้ถูกทำลาย โดยเฉพาะเครือข่ายและข้อมูลข่าวสารของโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญหรือ Critical Information Infrastructures (CII) อาทิ เครือข่ายการสื่อสารของระบบการไฟฟ้า เครือข่ายการสื่อสารของระบบส่งก๊าซธรรมชาติ เครือข่ายโทรคมนาคม เป็นต้น ซึ่งล้วนส่งผลกระทบต่อเศรษฐกิจ และความมั่นคงของชาติ หากการรักษาความปลอดภัยบกพร่อง

ITU Development (Development, 2012) ได้กล่าวถึง Cybercrime ในทำนองว่า เป็นอาชญากรรมทุกรูปแบบที่เกิดจากการใช้ประโยชน์เครือข่ายโทรคมนาคมและเทคโนโลยีสารสนเทศ (ICT Network) ซึ่งเป็นเรื่องวิกฤติสำหรับหน่วยงานสืบสวนสอบสวน และเป็นประเด็นท้าทายในการบังคับใช้กฎหมายในปัจจุบัน

ปัจจุบันอาชญากรรมไซเบอร์เติบโตกว้างขวางไปมาก มิได้เป็นเพียงการขโมยข้อมูล ปลอมแปลงข้อมูล ทำลายข้อมูลหรือเจาะระบบคอมพิวเตอร์ผ่านช่องทางการสื่อสารอินเทอร์เน็ต ที่เรียกว่า Cyber Security เพียงเท่านั้น

ปีเตอร์ ก็อตสชอร์ค (Gottschalk, 2010) ได้อธิบายเพิ่มเติมว่าอาชญากรรมไซเบอร์ยังรวมถึงการนำเทคโนโลยีการสื่อสารไปประกอบอาชญากรรม นำไปใช้ประโยชน์ อาทิ การฉ้อโกง (Ponzi scheme or Fraud) การหลอกลวง (Cyber Scam) อาชญากรรมการเงิน (Financial Crime)

ตลอดจนเป็นเทคโนโลยีการสื่อสารของอาชญากร เครือข่ายการเงินอาชญากร (Criminal Financial via Fintech) การระดมเงินทุนเพื่อการก่อการร้ายด้วยบิตคอยน์ (ISIS bitcoin raised fund) การจ้างสังหารผ่าน Tor Browser (Online hire a Hitman) ตลอดจนเป็นภัยต่อความมั่นคงของชาติจากการสร้างความแตกแยกด้วยเนื้อหาในอินเทอร์เน็ต (Hate crime by Content) เกิดอาชญากรรมแห่งความเกลียดชัง

เอ็ม.อี. คาร์เบย์ (Kabay, 2008) นับจากโลกมีคอมพิวเตอร์ถือกำเนิดขึ้นไม่นานก็มีอาชญากรรมคอมพิวเตอร์ (Computer crime) เกิดขึ้น จากการทำลายเครื่องคอมพิวเตอร์ทางกายภาพและทำลายข้อมูลคอมพิวเตอร์ สังคมเริ่มตระหนักว่าสิ่งเหล่านี้มีมูลค่ามากกว่าความเสียหายในรูปทรัพย์สินทั่วไป แต่ส่งผลเสียหายใหญ่หลวงต่อคนจำนวนมาก และการก้าวหน้าของสังคม จึงค่อยๆ พัฒนาเป็นกฎหมายอาญาต่อมา

เอ็ม.อี. คาร์เบย์ (Kabay, 2008)ได้อ้างถึงอาชญากรรมคอมพิวเตอร์เกิดขึ้นครั้งแรก ในปี ค.ศ. 1969 จากการที่นักศึกษาแคนาดารวมตัวประท้วงศาสตราจารย์ผู้หนึ่งในมหาวิทยาลัยที่กระทำการเหยียดเชื้อชาติ และเมื่อตำรวจมาถึงก็เกิดจลาจลวุ่นวายขึ้น จนเกิดไฟลุกไหม้ห้องคอมพิวเตอร์ของมหาวิทยาลัยถูกทำลายมูลค่าเสียหายราว 2 ล้านดอลลาร์ และนักศึกษาถูกจับ 97 คน

นอกจากนั้น เอ็ม.อี. คาร์เบย์ (M.E.Kabay, 2008) ยังได้อธิบายถึงประวัติศาสตร์อาชญากรรมคอมพิวเตอร์ในยุคแรก คือการทำลายคอมพิวเตอร์ทางกายภาพ ทุบ ทำลาย ถูกยิง ถูกระเบิด ซึ่งเกิดจากอุบัติเหตุบ้าง เกิดจากการก่อวินาศกรรม (Computer sabotages) และการจารกรรมอุตสาหกรรม (Industrial espionage) ในช่วงปี ค.ศ. 1960-1970 ต่อมาเกิดการขโมยข้อมูลเปลี่ยนแปลงข้อมูล บุคคล ธุรกิจ และธนาคาร เช่น ปลอมบัตรเครดิต ปลอมบัญชีธนาคาร เป็นยุคแรกของ Identity Theft และเกิดอาชีพ Dumpster Diver (คนคุ้ยขยะ) ทำหน้าที่ขุดคุ้ยขยะหาข้อมูลใบเสร็จ สำเนาบัตรเครดิต ข้อมูลลูกค้า ข้อมูลธุรกิจ ไปขายต่อให้อาชญากรนำข้อมูลมาปลอมแปลงเพื่อใช้งานเป็นอาชีพที่สร้างรายได้มากในอเมริกา โดยมีอาชญากรวัยรุ่นชื่อดังอย่าง Jerry Neal Schneider เป็นผู้นำ สร้างความเสียหายต่อธุรกิจหลายแห่ง กระทั่งเริ่มมีการเข้าถึงข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุคปี 1980 (ยังไม่มีอินเทอร์เน็ต)

จากนั้นในยุค ค.ศ.1990 การทำลายข้อมูลคอมพิวเตอร์จาก ไวรัส ได้ก่อตัวขึ้นพร้อมกับอินเทอร์เน็ตถือกำเนิดขึ้นจากอาชญากรรมคอมพิวเตอร์ กลายเป็น อาชญากรรมไซเบอร์ (Cybercrime) เมื่อการทำลายอุปกรณ์คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ได้เปลี่ยนช่องทางการทำความเสียหายผ่านอินเทอร์เน็ต และปัจจุบันอาชญากรรมไซเบอร์เติบโตกว้างไกลมากดังจะได้กล่าวต่อไป

ผู้วิจัยเห็นว่าบางครั้งได้ปรากฏเรียก Cyber crime ว่า “อาชญากรรมคอมพิวเตอร์” (Computer Crime) ซึ่ง Cybercrime แตกต่างกับ Computer Crime ที่การเชื่อมต่ออินเทอร์เน็ต ดังที่กล่าวถึงประวัติศาสตร์ข้างต้น ปัจจุบันยังไม่มีที่ใดนิยามเป็นทางการจึงเรียกทับศัพท์ว่า “อาชญากรรมไซเบอร์”

การใช้คำว่า "คอมพิวเตอร์" เป็นความหมายที่แคบกว่าคำว่า ไซเบอร์ (Handbook) เพราะนอกจากคอมพิวเตอร์ (ข้อมูล ชุดคำสั่ง อุปกรณ์อิเล็กทรอนิกส์และหน่วยประมวลผล ตามมาตรา 7 พรบ. คอมฯ) อาชญากรรมไซเบอร์ยังหมายรวมถึงการเข้าถึงโครงข่ายโทรคมนาคม (Telecommunications Network) อุปกรณ์โทรคมนาคม (Telecommunications Equipment) โดยมิชอบ ไปจนถึงเนื้อหา (Contents) ผิดกฎหมายและการนำไซเบอร์เทคโนโลยีไปประกอบอาชญากรรม แลร์รี่ และลาร์ส.อี.แดเนียล (Larry and Lars E. Daniel, 2016) เห็นด้วยว่าอาชญากรรมไซเบอร์เติบโตกว้างขวางไปมากมายหลายมิติในปัจจุบัน กล่าวคือ เป็นอาชญากรรมที่จะเกิดขึ้นไม่ได้ “หากไม่มีการใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่ออินเทอร์เน็ต” และปัจจุบันตำรวจทั่วโลกกำลังเผชิญหน้ากับความท้าทายจากภัยคุกคามในรูปแบบใหม่แห่งศตวรรษที่ 21

แนวทางหลักของกฎหมายในการกำกับดูแลอาชญากรรมไซเบอร์ของไทยนั้น เริ่มแรกได้รับอิทธิพลจาก Convention on Cyber crime โดยสภาแห่งยุโรป (The Council of Europe) และกฎหมายหลายฉบับของสหรัฐอเมริกา อาทิ กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Fraud and Abuse Act 1986) ซึ่งเป็นกฎหมายกำหนดฐานความผิด เช่น การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินขอบเขตที่ได้รับอนุญาต กฎหมาย แคนสแปม (CAN-SPAM Act ย่อมาจาก Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003) เป็นการกำหนดมาตรฐานการห้ามการส่งอีเมลล์ขยะ กฎหมายการขโมยข้อมูลระบุตัวตน และการปลอมตน (Identity Theft and Assumption Deterrence Act) ส่วนในฝั่งอังกฤษ เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) และกฎหมายการคุ้มครองข้อมูล (Data Protection Act) เป็นต้น ซึ่งรากฐานเหล่านี้ก็ได้เกิดเป็น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) ได้ประกาศบังคับใช้เป็นการทั่วไปแล้ว

พ.ร.บ.คอมพิวเตอร์ฯ มิได้เพียงแค่ห้ามกระทำความผิดทางอาญาต่อคอมพิวเตอร์ หากแต่รวมถึงการนำคอมพิวเตอร์ไปก่ออาชญากรรมอีกด้วย โดยเฉพาะเป็นภัยต่อ บุคคล สังคม ระบบเศรษฐกิจ และความมั่นคงของชาติ

ปัจจุบัน พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ได้ผ่านการทบทวนจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และมีการเปิดการรับฟังความคิดเห็นมาแล้วหลายครั้ง โดยมีต้นแบบมาจากกฎหมาย Cybersecurity Act 2018 ของประเทศสิงคโปร์ มุ่งหมายปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แต่ความท้าทายของอาชญากรรมไซเบอร์ในศตวรรษที่ 21 มิใช่เพียงแค่การเจาะระบบ ขโมยข้อมูล แก้ไขข้อมูล ทำลายข้อมูล ที่เรียกว่าความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เท่านั้น แต่กลับเกิดการนำเทคโนโลยีดิจิทัลด้านไซเบอร์มาประกอบอาชญากรรมในเกือบทุกประเภท มีวิวัฒนาการเป็นเทคโนโลยีอาชญากร (Criminal Cyber Technology) และยังเกิดอาชญากรรมประเภทใหม่ๆ (Hybrid crime) อันเป็นผลกระทบจากการมีเทคโนโลยีสมัยใหม่เกิดขึ้น ซึ่งนอกจากทำให้อาชญากรนำไปประกอบอาชญากรรมสำเร็จผลได้ง่าย ยังทำให้การสืบสวนจับกุมเป็นไปได้ยาก ดังปรากฏการณ์อาชญากรรมร่วมสมัยที่เกิดขึ้นหลายรูปแบบในปัจจุบัน

อาชญากรรมหลายประเภทที่เกี่ยวข้องกับการนำนวัตกรรมไซเบอร์ไปประกอบอาชญากรรม โดยเฉพาะนวัตกรรมที่ช่วยปิดบังตัวตนให้พวกเขาหลบพ้นจากการสืบสวนจับกุม ทำให้ผู้วิจัยได้สังเกตพบความสัมพันธ์ที่เชื่อมโยงระหว่างอาชญากรรมกับนวัตกรรมการปิดบังอำพรางตน และความสามารถในการสืบสวนสอบสวนทางดิจิทัล (Digital Detective) มีส่วนสำคัญในการกำหนดการเพิ่มขึ้นหรือลดลงของอัตราการเกิดอาชญากรรม ซึ่งผู้วิจัยเชื่อว่าสามารถนำมาเชื่อมโยงสร้างตัวแบบจำลองเป็น Conceptual Model ในรูปแบบกราฟ และสมการคณิตศาสตร์ ที่สามารถอธิบายให้เข้าใจปรากฏการณ์ที่เกิดอาชญากรรมในสังคมได้

โดยการศึกษาวิจัยในดุษฎีนิพนธ์นี้ มิได้มุ่งศึกษาวิจัยไปที่ปัจจัยที่ก่อให้เกิดอาชญากรรมไซเบอร์ประเภทใดประเภทหนึ่งเท่านั้น แต่ต้องศึกษารวบรวมอาชญากรรมที่ใช้นวัตกรรมหลายประเภทให้มากที่สุดว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมทุกประเภทอย่างไร ประกอบกับการสัมภาษณ์หรือค้นหาบทสัมภาษณ์ของอาชญากรที่เคยใช้นวัตกรรมมาประกอบอาชญากรรม จากข่าว คำพิพากษา บทความ หนังสือ หรือสื่ออื่นๆ ที่เคยเกิดขึ้นจากอดีตจนถึงปัจจุบัน เป็นการศึกษาข้อมูลเชิงคุณภาพ แล้วใช้ทฤษฎีเกมเป็นวิธีการวิจัยกระบวนการตัดสินใจของอาชญากรไซเบอร์กับทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลมาเป็นฐานแนวคิด ให้สามารถมีพลังในการอธิบาย ทำนายอาชญากรรมไซเบอร์ในอนาคตที่จะเกิดขึ้น และอาจจะควบคุมอาชญากรรมไซเบอร์ได้ อันสอดคล้องกับวัตถุประสงค์การวิจัย เป็นข้อเสนอทฤษฎีบทใหม่ในงานวิชาการอาชญาวิทยาต่อไป

1.2 **วัตถุประสงค์ของการวิจัย**

1.2.1 เพื่อศึกษา และรวบรวมรูปแบบการประกอบอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นจากอดีตมาจนถึงปัจจุบัน อันเป็นกรณีศึกษาเกี่ยวข้องกับการไร้ตัวตนมีความสัมพันธ์กับการเกิดอาชญากรรม

1.2.2 เพื่อศึกษาความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตน (Anonymous Factor) อันเป็นเหตุให้รอดพ้นจากการสืบสวนจับกุม (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) กับการตัดสินใจก่ออาชญากรรมไซเบอร์ของอาชญากร

1.2.3 เพื่อสร้างรูปแบบความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์ ด้วยทฤษฎีเกม

1.3 **นิยามศัพท์**

เนื่องจากศัพท์บางคำยังใหม่และยังไม่มีคำนิยามอย่างเป็นทางการ ณ ปัจจุบัน (พ.ศ. 2564) ในดุษฎีนิพนธ์นี้ จึงขอนิยามศัพท์เป็นการเฉพาะเพื่อให้เข้าใจเป็นไปในทิศทางเดียวกันดังนี้

“อาชญากรรมไซเบอร์” (Cybercrime) หมายถึง อาชญากรรมทุกประเภทที่มีกฎหมายบัญญัติโทษเป็นความผิดอาญาไว้และใช้เทคโนโลยีอินเทอร์เน็ตประกอบอาชญากรรม อาทิ

การทำลายระบบคอมพิวเตอร์ ทำลายข้อมูลคอมพิวเตอร์ การขัดขวางการทำงานของระบบคอมพิวเตอร์ของบุคคลหรือองค์กร การเรียกค่าไถ่ข้อมูลหรือระบบคอมพิวเตอร์ การจารกรรมข้อมูลคอมพิวเตอร์ การนำคอมพิวเตอร์กับเทคโนโลยีอินเทอร์เน็ตไปประกอบอาชญากรรม การยึดระบบเทคโนโลยีสารสนเทศโครงสร้างพื้นฐานสาธารณะสำคัญเพื่อก่อวินาศกรรม การก่ออาชญากรรมเศรษฐกิจ การก่ออาชญากรรมการเงิน การฉ้อโกง การละเมิดสิทธิ การขายสินค้าผิดกฎหมายผ่านอินเทอร์เน็ต การฟอกเงิน การหมิ่นประมาท การบิดเบือนข้อมูลข่าวสารหรือข้อมูลเท็จเพื่อทำลายผู้อื่น การโฆษณาชวนเชื่อหรือการหลอกลวงหรือชักจูงหรือโน้มน้าวจูงใจให้เชื่อบางสิ่งหรือให้เสียทรัพย์หรือประโยชน์อื่นใดให้อาชญากรด้วยเทคโนโลยีสารสนเทศผ่านอินเทอร์เน็ต ตลอดจนการทำสงครามจิตวิทยาผ่านอินเทอร์เน็ตเพื่อแย่งชิงมวลชนหรือทำลายความมั่นคงของชาติ เป็นต้น

“การไร้ตัวตน” (Anonymity) หมายถึง องค์ประกอบ 2 ปัจจัยหลัก (Anonymous Factors) ที่ช่วยให้อาชญากรรอดพ้นโทษอาญาได้ คือ

(ก.) การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective)

(ข.) การรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

ขยายความดังนี้ นอกจากเหตุผลทฤษฎีวิชาการทางอาชญาวิทยาอื่นๆ ที่ใช้ในการอธิบายสาเหตุการประกอบอาชญากรรมแล้ว ดุษฎีนิพนธ์นี้ตั้งข้อสันนิษฐานจากการสังเกตปรากฏการณ์ของผู้วิจัยพบว่า

เหตุผลหนึ่ง คะเนว่าการตัดสินใจลงมือก่ออาชญากรรมไซเบอร์อาจเป็นเพราะอาชญากรเชื่อมั่นว่า พวกเขาจะไม่มีวันถูกจับ สามารถหลบพ้นจากการสืบสวนจับกุมทางดิจิทัลได้ จึงกล้าลงมือประกอบอาชญากรรม แต่หากเจ้าหน้าที่สามารถสืบสวนจับกุมได้โดยง่ายหรือหาตัวอาชญากรได้รวดเร็ว อาชญากรจะชั่งน้ำหนักเหตุผลไม่ลงมือก่ออาชญากรรม เช่น หากอาชญากรต้องการลักทรัพย์ย่อมเลือกลักทรัพย์บ้านหลังที่ไม่มีกล้องวงจรปิดหรือหาวิธีทำลายกล้องวงจรปิดเสียก่อน

เหตุผลอีกประการ กล่าวคือ อาชญากรอาจจะยังเชื่อมั่นว่า แม้ถูกจับกุมตัวได้ในที่สุด แต่เจ้าหน้าที่จะไม่สามารถรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีเอาผิดได้ จึงยังคงกล้าตัดสินใจประกอบอาชญากรรม

รูปแบบการก่ออาชญากรรมไซเบอร์แต่ละประเภท จะขึ้นอยู่กับเทคโนโลยีการไร้ตัวตนในแต่ละชนิด และยุคสมัย

กล่าวคือ ในยุคหนึ่งหรือในอดีต เทคโนโลยีประเภทหนึ่งสามารถช่วยอาชญากรปิดบังตัวตนล่องหนหายตัวได้ แต่พอเวลาผ่านไปเทคโนโลยีการสืบสวนจับกุมพัฒนาก้าวหน้าขึ้น จนสามารถสืบสวนจับกุมเทคโนโลยีปิดบังตัวตนเดิมของอาชญากรเดิมนั้นได้ เช่น ในอดีตแก๊งค์คอลเซ็นเตอร์ใช้เทคโนโลยี โทรศัพท์เสียงผ่านอินเทอร์เน็ต (VOIP) ปิดบังอำพรางตัวตนในการก่ออาชญากรรมมาหลายปี แต่ปัจจุบันเทคโนโลยีการสืบสวนจับกุมก้าวหน้า จนอาชญากรรมแก๊งค์คอลเซ็นเตอร์หมดสิ้นไป

ถ้าหากอาชญากรรมไซเบอร์ประเภทใดทำการ สืบสวนจับกุมไม่ได้หรือรวบรวมพยานหลักฐานเพื่อดำเนินคดีไม่ได้ อาชญากรรมไซเบอร์ประเภทนั้นจะเติบโตอย่างรวดเร็ว แต่ถ้าหากเมื่อใดเจ้าหน้าที่ตำรวจสามารถสืบสวนจับกุมอาชญากรรมไซเบอร์ประเภทนั้นได้ และสามารถรวบรวมพยานหลักฐานเพื่อดำเนินคดีได้ครบถ้วน อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงจนหมดสิ้นไป

เดิมที Anonymous หรือ Anonymity หลายบทความใช้ภาษาไทยว่า “นิรนาม” ซึ่งพจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ.2554 ได้ให้ความหมายว่า ไม่รู้ว่าชื่ออะไร

แต่ Anonymous หรือ Anonymity ในความหมายของโลกไซเบอร์ มิได้หมายถึงเพียงการปิดบังเลขหมาย IP Address การปิดบังชื่อจริงหรือนามสกุลเท่านั้น แต่ยังหมายถึงอาชญากรที่ไม่มีตัวตนจริง อย่างเช่น มัลแวร์หรือซอมบี้สมัยใหม่สามารถที่คิดได้เองว่าจะซ่อนตัวอย่างไร และจะโจมตีเหยื่อเมื่อใด เจตนาของอาชญากรจึงขาดตอนตามลักษณะกระบวนการยุติธรรมทางอาญา ที่ต้องหา

องค์ประกอบความผิดทั้งภายนอกและภายใน ตลอดจนล่องหนหายตัวหรือสลายตัวไปได้เอง ผู้วิจัยจึงใช้คำว่า “การไร้ตัวตน”

อย่างไรก็ตามนิยาม “การไร้ตัวตน” ในดุษฎีนิพนธ์นี้มุ่งศึกษาวิจัยเฉพาะเจาะจงไปที่การไร้ตัวตนเพื่อก่อคดีอาชญากรรม มิได้รวมถึงกรณีปิดบังชื่อจริง (นิรนาม) หรือสร้างตัวตนปลอม (Avatar) ที่ไม่ได้กระทำความผิดกฎหมายอาญา อาทิ กลุ่ม Cypherpunk และกลุ่ม Crypto-Anarchy ที่ให้ความสำคัญกับเสรีภาพในโลกออนไลน์ด้วยการปิดบังตัวตนว่าเป็น สิทธิเสรีภาพ และความเท่าเทียม อย่างไรก็ตามหากปิดบังตัวตนไปกระทำการละเมิดสิทธิผู้ใด อันมีบทบัญญัติความผิดอาญาก็จะเข้าสู่อาชญากรรมไซเบอร์ตามนิยามการไร้ตัวตนในดุษฎีนิพนธ์นี้

1.4 ขอบเขตของงานวิจัย

ในการศึกษาวิจัย คำถามวิจัยคือ “การไร้ตัวตน (Anonymity) มีความสัมพันธ์กับการเกิดอาชญากรรมไซเบอร์อย่างไร?” โดยจะทำการศึกษารวบรวมกรณีศึกษาอาชญากรรมไซเบอร์ทั้งในประเทศไทยและต่างประเทศ บทความวิชาการหรือบทความในนิตยสารหรืออินเทอร์เน็ตที่น่าเชื่อถือ บทสัมภาษณ์อาชญากรจากสื่อต่างๆ คำพิพากษา สถิติอาชญากรรมของทางราชการ ผลสำรวจความเห็น และการสัมภาษณ์เชิงลึก ที่เกิดขึ้นในอดีตและปัจจุบัน อันเกี่ยวข้องกับการไร้ตัวตนที่เห็นได้เด่นชัดว่ามีผลต่อการเกิดอาชญากรรมไซเบอร์

จากนั้นนำกรณีศึกษาต่างๆ ดังกล่าวมาวิเคราะห์ผลหาความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ในแต่ละยุคสมัย เมื่อเทคโนโลยีช่วยให้รอดพ้นการสืบสวนจับกุม (Digital Detective) และเจ้าหน้าที่ไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เอาผิดอาญาได้ จะส่งผลต่ออัตราการเพิ่มขึ้นหรือลดลงของการเกิดอาชญากรรมไซเบอร์ในแต่ละประเภทอย่างไร และจะควบคุมการเกิดอาชญากรรมไซเบอร์ในสังคมอย่างไร เมื่อมีเทคโนโลยีไซเบอร์ใหม่เกิดขึ้นในสังคม โดยใช้ทฤษฎีเกม และทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลเป็นเครื่องมือในการวิเคราะห์ความสัมพันธ์ระหว่างกระบวนการตัดสินใจของอาชญากรประกอบอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน โดยใช้เวลาในการศึกษาวิจัยไม่น้อยกว่า 1 ปี

1.5 ประโยชน์ที่จะได้รับจากการวิจัย

นักวิจัยทางอาชญาวิทยาได้พยายามศึกษาวิธีวิจัยกระบวนทัศน์ทางเลือกแบบใหม่อยู่เสมอ และผู้วิจัยได้พบว่า ทฤษฎีเกม (Game theory) ที่ใช้วิจัยพฤติกรรมมนุษย์ในวิชาเศรษฐศาสตร์สามารถนำมาใช้กับงานวิจัยทางอาชญาวิทยาได้อย่างดี เมื่ออาชญากรเลือกอย่างเป็นเหตุเป็นผล (Rational) คือ หาประโยชน์ให้ตนมากที่สุด บนความเสียประโยชน์ของผู้อื่น

ผู้วิจัยจึงนำ ทฤษฎีเกม มาเป็นเครื่องมือบุกเบิกงานวิจัยทางอาชญาวิทยาในดุษฎีนิพนธ์นี้ และได้ผลที่น่าพอใจอย่างดี ซึ่งทฤษฎีเกมสามารถใช้ได้ทั้งการวิจัยเชิงปริมาณในการหาความน่าจะเป็นเพื่อประกอบการตัดสินใจหรือในการวิจัยเชิงคุณภาพให้เห็นรูปแบบการตัดสินใจ แม้ในกรณีการวิจัยที่ไม่มีข้อมูลทางสถิติเพียงพอในการวิเคราะห์ ก็สามารถใช้ทฤษฎีเกมพิสูจน์สมมติฐานทางการวิจัยได้ การศึกษาวิจัยในดุษฎีนิพนธ์นี้ จึงนับประโยชน์ที่จะได้รับจากการวิจัยดังนี้

1.5.1 ได้ประโยชน์จากผลการศึกษารวบรวมกรณีศึกษารูปแบบการประกอบอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นจากอดีตมาจนถึงปัจจุบัน และช่วยให้สามารถคาดการณ์อนาคตได้

1.5.2 ได้ผลการศึกษาความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตน (Anonymous Factor) กับอาชญากรรมไซเบอร์ โดยใช้ทฤษฎีเกมวิเคราะห์การเลือกอย่างเป็นเหตุเป็นผลในการตัดสินใจประกอบอาชญากรรมไซเบอร์ของอาชญากร

1.5.3 ได้แนวทางหรือมาตรการในการ แก้ไข ป้องกัน และปราบปรามอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นในรูปแบบต่างๆ ด้วยการสร้างความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) และการเกิดอาชญากรรมไซเบอร์ เป็นแบบจำลองความคิด (Conceptual Model) ในรูปแบบความสัมพันธ์อย่าง กราฟ และสมการคณิตศาสตร์ เพื่อบรรยายว่ามีความสัมพันธ์กันอย่างไรอันส่งผลต่ออัตราการเพิ่มขึ้นหรือลดลงของการเกิดอาชญากรรมไซเบอร์ และจะได้ข้อเสนอแนะทางวิชาการทางอาชญาวิทยาใหม่ ซึ่งอาจจะสามารถนำมาใช้อธิบายอาชญากรรมไซเบอร์ในสังคมปัจจุบันสามารถทำนายอนาคต และควบคุมปรากฏการณ์อาชญากรรมไซเบอร์ในอนาคตได้

บทที่ 2

ทบทวนวรรณกรรม

ดุษฎีนิพนธ์นี้ ต้องอาศัยความรู้หลายแขนงทั้ง อาชญาวิทยา วิศวกรรมศาสตร์ นิติศาสตร์ การรวบรวมพยานหลักฐานดิจิทัล ปรัชญาการวิจัย และทฤษฎีทางสังคมวิทยา โดยจำเป็นต้องทบทวนวรรณกรรมที่เกี่ยวข้อง ดังต่อไปนี้

2.1 **อาชญากรรมคอมพิวเตอร์** (Computer crime)

นับแต่อดีตที่มนุษย์พยายามสร้างเครื่องจักรในการคำนวณ (Computer) หรือคอมพิวเตอร์ ก็ได้เกิดวิธีการที่พยายามจะปกป้องรักษาอุปกรณ์คอมพิวเตอร์ และสร้างความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ (Information Security) ให้พ้นภัยจากความพยายามทำลายข้อมูลหรือเพื่อปกปิดความลับข้อมูล อันเป็นการกระทำที่เรียกว่าการก่อ อาชญากรรมคอมพิวเตอร์ (Computer crime)

เทรซี่ ลินเดอแมน (Lindeman, 2014) อาชญากรรมคอมพิวเตอร์ (Computer crime) ครั้งแรกเกิดขึ้นในปี ค.ศ. 1969 นักศึกษามหาวิทยาลัย Sir George Williams แคนาดา รวมตัวประท้วงในอาคารมหาวิทยาลัย 14 วัน จากกรณีที่ศาสตราจารย์ผู้หนึ่งในมหาวิทยาลัยทำการเหยียดเชื้อชาติและให้เกรดลำเอียง

รูปที่ 1 บัตรเจาะรูข้อมูลสำหรับประมวลผล (Punched card) ถูกโปรยออกมาทางหน้าต่าง

ที่มา Tracey Lindeman, CBC News[1]

[1] Tracey Lindeman (2014). A look back at Montreal's race-related 1969 Computer Riot Social Sharing. CBC News · Posted: Feb 15, 2014. Available from URL : https://www.cbc.ca/news/canada/montreal/a-look-back-at-montreal-s-race-related-1969-computer-riot-1.2538765

วันที่ 10 กุมภาพันธ์ ค.ศ.1969 นักศึกษาราว 200 คนได้ยึดศูนย์คอมพิวเตอร์ของมหาวิทยาลัยชั้น 9 อาคาร Hall building เป็นที่ตั้งใหม่ การเจรจาต่อรองระหว่างนักศึกษาและผู้บริหารมหาวิทยาลัยดำเนินไป 11 ชั่วโมงนักศึกษาร้อยกว่าคนยอมออกมาจากศูนย์คอมพิวเตอร์ แต่อีกจำนวนหนึ่งยังคงปักหลักอยู่ที่นั่น ล่วงเข้าสู่วันที่ 11 กุมภาพันธ์ ค.ศ.1969 เกิดไฟลุกไหม้ศูนย์คอมพิวเตอร์ของมหาวิทยาลัยในชั้น 9 ชั้น อาคาร Hall building และบัตรเจาะรูข้อมูลสำหรับประมวลผล (Punched card) จำนวนมากถูกโปรยออกมาทางหน้าต่าง

ในที่สุดเมื่อตำรวจมาถึงจึงบุกเข้าไปควบคุมตัวนักศึกษาทั้งหมด มูลค่าความเสียหายของคอมพิวเตอร์ราว 2 ล้านดอลลาร์ และนักศึกษาถูกจับ 97 คน

รูปที่ 2 ศูนย์คอมพิวเตอร์ของมหาวิทยาลัย Sir George Williams ถูกเผา

ที่มา Tracey Lindeman, CBC News[2]

โธมัส ไวต์ไซด์ (Whiteside, 1978) ได้ย่อเหตุการณ์ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์ในยุคแรกในช่วงต้น ค.ศ. 1970s คือการทำลายคอมพิวเตอร์ทางกายภาพ (physical attacks on computer) ถูกทุบ ถูกทำลาย ถูกยิง ถูกระเบิด ซึ่งเกิดจากอุบัติเหตุ การจลาจล การประท้วง การก่อวินาศกรรม (Computer sabotages) การจารกรรมอุตสาหกรรม (Industrial espionage) เกิดขึ้นหลายแห่งทั้งใน สหรัฐอเมริกา อิตาลี ออสเตรเลีย แอฟริกาใต้ โดยเฉพาะมหาวิทยาลัยหลายแห่งในสหรัฐอเมริกา เกิดการรวมตัวประท้วงของนักศึกษาต่อต้านสงครามเวียดนาม และเมื่อการประท้วง

[2] Tracey Lindeman (2014). A look back at Montreal's race-related 1969 Computer Riot Social Sharing. CBC News · Posted: Feb 15, 2014. Available from URL : https://www.cbc.ca/news/canada/montreal/a-look-back-at-montreal-s-race-related-1969-computer-riot-1.2538765

เกิดความรุนแรงขึ้น ผลกระทบนอกจากความเสียหายต่ออาคารเรียน ยังรวมถึงระบบคอมพิวเตอร์ของมหาวิทยาลัย ดังตัวอย่างเช่น

ค.ศ. 1970 มหาวิทยาลัยแห่งวิสคอนซิน เกิดการประท้วงของนักศึกษาและมีการวางระเบิดเกิดขึ้นมีผู้เสียชีวิตและบาดเจ็บรวมทั้งระบบคอมพิวเตอร์เสียหายเป็นมูลค่า $16 millions

ค.ศ. 1970 วิทยาลัย Fresno State เกิดการชุมนุมประท้วง และปาระเบิดขวด (Molotov cocktail) ทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์เป็นมูลค่า $1 million

ค.ศ. 1970 มหาวิทยาลัยนิวยอร์ก นักศึกษากลุ่มหนึ่งวางระเบิดระบบคอมพิวเตอร์ของศูนย์ Atomic Energy Commission เพื่อปลดปล่อย Black Panther ให้พ้นโทษ

ค.ศ. 1972 เมืองโจฮันเนสเบิร์ก แอฟริกาใต้ ระบบคอมพิวเตอร์ของเทศบาลเมืองถูกยิงด้วยกระสุน 4 นัดทะลุกระจกหน้าต่างอาคารเข้ามา

ค.ศ. 1973 เมลเบิร์น ออสเตรเลีย ผู้ประท้วงต่อต้านสงคราม ใช้ปืนลูกซองแฝดยิงใส่ร้านคอมพิวเตอร์ของชาวอเมริกัน

ค.ศ. 1974 ฐานทัพอากาศ Wright Patterson Air Force Base มีการลักลอบพยายามก่อวินาศกรรมคอมพิวเตอร์ 4 ครั้ง

ค.ศ. 1977 กรุงโรม ผู้ก่อการร้าย 4 ราย เทน้ำมันเชื้อเพลิงราดบนคอมพิวเตอร์ในมหาวิทยาลัย และจุดไฟเผาจนกลายเป็นเถ้าถ่าน

ค.ศ. 1978 ฐานทัพอากาศ Vandenburg ในแคลิฟอร์เนีย ถูกนักเคลื่อนไหวเพื่อสันติภาพทำลาย เครื่องคอมพิวเตอร์ IBM 3031 ที่ยังไม่ได้ใช้ด้วยค้อน ชะแลง เครื่องตัดสายไฟ และสว่านไร้เพื่อต่อต้านระบบนำร่องดาวเทียม NAVSTAR

สังคมจึงได้เริ่มตระหนักถึงผลร้ายจากทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ว่าสิ่งเหล่านี้มีมูลค่ามากกว่าความเสียหายในรูปทรัพย์สิน และส่งผลกระทบเกิดความเสียหายใหญ่หลวงต่อคนจำนวนมาก จึงค่อยๆ พัฒนาเป็นกฎหมายอาญาต่อมา และถือเป็นการก่ออาชญากรรมประเภทหนึ่ง

ในปี ค.ศ.1970 รัฐ Hesse ในเยอรมนี ได้ออกฎหมายคุ้มครองเฉพาะคอมพิวเตอร์ขึ้นเป็นฉบับแรกของโลก ซึ่งบทบัญญัติมีลักษณะเป็นแนวทางการคุ้มครองข้อมูล (Data Protection Act, 1970)

ในปี ค.ศ. 1970-1972 เกิดความโกลาหลจาก คอมพิวเตอร์เมนเฟรม (Main frame computer) ยี่ห้อ Burroughs รุ่น B3500 ของ National Farmers Union Service Corporation แห่ง เดนเวอร์ เหตุที่หัวอ่านข้อมูลดิสก์คอมพิวเตอร์เกิดความเสียหายถึง 56 ครั้งใน 2 ปี

รูปที่ 3 คอมพิวเตอร์เมนเฟรม (Main frame computer) ยี่ห้อ Burroughs รุ่น B3500

ที่มา Computer history museum[3]

ผู้เชี่ยวชาญของ Burroughs บินมาจากทั่วสหรัฐ อเมริกา ช่วยกันค้นคว้าหาสาเหตุ แต่ก็ไม่พบ ทางบริษัทได้เปลี่ยนอุปกรณ์ให้ใหม่ เดินสายไฟใหม่ ติดตั้ง motor generators ใหม่ ติดตั้ง circuit breakers ใหม่ทั้งหมด รวมถึงสายไฟของจอคอมพิวเตอร์ด้วย รวมค่าจ่ายทั้งหมดราว $500,000 ยังไม่รวมค่าเสียหายจากธุรกิจที่คอมพิวเตอร์ไม่สามารถทำงานได้

ผู้เชี่ยวชาญตั้งข้อสงสัยว่า อาจจะเกิดจากการลักลอบก่อวินาศกรรม เพราะในยุคนั้นเกิดเหตุการณ์ทำนองนี้บ่อย แต่ศูนย์คอมพิวเตอร์ดังกล่าวมีชายสูงอายุชื่อ อัลเบิร์ต เป็นคนเฝ้าในช่วงกลางคืนตลอด และ อัลเบิร์ต เป็นคนนิสัยดีคอยเสริฟกาแฟ และโดนัท ให้ทีมช่างตลอด และเขาเป็นคนแก้ปัญหาเบื้องต้นเมื่อคอมพิวเตอร์ประสบปัญหาทุกครั้ง แต่คอมพิวเตอร์เกิดการทำงานล้มเหลวเฉพาะช่วงเวลากลางคืน และเป็นตอนที่ อัลเบิร์ต เข้าทำงานตลอด

ผู้บริหารศูนย์คอมพิวเตอร์จึงติดตั้งกล้องวงจรปิด โดยไม่บอกให้อัลเบิร์ตทราบ และในที่สุดคืนหนึ่ง ศูนย์คอมพิวเตอร์เกิดการทำงานล้มเหลว กล้องวงจรปิดจับภาพได้ว่า อัลเบิร์ต เป็นคนเปิดตู้เก็บดิสก์ แล้วเขาเอากุญแจรถกระแทกลงไปที่หัวอ่านดิสก์ และนั่นคือสาเหตุที่หัวอ่านข้อมูลดิสก์คอมพิวเตอร์เกิดความเสียหายเป็นครั้งที่ 57

ได้มีการสืบสวนทางจิตวิทยา (Psychological investigation) เพื่อหาเหตุผลของการก่ออาชญากรรมของอัลเบิร์ตพบว่า เขาอยู่เวรในกะกลางคืนมาเป็นปีโดยไม่ได้พบปะกับใครในบริษัทเลย เขาเข้างานตอนที่ทุกคนกลับหมดแล้วและเขาอยู่คนเดียวตลอดมาโดยปราศจากการปฏิสัมพันธ์กับมนุษย์

[3] Available from URL : https://www.computerhistory.org/revolution/digital-logic/12/278/1444

เมื่อคอมพิวเตอร์เกิดความเสียหายครั้งแรก เขาตื่นเต้นมากที่ได้ต้อนรับการมายืนของทีมช่างซ่อม เขารู้สึกมีประโยชน์ มีคุณค่า เวลาเล่าให้ทีมช่างฟังว่าเกิดอะไรขึ้นบ้าง และเมื่อเขาต้องการเพื่อนหัวอ่านข้อมูลดิสก์คอมพิวเตอร์จะเกิดความเสียหายอีกครั้ง แต่นั่นไม่ใช่เพื่อการก่อวินาศกรรม

ยุคปี ค.ศ.1980 คอมพิวเตอร์ถูกใช้แพร่หลายมากขึ้น และเริ่มมีคอมพิวเตอร์ส่วนบุคคล (Personal computer) ออกวางจำหน่ายในท้องตลาด แม้ยังไม่มีอินเทอร์เน็ต แต่ระบบโทรศัพท์เติบโตกว้างขวางขึ้นมาก

เอ็ม.อี. คาเบย์ (M.E.Kabay, 2008) ยุคต่อมาเกิดการขโมยข้อมูล เปลี่ยนแปลงข้อมูลของบุคคล ธุรกิจ และธนาคาร เช่น ปลอมบัตรเครดิต ปลอมบัญชีธนาคาร เป็นยุคแรกของอาชญากรรมประเภท Identity Theft และเกิดอาชีพ Dumpster Diver (คนคุ้ยขยะ) ทำหน้าที่ขุดคุ้ยขยะหาข้อมูลใบเสร็จ สำเนาบัตรเครดิต ข้อมูลลูกค้า ข้อมูลธุรกิจ ไปขายต่อ เพื่อที่อาชญากรจะได้นำข้อมูลมาปลอมแปลงเพื่อใช้งาน เป็นอาชีพที่สร้างรายได้มากในอเมริกา โดยมีอาชญากรวัยรุ่นชื่อดังอย่าง Jerry Neal Schneider เป็นผู้นำ สร้างความเสียหายต่อธุรกิจหลายแห่ง กระทั่งเริ่มมีการเข้าถึงข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุคปี 1980

เอ็ม.อี. คาเบย์ (M.E.Kabay, 2008) ราวปี ค.ศ. 1986 โปรแกรมไวรัสที่มีเป้าหมายในการทำลายล้าง หรือเพื่อก่อวินาศกรรม (Sabotage) ตัวแรกถูกเขียนขึ้นในชื่อ “Pakistani Brain” ลักษณะการประกอบอาชญากรรมคือเขียนโปรแกรมขึ้นเพียงครั้งเดียว แต่สามารถส่งต่อ เผยแพร่สร้างความเสียหายให้เหยื่อได้จำนวนมาก โดยการทำลายนี้มีผลต่อ Bootsektor อันเป็นส่วนประกอบสำคัญของเครื่องคอมพิวเตอร์

อย่างไรก็ตาม โปรแกรมไวรัสมีจำนวนมากและหลากหลายชนิด ถูกเขียนขึ้นมาก่อนหน้าไวรัส “Pakistani Brain” ก็มี เพียงแต่ยังไม่ได้ถูกนำมาใช้เพื่อเป้าหมายในการโจมตีเหยื่อหรือก่อวินาศกรรม โดยไวรัสตัวแรก เป็นผลงานปริญญาเอกของ Fred Cohen เมื่อปี ค.ศ. 1983

ค.ศ. 1988 โปรแกรมวอร์ม (Worm) ที่โด่งดังเกิดขึ้นชื่อ “INTERNET-Worm” หลังจากมีการเผยแพร่โปรแกรมเพียงไม่กี่วัน สามารถทำลายเครื่องคอมพิวเตอร์ไปกว่า 6,000 เครื่อง

ค.ศ. 1990 ก้าวเข้าสู่ยุคกำเนิดอินเทอร์เน็ต การทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ด้วยไวรัส ผ่านโครงข่ายอินเทอร์เน็ตได้ก่อตัวขึ้น จากอาชญากรรมคอมพิวเตอร์ กลายเป็น อาชญากรรมไซเบอร์ (Cybercrime) เมื่อการทำลายอุปกรณ์คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ จากคอมพิวเตอร์ Stand alone ได้เปลี่ยนช่องทางการทำลายผ่านเครือข่ายอินเทอร์เน็ตขยายอำนาจสร้างความเสียหายในวงกว้างขึ้น

2.2 อาชญากรรมไซเบอร์ (Cyber Crime)

ปัจจุบันอาชญากรรมไซเบอร์เติบโตกว้างขวางไปมาก นอกจากการ ขโมยข้อมูล ปลอมแปลงข้อมูล ทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ผ่านช่องทางการสื่อสารอินเทอร์เน็ต ที่เรียกว่า Cyber Security ยังรวมถึงการนำเทคโนโลยีการสื่อสารไปประกอบอาชญากรรม กลายเป็นเทคโนโลยีอาชญากร (Criminal Cyber Technology) การฉ้อโกง การหลอกลวง การสร้างความแตกแยกด้วยอาชญากรรมแห่งความเกลียดชังจากเนื้อหาในอินเทอร์เน็ต ไปจนสร้างภัยต่อความมั่นคงของชาติต่างๆ

ซึ่งนอกจากทำให้อาชญากร นำไปประกอบอาชญากรรมสำเร็จผลได้ง่าย ยังทำให้การสืบสวนจับกุมเป็นไปได้ยาก ดังปรากฏการณ์อาชญากรรมร่วมสมัยที่เกิดขึ้นหลายรูปแบบในปัจจุบัน รัฐบาลทั่วโลกกำลังเผชิญหน้ากับความท้าทายจากภัยคุกคามรูปแบบใหม่ในศตวรรษที่ 21

Cyber crime หรือ “อาชญากรรมไซเบอร์” ผู้วิจัยยังไม่พบที่ใดให้นิยามไว้เป็นทางการชัดเจน จึงได้นิยามไว้ในบทที่ 1 ข้อ 1.3 และขอเรียกว่า “อาชญากรรมไซเบอร์” ในบางครั้งได้ปรากฏเห็นเรียก Cyber crime ว่า “อาชญากรรมคอมพิวเตอร์” ซึ่งผู้วิจัยเห็นว่า Cyber crime นั้น แตกต่างกับ Computer Crime ตรงการเชื่อมต่ออินเทอร์เน็ต ดังที่กล่าวถึงประวัติศาสตร์ข้างต้น

นอกจากนั้นการใช้คำว่า "คอมพิวเตอร์" เป็นความหมายที่แคบกว่าคำว่า Cyber เพราะนอกจากคอมพิวเตอร์ (ข้อมูล ชุดคำสั่ง อุปกรณ์อิเล็กทรอนิกส์ และหน่วยประมวลผล ตามนิยามในมาตรา 7 พรบ. คอมฯ) แล้ว อาชญากรรมไซเบอร์ยังหมายรวมถึงการเจาะเข้าถึงโครงข่ายโทรคมนาคม (Telecommunications Network) อุปกรณ์โทรคมนาคม (Telecommunications Equipment) ไปจนถึงเนื้อหา (Contents) และการนำเทคโนโลยีการสื่อสารผ่านอินเทอร์เน็ตไปประกอบอาชญากรรม

อาชญากรรมไซเบอร์เติบโตกว้างขวางไปมากมายในหลายมิติในปัจจุบัน กล่าวคือ เป็นอาชญากรรมที่จะเกิดขึ้นไม่ได้ “หากไม่มีการใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่ออินเทอร์เน็ต” ดังที่จะอธิบายเพิ่มเติมต่อไป

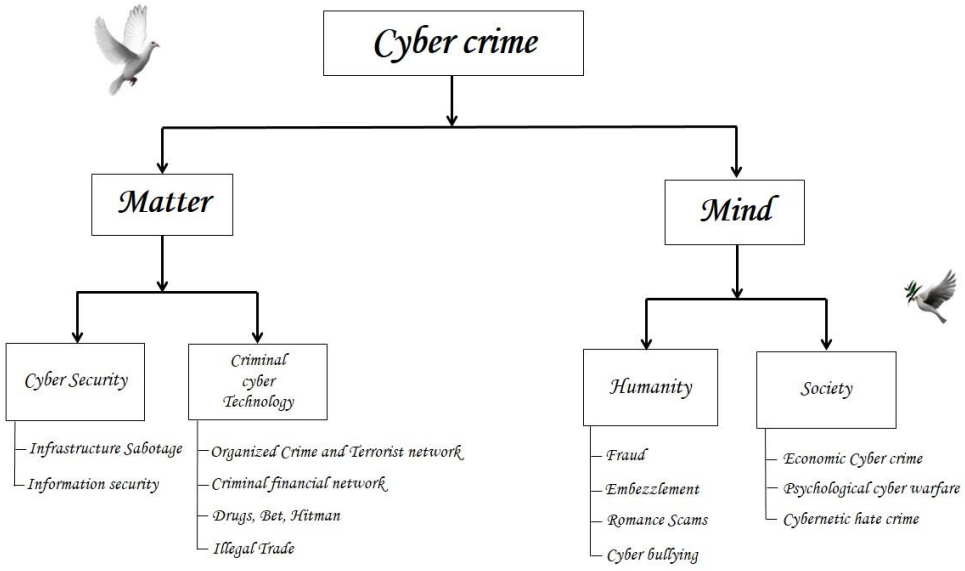
แนวทางหลักในการกำกับดูแลอาชญากรรมไซเบอร์ของไทยนั้น ได้รับอิทธิพลมาจาก Convention on Cyber crime โดยสภาแห่งยุโรป (The Council of Europe) และกฎหมายหลายฉบับของสหรัฐอเมริกา เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Fraud and Abuse Act 1986) ซึ่งเป็น กฎหมายกำหนดฐานความผิด เช่น การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินขอบเขตที่ได้รับอนุญาต กฎหมาย แคนสแปม (CAN-SPAM Act ย่อมาจาก Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003) เป็นการกำหนดมาตรฐานการห้ามการส่งอีเมล์ขยะ กฎหมายการขโมยข้อมูลระบุตัวตน และการปลอมตน

(Identity Theft and Assumption Deterrence Act) ส่วนในฝั่งอังกฤษ เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) และกฎหมายการคุ้มครองข้อมูล (Data Protection Act) เป็นต้น

ซึ่งรากฐานเหล่านี้ก็ได้เกิดเป็น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) ได้ประกาศบังคับใช้เป็นการทั่วไปแล้ว

พรบ.คอมพิวเตอร์ฯ มิได้เพียงแค่ห้ามกระทำความผิดทางอาญาต่อคอมพิวเตอร์ และหากแต่รวมถึงการนำคอมพิวเตอร์ไปก่ออาชญากรรมด้วย โดยเฉพาะเป็นภัยต่อความมั่นคงของชาติและระบบเศรษฐกิจ

ผู้วิจัยได้ริเริ่มต้นจัดหมวดหมู่การศึกษาอาชญากรรมไซเบอร์ ตามปรัชญาการวิจัยในมิติทางภววิทยา (Ontology) ที่แตกต่างกัน เพื่อที่จะเข้าไปถึงความรู้หรือความจริง ที่เป็นอัตวิสัย (Subjective) หรือ ภววิสัย (Objective) และ ญาณวิทยา (Epistemology) ที่แตกต่างกัน เพื่อที่จะเลือกใช้วิธีวิทยาที่มีเครื่องมือในการวิจัยแตกต่างกัน โดยจัดหมวดหมู่ดังนี้



รูปที่ 4 การจัดหมวดหมู่อาชญากรรมไซเบอร์ของผู้วิจัย

จากรูปที่ 4 ได้แยกอาชญากรรมไซเบอร์แบ่งไว้เป็น 2 หลักใหญ่ คือ การก่ออาชญากรรมไซเบอร์ที่จับต้องได้เป็นการกระทำทาง วัตถุ (Matter) และ การก่ออาชญากรรมไซเบอร์ที่จับต้องไม่ได้เป็นการกระทำต่อ จิตใจ (Mind) โดยอธิบายเพิ่มดังนี้

2.2.1 การก่ออาชญากรรมไซเบอร์ที่จับต้องได้เป็นการกระทำทางวัตถุ (Matter)

การก่ออาชญากรรมที่กระทำต่อ วัตถุ (Matter) หรือ ภววิสัย (Objective) โดยใช้วิธีการวิจัยแบบวิทยาศาสตร์หรือวิศวกรรมศาสตร์ในการเข้าถึงความรู้หรือความจริง ตัวอย่างเช่น

2.2.1.1 ***ความมั่นคงปลอดภัยทางไซเบอร์*** **(Cyber Security)**

การก่ออาชญากรรมต่อความมั่นคงปลอดภัยทางไซเบอร์ เป็นการทำลายข้อมูล แก้ไขข้อมูล ทำลายระบบ ถอดรหัส ไปจนถึงการโจมตีระบบการสื่อสารของโครงสร้างพื้นฐานบริการสาธารณะ (Critical Infrastructure) เพื่อการก่อวินาศกรรม (Sabotage)

สหภาพโทรคมนาคมระหว่างประเทศ (ITU Development, 2012, น.13) โปรแกรมทำลายระบบคอมพิวเตอร์ให้เสียหายที่แอบแฝงมาเป็นไฟล์ (Computer Program File) ที่ได้รับมาจากอีเมล์หรือจากเว็บไซต์ ที่เรียกว่า Malware (มัลแวร์) ย่อมาจากคำว่า Malicious Software ซึ่งเป็นไฟล์ ที่เป็นอันตรายต่อคอมพิวเตอร์ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล Malware แบ่งออกได้หลากหลายประเภท อาทิ

Virus คือ โปรแกรมทำลายข้อมูลและระบบคอมพิวเตอร์

Worm คือ โปรแกรมไวรัสที่เคลื่อนที่ไปในระบบเครือข่ายได้เอง

Trojan horse คือ โปรแกรมที่แอบทำงานแบบลับๆ ด้วยการเปิดให้มีการบุกรุกเข้าสู่ระบบ

Spyware คือ โปรแกรมที่แอบทำงานแบบลับ ๆ เพื่อดักจับข้อมูล

Logic Bomb คือ โปรแกรมที่ทำงานตามเหตุการณ์ที่กำหนดไว้

Botnet คือ โปรแกรมขนาดเล็กที่ฝังตัวโดยเจ้าของเครื่องไม่รู้ตัว อาชญากรจะสั่งคอมพิวเตอร์ที่มี BOT อยู่ โจมตีเครื่องแม่ข่ายเพื่อสร้างความเสียหายให้แก่ระบบและองค์กร

Malware คือ โปรแกรมที่ติดเชื้อมาในเครื่องคอมพิวเตอร์ของเหยื่อ

Brute Force Attack คือ การเดารหัสผ่านของเหยื่อเป้าหมาย ซึ่งเหยื่อก็มักใช้ชื่อจริง ชื่อเล่น วันเดือนปีเกิด มาใช้งาน

Spoofing คือ เทคนิคการเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ระยะไกลโดยการปลอมแปลงที่อยู่อินเตอร์เน็ต หรือ IP Address ของเหยื่อที่เข้าถึงได้ง่าย และลักลอบเข้าไปในคอมพิวเตอร์นั้น

Sniffer คือ โปรแกรมที่ถูกสร้างขึ้นเพื่อใช้ดักจับข้อมูลที่ส่งผ่านระบบเครือข่ายคอมพิวเตอร์ ทำให้ทราบรหัสผ่าน (Password) ของบุคคลอื่นที่ส่งผ่านระบบเครือข่ายนั้น

Modification คือ การเปลี่ยนแปลงข้อมูล อาชญากรอาจอยู่ใน ISP ซึ่งสามารถตรวจจับแพ็กเก็ตข้อมูลที่รับส่งในเครือข่ายนั้นได้ โดยอ่านข้อมูลจากผู้ส่งแล้วแก้ไขข้อมูลก่อนส่งไปยังผู้รับ ทำให้ได้ข้อมูลที่ผิดพลาด

Ransomware คือ Malware ที่แตกต่างกับ Malware ประเภทอื่น คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของคนอื่น แต่จะทำการบล็อกไฟล์ผู้อื่นไม่ให้ใช้งานได้ ไม่ว่าจะเป็นไฟล์ เอกสาร ภาพ วิดีโอ แล้วอาชญากรก็จะส่งข้อความมา “เรียกค่าไถ่” โดยโอนเงินผ่านทาง อินเทอร์เน็ต ด้วย Crypto currency หรือ Bitcoin เป็นต้น แล้วอาชญากรจะส่งรหัสในการปลดล็อกการบล็อคไฟล์คืนมา แต่อย่างไรก็ตามเมื่อโอนเงินแล้วก็ไม่ได้หมายความว่าอาชญากรจะส่งรหัสการกู้คืนไฟล์กลับมาให้เพราะ ไม่มีสัจจะในหมู่โจร

Denial of service คือ การปฏิเสธการให้บริการ โดย Server ถูกโจมตีจากหลายวิธีหรือถูกโจมตีจากข้อมูลขยะที่ส่งมาเป็นแพ็กเก็ตจำนวนมากทำให้ระบบล่มเพราะการจราจรหนาแน่น

Delay คือ การหน่วงเวลา เมื่ออาชญากรสามารถควบคุมระบบบางส่วนได้ เช่น ควบคุม server สำรองได้ และสามารถหน่วงเวลาการใช้งาน server หลักให้ทำงานช้ามาก จนในที่สุดก็ต้องเข้ามาใช้ server สำรอง

Hivenets คือ การฝังตัวแทน Botnet และแบ่งปันข้อมูลระหว่างกันและเรียนรู้แบบ self-learning มีปัญญาประดิษฐ์หรือ AI ที่จะสร้าง malware ใหม่ตลอดเวลาเพื่อโจมตีโครงสร้างพื้นฐานบริการสาธารณะเรียกว่า Next-gen Morphic malware เพื่อการก่อวินาศกรรม (Sabotage)

2.2.1.2 *เทคโนโลยีไซเบอร์ที่อาชญากรใช้ประกอบอาชญากรรม* *(***Criminal Cyber Technology)**

เป็นการนำนวัตกรรมเทคโนโลยีการสื่อสารเพื่อนำไปประกอบอาชญากรรมประเภทต่างๆ ซึ่งมิใช่เทคโนโลยีที่มีฐานความผิดนอกเหนือไปจากการ แก้ไขข้อมูล ดักรับ ทำลายระบบถอดรหัสคอมพิวเตอร์ อันเกี่ยวกับ พรบ.คอมพิวเตอร์ฯ และก่อวินาศกรรมโครงสร้างสาธารณะสำคัญด้วยระบบสารเทศของตาม พรบ.ความมั่นคงปลอดภัยไซเบอร์ฯ เท่านั้น อาทิ

Darkweb and Crypto currency คือ การใช้เครือข่าย Tor network ปิดบังอำพรางตัวตนของเว็บไซต์ และผู้เข้าใช้บริการ ด้วยการใช้เงินเสมือนเพื่อการค้ายาเสพติด สินค้าผิดกฎหมาย การจ้างสังหาร

Digital Financial Crime คือ การใช้เทคโนโลยีไซเบอร์เคลื่อนย้ายเส้นทางการเงินก่อการร้าย องค์กรอาชญากรรมข้ามชาติ และการฟอกเงินผิดกฎหมาย

Virtual private network คือ การปิดบังอำพราง IP Address ของอาชญากรเพื่อก่ออาชญากรรมไซเบอร์ โดยหมายเลข IP Address ของอาชญากรจะถูกซ่อนไว้ในเครือข่าย แต่เลขหมายที่ปรากฏสู่สาธารณะจะซ่อนเลขอื่น

Avatar หรือ Fake account คือ การสร้างบัญชี Social media ปลอมเพื่อปิดบังอำพรางตัวตนเพื่อก่ออาชญากรรมฉ้อโกงออนไลน์หรือหลอกลวงเพื่อค้ามนุษย์

VoIP หรือ Fake ID คือ การใช้เทคโนโลยีไซเบอร์เพื่อการสนทนาของแก๊งค์ คอลเซ็นเตอร์

Drone spy and killer คือ การใช้นวัตกรรมโดรน ร่วมกับไซเบอร์เทคโนโลยีเดินทางตาม Target location เพื่อสอดแนม และสังหารเหยื่อเป้าหมาย โดยมีปัญญาประดิษฐ์ (Fairclough) ค้นหาเส้นทางอัตโนมัติ และมี Face recognition เพื่อค้นหาเหยื่อ เรียกว่า

Lethal autonomous weapon (Cohen, E., & Felson) คือ การใช้นวัตกรรมการรบ อาทิเช่น รถถัง อากาศยานไร้คนขับ เรือดำน้ำ (ที่อาจจะไม่ปรากฏสัญชาติ) ร่วมกับไซเบอร์เทคโนโลยี เดินทางตาม Target

location เพื่อสอดแนม หรือค้นหาเหยื่อเพื่อสังหารอย่างอัตโนมัติ โดยมีปัญญาประดิษฐ์ (Fairclough) ค้นหาเส้นทางอัตโนมัติ

Cyber Espionage คือ การใช้นวัตกรรมเทคโนโลยีการสื่อสาร เพื่อการจารกรรมข้อมูลทางการค้า ข้อมูลทางเทคโนโลยี ข้อมูลความลับทางราชการ เป็นต้น

Zombie คือ โปรแกรมที่ทำให้เครื่องคอมพิวเตอร์อื่นๆ เป็นเครื่องมือโจมตีคอมพิวเตอร์หรือ Server ของเหยื่อ

2.2.2 การก่ออาชญากรรมไซเบอร์ที่จับต้องไม่ได้เป็นการกระทำทางจิตใจ (Mind)

การก่ออาชญากรรมที่กระทำต่อ จิตใจ (Mind) หรือ อัตวิสัย (Subjective) โดยใช้วิธีการวิจัยแบบสังคมศาสตร์หรือมนุษยศาสตร์ในการเข้าถึงความรู้หรือความจริง เช่น

2.2.2.1 อาชญากรรมไซเบอร์ที่คุกคามจิตใจบุคคล *(***Cybercrime Threat to Humanity)** การก่ออาชญากรรมที่กระทำต่อ จิตใจ เป็นภัยคุกคามต่อบุคคล มีดังตัวอย่างต่อไปนี้

Identity Theft คือ การที่อาชญากรเอาข้อมูลของเหยื่อที่ปรากฏในสื่อออนไลน์ เช่น ข้อมูลใน facebook หรือสมาร์ตโฟนที่ไม่ได้ Lock Screen หรือใช้คอมพิวเตอร์แล้วไม่ได้ sign out อีเมลล์หรือเว็บไซต์ที่มีข้อมูลส่วนตัว มาสวมรอยเอาข้อมูลส่วนตัวของเหยื่อไปใช้ เช่น เอาชื่อไปเปิดบัญชีธนาคาร ทำบัตรเครดิต ทำธุรกรรมการเงิน ยืมเงินเพื่อนหรือเอาชื่อไปก่ออาชญากรรม

Phishing คือ การโจรกรรมข้อมูลทางอินเตอร์เน็ตในรูปแบบของการสร้าง web site เลียนแบบเพื่อให้เหยื่อ login หรือกรอกข้อมูลเพื่อล่อลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น เอาเลขที่บัตรเครดิต และ user name/password

Vishing คล้าย Phishing ที่แปลว่าตกปลา เป็นคำที่พ้องเสียงกับคำว่า fishing โดย Phishing เป็นการโจรกรรมข้อมูลทางอินเตอร์เน็ตในรูปแบบของการสร้าง web site เลียนแบบเพื่อให้ login หรือกรอกข้อมูลเพื่อล่อลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น เอาเลขที่บัตรเครดิต หรือ user name/password เพื่อไปโจรกรรมทรัพย์สินต่อไป ส่วน Vishing นั้นเป็นลักษณะอาชญากรรมที่ หมายถึง อาชญากรรมที่ใช้การลวงข้อมูลส่วนตัวและข้อมูลด้านการเงินผ่านทางโทรศัพท์ผ่านอินเทอร์เน็ตหรือ Voice over IP (VoIP) โดยโทรมาอ้างว่าบัญชีของผู้ใช้ถูกระงับชั่วคราว ถูกยกเลิก ต้องสงสัยว่ากระทำความผิด เพื่อต้องการทราบข้อมูลสำคัญ เช่น หมายเลขบัตรเครดิต วันหมดอายุ

รหัส หมายเลขบัญชีธนาคาร วันเดือนปีเกิด ตลอดจนหลอกให้โอนเงิน เป็นต้น และเหยื่อไม่สามารถระบุตำแหน่งที่ตั้งของอาชญากรได้เนื่องจากไม่มีการแสดงรหัสโทรศัพท์พื้นที่ หรือสื่อมวลชนเรียกว่า “แก๊งค์ คอลเซ็นเตอร์” ดังนั้น Vishing จึงเป็นคำศัพท์คำที่เกิดจากการประสมคำว่า voice และ phishing เข้าด้วยกัน ดังนั้นทั้ง Vishing กับ Phishing คล้ายกัน คือ หลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัวและหลอกให้เสียทรัพย์

Cyber stalking คือ การใช้อินเตอร์เน็ตผ่าน Social media หรือส่งอีเมล์ หรือการใช้เครื่องมือสื่อสารเพื่อเฝ้าติดตามผู้อื่นให้เกิดความกลัว

Cyber bullying คือ การคุกคามทางอินเทอร์เน็ตนำเรื่องมาประจานให้อับอายหรือมีพฤติกรรมข่มขู่ คุกคามให้หวาดกลัว

Cyber smear คือ การปลอมแบบฟอร์มหรือเครื่องหมายการค้าองค์กรธุรกิจ ในลักษณะหมิ่นประมาทหรือทำให้เกิดภาพลักษณ์เสียหายต่อลูกค้าหรือผู้ถือหุ้นของธุรกิจ โดยเผยแพร่ในอินเทอร์เน็ต

Romance scams คือ อาชญากรใช้ภาพของบุคคลอื่นมาสร้างตัวตนบนโลกออนไลน์จีบจนเหยื่อหลงรักแล้วหลอกลวงเอาทรัพย์หรือลวงไปร่วมองค์กรอาชญากรรม

รูปที่ 5 กรมสอบสวนคดีพิเศษได้ออกประกาศระวังการลอกลวงฉ้อโกงการลงทุน Crypto currency เกิดคดีขึ้นจำนวนมากในประเทศไทย

ที่มา กรมสอบสวนคดีพิเศษ (dsi.go.th)

2.2.2.2 อาชญากรรมไซเบอร์ที่คุกคามจิตใจในระดับสังคม *(***Cybercrime Threat to Society)** การก่ออาชญากรรมที่กระทำต่อ จิตใจ (Mind) อันเป็นภัยคุกคามต่อสังคม มีดังตัวอย่างต่อไปนี้

1. Hoax คือ ข่าวหลอกลวงเพื่อสร้างความสับสนวุ่นวาย หรือการสร้างเนื้อหาเพื่อสุขภาพที่ไม่เป็นจริงหรือกุข่าวขึ้นมาเพื่อสร้าง rating เว็บไซต์ เพื่อขายโฆษณา

2. Fake news and Deep fake คือ การสร้างข่าวปลอมเพื่อด้อยค่าหรือสร้างความเกลียดชังให้คนในสังคมมีต่อเหยื่อเป้าหมาย และ deep fake เป็นวิดีโอของเหยื่อที่พูดให้คนเข้าใจผิดเป็นการใช้เทคโนโลยีในเหยื่อเป้าหมายขยับท่าทาง การพูด และเสียง ตามที่อาชญากรต้องการ

3. Economic Cybercrime คือ ภัยคุกคามจากอาชญากรรมเศรษฐกิจจากโลกออนไลน์ เช่น แชร์ลูกโซ่ ขายตรงออนไลน์ และภัยต่อระบบเศรษฐกิจจากผลกระทบของเงินเสมือน (Virtual Currency) เป็นต้น

4. Psychological cyber warfare คือ การทำสงครามปฏิบัติการจิตวิทยาบนสื่ออินเทอร์เน็ตด้วยการสร้างเนื้อหาหรือวาทกรรม (Discourse) เพื่อปลุกระดมทางการเมือง และสร้างความแตกแยกจนทำลายล้างกันเองในที่สุด (Genocide)

5. Persuasive cyber technology คือ การใช้เทคโนโลยีไซเบอร์ในการโน้มน้าวจูงใจให้ผู้บริโภคเปลี่ยนทัศนคติที่มีต่อสินค้าหรือบริการหรือลัทธินอกรีต ด้วยอัลกอริธึมใน Social media เพื่อให้กลุ่มเป้าหมายเห็น Content บ่อยขึ้น และคล้อยตามในที่สุด ซึ่งสามารถเปลี่ยนแปลงความเชื่อ ความคิด ทัศนคติของคนในสังคมจำนวนมากได้

6. Cybernetic hate crime คือ ยังไม่มีนิยามที่ชัดเจนในปัจจุบัน แต่ถูกนำมาใช้เรียกอาชญากรรมแห่งความเกลียดชังในหลายมิติจากไซเบอร์เทคโนโลยี ทั้งความเกลียดชังผู้ใช้เทคโนโลยีไซเบอร์จากคนหัวโบราณ ความเกลียดชังจากการหมิ่นประมาทออนไลน์ ความเกลียดชังที่ถูกขัดขวางการใช้เทคโนโลยีไซเบอร์ ตลอดจนการทำสงครามวัฒนธรรมด้วย Content เพื่อสร้างความแตก เป็นต้น

7. Political cybercrime คือ การใช้ไซเบอร์เทคโนโลยีร่วมกับการก่ออาชญากรรมการเมือง ทั้งฝ่ายต่อต้านรัฐบาล เช่น การประท้วง ขับไล่ ปลุกระดม จนผู้นำประเทศต้องลี้ภัยดังในเหตุการณ์อาหรับสปริง และนักการเมืองใช้ไซเบอร์เทคโนโลยีโน้มน้าวจูงใจให้ชนะเลือกตั้ง อีกทั้งด้อยค่าคู่แข่งทางการเมือง

2.3 ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

มาร์กัส เฟลสันและลอว์เรนซ์ โคเฮน (Cohen et al., 1979)(Marcus Felson and Lawrence E. Cohen, 1974-1975) ได้อธิบายไว้ในงานเรื่อง "Social Change and Crime Rate Trends: A Routine Activity Approach" ซึ่งได้จากการสังเกตปรากฏการณ์สังคมอเมริกันหลังสงครามโลกครั้งที่สอง ที่ได้พัฒนาทฤษฎี Routine activity theory อันเกี่ยวเนื่องกับมนุษยนิเวศวิทยา (Human ecology) และทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational choice theory) ได้ชี้ให้เห็นว่า อาชญากรรมจะเกิดขึ้นเมื่อมีองค์ประกอบครบ 3 ประการดังนี้

1. เหยื่อ (Victim) หรือเป้าหมาย (Target) หมายถึง บุคคล สถานที่ วัตถุ หรือองค์กรที่อาชญากรหมายมุ่งประกอบอาชญากรรมสร้างความเสียหายเพื่อให้ตนได้อรรถประโยชน์

2. โอกาส (Opportunity) หมายถึง ช่วงเวลา (Time) และสถานที่ (Place) ที่เหมาะสม ที่อาชญากรเชื่อว่าสามารถลงมือก่ออาชญากรรมได้หรือเชื่อว่าไม่มีใครจะจับได้

3. อาชญากร (Criminal/Offender) หมายถึง ผู้ที่มีความต้องการ (Crave) จะก่ออาชญากรรม โดยแสวงหาโอกาสตลอดเวลาจากเหยื่อที่อ่อนแอ

หากปัจจัยทั้ง 3 ด้านครบ อาชญากรรมจะเกิดขึ้นทันที ในทางกลับกันหากองค์ประกอบใดอันหนึ่งหายไป อาชญากรรมจะไม่เกิดขึ้น อธิบายเพิ่มเติมในรูปที่ 6 ดังนี้

รูปที่ 6 ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

ความเกี่ยวข้องกับการวิจัย

โดยทั่วไปเหยื่ออ่อนแอ ย่อมไม่สามารถแก้ไขอะไรได้มาก ส่วนจิตใจของอาชญากรนั้น จะสามารถแก้ไขหรือตัดองค์ประกอบการเกิดอาชญากรรมได้ ก็ต่อเมื่ออาชญากรมีการคิดแบบเป็นเหตุเป็นผล ขึ้นอยู่กับการชั่งน้ำหนักกระบวนการตัดสินใจว่า ถ้าหากลงมือไปแล้วได้อรรถประโยชน์ (Gain) มากกว่าโทษ (Pain) ที่ได้รับ อาชญากรจะลงมือทันที แต่ถ้าหากลงมือก่ออาชญากรรมไปแล้วได้รับโทษมากกว่าอรรถประโยชน์ที่ได้รับ อาชญากรจะไม่ก่ออาชญากรรม

การไร้ตัวตน คือ โอกาส หากอาชญากรมั่นใจว่าตนมีความสามารถล่องหนหายตัวหรือจับกุมตัวไม่ได้ จะตัดสินใจลงมือก่ออาชญากรรมทันที ดังนั้นสิ่งที่ป้องกันการเกิดอาชญากรรมไซเบอร์ได้คือการตัด “โอกาส”หากไซเบอร์เทคโนโลยีใด มีความเป็นไปได้ว่าจะปิดบังอำพรางอย่างไร้ตัวตนได้ดี โอกาสในการเกิดอาชญากรรมจะสูงมาก และไซเบอร์เทคโนโลยีนั้นจะถูกนำมาใช้ประกอบอาชญากรรมอย่างสูง ในทางกลับกัน หากไซเบอร์เทคโนโลยีใดไม่สามารถปิดบังอำพราง ไม่มีการไร้ตัวตนของผู้ใช้งาน และ ไซเบอร์เทคโนโลยีนั้นจะไม่ถูกนำมาใช้ประกอบอาชญากรรม ซึ่งการไร้ตัวตน คือ โอกาส ในทฤษฎีสามเหลี่ยมอาชญากรรม ที่อาชญากรจะใช้ชั่งน้ำหนักอย่างเป็นเหตุเป็นผลก่อนตัดสินใจลงมือประกอบอาชญากรรม

2.4 ทฤษฎีการกระทำที่เป็นกิจวัตร (Theory of Routine Activity)

ทฤษฎีการกระทำที่เป็นกิจวัตร เสนอครั้งแรกโดย โคเฮนและเฟลสัน (Lawrence E. Cohen and Marcus Felson, 1979) อธิบายเชิงลึกไปที่โอกาสอาชญากรรม (crime opportunity) ในสถานการณ์ที่หลอมรวมกันพอดีของพื้นที่และเวลา (Space and Time) เมื่อเหยื่อมีพฤติกรรมที่เป็นกิจวัตร เช่น กินอาหารร้านเดิมเป็นประจำ เดินทางไปทำงานเส้นทางเปลี่ยวเป็นประจำ เปิดหน้าต่างห้องนอนเป็นประจำ ไม่ล็อคประตูหอพักเป็นประจำ สวมเครื่องประดับราคาแพงเป็นประจำ โดยมีองค์ประกอบ 3 ประการที่เป็นเหตุทำให้เกิดอาชญากรรม ได้แก่

1. **แรงจูงใจอาชญากร (Likely/Motivated offender)**
   อาชญากรมีความปรารถนาหรือความพึงพอใจที่จะหาอรรถประโยชน์จากเหยื่อตลอดเวลา และอาชญากรเห็นโอกาสจากเหยื่อในการดำเนินกิจวัตรจูงใจให้ก่ออาชญากรรมหาประโยชน์จากเหยื่อได้ เกิดเป็นแรงจูงใจให้ก่ออาชญากรรม เช่น เห็นกิจวัตรเหยื่อผ่านโซเชียลมีเดีย สถานที่ ภาพถ่าย เวลา หรือช่องว่างของเว็บไซต์หรือระบบคอมพิวเตอร์ขององค์กร ที่อาชญากรเห็นโอกาสที่จะบุกรุกเข้าไปได้ เป็นต้น

2. **มีเป้าหมายที่เหมาะ (Suitable target)**

อาชญากรจะมองหาเหยื่อเป้าหมายที่เป็นบุคคลหรือองค์กรที่เหมาะสมกับความสามารถของอาชญากรในการก่ออาชญากรรม เหยื่ออาจจะมีลักษณะอ่อนแอ เหยื่ออาจจะมีบุคลิกสับเพร่าไม่ระมัดระวังตัว เช่น เหยื่อ Romance scam อาชญากรจะมองหาหญิงที่มีทรัพย์สิน สูงวัย ขาดประสบการณ์ในการรู้จักคนจากโลกออนไลน์ เชื่อคนง่าย ขาดความอบอุ่น ขาดความรัก หรือกลุ่ม แฮ็กเกอร์ Darkside มองหาเหยื่อเป้าหมายการเรียกค่าไถ่ระบบคอมพิวเตอร์ (Ransomware) เป็นผู้ใช้ระบบปฏิบัติการวินโดว์ที่ไม่ได้ปิดช่องโหว่ External blue เป็นต้น

3. **ขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian)**

เหยื่อมีความอ่อนแอเป็นปกติทั่วไป จึงต้องมีผู้พิทักษ์ที่คอยสอดส่องดูแลความสงบเรียบร้อย เช่น ตำรวจ ผู้ปกครอง รัฐบาล หรือผู้ดูแลความมั่นคงปลอดภัยไซเบอร์ โอกาสในการเกิดอาชญากรรมจะเกิดขึ้นเมื่อขาดผู้พิทักษ์ที่มีความสามารถเพียงพอในการป้องกันอาชญากรรม

ความเกี่ยวข้องกับการวิจัย

ทฤษฎีการกระทำที่เป็นกิจวัตร (Theory of Routine Activity) อธิบายเรื่องโอกาสในทฤษฎีสามเหลี่ยมอาชญากรรมให้ลึกซึ้งยิ่งขึ้น ตั้งแต่การดำเนินกิจวัตรที่เป็นปกติของเหยื่อที่อ่อนแอต่อการป้องกันโอกาสในการเกิดอาชญากรรมทำให้เกิดแรงดึงดูดจูงใจให้อาชญากรก่ออาชญากรรม ความอ่อนแอของเหยื่ออาจจะเป็นเรื่องพ้นวิสัยในการปกป้องดูแลตนเอง จึงต้องมีผู้พิทักษ์ทั้งในครอบครัว ในองค์กรและในสังคม แต่เมื่อผู้พิทักษ์อ่อนแอโอกาสในการเกิดอาชญากรรมจึงเกิดขึ้น ในการวิจัยนี้ผู้พิทักษ์แทนด้วยตำรวจที่มีหน้าที่สืบสวนจับกุมและรวบรวมพยานหลักฐานเพื่อดำเนินคดี

2.5 ทฤษฎีคิดก่อนกระทำผิด หรือ ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory)

ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory: RCT) เป็นทฤษฎีที่มีอิทธิพลอย่างสูงต่อวงการวิชาการด้าน สังคมวิทยา มานุษยวิทยา และอาชญาวิทยา ตลอดจนวิชารัฐศาสตร์การเมืองการปกครอง ด้วยสมมติฐานที่ง่ายต่อการเข้าใจว่าทุกอย่างขึ้นอยู่กับการตัดสินใจ

ของปัจเจกชนที่จะเลือกหนทางที่เห็นแก่ตัวเพื่อให้ได้ประโยชน์สูงสุด และทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลหรือ Rational Choice Theory ได้มีนักคิด นักวิชาการได้กล่าวถึงมากมายดังนี้

ในศตวรรษที่ 18 มีการพัฒนาความรู้ด้าน การเมือง การปกครอง และกระบวนการยุติธรรมไปอย่างกว้างขวาง ซีซาร์ แบ็คคาเรีย (Cesare Beccaria) ได้ตีพิมพ์บทความที่มีชื่อเสียงเรื่อง “On crime and Punishment” ในปี ค.ศ. 1764 ได้อธิบายสาเหตุพฤติกรรมการก่ออาชญากรรมของมนุษย์ ที่พ้นจากความเชื่อเรื่องไสยศาสตร์หรือสิ่งลี้ลับภูติ ผี ปีศาจ ซาตาน หรือบาปที่มาสิงสู่มนุษย์ให้กระทำความผิด แต่เปลี่ยนมาริเริ่มว่า มนุษย์สามารถควบคุมพฤติกรรมของตนได้ โดยมนุษย์มีเหตุมีผล รู้จักคิดก่อนมีพฤติกรรม และแสวงหาความสุขตลอดเวลา ดังนั้นอาชญากรรมเป็นผลมาจากการที่มนุษย์ตัดสินใจเลือกที่จะมีพฤติกรรมเช่นนั้น โดยผ่านกระบวนการตัดสินใจอย่างมีระบบแล้ว เช่น บุคคลลักทรัพย์เพราะตอบสนองการอยากได้ทรัพย์ผู้อื่น บุคคลฆ่าผู้อื่นเพราะตอบสนองความโกรธแค้นของตน บุคคลข่มขืนผู้อื่นเพราะตอบสนองความต้องการทางเพศของตน เป็นต้น

สำนักอาชญาวิทยาดั้งเดิม (Classical criminology school) มีแนวคิดหลักอยู่ 2 ประการ คือ

1. ต้องมีสัญญาระหว่างรัฐกับประชาชน เพื่อป้องกันความวุ่นวายไม่ให้เกิดขึ้นในสังคม
2. ธรรมชาติบุคคลมี 3 ประการ คือ การมีเจตจำนงอิสระในการควบคุมตนเอง (Free will) การคิดอย่างเป็นเหตุเป็นผล (Rationality) และแสวงหาความสุขตลอดเวลา (Utilitarian)

นักคิดสำนักอาชญาวิทยาดั้งเดิมอีกท่านที่สืบต่อแนวคิดของ ซีซาร์ แบ็คคาเรีย คือ เจอรามี เบ็นธัม (Jeremy Bentham; 1748-1832) ได้แต่งหนังสือชื่อ “An Introduction to Principles of Morals and Legislation” ในปี ค.ศ. 1789 เบ็นธัมยังยึดแนวคิดเจตจำนงอิสระของ แบ็คคาเรีย ว่าด้วยพฤติกรรมของมนุษย์ โดยปรัชญาแนวความคิดของเบ็นธัมที่สำคัญมี 2 ประการคือ

1. ลัทธิประโยชน์นิยม (Utilitarian) เบ็นธัม เชื่อว่าพฤติกรรมมนุษย์ถูกควบคุมโดยหลักธรรมชาติ 2 ประการ คือ ความพึงพอใจ (Pleasure) และความทุกข์ทรมาน (Pain) ซึ่งจากการที่มนุษย์เป็นผู้คิดอย่างเป็นเหตุเป็นผล ก่อนที่จะมีพฤติกรรมมนุษย์จะคิดคำนวณเปรียบเทียบระหว่าง ความพึงพอใจที่จะได้รับกับความทุกข์ทรมานที่จะได้รับจากผลของการมีพฤติกรรมนั้นๆ สำหรับอาชญากรรมก็เช่นกัน หากมนุษย์คำนวณแล้วว่าความพึงพอใจที่จะได้รับมากกว่าความทุกข์ทรมานที่จะได้รับ มนุษย์จะเลือกประกอบอาชญากรรม

2. กฎหมายและการลงโทษ (Law and Punishment) หลักปรัชญาของเบ็นธัมเกี่ยวกับกฎหมายคือ กฎหมายมีไว้เพื่อสร้างและสนับสนุนความสุขของคนในสังคม ดังนั้นกฎหมายที่ดีจะต้องป้องกันความชั่วร้ายที่จะเกิดขึ้นในสังคม เบ็นธัมได้เสนอให้ออกกฎหมายในลักษณะที่บุคคลทั่วไปคิดว่า หากกระทำผิดกฎหมายแล้ว จะได้รับความทุกข์ทรมานมากกว่าความพึงพอใจ

พรชัย ขันตี (2558) ประการแรก นักทฤษฎีกลุ่มนี้มีความเชื่อว่า บุคคลเป็นผู้มีอิสระในการเลือกที่จะกระทำผิดกฎหมาย และประการที่สอง แนวทางในการเลือกพฤติกรรมผิดกฎหมาย ขึ้นอยู่กับการที่บุคคลจะได้รับความพึงพอใจหรือผลประโยชน์สูงสุด ซึ่งความพึงพอใจหรือผลประโยชน์ไม่ได้ขึ้นอยู่กับทรัพย์สินเท่านั้น แต่อาจรวมถึงความพึงพอใจด้านจิตใจด้วย สมมติฐานนี้คล้ายกับสมติฐานของนักอาชญาวิทยาของสำนักอาชญาวิทยาแนวดั้งเดิม

หลักการที่ทฤษฎีนี้ได้เพิ่มเติมแนวคิดของสำนักอาชญาวิทยาแนวดั้งเดิมก็คือ การที่บุคคลได้คิดคำนวณถึงผลที่จะตามมาหลังจากประกอบอาชญากรรมแล้ว ไม่ว่าจะเป็นประโยชน์ที่ได้รับ ความเป็นไปได้ที่จะถูกจับกุม อัตราโทษหากถูกจับกุม ตลอดจนทางเลือกอื่นที่ถูกกฎหมาย

โรแนล คาร์กและดีเร็ค คอร์นิส (Clark, Cornish, 1986) เสนอว่า อาชญากรรมมีคุณสมบัติสองประการคือ คุณสมบัติการประกอบอาชญากรรม และคุณสมบัติของอาชญากร

คุณสมบัติการประกอบอาชญากรรม (Offense Specific) หมายถึง ข้อเท็จจริงที่ว่าอาชญากรจะมีพฤติกรรมแตกต่างกันออกไปตามรูปแบบอาชญากรรม ซึ่งจะแตกต่างกันในด้านความชำนาญในการประกอบอาชญากรรม ทรัพย์สินหรือผลประโยชน์ที่จะได้รับจากการกระทำความผิด และการมีอยู่อย่างแพร่หลายของเหยื่ออาชญากรรม

ส่วนคุณสมบัติของตัวอาชญากร (Offender Specific) หมายความถึง ความแตกต่างของตัวอาชญากรในการตัดสินใจประกอบอาชญากรรม ก่อนที่จะกระทำผิดกฎหมายอาชญากรต้องคำนึงถึงสภาพแวดล้อมโดยทั่วไปอันได้แก่ โอกาสในการกระทำความผิด ผลเสีย ผลประโยชน์ ตลอดจนความเสี่ยง รวมทั้งแรงกระตุ้นหรือมูลเหตุจูงใจในการกระทำความผิดของอาชญากรด้วย ซึ่งหลังจากบุคคลคำนวณถึงปัจจัยต่างๆ ที่เกี่ยวข้องกับการประกอบอาชญากรรมแล้ว จึงจะตัดสินใจว่าจะประกอบอาชญากรรมหรือไม่

พิชาย รัตนดิลก ณ ภูเก็ต (2559)[4] ปรากฏการณ์ทางสังคมเป็นผลมาจากกิจกรรมของมนุษย์และมนุษย์คือผู้กระทำที่ถูกชี้นำโดยความเชื่อ เป้าประสงค์ ความหมาย ค่านิยม ข้อห้ามและศีลธรรม

[4] พิชาย รัตนดิลก ณ ภูเก็ต (2559).วิพากษ์การอธิบายทางเลือกเชิงเหตุผล. วารสารเศรษฐศาสตร์การเมืองบูรพา ปีที่ 1 ฉบับที่ 1 กรกฎาคม-ธันวาคม 2556.

มนุษย์เป็นสิ่งมีชีวิตที่มีความเจตนาหรือความมุ่งหมาย ซึ่งกระทำบนพื้นฐานของเหตุผล (Reasons) ความคิดที่ว่าการกระทำของมนุษย์อยู่บนพื้นฐานของเหตุผลมีนัยสำคัญหลายประการต่อสังคมศาสตร์ ประการแรกมีนัยว่าแบบแผนทางสังคมมีความสัมพันธ์เชิงสาเหตุที่หลากหลายกว่าแบบแผนทางธรรมชาติ เพราะว่าแบบแผนทางธรรมชาติ มีลักษณะที่ตายตัวอันเกิดจากความสัมพันธ์ของสรรพสิ่งเชิงภววิสัย และถูกควบคุมโดยกฎที่แน่นอนกฎใดกฎหนึ่ง ขณะที่แบบแผนทางสังคมเกิดมาจากสภาวะที่ตั้งใจของมนุษย์ที่เป็นผู้กระทำทางสังคม ประการที่สอง ลักษณะเชิงความตั้งใจของปรากฏการณ์ทางสังคมทำให้มีโอกาสเกิดรูปแบบการอธิบายเชิงสาเหตุได้หลากหลายมากกว่าในวิทยาศาสตร์ธรรมชาติ ปรากฏการณ์ทางสังคมหลายอย่างสามารถได้รับการอธิบายในรูปของผลลัพธ์ โดยรวมของการกระทำที่มีเป้าประสงค์ร่วมกันของปัจเจกบุคคลจำนวนมาก หากเราเข้าใจสิ่งที่บุคคลเหล่านั้นต้องการ อะไรคือสิ่งที่พวกเขาเชื่อ และวิธีการที่พวกเขากระทำ ซึ่งพวกเขาคาดหวังว่าจะนำไปสู่เป้าประสงค์ เราก็สามารถอธิบายการเกิดขึ้นของผลลัพธ์ที่ตามมาได้ด้วย

กระบวนทัศน์ทางเลือกเชิงเหตุผล (Rational Choice Paradigm) ตั้งอยู่บนพื้นฐานของหลักการสำคัญเชิงพฤติกรรมที่สำคัญ คือ การมีเป้าประสงค์ และการคำนวณประโยชน์ที่ได้รับ กล่าวอีกนัยหนึ่ง ปัจเจกบุคคลย่อมมีความคาดหวังเชิงเป้าหมายเกี่ยวกับผลประโยชน์ และเขาจะกำหนดทางเลือกของการกระทำหลากหลายทางเลือกและวิเคราะห์ต้นทุนและประโยชน์ รวมทั้งข้อดีข้อเสียต่าง ๆ ของแต่ละทางเลือกเหล่านั้น จากนั้นนำมาเปรียบเทียบกันและตัดสินใจเลือกทางเลือกที่ดีที่สุด ซึ่งเขาประเมินว่าจะนำไปสู่เป้าหมายที่ตั้งเอาไว้ ดังนั้นการอธิบายแบบทางเลือกเชิงเหตุผล จึงขึ้นอยู่กับทฤษฎี “วิถี-เป้าหมาย” (Means-end Theory) ของการกระทำเชิงเหตุผล กล่าวคือการกระทำใดถือว่าเป็นการกระทำที่มีเหตุผลก็ต่อเมื่อการกระทำนั้นมีวิธีการที่เหมาะสมในการนำไปสู่เป้าหมายที่กำหนด ภายใต้ความเชื่อที่มีอยู่ของผู้กระทำเกี่ยวกับสถานการณ์ของทางเลือกนั้น ดังนั้นในการอธิบายการกระทำของปัจเจกบุคคล ผู้อธิบายจะต้องระบุความเชื่อพื้นฐานและเป้าประสงค์ของบุคคลนั้น และแสดงให้เห็นว่าแนวทางการกระทำที่ถูกเลือกจากบุคคลนั้น มีความสมเหตุผลในการบรรลุเป้าประสงค์ภายใต้ความเชื่อที่กำหนด และนั่นหมายความว่าในการอธิบายแบบนี้มีเงื่อนไขสำคัญ คือ จะต้องหาความสัมพันธ์ระหว่างความเชื่อ (Beliefs) กับความปรารถนา (Desires) และการกระทำ ((FATF))

ไชยยันต์ ไชยพร (2560) ได้ให้คำแปล “Rational choice theory” ว่าเป็น “ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล” ภาษาไทยมีคำว่า “เหตุผล” “ความสมเหตุสมผล” และ “ความมีเหตุผล” ไม่ค่อยได้ยินคำว่า “ความเป็นเหตุเป็นผล” ต่างจากความหมายภาษาอังกฤษ “Reason” กับ “Rationality” โดยอธิบายเพิ่มว่า Rational choice theory ที่เชื่อว่า หลักการแบบแผนพฤติกรรมของผู้คนในสังคมสะท้อนถึงตัวเลือกต่างๆ ที่ปัจเจกแต่ละบุคคลเลือก ซึ่งแต่ละคนจะเลือกโดยเปรียบเทียบดูว่า วิธีการแบบไหนที่จะทำให้เขาได้ประโยชน์สูงสุด โดยตนเองลงทุนน้อยที่สุด ความคิด

ดังกล่าวนี้จะเป็นเหตุผลได้ เพราะมันจะเป็นข้ออ้างหรือการกล่าวถึง สาเหตุ (Cause) และผลที่ตามมา (Effect) นั่นคือสาเหตุความเห็นแก่ตัว

เอลสเตอร์[5] กล่าวว่า ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล ตั้งสมมุติฐานว่า การกระทำหนึ่งๆ ที่เกิดขึ้น ถือว่าเป็นการกระทำที่สนองเงื่อนไขที่น่าพอใจที่สุด (Optimality conditions) สามประการ

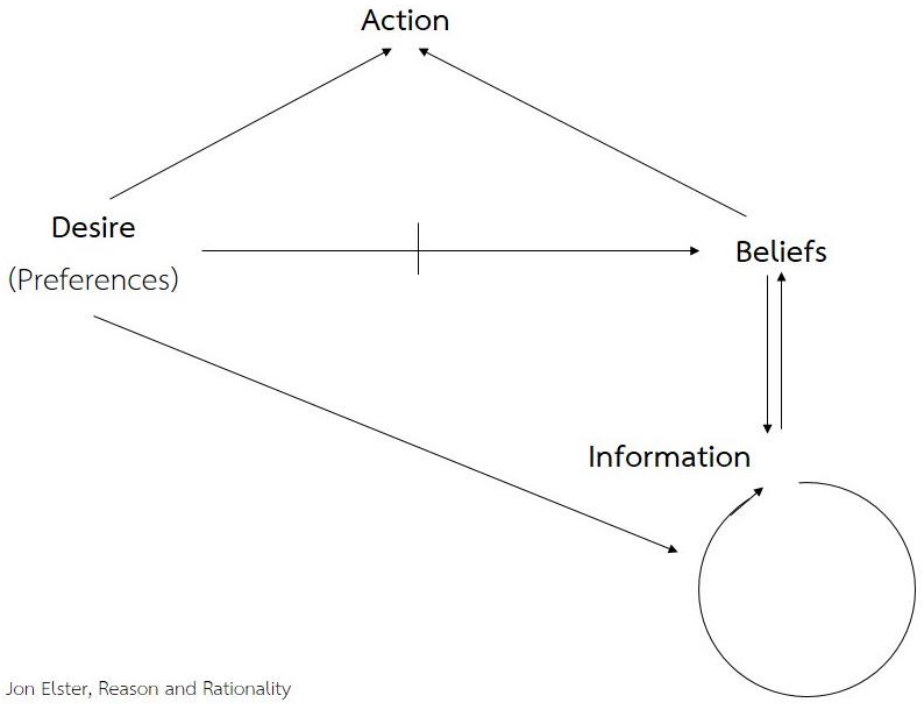
เงื่อนไขแรก ผู้กระทำจะต้องมีความปรารถนาหรือมีความชอบอะไรไว้บางอย่าง (Preferences or desires) ขณะเดียวกัน ความปรารถนาไม่จำเป็นว่าจะต้องเป็นความปรารถนาที่เป็นเหตุเป็นผลเท่านั้น ความปรารถนาหรือความชอบที่ว่านี้ปฏิบัติการในฐานะที่เป็น “ตัวขับเคลื่อนที่คงที่ของทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล” (The unmoved mover of the theory)

เงื่อนไขประการที่สอง ตัวการกระทำ จะต้องเป็นหนทางที่ดีที่สุด ที่สามารถทำให้บรรลุความปรารถนาได้ ทั้งนี้ขึ้นอยู่กับความเชื่อ และข้อมูลข่าวสารที่ตัวผู้กระทำมีอยู่

เงื่อนไขประการที่สาม ตัวความเชื่อเหล่านี้ จะต้องเป็นข้อมูลที่เหมาะสมที่สุด เท่าที่ผู้กระทำจะมีได้ อีกทั้งปริมาณของข้อมูลก็คือ ปริมาณทรัพยากรที่ใช้เพื่อให้ได้มาซึ่งข้อมูลนั้น จะต้องเหมาะสมที่สุดหรือน่าพอใจที่สุดด้วย

บุคคลเรียนรู้ที่จะกระทำพฤติกรรม โดยอาศัยกระบวนการทางปัญญาเป็นสำคัญ หากแต่อาชญากรมีรูปแบบความคิดผิดไปจากคนทั่วไป ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลนี้สามารถแสดงมาในรูปแบบกราฟที่แสดงฟังก์ชันอรรถประโยชน์ที่จุดต่างๆ กันได้ โดยแต่ละจุดมีค่าที่แสดงไว้ ทำให้บอกได้ว่าผู้ที่เลือกอย่างเป็นเหตุเป็นผลจะเลือกการกระทำใดที่จะให้ผลลัพธ์สูงสุด (Maximizing utility) ต่ออรรถประโยชน์ของตน แต่ความปรารถนานี้คือความปรารถนาที่เห็นแก่ตัวหรือให้ประโยชน์ผู้อื่นที่ตนพึงพอใจหรือชั่วร้าย ด้วยเอาประโยชน์จากผู้อื่น ในส่วนความเชื่อ (Belief) ที่รองรับการเลือกอย่างเป็นเหตุเป็นผล ต้องเป็นความเชื่อที่มีพื้นฐานที่ดีรองรับ นั่นคือ “ข้อมูล” จำนวนมากที่สนับสนุน ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ ที่ให้แผนภาพลึกซึ้งมากยิ่งขึ้นดังนี้

[5] ไชยยันต์ ไชยพร (2560). Jon Elster & Rational choice theory. พิมพ์ครั้งที่ 2. สำนักพิมพ์ Way of book กรุงเทพ. มีนาคม 2560



รูปที่ 7 แบบแผนจำลองการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์

ที่มา ไชยยันต์ ไชยพร (2560)

แบบแผนจำลองอธิบายการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ ตั้งบนสมมติฐานว่า การกระทำหนึ่งๆ ที่เกิดขึ้น ถือว่าเป็นการกระทำที่เกิดจากการตัดสินใจเลือกอย่างเป็นเหตุเป็นผลได้ ต้องเป็นการกระทำบนเงื่อนไขที่น่าพอใจที่สุด (Optimality conditions) ทั้ง 3 ประการ คือ

1. ความปรารถนา (Desire)

ผู้กระทำต้องมีความปรารถนาหรือมีความชอบอะไรบางอย่าง (Preference or Desire) ขณะที่ความปรารถนานี้ไม่จำเป็นต้องเป็นความปรารถนาที่เป็นเหตุเป็นผลเท่านั้น แต่ความปรารถนาหรือความชอบนี้ปฏิบัติการในฐานะที่เป็น “ตัวขับเคลื่อนคงที่ของทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (The unmoved mover of the theory)”

2. การกระทำ ((FATF))

ต้องเป็นหนทางที่ดีที่สุดที่จะทำให้ผู้กระทำสามารถบรรลุในสิ่งที่ปรารถนา ทั้งนี้ขึ้นอยู่กับความเชื่อ (Belief) และข้อมูลข่าวสารที่ผู้กระทำนั้นมีอยู่

3. ความเชื่อ (Belief)

ต้องเป็นข้อมูล (Information) ที่เหมาะสมที่สุด เท่าที่ผู้กระทำจะมีได้ อีกทั้งปริมาณของข้อมูลหรือทรัพยากรในการได้มาซึ่งข้อมูล จะต้องเหมาะสมหรือน่าพอใจที่สุดด้วย

ในเบื้องต้นการกระทำที่เป็นเหตุเป็นผลคือ การที่คนแต่ละคนเลือกทำในส่งที่ตนได้รับประโยชน์สูงสุด (Maximization) โดยประโยชน์นี้อยู่ในรูป อรรถประโยชน์ (Utility) การสนองความพึงพอใจ (Preference) การสนองความต้องการ (Want) ฯลฯ ที่สูงที่สุดเท่าที่จะได้รับจากทางเลือกแบบต่างๆ ที่มีอยู่

เอลสเตอร์ มีจุดยืนตรงข้ามกับทฤษฎีสังคมศาสตร์ที่ใช้การอธิบายปรากฏการณ์แบบ Functionalism หรือทฤษฎีหน้าที่นิยมหรือทฤษฎีโครงสร้างหน้าที่ ที่มองว่าโครงสร้างสังคมหรือสถาบันเป็นตัวกำหนดควบคุมความเป็นไปในสังคม โดยเอลสเตอร์กล่าวใน The Cement of Society: A Study of Social Order ซึ่งตีพิมพ์เมื่อปี ค.ศ. 1989 ไว้ว่า “หน่วยพื้นฐานของชีวิตทางสังคม คือ การกระทำของปัจเจกบุคคล”

ดังนั้นกล่าวได้ว่า การเลือกตัดสินใจของปัจเจกบุคคลต่างหาก คือตัวกำหนดความเป็นไปของสังคม โดยเฉพาะการชั่งน้ำหนักการใช้เหตุและผลของอาชญากร ก่อนตัดสินใจลงมือก่ออาชญากรรมว่าจะเลือกวิธีการใดให้ได้ประโยชน์สูงสุดแก่ตน และหลีกเลี่ยงการถูกลงโทษ การตัดสินใจของอาชญากรผู้วิจัยเห็นว่า เป็นต้นกำเนิดของ บรรทัดฐานสังคม ต้นกำเนิดของกฎหมาย และกระบวนการยุติธรรม

การทำความเข้าใจวิธีการตัดสินใจของอาชญากรด้วย ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลทำอย่างไรให้บรรลุความปรารถนา และหลีกเลี่ยงสิ่งที่ไม่พึงปรารถนา ภายใต้สถานการณ์สังคมและเงื่อนไข จัดเป็นทฤษฎีเชิงคุณค่า (Normative Theory) หรือเชิงปทัสถาน

ความเกี่ยวข้องกับการวิจัย

ทฤษฎีการคิดอย่างเป็นเหตุเป็นผล คือ จุดกำเนิดของอาชญากรรมไซเบอร์ เมื่ออาชญากรคำนวณแล้วว่า การไร้ตัวตน จะเป็นประโยชน์แก่ตนมาก จะไม่มีความเป็นไปได้ที่จะถูกจับกุมหรือถูกจับกุมแล้วก็ไม่อาจเอาผิดได้ตามกฎหมาย การไร้ตัวตน และจะไม่ส่งผลให้โทษตามมาหลังจากประกอบอาชญากรรมแล้ว

ทฤษฎีการคิดอย่างเป็นเหตุเป็นผล จะเป็นเหตุเป็นผลก็เมื่อ อาชญากรนั้นเห็นแก่ตัว จ้องหาประโยชน์จากเหยื่อตลอดเวลา และเมื่ออาชญากรมั่นใจว่าตนล่องหนหายตัวอย่างไร้ตัวตนจับกุมตัวไม่ได้ อาชญากรจะตัดสินใจลงมือก่ออาชญากรรมทันที

2.6 ประเภทอาชญากร

กัญญ์ฐิตา ศรีภา (2563) การจำแนกประเภทอาชญากรตามศาสตร์ทางจิตวิทยา (Criminal Psychological Typologies) โดยจิตแพทย์ Havelock Ellis (Miller, 2012) ได้แบ่งประเภทอาชญากรไว้ดังนี้

1. **อาชญากรโดยสัญชาตญาณ (Instinctive criminals)** หรืออาชญากรโดยกำเนิด (born criminal) ได้รับพันธุกรรมจากบรรพบุรุษ มีความผิดปกติของบุคลิกภาพ มีลักษณะต่อต้านสังคม ไม่รู้สึกผิด และมีพฤติกรรมรุนแรงไม่ยับยั้ง
2. **อาชญากรตามโอกาส (Occasional criminals)** หมายถึงผู้ที่ไม่มีความผิดปกติทางจิตหรือบกพร่องทางร่างกาย แต่เป็นผู้ที่ละเมิดต่อกฎหมายและยอมจำนนต่อสิ่งล่อใจในการก่ออาชญากรรมหรืออยู่ภายใต้เงื่อนไขบางประการที่จูงใจให้กระทำความผิด เช่น ความจำเป็นทางเศรษฐกิจ ความกดดันจากสังคมหรือเหตุจูงใจจากสถานการณ์ต่างๆ เป็นต้น อาชญากรประเภทนี้หากกระทำความผิดแล้ว ได้รับแรงส่งเสริมหรือแรงสนับสนุนให้กระทำความผิดซ้ำๆ จะกลายเป็นอาชญากรติดนิสัย
3. **อาชญากรติดนิสัย (Habitual criminals)** อาชญากรประเภทนี้จะกระทำความผิดซ้ำๆ จนติดเป็นนิสัย และไม่คิดที่จะเลิกกระทำความผิดจนยากที่จะแก้ไข แม้อาชญากรประเภทนี้จะไม่มีลักษณะป่าเถื่อนรุนแรงเหมือนอาชญากรโดยกำเนิด แต่เริ่มจากความจำเป็นหรือการถูกบีบบังคับหรือโอกาสบางอย่างที่จูงใจให้กระทำความผิดทีละเล็กทีละน้อยจนเป็นความเคยชิน และกลายเป็นผู้มีวิถีอย่างอาชญากรสมบูรณ์แบบ

ความเกี่ยวข้องกับการวิจัย

ประเภทอาชญากร ช่วยให้เข้าใจอาชญากรไซเบอร์มากขึ้นในระดับหนึ่ง จากการสังเกตของผู้วิจัยพบว่า อาชญากรไซเบอร์อาจจะเป็น อาชญากรตามโอกาส (Occasional criminals) หากไม่พบโอกาส “การไร้ตัวตน” อาชญากรประเภทนี้จะไม่ลงมือก่ออาชญากรรม และอาชญากรไซเบอร์อาจจะเป็นอาชญากรติดนิสัย (Habitual criminals) จะทดลองเครื่องมือต่างๆ ที่ตนมีเมื่อพบระบบคอมพิวเตอร์ใหม่ๆ หรือเว็บไซต์ใหม่ๆ เขาจะทดลองเจาะระบบว่าจะสามารถปิดบังอำพรางตนเพื่อเข้า

ไปหาอรรถประโยชน์ได้หรือไม่หรือทดลองศึกษาว่าสามารถนำไปใช้ประกอบอาชญากรรมอื่นได้หรือไม่

2.7 รูปแบบการคิดของอาชญากร

วิวัฒนาการของแนวความคิดทางจิตวิทยาเริ่มจากทฤษฎีจิตวิเคราะห์ ที่เชื่อว่าพฤติกรรมเกิดจากแรงขับจากจิตไร้สำนึก (Unconscious) และอิทธิพลในวัยเด็ก ซึ่งต่อมาพัฒนาเป็นจิตวิเคราะห์แนวใหม่ (Neo-Freudian) ที่ให้ความสำคัญเพิ่มขึ้นกับประสบการณ์ปัจจุบัน และความคาดหวังในอนาคตที่มีผลต่อพฤติกรรม รวมไปถึงแนวความคิดปัญญานิยม (Cognitive revolution) ที่ให้ความสำคัญต่อการรู้คิด และปัญญามนุษย์ที่มีอิทธิพลต่อพฤติกรรมของเขา ซึ่งในแง่ของการศึกษาพฤติกรรมอาชญากร เชื่อว่ามีรูปแบบความคิดที่แตกต่างจากคนปกติทั่วไป งานวิจัยที่สำคัญของ โยเซลสันและแซมีนาว (Yochelson and Samenow, 1976) ได้ทำการศึกษาวิจัยเชิงคุณภาพเกี่ยวกับรูปแบบการคิดของอาชญากร (Criminal thinking style) โดยแบ่งเป็น 3 ลักษณะ หลังจากนั้นได้มีนักวิชาการ (Walter, 1990, 2020) ได้เสนอแบบแผนการคิดของอาชญากร (Criminal cognitive patterns) แบ่งออกเป็น 8 รูปแบบ ดังนี้

1. **การคิดหาเหตุผลให้ตัวเองดูดีขึ้น (Mollification)** เป็นการคิดแบบหาเหตุผลกล่าวอ้างโดยการโทษผู้อื่นหรือสิ่งอื่น เช่น “ผมไม่ได้เป็นคนไม่ดีนะ เขามาดูถูกผมก่อน ผมเลยชกเขา”
2. **คิดแบบตัดบท (Cutoff)** เป็นการคิดตัดบทหรือไม่พยายามคิดอะไรให้มาก เพื่อที่จะตัดสินใจได้ง่ายขึ้นที่จะก่ออาชญากรรม เช่น “รีบๆ ทำซะ อย่าใจเสาะไปหน่อยเลย”
3. **คิดอ้างสิทธิ (Entitlement)** เป็นการคิดให้ตัวเองรู้สึกว่าสิ่งที่เขาทำเป็นสิ่งที่ชอบธรรม พอ คนที่คิดแบบนี้มักจะมองตนเองเป็นคนพิเศษหรือมีสิทธิที่จะทำหรือก่ออาชญากรรม เช่น “ผมจ่ายทุกสิ่งทุกอย่างให้เธอ ดังนั้นไม่แปลกอะไรที่เธอจะต้องเป็นของผม”
4. **คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation)** เป็นการคิดว่าตนเองมีอำนาจเหนือกว่าคนอื่นๆ สามารถควบคุมคนอื่นได้ และต้องการประกาศศักดา เช่น “แกควรรู้ว่าฉันเป็นใคร อย่ามายุ่งกับฉัน”
5. **คิดจากความอ่อนไหวทางจิตใจ (Sentimentality)** บางกรณีการกระทำความผิดเกิดจากจิตใจที่อ่อนไหวของผู้กระทำ เช่น ก่ออาชญากรรมเพราะสงสาร อยากช่วยเหลือครอบครัว อาชญากรประเภทนี้มักรู้สึกได้ถึงการกระทำผิดของตนเอง จึงพยายามดึงเอาสิ่งดีๆ ที่ตนทำ เพื่อเอามาชดเชยความรู้สึกผิดของตนเอง เช่น “ที่ผมต้องปล้นธนาคาร

เพราะผมต้องเอาเงินไปรักษาแม่กับลูกชาย ผมว่าลูกผู้ชายที่ไหนก็ทำ เพื่อให้คนที่รักมีชีวิตรอด”

6. **คิดแบบขอไปที (Cognitive indolence)** เป็นการคิดแบบลวกๆ ขอแค่ให้ผ่านๆ ไป แทนที่จะพิจารณาถึงปัญหาหรือผลกระทบให้ถ้วนถี่พูดง่ายๆ เช่น “ผมไม่มีเวลาที่จะคิดอะไรที่วุ่นวาย ก็เลยทำเลย เกิดอะไรขึ้นค่อยว่าทีหลัง”
7. **คิดไม่หนักแน่นมั่นคง (Discontinuity)** อาชญากรประเภทนี้มักดำเนินชีวิตไปแบบไม่มีความหนักแน่นมั่นคงทางความคิด ขาดความยับยั้งชั่งใจ มักถูกครอบงำหรือกระตุ้นจากสิ่งเร้าต่างๆ ให้กระทำผิดง่าย พฤติกรรมส่วนใหญ่มักเกิดจากความหุนหันพลันแล่นมากกว่าการพยายามไตร่ตรองต่อสิ่งที่เกิดขึ้น เช่น “จะเสียสมองคิดไปทำไม ทำอย่างนั้นดีอยู่แล้ว”
8. **คิดได้ใจจนเกินจริง (Super-optimism)** เป็นความคิดที่มั่นใจจนเกินจริงของอาชญากรว่า เขาสามารถที่จะหลีกพ้นโทษจากการกระทำความผิดของตนเองได้อย่างแน่นอน หรือมั่นใจว่าตนไม่มีทางถูกจับหรือถูกทำร้ายจากใครได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ เช่น “คุณก็เห็นว่าผมหนีรอดได้มาทุกครั้ง ไม่มีทางหรอกที่ตำรวจหรือใครจะจับผมได้

ลักษณะและรูปแบบการคิดของอาชญากรในลักษณะต่างๆ ดังกล่าว สอดคล้องกับแนวความคิดปัญญานิยมที่เชื่อว่า บุคคลเรียนรู้ที่จะกระทำพฤติกรรม โดยอาศัยกระบวนการทางปัญญาเป็นสำคัญ หากแต่อาชญากรมีรูปแบบความคิดผิดไปจากคนปกติ

ความเกี่ยวข้องกับการวิจัย

รูปแบบการคิดของอาชญากรไซเบอร์ อาจจะไม่เข้าลักษณะประเภทรูปแบบการคิดของอาชญากรตามทฤษฎีอาชญาวิทยาที่ยกมาหรือเคยมีมาก่อน เพราะเป็นอาชญากรไซเบอร์มีความแตกต่างจากอาชญากรประเภทอื่นตรงที่มีความรู้ความสามารถสูง และไม่ว่าวาม ในการศึกษาวิจัยอาจจะพบข้อเท็จจริงใหม่ที่เป็นประโยชน์ต่อไป

2.8 **ทฤษฎีเกม (Game Theory)**

ทฤษฎีเกม เป็นวิธีการศึกษาพฤติกรรมการตัดสินใจอย่างเป็นเหตุเป็นผลของมนุษย์ โดยใช้ภาษาทางคณิตศาสตร์มาอธิบายทางเลือกของมนุษย์ในการตัดสินใจ เมื่อต้องพิจารณาทางเลือกใดที่จะ

ให้ผลประโยชน์มากที่สุด (Single-person Scenario) หรือทางเลือกในการตัดสินใจแข่งขันกับบุคคลอื่นหรือมากกว่า 1 คน จะเลือกกลยุทธ์ใดให้ได้ชัยชนะมา

ธีโอดอร์, ทูโรซี่ และ เบอร์ฮาร์ด (Theodore. Turocy and Bernhard, 2001) อธิบายว่า ทฤษฎีเกม[6] เป็นการศึกษาความขัดแย้งและความร่วมมือ (conflict and cooperation) ทั้งระหว่างบุคคล ระหว่างกลุ่มคน ระหว่างกลุ่มธุรกิจ ฯลฯ

ทฤษฎีเกม ได้ถูกเริ่มต้นโดย Antoine Cournot มาตั้งแต่ปี ค.ศ.1838 ต่อมาได้ถูกพัฒนาโดยนักคณิตศาสตร์ชื่อว่า Emile Borel ในปี ค.ศ.1921 และมาโด่งดังจากการพัฒนาต่อโดย John Von Neumann ในปี ค.ศ.1928 ในผลงานเรื่อง “theory of parlor games”

ในปี ค.ศ.1921 John Nash ได้เสนอให้เห็นว่า เกมมีขอบเขต คือมี “จุดสมดุล” ซึ่งผู้แข่งขันทุกคนจะเลือกเมื่อพิจารณาแล้วว่าได้ผลประโยชน์สูงสุด

ในช่วงปี ค.ศ.1950-1960 ทฤษฎีเกมถูกนำมาใช้อธิบายปรากฏการณ์สงคราม และการเมือง ซึ่งนอกจากใช้อธิบายพฤติกรรมการเลือกผลประโยชน์ทางเศรษฐศาสตร์แล้ว ยังถูกนำมาประยุกต์ใช้กับงานวิชาการด้าน สังคมวิทยา และจิตวิทยา

ในปี ค.ศ.1994 ทฤษฎีเกมได้รับรางวัลโนเบลสาขาเศรษฐศาสตร์ โดย Nash และเพื่อนนักวิชาการที่ร่วมพัฒนาต่อมา คือ John Harsanyi และ Reinhard Selten

2.8.1 นิยามของเกม (Definitions of games)

ทฤษฎีเกม[7] มีหลักแนวคิดอยู่ว่า เกมหนึ่งเกมประกอบด้วย ผู้เล่น (Players) จำนวนหนึ่ง โดยผู้เล่นแต่ละคนจะสามารถเลือกใช้กลยุทธ์ (Strategy) ได้หนึ่งกลยุทธ์ จากหลายๆ กลยุทธ์ที่เป็นไปได้สำหรับเกมดังกล่าว ผู้เล่นอาจเลือกใช้กลยุทธ์เดียวกันหรือต่างกันกับผู้เล่นอื่นๆ และกติกาจะกำหนดชัดเจนว่า ผลตอบแทน (payoff) ที่ผู้เล่นแต่ละคนจะได้รับเป็นเท่าใด โดยขึ้นอยู่กับกลยุทธ์ที่ผู้เล่นทุกคนเลือกใช้

โดยกลยุทธ์เด่น (Dominant strategy) หมายถึง กลยุทธ์ที่ดีที่สุด ที่จะนำไปสู่ผลลัพธ์ที่ดีที่สุดแก่ผู้เล่นแต่ละคน กลยุทธ์เด่นของแต่ละเกม อาจเป็นกลยุทธ์แบบ *ร่วมมือกัน (Cooperative game)* หรือ เกม*ไม่ร่วมมือกัน (Non-cooperative game)* ก็ได้ โดยทฤษฎีเกมอธิบายว่ากลยุทธ์เด่นจะเป็น

---

[6] Theodore L. Turocy and Bernhard von Stengel. Game Theory. CDAM Research Report LSE-CDAM-2001-09. October 8, 2001

[7] ไชยยันต์ ไชยพร (2560). Jon Ester & Rational choice theory. พิมพ์ครั้งที่ 2. สำนักพิมพ์ Way of book กรุงเทพ. มีนาคม 2560

เช่นใดนั้น ขึ้นอยู่กับข้อมูล (Information) ที่ผู้เล่นแต่ละคนได้รับทราบเกี่ยวกับผลประโยชน์ที่ตนจะได้รับ ผลประโยชน์ที่คนอื่นจะได้รับ และข้อมูลที่ผู้เล่นอื่นมีด้วย

รูปแบบทฤษฎีเกมนั้น จะสร้างแบบจำลอง (Model) หรือสมการคณิตศาสตร์ แสดงทางเลือกการตัดสินใจในสถานการณ์ต่างๆ ใด (Decision Problem) และชี้ให้เห็นว่าผู้เลือกจะตัดสินใจเลือกกลยุทธ์ที่ให้ผลตอบแทนดีที่สุด

แต่ละฝ่ายในเกมเรียกว่า "ผู้เล่น" (Player) โดยผู้เล่นมีหน้าที่ตัดสินใจเลือกกลยุทธ์ ทฤษฎีเกมตั้งข้อสมมติว่าผู้เล่นทุกฝ่ายตัดสินใจ "**อย่างเป็นเหตุเป็นผล" (Rationale)** ซึ่งผู้เล่นแต่ละฝ่ายต้องการให้ตัวเองได้รับประโยชน์สูงสุด ทฤษฎีเกมมุ่งศึกษาการตัดสินใจในสถานการณ์ที่หลายฝ่ายทำการตัดสินใจแย่งผลประโยชน์ระหว่างกัน หรือบางเกมมีผู้ตัดสินใจรายเดียว เพื่อหากลยุทธ์ที่ดีที่สุดเพื่อตนได้อรรถประโยชน์สูงสุดในการตัดสินใจกระทำการใดสักอย่าง

ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory) ที่ศึกษาเหตุผลการตัดสินใจของอาชญากร ในทางอาชญาวิทยา เมื่อนำทฤษฎีเกมมาประยุกต์ใช้ จะมีพลังในการอธิบายอย่างสูงมาก ตลอดจนสามารถใช้ทำนายปรากฏการณ์ หรือควบคุมอาชญากรรมในสังคมได้อย่างดี เมื่อปัจจัยในสถานการณ์นั้นครบ อาชญากรเห็นโอกาส อาชญากรจะตัดสินใจลงมือก่ออาชญากรรมทันที

จุดดุลยภาพ (Equilibrium) หมายถึง เกมหนึ่ง ที่ผู้เล่นทุกคนมีกลยุทธ์เด่นตัดสินใจเลือกใช้ไว้ในเกมนั้น วิธีหาจุดดุลยภาพมี 3 วิธีคือ

Iterated Elimination of Dominated Strategy คือการดูว่า มีกลยุทธ์ใดที่แย่ที่สุดหรือให้ผลตอบแทนน้อยที่สุดกว่ากลยุทธ์อื่นให้ตัดทิ้งไปเรื่อยๆ จนเหลือกลยุทธ์ที่ให้ผลตอบแทนดีที่สุด

Nash Equilibrium คือ ทางเลือกที่ดีที่สุด ภายใต้กลยุทธ์ที่คู่แข่งกำลังเล่นอยู่นั่นคือ ถ้าคู่แข่งเลือกทางเลือกไปแล้ว และผู้เล่นอีกฝ่ายไม่มีแรงจูงใจหรือกฎเกณฑ์มาบังคับให้เปลี่ยนกลยุทธ์ไปเลือกทางอื่น จุดนั้นคือ จุดสมดุลย์ของแนช หรือ Nash Equilibrium ซึ่งก็มาจากชื่อของ John Nash (ซึ่งบางเกมอาจจะมีจุด Nash Equilibrium ได้หลายจุด)

Maximin Equilibrium คือ เลือกกลยุทธ์ที่ให้ Pay off สูงสุด จากกลยุทธ์ที่ให้ Pay off ต่ำสุด นั่นคือ ให้หาค่า Min มาก่อน แล้วค่อยพิจารณาว่าค่า Min อันไหนที่มาค่ามากที่สุด (Max)

2.8.2 ชนิดของเกมพื้นฐาน

ทฤษฎีเกม มี 3 รูปแบบหลักๆ ดังนี้

2.8.2.1 Normal form Games เป็นเกมในลักษณะที่ผู้เล่นทุกคนต้องทำการตัดสินใจเลือกทางเลือกพร้อมๆ กัน เช่น เป่ายิงฉุบ เก้าอี้ดนตรี หักเรือหลบไม่ให้ชนกัน

2.8.2.2 Extensive form Games เป็นเกมในลักษณะที่มีลำดับการเล่นหรือผลัดกันเลือกทางตัดสินใจของผู้เล่น ที่ได้กำหนดกติกาไว้อย่างชัดเจน เช่น การเล่นหมากรุก การเล่นเทนนิส

2.8.2.3 Zero sum Games เป็นเกมในลักษณะที่มีฝ่ายผู้แพ้และมีฝ่ายผู้ชนะ อีกฝ่ายหนึ่งจะได้ผลประโยชน์เท่าที่อีกฝ่ายเสียผลประโยชน์หรือจะมีผู้เล่นหลายฝ่าย แต่ผู้ชนะคือผู้ที่ได้ผลประโยชน์ทั้งหมดไป ไม่มีผู้ชนะลำดับที่สอง สาม หรือสี่ เช่น การเล่นโป๊กเกอร์

โดยผลลัพธ์หรือผลประโยชน์ที่จะได้รับ จะขึ้นอยู่กับกลยุทธ์ที่ผู้เล่นทุกคนในเกมนั้นเลือก โดยประกอบไปด้วย

1. ผู้เล่น i = (Prisner, 2014...N)
2. กลยุทธ์ที่ทุกคนจะเลือกใช้ (Strategy set)
3. ฟังก์ชันผลตอบแทน (Payoff Function) จากผลลัพธ์ในแต่ละเหตุการณ์ของเกม

		นาย ข.	
		กลยุทธ์ที่ 1	**กลยุทธ์ที่ 2**
นาย ก.	**กลยุทธ์ที่ 1**	(ก.1, ข.1)	(ก.1, ข.2)
	กลยุทธ์ที่ 2	(ก.2, ข.1)	(ก.2, ข.2)

ตารางที่ 1 แมตริกซ์ผลตอบแทน (payoff matrix)

จากเกมในตารางที่ 1 สามารถอธิบายได้ว่า ผู้เล่นมี 2 ฝ่ายคือ นาย ก. และนาย ข. แต่ละคนมีทางเลือก 2 ทางเลือก จะมีเหตุการณ์เกิดขึ้นทั้งหมด 4 เหตุการณ์ คือ

- นาย ก. เลือกกลยุทธ์ที่ 1 (ก.1) แต่นาย ข. จะเลือกกลยุทธ์ที่ 1 (ข.1) หรือ กลยุทธ์ที่ 2 (ข.2) ก็ได้

บรรทัดที่ 1 ในตารางจึงเขียนได้เป็น (ก.1, ข. 1) และ (ก.1, ข.2)

- นาย ก. เลือกกลยุทธ์ที่ 2 (ก.2) แต่นาย ข. จะเลือกกลยุทธ์ที่ 1 (ข.1) หรือ กลยุทธ์ที่ 2 (ข.2) ก็ได้

บรรทัดที่ 2 ในตารางจึงเขียนได้เป็น (ก.2, ข. 1) และ (ก.2, ข.2)

ดังนั้นหาก เซ็ต เหตุการณ์ (Event) ทั้งหมดที่จะเกิดขึ้นได้ในเกมนี้จึงเขียนดังเป็น

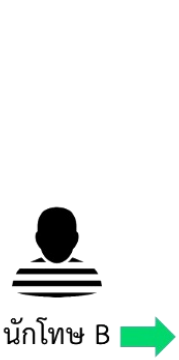
E = {(ก.1, ข.1), (ก.1, ข.2), (ก.2, ข.1), (ก.2, ข.2)}

ตัวอย่างเช่น

เกมความลำบากใจของนักโทษ (Prisoner's dilemma)

เป็นเกมที่สมมุติว่ามีนักโทษ 2 คน คือ คือนาย A และ นาย B ซึ่งเป็นเพื่อนกันมาก่อน แต่ก่ออาชญากรรมร้ายแรงจนถูกจับกุม (นักโทษคือผู้เล่น) นักโทษแต่ละคนมีทางเลือก 2 ทาง คือ “รับสารภาพหรือไม่รับสารภาพ” ทั้งคู่ตกลงร่วมมือกันว่า จะไม่รับสารภาพ ศาลจะไม่สามารถดำเนินคดีกับนักโทษทั้งสองได้เพราะไม่มีพยานหลักฐาน เรียกว่าเป็นเกมแห่งความร่วมมือ (cooperative game)

ในชั้นสอบสวน เมื่อทั้งคู่ไม่รับสารภาพ ตำรวจจึงแยกไปสอบปากคำทีละคน โดยยื่นข้อเสนอใหม่ให้นักโทษแต่ละคน ตำรวจจะกันคนที่รับสารภาพไว้เป็นพยานและปล่อยตัวไป แต่ถ้านักโทษคนหนึ่งรับสารภาพ แต่อีกคนไม่รับ จะส่งฟ้องนักโทษที่ไม่รับสารภาพ โดยมีพยานคือนักโทษอีกคนที่ยืนยันแล้ว คนที่ไม่รับสารภาพจะต้องรับโทษจำคุก 20 ปี แต่ถ้านักโทษทั้งสองคนรับสารภาพจะได้รับการลดโทษเหลือจำคุกคนละ 10 ปี สามารถเขียน “แมตริกซ์ผลตอบแทน (payoff matrix)” ในรูปแบบตารางได้ดังนี้



	รับสารภาพ	ไม่รับสารภาพ
รับสารภาพ	(-10, -10)	(0, -20)
ไม่รับสารภาพ	(-20, 0)	(0, 0)

ในวงเล็บคือ จำนวนปีที่รับโทษ

(ผลลัพธ์ของนักโทษ B, ผลลัพธ์ของนักโทษ A)

ตารางที่ 2 เกมความลำบากใจของนักโทษ (Prisoner's dilemma)

จากตารางที่ 2 จะเห็นได้ว่าเมื่อตำรวจแยกนักโทษแยกไปสอบปากคำทีละคน สถานการณ์เปลี่ยนไปผลประโยชน์ต่อรองค่อนข้างสูงระหว่างการไม่รับโทษจำคุกเลยกับจำคุก 20 ปี การตัดสินใจของนักโทษทั้งสองอยู่บนความเชื่อใจระหว่างกันและสัจจะอาจจะไม่มีในหมู่โจร

ทางเลือกทั้งหมดมี 4 ทางเลือกคือ

ก. นาย A รับสารภาพ และ นาย B รับสารภาพ ทั้งคู่ต้องได้รับโทษคนละ 10 ปี
ข. นาย A ไม่รับสารภาพ ได้รับโทษ 20 ปี แต่ นาย B รับสารภาพ ไม่ต้องได้รับโทษ
ค. นาย A รับสารภาพ ไม่ต้องได้รับโทษ แต่ นาย B ไม่รับสารภาพ ได้รับโทษ 20 ปี
ง. นาย A ไม่รับสารภาพ และ นาย B ไม่รับสารภาพ ทั้งคู่ต้องไม่ต้องได้รับโทษ

เมื่อตำรวจให้ข้อมูล (information) เพิ่มเติม ในการตัดสินใจ นักโทษย่อมเกิดความลังเลชั่งเหตุและผล เพราะทั้งสองคนจะคิดเหมือนกันว่า ถ้าหากเพื่อนเขาไม่รับสารภาพตามที่สัญญาไว้ด้วยกันก็ไม่ต้องโทษจำคุก หรือถ้าเพื่อนเขารับสารภาพ แต่ถูกกันไว้เป็นพยาน เพื่อนเขาจะไม่ต้องได้รับโทษจำคุกเลยในทุกทางเลือก เมื่อแยกกันตัดสินใจใช้กลยุทธ์ เป็นเกมแห่งความไม่ร่วมมือ (Non-cooperative game)

แต่ถ้าสารภาพทั้งคู่ โทษก็ลดเหลือ 10 ปี ลดลงถึงครึ่งหนึ่ง ถ้าเสี่ยงไม่รับสารภาพโทษจะหนักมาก เมื่อขึ้นอยู่กับความไว้ใจเพื่อน และข้อเสนอตำรวจเพื่อนไม่มีความเสี่ยงเลย ถ้าตัวเขาไม่สารภาพ

ยกเว้นทั้งคู่สารภาพพร้อมกัน ซึ่งนักโทษทุกคนจะชั่งน้ำหนักด้วยเหตุและผลว่า กลยุทธ์ใดให้ผลตอบแทนดีที่สุดสำหรับตน แม้ไม่ได้ประโยชน์สูงสุด (ไม่ได้รับโทษ) ก็ตาม

ดังนั้นทางเลือกที่พวกเขาแต่ละคนจะได้ประโยชน์ดีที่สุดคือการ “รับสารภาพ” และจุด (-10, -10) เรียกว่าเป็นจุดสมดุลของแนช (Nash’s Equilibrium) ในเกมนี้

จากตัวอย่างเกม prisoner-dilemma ข้างต้น สามารถเขียน pure strategy profile ในเทอมของ เซ็ต ทั้งหมดได้ดังนี้

S = {(สารภาพ, สารภาพ), (สารภาพ, ไม่สารภาพ), (ไม่สารภาพ, สารภาพ), (ไม่สารภาพ, ไม่สารภาพ)}

นั่นคือ สวนผสมระหว่างกลยุทธ์ของผู้เล่นทั้งสองคนที่เป็นไปได้ทั้งหมด ซึ่งก็คือช่องทั้งหมดในตารางผลตอบแทน

2.8.3 กลยุทธ์ในการเล่นเกม

กลยุทธ์ (Strategies) ในการเล่นเกม คือทางเลือกที่ให้ผลตอบแทนดีที่สุดที่ผู้เล่นแต่ละฝ่ายจะเลือกใช้ ซึ่งผู้เล่นแต่ละฝ่ายจะมีกี่ทางเลือกก็ได้ขึ้นอยู่กับความสามารถของผู้เล่นแต่ละฝ่าย กลยุทธ์ในเกมมี 2 ประเภท คือ กลยุทธ์แท้ (Pure Strategies) และกลยุทธ์ผสม (Mixed Strategies)

4 วิธีในการเลือกกลยุทธ์ คือ หลักการ Maximax, Maximin, Minimax และ Win-Win อธิบายได้ดังนี้

1. หลักการ Maximax เป็นวิธีการที่ผู้เล่นเลือกกลยุทธ์ที่ให้ผลตอบแทนมากที่สุด โดยไม่สนใจว่า อาจเกิดสิ่งเลวร้ายเกิดขึ้น แม้จะมีเพียงเล็กน้อยก็ตาม

2. หลักการ Maximin เป็นวิธีการที่ผู้เล่นที่เสียเปรียบในเกม จะเลือกกลยุทธ์แบบมองโลกในแง่ร้ายเพื่อหลีกเลี่ยงความเสี่ยงในการพ่ายแพ้ โดยไม่เลือกกลยุทธ์ที่ให้ผลตอบแทนต่ำที่สุด แต่เลือกกลยุทธ์ที่ให้ผลตอบแทนสูงสุดจากบรรดาผลตอบแทนน้อยที่สุดในแต่ละทางเลือก โดยไม่สนใจว่าโอกาสที่จะได้ผลประโยชน์นั้นมีมากแค่ไหน

3. หลักการ Minimax เป็นวิธีการที่ผู้เล่นที่ได้เปรียบในเกมเมื่อมีการพยายามแข่งขันกัน เป็นการผสมผสานระหว่างการมองโลกในแง่ดีกับแง่ร้าย โดยจะเลือกกลยุทธ์ที่มีโอกาสได้ผลตอบแทนมากที่สุดในแต่ละทางเลือก แล้วเลือกทางที่มีค่าต่ำที่สุด

4. หลักการ win-win นิยมใช้ในการเจรจาต่อรอง ในสงครามหรือในทางธุรกิจ ด้วยการเจรจาประสานความขัดแย้ง และแสวงหาผลประโยชน์ร่วมกันของทุกฝ่าย เพราะหากทั้งมุ่งเอาชนะ หรือพยายามได้เปรียบอีกฝ่ายนั้น อาจนำมาซึ่งความสูญเสียของทุกฝ่ายได้

2.8.3.1 *กลยุทธ์แท้* (Pure Strategies)

เป็นการเลือกใช้วิธีใดวิธีหนึ่งเป็นประจำ โดยไม่สนใจว่าคู่แข่งอีกฝ่ายจะใช้กลยุทธ์ใด หรือทั้งสองฝ่ายเลือกใช้วิธีใดวิธีหนึ่งเพียงวิธีเดียวอยู่ตลอดเวลา ไม่มีการเล่นหลายวิธีผสมกัน จากตัวอย่างเกมในตารางที่ 3 วิธีการคำนวณเกมใดมีกลยุทธ์แท้มีหลักการดังนี้

ค่าของเกม คำนวณได้โดยอาศัยหลักเกณฑ์ แถวนอนจะพิจารณาค่าผลตอบแทนที่น้อยที่สุดของแต่ละกลยุทธ์ และในบรรดาผลตอบแทนที่ค่าน้อยที่สุด ก็จะเลือกผลตอบแทนที่มีค่ามากที่สุดเป็นกลยุทธ์ เรียกว่า “Maximin”

ส่วนในแถวตั้งจะเลือกค่าผลตอบแทนที่มีค่ามากที่สุดในแต่ละกลยุทธ์มาพิจารณา และในบรรดาผลตอบแทนที่มีค่ามากที่สุด ก็จะเลือกค่าผลตอบแทนที่มีค่าน้อยที่สุดเป็นกลยุทธ์ เรียกว่า “Minimax” จุดที่ Maximin มีค่าเท่ากับ Minimax ค่านั้นคือค่าของเกม และนั่นคือกลยุทธ์แท้

ตัวอย่าง สมมุติการแข่งขันทางธุรกิจระหว่างนาย ก กับนาย ข

นาย ข. ↓

นาย ก. →	กลยุทธ์ที่ 1	กลยุทธ์ที่ 2	นาย ก. ใช้เกณฑ์ Maximin
กลยุทธ์ที่ 1	4	-3	-3
กลยุทธ์ที่ 2	3	-2	-2
กลยุทธ์ที่ 3	6	7	6*
นาย ข. ใช้เกณฑ์ Minimax	6*	7	

ตารางที่ 3 สมมุติการแข่งขันทางธุรกิจระหว่างนาย ก กับนาย ข

จากตารางที่ 3 ค่าของเกม คือค่าที่ Maximin มีค่าเท่ากับ Minimax ค่านั้นคือ 6 และนั่นคือกลยุทธ์แท้ทั้งนาย ก. และ นาย ข. จะเลือกใช้กลยุทธ์เพียงกลยุทธ์เดียวเท่านั้น นั่นคือ นาย ก. จะเลือกใช้กลยุทธ์ที่ 3 และนาย ข. จะเลือกใช้กลยุทธ์ที่ 1 เรียกว่าจุดศูนย์ถ่วง หรือจุดอานม้า (Saddle point)

2.8.3.2 *กลยุทธ์ผสม* (Mixed Strategies)

เป็นกลยุทธ์ที่ใช้ในการเล่นเกมระหว่างสองฝ่าย โดยผู้เล่นแต่ละฝ่ายไม่ได้เล่นกลยุทธ์ใดกลยุทธ์หนึ่งเพียงวิธีเดียว แต่จะเล่นหลายวิธีผสมกัน ต้องใช้สมการคณิตศาสตร์คำนวณอธิบายว่า ผู้เล่นจะเล่นแต่ละวิธีเป็นสัดส่วนเท่าใด และถ้าเล่นตามสัดส่วนจะมีค่าเกมเป็นเท่าใด ลักษณะสำคัญที่ชี้ให้เห็นว่าเป็นกลวิธีผสมคือ ไม่มีจุดศูนย์ถ่วง หรือจุดอานม้า (Saddle point) ไม่มีจุดที่ Maximin มีค่าเท่ากับ Minimax

วิธีการหาค่าเกม ทำได้หลายวิธี ได้แก่ คำนวณโดยใช้ความน่าจะเป็น คำนวณโดยใช้คณิตศาสตร์ คำนวณโดยกราฟ และคำนวณโดยใช้โปรแกรมเชิงเส้น

ตัวอย่าง ห้างสรรพสินค้า A และ B แข่งขันกันจัดโปรโมชั่นดึงดูดลูกค้าในแต่ละสัปดาห์ โดยใช้กลยุทธ์ลดราคาสินค้าสองประเภทสลับกัน คือ เสื้อผ้า และเครื่องใช้สำนักงาน เพื่อเรียกลูกค้าเข้าห้างสรรพสินค้าของตน

ห้างสรรพสินค้า B พบว่า ถ้าสุดสัปดาห์ใดจัดโปรโมชั่นลดราคาเสื้อผ้าเหมือนกับห้างสรรพสินค้า A จะเสียลูกค้าให้ห้างสรรพสินค้า A จำนวน 250 คน และถ้าจัดโปรโมชั่นลดราคาเครื่องใช้สำนักงานพร้อมๆ กับ ห้างสรรพสินค้า A จะเสียลูกค้าให้ห้างสรรพสินค้า A จำนวน 200 คน

แต่ถ้าจัดโปรโมชั่นลดราคาสินค้าสองประเภทนี้ไม่ตรงกัน จัดสลับกับห้างสรรพสินค้า A โดยถ้าหากห้างสรรพสินค้า A ลดราคาเครื่องใช้สำนักงาน ห้างสรรพสินค้า B จะลดราคาเสื้อผ้า ซึ่งจะดึงลูกค้าเข้ามาได้ 180 คน และถ้าห้างสรรพสินค้า A ลดราคาเสื้อผ้า ห้างสรรพสินค้า B จะลดราคาเครื่องใช้สำนักงาน ซึ่งจะดึงลูกค้าเข้ามาห้างสรรพสินค้า B ได้ 150 คน ดังตารางที่ 4

โจทย์ให้หาว่าแต่ละห้างสรรพสินค้า

1. หากลยุทธ์ที่แต่ละฝ่ายจะเลือกใช้
2. หาค่าของเกม
3. หาค่าคาดหมายโอกาสที่จะได้ลูกค้า ลด/เพิ่ม ของแต่ละฝ่าย?

ขั้นตอนแรก คำนวณหาค่าสัดส่วนการแข่งขันกันจัดโปรโมชั่นห้างสรรพสินค้า A และ B

โดยให้ **ห้างสรรพสินค้า B**

มีสัดส่วนการลดราคาเสื้อผ้า และเครื่องใช้สำนักงาน ดังนี้

P + (1-P) = 100% หรือมีค่าเท่ากับ 1

โดยที่

P คือ ความน่าจะเป็นที่ห้างสรรพสินค้า B จะใช้กลยุทธ์ลดราคาเสื้อผ้า

1 – P คือ ความน่าจะเป็นที่ห้างสรรพสินค้า B จะใช้กลยุทธ์ลดราคาเครื่องใช้สำนักงาน

และให้ **ห้างสรรพสินค้า A**

มีสัดส่วนการลดราคาเสื้อผ้า และเครื่องใช้สำนักงาน ดังนี้

Q + (1-Q) = 100% หรือมีค่าเท่ากับ 1

โดยที่

Q คือ ความน่าจะเป็นที่ห้างสรรพสินค้า A จะใช้กลยุทธ์ลดราคาเสื้อผ้า

1 – Q คือ ความน่าจะเป็นที่ห้างสรรพสินค้า A จะใช้กลยุทธ์ลดราคาเครื่องใช้สำนักงาน

ห้างสรรพสินค้า B

ห้างสรรพสินค้า A	เสื้อผ้า (P)	เครื่องใช้สำนักงาน (1-P)	ห้างสรรพสินค้า A ใช้เกณฑ์ Maximin
เสื้อผ้า (Q)	250	-150	-150
เครื่องใช้สำนักงาน (1-Q)	-180	200	-180*
ห้างสรรพสินค้า B ใช้เกณฑ์ Minimax	250	200*	

ตารางที่ 4 แสดงผลตอบแทนของห้างสรรพสินค้า A และ B

จากตารางที่ 4 ค่าของเกม ไม่มีจุดที่ค่า Maximin เท่ากับ Minimax เรียกว่าเกมนี้ไม่มีจุดศูนย์ถ่วง หรือจุดอานม้า (Saddle point) เหตุที่เลือก -180 เป็นค่าสูงสุดใน Maximin นั้น ทฤษฎีเกมให้เลือกตัวเลขที่มีค่ามากที่สุดแม้จะมีเครื่องหมายลบนำหน้า ยกเว้นในกรณีที่มีเครื่องหมายบวกลบต่างกันให้เลือกค่าบวกสูงสุด

ในการอธิบาย Payoff เจ้าของตารางมักใช้ผู้เล่นทางซ้ายมือหรือแนวนอนเป็นแนวทางอธิบายผลตอบแทนของแต่ละฝ่าย โดยอธิบายได้ดังนี้

ก. ถ้าห้างสรรพสินค้า A และ B ลดราคาเสื้อผ้าเหมือนกัน ห้างสรรพสินค้า A จะได้ลูกค้า 250 คน นั่นหมายความว่าในทางตรงข้าม ห้างสรรพสินค้า B เสียลูกค้าไป 250 คน

ข. ถ้าห้างสรรพสินค้า A และ B ลดราคาเครื่องใช้สำนักงานเหมือนกัน ห้างสรรพสินค้า A จะได้ลูกค้า 200 คน นั่นหมายความว่าในทางตรงข้าม ห้างสรรพสินค้า B เสียลูกค้าไป 200 คน

ค. ถ้าห้างสรรพสินค้า A ลดราคาเสื้อผ้า แต่ห้างสรรพสินค้า B ลดราคาเครื่องใช้สำนักงาน ห้างสรรพสินค้า A จะเสียลูกค้า 150 คน นั่นหมายความว่าในทางตรงข้าม ห้างสรรพสินค้า B จะได้ลูกค้า 150 คน

ง. ถ้าห้างสรรพสินค้า A ลดราคาเครื่องใช้สำนักงาน แต่ห้างสรรพสินค้า B ลดราคาเสื้อผ้า ห้างสรรพสินค้า A จะเสียลูกค้า 150 คน นั่นหมายความว่าในทางตรงข้าม ห้างสรรพสินค้า B จะได้ลูกค้า 150 คน

จากตารางผลตอบแทนจะเห็นได้ว่าทางเลือกของ ห้างสรรพสินค้า B จะเลือกใช้กลยุทธ์ตรงข้ามกับ ห้างสรรพสินค้า A ส่วนห้างสรรพสินค้า A จะเลือกลดราคาตามห้างสรรพสินค้า B

ห้างสรรพสินค้า B

ห้างสรรพสินค้า A		เสื้อผ้า (P)	เครื่องใช้สำนักงาน (1-P)
	เสื้อผ้า (Q)	250 x P	-150 x (1-P)
	เครื่องใช้สำนักงาน (1-Q)	-180 x P	200 x (1-P)

ตารางที่ 5 สัดส่วนผลตอบแทนของห้างสรรพสินค้า B

คำนวณสัดส่วนผลตอบแทนของห้างสรรพสินค้า B จากตารางที่ 5 ได้ดังนี้

จาก **P = (1 - P)** จะได้

$$250P - 150(1-P) = -180P + 200(1-P)$$

$$250P - 150 + 150P = -180P + 200 - 200P$$

$$400P - 150 = -380P + 200$$

$$780P = 350$$

$$P = 350/780$$

$$P = 0.45$$

ดังนั้น

$$1-P = 1- 0.45$$

$$= 0.55$$

ห้างสรรพสินค้า B

ห้างสรรพสินค้า A		เสื้อผ้า (P)	เครื่องใช้สำนักงาน (1-P)
	เสื้อผ้า (Q)	250 x Q	-150 x Q
	เครื่องใช้สำนักงาน (1-Q)	-180 x (1-Q)	200 x (1-Q)

ตารางที่ 6 สัดส่วนผลตอบแทนของห้างสรรพสินค้า A

คำนวณสัดส่วนผลตอบแทนของห้างสรรพสินค้า A จากตารางที่ 6 ได้ดังนี้

จาก **Q = (1 - Q)** จะได้

$$250Q - 180(1-Q) = -150Q + 200(1-Q)$$

$$250Q - 180 + 180Q = -150Q + 200 - 200Q$$

$$430Q - 180 = -350Q + 200$$

$$780Q = 380$$

$$Q = 380/780$$

$$Q = 0.49$$

ดังนั้น

$$1- Q = 1 - 0.49$$

$$= 0.51$$

ขั้นตอนที่สอง จากนั้นนำไปหาค่าของเกม

โดยใช้สัดส่วนผลตอบแทนของห้างสรรพสินค้า A ในการคำนวณดังนี้

ห้างสรรพสินค้า B

ห้างสรรพสินค้า A		เสื้อผ้า P = 0.45	เครื่องใช้สำนักงาน 1-P = 0.55
	เสื้อผ้า Q =0.49	250	-150
	เครื่องใช้สำนักงาน 1-Q = 0.51	-180	200

ตารางที่ 7 สัดส่วนผลตอบแทนของห้างสรรพสินค้า A

มูลค่าของเกมเท่ากับ

$$P(Q + (1 - Q)) = (1 - P)(Q + (1 - Q))$$

ได้ดังตารางที่ 8 ดังนี้

ห้างสรรพสินค้า B

ห้างสรรพสินค้า A		เสื้อผ้า P = 0.45	เครื่องใช้สำนักงาน 1-P = 0.55
	เสื้อผ้า Q =0.49	250 (0.49)	-150 (0.49)
	เครื่องใช้สำนักงาน 1-Q = 0.51	-180(0.51)	200 (0.51)

ตารางที่ 8 สัดส่วนผลตอบแทนของห้างสรรพสินค้า A

มูลค่าของเกมเท่ากับ

= {0.45 (250(0.49) – 180 (0.51))} + {0.55 (-150 (0.49) + 200(0.51))}

= 0.45 {122.5 – 91.8} + 0.55 {-73.5 + 102}

= 13.82 + 15.68

= 29.5 หรือประมาณ 30 คน

ขั้นตอนที่สาม ค่าคาดหมายโอกาสที่จะได้ลูกค้า ลด/เพิ่ม ของแต่ละฝ่าย?

ค่าของเกม ประมาณ 30 คน หมายความว่า เป็นค่าเฉลี่ยที่คาดหมายทุกการเปลี่ยนเกมว่า

ห้างสรรพสินค้า A มีค่าคาดหมายโอกาสที่จะได้ลูกค้าเพิ่ม 30 คน ต่อครั้งที่เล่นเกม

และห้างสรรพสินค้า B มีค่าคาดหมายโอกาสที่จะเสียลูกค้า 30 คน ต่อครั้งที่เล่นเกม

ดังนั้น คำแนะนำห้างสรรพสินค้า A ในการเลือกใช้กลยุทธ์

ใน 1 ปี หรือ 12 เดือน ห้างสรรพสินค้า A ควรใช้กลยุทธ์ที่ 1 และกลยุทธ์ที่ 2 ผสมกันในอัตราส่วน ร้อยละ 0.49 และ ร้อยละ 0.51 กล่าวคือ

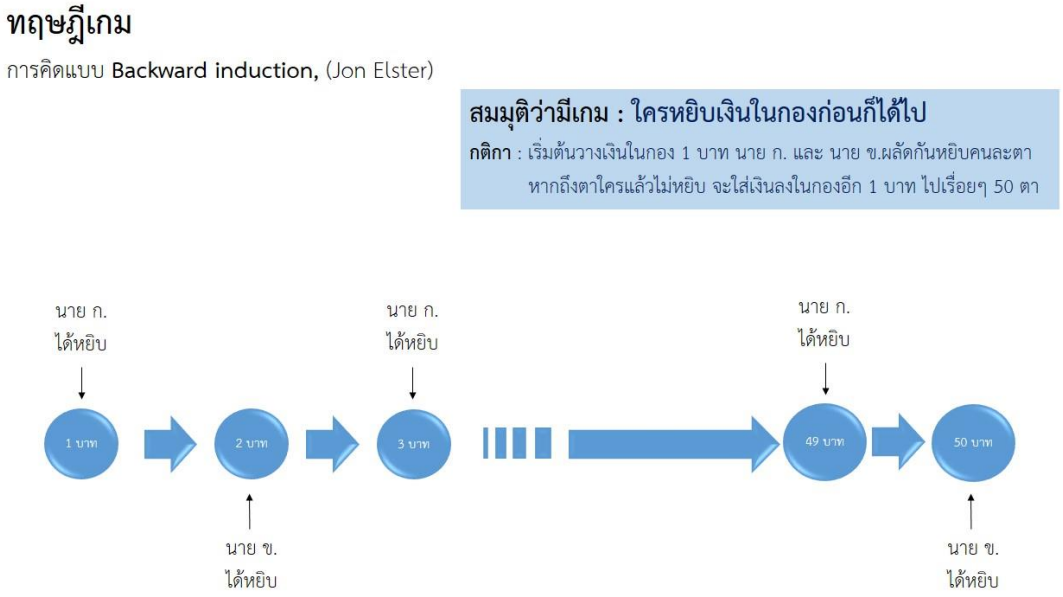
ใน 1 ปี ควรจัดให้มีการลดราคาเสื้อผ้า 5.88 เดือนหรือ 5 เดือนครึ่ง และจัดลดราคาเครื่องใช้สำนักงาน 6.12 เดือน หรือ 6 เดือนครึ่ง

2.8.3.3 *หลักการคิดย้อนกลับ (***Backward induction)** *ของทฤษฎีเกม*

หลักการคิดย้อนกลับ (Backward induction) ของทฤษฎีเกม เป็นการการให้เหตุผลแบบ โดยชี้ให้ดูผลลัพธ์ของเหตุการณ์ว่าท้ายสุดจะเกิดอะไรขึ้น แล้วคิดถอยหลังกลับมาหาปัจจุบัน เพื่อทำนายเหตุการณ์ล่วงหน้า

อาทิ มีเกมๆ หนึ่ง กรรมการกำหนดกติกาว่า จะวางเหรียญบาททีละครั้ง โดยให้ นาย ก.หยิบก่อน ถ้านาย ก. ไม่หยิบ กรรมการจะวางเหรียญเพิ่มอีก 1 บาท แล้วให้ นาย ข. หยิบ ถ้านาย ข. ไม่หยิบ กรรมการจะวางเพิ่มอีก 1 บาท ซึ่งในกองจะรวมเป็น 3 บาท แล้วให้ นาย ก. หยิบ ก่อนอีกครั้ง ถ้านาย ก. ไม่หยิบ กรรมการจะวางเพิ่มอีก 1 บาท แล้วเป็นโอกาสนาย ข. เป็นคนหยิบ....จนถึงครั้งที่ 50 เรียกว่าเกมแบบ Two-player sequential-play game: LEADER and FOLLOWER

เกมจะสลับโอกาสเช่นนี้ไปเรื่อยๆ ทั้งหมดจะมีทั้งหมด 50 ครั้ง หรือมีโอกาสที่จะมีเงินเต็มกอง 50 บาท ถามว่า เกมนี้ใครจะได้เงิน และได้เท่าไร?



รูปที่ 8 ตัวอย่างเกมหยิบเหรียญหากใช้หลักการคิดย้อนกลับของทฤษฎีเกมหาคำตอบ

Backward induction ให้ไปดูในครั้งสุดท้ายในกองที่มีเงิน 50 บาท ซึ่งจะเป็นโอกาสของ นาย ก. ได้หยิบ ดังนั้นเป็นไปไม่ได้ที่ นาย ข. จะปล่อยให้ถึงครั้งที่ 50

ดังนั้นนาย ข. จะหยิบในครั้งที่ 49 และแน่นอน นาย ก. ก็รู้ดีว่า นาย ข. จะหยิบครั้งที่ 49 นาย ก. จึงต้องยอมหยิบที่เกมครั้งที่ 48 แม้ยอดไม่เต็ม 50

เมื่อถอยหลังเหตุการณ์มาถึงครั้งที่ 1 เงินในกองมี 1 บาท และเป็นโอกาสของ นาย ก. ได้หยิบก่อน **คำตอบของเกมคือ** นาย ก. คือผู้ชนะในเกมนี้ และเขาได้เงินไป 1 บาท ในการหยิบครั้งแรก เพราะดีกว่าไม่ได้อะไรเลย

ความเกี่ยวข้องกับการวิจัย

ทฤษฎีเกมจะบอกให้เห็นว่า เมื่อมีเทคโนโลยีใดที่มีการไร้ตัวตนช่วยในการประกอบอาชญากรรม อาทิ ค้ายา การพนัน ฉ้อโกงหรือแม้แต่จ้างสังหาร โอกาสทางเทคโนโลยีการไร้ตัวตนจะสะสมความมั่งคั่งรออาชญากรอยู่และมูลค่าในอาชญากรรมแต่ละประเภทจะเพิ่มขึ้นเรื่อยๆ ดังนั้น ถ้าคุณไม่ทำเขาก็ทำและผู้ที่ลงมือก่อนจะ Maximizing utility

ทฤษฎีเกม (Game Theory) เป็นเครื่องมือวิจัยที่สำคัญที่สุดประการหนึ่ง ที่สามารถใช้ถอดรหัสการตัดสินใจของมนุษย์ มีพลังในการอธิบายการตัดสินใจและประกอบด้วยคณิตศาสตร์ความน่าจะเป็นทุกขั้นตอนในกระบวนการตัดสินใจในสถานการณ์ต่างๆ และไม่ได้อธิบายการตัดสินใจของฝ่ายหนึ่งฝ่ายใดเท่านั้น แต่สามารถอธิบายการตัดสินใจของทุกฝ่ายที่เกี่ยวข้องได้ด้วย ทฤษฎีเกมจึงเป็นเครื่องมือสำคัญที่สุดอีกชนิดหนึ่งที่ใช้สำหรับงานวิจัยทางอาชญาวิทยา

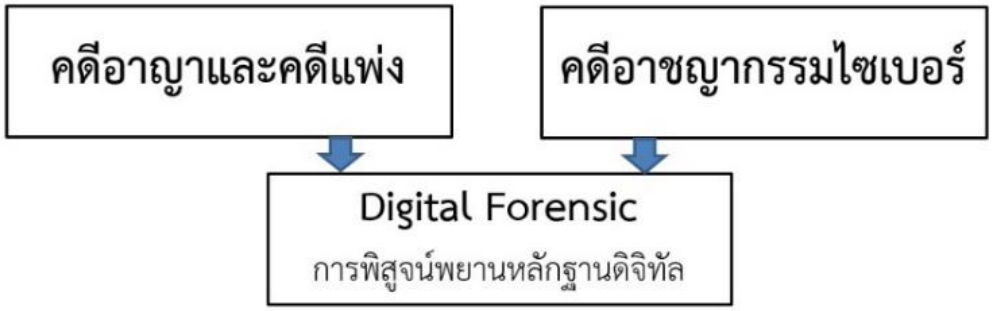
ข้อสรุปทฤษฎีเกมที่เกี่ยวข้องการวิจัยนี้ คือ เกมระหว่างอาชญากรไซเบอร์กับผู้พิทักษ์ (ตำรวจ) มีตัวแปรควบคุมสถานการณ์การเกิดอาชญากรรมไซเบอร์เป็นการไร้ตัวตนและเมื่ออาชญากรมีการคิดอย่างเป็นเหตุเป็นผล ทฤษฎีเกมจะอธิบายให้เห็นรูปแบบความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์และการไร้ตัวตนมีความสัมพันธ์กันอย่างไรตามวัตถุประสงค์การวิจัยนี้

2.9 หลักการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล (Digital Evidence and Digital Forensic)

พยานหลักฐาน ดิจิทัล หมายถึง สิ่งที่ใช้พิสูจน์ข้อเท็จจริง ส่วนพยานหลักฐานดิจิทัล (Digital Evidence) ความหมายในวิทยานิพนธ์นี้ หมายถึง “ข้อมูลคอมพิวเตอร์” ตาม พรบ. คอมพิวเตอร์ฯ และหมายถึงข้อมูลอิเล็กทรอนิกส์ ตาม พรบ. ธุรกรรมอิเล็กทรอนิกส์ฯ ที่นำมาใช้พิสูจน์ข้อเท็จจริง อาทิเช่น ข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ที่ถูกบันทึกอยู่ในรูปแบบ ธุรกรรมการเงิน (Transaction) เอกสาร (Document) เสียง (Voice) ภาพนิ่ง (Photo) ภาพเคลื่อนไหว (Video) อักษร (Letter) สื่อสังคมออนไลน์ (Social Media) ฯลฯ

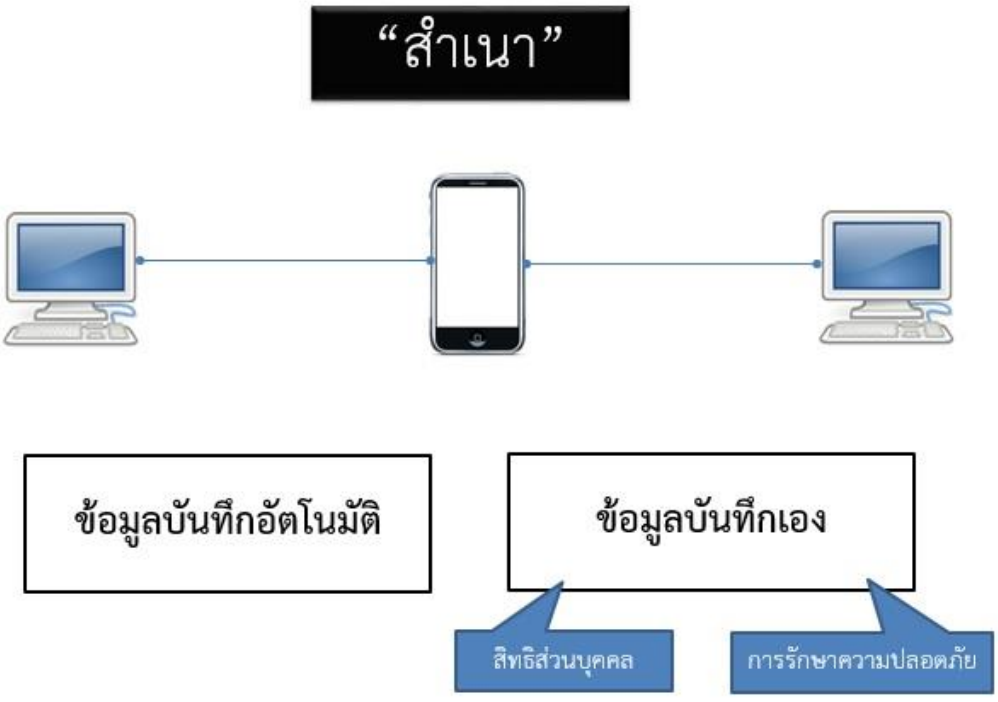
พยานหลักฐานดิจิทัล ไม่ได้อยู่ในอาชญากรรมไซเซอร์เท่านั้น แต่อยู่ทุกคดีในปัจจุบัน ทั้งคดีอาญาและคดีแพ่ง เพราะอะไรน่ะเหรอ? เพราะทุกๆ ที่เราไป ทุกๆ ที่ๆ ทำอะไรล้วนแล้วแต่ทิ้งรอยเท้า และลายนิ้วมือดิจิทัลไว้ทั้งสิ้น

การตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล ในเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ (Computer or Electronics Forensic) ปัจจุบันก็หมายถึงข้อมูลในอุปกรณ์ที่ยังไม่เชื่อมอินเทอร์เน็ต เช่น ในกล้องถ่ายรูป ในโทรศัพท์มือถือ ไฟล์เสียง ไฟล์วิดีโอ หรือแม้แต่ในเครื่องเล่นเกม



รูปที่ 9 การตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล

การตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลในเครือข่ายคอมพิวเตอร์หรือเครือข่ายโทรคมนาคม (Network Forensic) การส่งผ่านในเครือข่ายการสื่อสารนั้น คือการทำ “สำเนา” ไม่ได้ส่งไฟล์ต้นฉบับเหมือนไปรษณีย์ เป็นการทำสำเนาส่งต่อกันเรื่อยๆ เพราะฉะนั้น หากไม่สามารถหาข้อมูลที่ปลายทางได้ แต่รู้ข้อมูลที่ต้นทางหรือระหว่างทางนั่นก็สามารถพิสูจน์ได้ว่าข้อมูลปลายทางคืออะไร



รูปที่ 10 การส่งข้อมูลดิจิทัลในเครือข่ายคอมพิวเตอร์หรือเครือข่ายโทรคมนาคม

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีหลักการ 4 ข้อ ประกอบไปด้วย

- การรวบรวมพยานหลักฐานดิจิทัล (Acquisition)
- การเก็บรักษาพยานหลักฐานดิจิทัล (Preservation)
- การวิเคราะห์พยานหลักฐานดิจิทัล (Analysis)
- การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล (Presentation)

อธิบายเพิ่มดังนี้

2.9.1 การรวบรวมพยานหลักฐานดิจิทัล (Acquisition)

เป็นจุดเริ่มต้น เจ้าหน้าที่พิสูจน์หลักฐานได้สัมผัสพยานหลักฐานดิจิทัลครั้งแรก สิ่งสำคัญที่สุดคือสร้างความเชื่อมั่นในเรื่องความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมด (ยึด) หรือทำสำเนา ฮาร์ด ไดรฟ์ เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุไม่ได้ถูกเปลี่ยนแปลงแก้ไขใดๆ ทั้งสิ้น

2.9.2 การเก็บรักษาพยานหลักฐานดิจิทัล (Preservation)

จะต้องเก็บรักษาไว้ในสภาพรับฟังได้ในชั้นศาล การเก็บรักษาเป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐาน (Chain of Custody) และ Hash value กล่าวได้ว่าในหลักสากล เขาจะมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่ทุกฝ่ายยอมรับ มีบันทึกขั้นตอนการคุ้มครองพยานหลักฐาน และวิธีการเก็บรักษา ให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับอุปกรณ์มาจากจำเลย กระบวนการ Hash นั้นก็เหมือนกับ Block chain จะเป็นฮาร์ดดิสก์ทั้งลูกหรือเป็นหน่วยความจำอื่น ทำการเข้ารหัสข้อมูลซะ แบบ SHA (Secure Hash Algorithm) และเก็บกุญแจไว้ ซึ่งมีเพียงเจ้าหน้าที่เท่านั้นที่มีกุญแจอยู่จะไขเข้าไปตรวจสอบข้อมูลได้

2.9.3 การวิเคราะห์พยานหลักฐานดิจิทัล (Analysis)

พยานหลักฐานแต่ละประเภทคดีแตกต่างกัน คดี Romance scam คดีฉ้อโกง คดีคอร์รัปชั่น คดีหมิ่นประมาท เป็นต้น วิธีวิเคราะห์จึงแตกต่างกัน เครื่องมือแตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงสำคัญที่สุด ผู้เชี่ยวชาญคอมพิวเตอร์ แตกต่างกับเจ้าหน้าที่พิสูจน์หลักฐานดิจิทัล การวิเคราะห์พยานหลักฐานดิจิทัลจึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์

2.9.4 การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล (Presentation)

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล “เป็นรายงานรวมบันทึกคำให้การผู้เชี่ยวชาญ” ซึ่งอธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล

ผู้เชี่ยวชาญ คือ กุญแจสำคัญของคดี โดยเฉพาะอย่างยิ่งการนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล ไม่ใช่แค่มีความรู้อย่างเดียว ต้องมีองค์ประกอบของความน่าเชื่อถือครบถ้วนด้วย ที่สำคัญที่สุดคือทักษะการสื่อสาร ทั้งการสื่อสารกับลูกความ และผู้ที่เกี่ยวข้องกับคดี ตลอดจนการให้การต่อศาลก่อนขึ้นศาล ผู้เชี่ยวชาญต้องชี้ให้ทนายเห็นข้อได้เปรียบข้อเสียเปรียบของหลักฐานดิจิทัลที่ส่งผลต่อคดี

ผู้เชี่ยวชาญ ตามประมวลกฎหมายวิธีพิจารณาความแพ่ง และประมวลกฎหมายวิธีพิจารณาความอาญา ได้แบ่งแยกพยานหลักฐานออกตามวิธีการนำสืบเป็น 4 ประเภท คือ พยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญ มีหลักเกณฑ์ในการรับฟังพยานหลักฐานทั้ง 4 ชนิดแตกต่างกัน

พยานผู้เชี่ยวชาญ คือ พยานบุคคลซึ่งเป็นผู้มีความรู้เชี่ยวชาญในศาสตร์สาขาใดสาขาหนึ่ง ซึ่งคนธรรมดาไม่อาจเข้าใจได้ง่าย และมาเบิกความโดยการให้ความเห็น ไม่ใช่มาเล่าสิ่งที่พบเจอหรือตัดสินคดี

พยานผู้เชี่ยวชาญ (Expert Witness) บางครั้งจึงถูกเรียกว่า “พยานความเห็น” (Opinion Witness) พยานผู้เชี่ยวชาญการตรวจพิสูจน์หลักฐานดิจิทัลไม่จำเป็นต้องจบวิศวกรรมศาสตร์หรือวิทยาศาสตร์ กล่าวได้ว่าอาจจะมีน้อยด้วยซ้ำไปที่จบตรงสาขา แต่เป็นผู้ที่มีความคุ้นเคยหรือเชี่ยวชาญการตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งเป็นศาสตร์แยกต่างหากจากงานโปรแกรมมิ่งหรือเน็ตเวิร์ค

พยานผู้เชี่ยวชาญมาจาก ศาลหรือบริษัทรับจ้างที่ปรึกษา ขึ้นอยู่กับความเหมาะสม โดยประมวลกฎหมายวิธีพิจารณาความแพ่ง วางหลักไว้ว่า

ผู้เชี่ยวชาญให้อยู่ในดุลพินิจของศาล (ศาลแต่งตั้ง) แต่ศาลจะเรียกคู่ความมาให้ตกลงกันกำหนดตัวผู้เชี่ยวชาญก็ได้ แต่ศาลจะบังคับบุคคลใดให้เป็นผู้เชี่ยวชาญไม่ได้ นอกจากบุคคลนั้นได้ยินยอมลงชื่อเป็นผู้เชี่ยวชาญไว้ในทะเบียนผู้เชี่ยวชาญของศาลแล้ว

ประมวลกฎหมายวิธีพิจารณาความอาญา วางหลักไว้ว่า ผู้เชี่ยวชาญในคดีอาญาถือเป็นผู้มีความรู้ความสามารถทำนองเดียวกับพยานความเห็นในคดีแพ่ง ศาลหรือคู่ความจะขอตั้งผู้เชี่ยวชาญก็ได้และศาลอาจสั่งให้ผู้เชี่ยวชาญให้ความเห็นเป็นหนังสือก็ได้แต่ต้องมาเบิกความประกอบความเห็นเพราะคดีอาญาพยานต้องเบิกความต่อหน้าจำเลย

ในคดีอาญาจำเลยอาจว่าจ้างผู้เชี่ยวชาญตรวจสอบการพิสูจน์พยานหลักฐานดิจิทัลของเจ้าหน้าที่รัฐเพื่อให้แน่ใจว่าหลักฐานนั้นถูกต้องก็เป็นได้

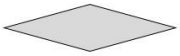
ความเกี่ยวข้องกับการวิจัย

ความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตน (Anonymous Factor) ในแต่ละยุคสมัย ขึ้นอยู่กับในสมัยนั้นการหลบพ้นจากความสามารถในการสืบสวนจับกุม (Digital Detective) และการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensic) กระทำได้ดี ส่งผลให้อาชญากรรมไซเบอร์ประเภทนั้นเติบโตอย่างรวดเร็ว

แต่เมื่อกาลเวลาผ่านไป เทคโนโลยีการสืบสวนสอบสวนทางดิจิทัลก้าวหน้า อาชญากรรมไซเบอร์ประเภทนั้นจะลดลง แต่ถ้าหากยังไม่สามารถตรวจสอบพิสูจน์และรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีเอาผิดอาชญากรไซเบอร์ได้ อาชญากรรมไซเบอร์นั้นอาจจะยังดำรงอยู่ในสังคม

2.10 การเขียนผังงาน (Flow chart) แสดงขั้นตอนการทำงานหรือกระบวนการตัดสินใจ

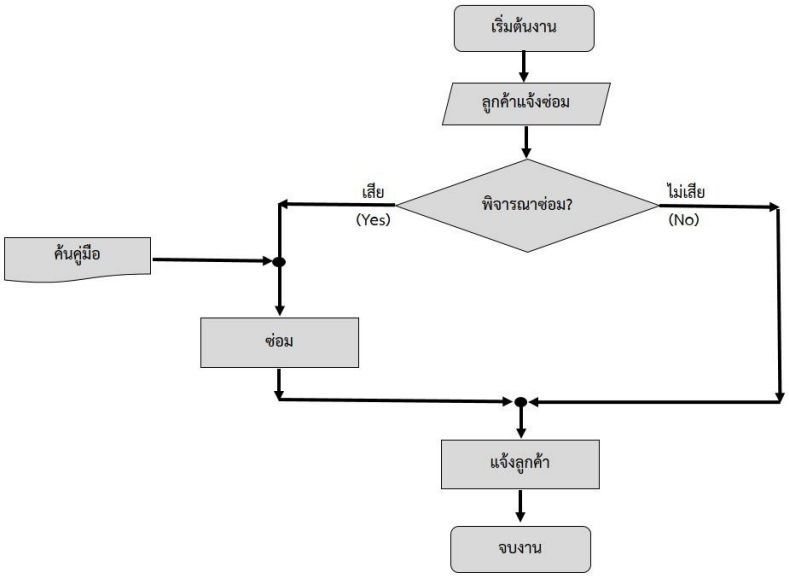
ผังงาน (Flow chart) เป็นการแสดงลำดับขั้นตอนการทำงานทางวิศวกรรมหรือกระบวนการตัดสินใจในภาษาคอมพิวเตอร์ เป็นมาตรฐานสากลที่ออกแบบโดยสถาบันมาตรฐานแห่งชาติสหรัฐอเมริกา หรือ ANSI (American National Standards Institute) เป็นการสื่อความหมายด้วยภาพทำให้ง่ายและสะดวกต่อการพิจารณาถึงลำดับขั้นตอนการทำงาน ตรวจสอบความถูกต้องของลำดับขั้นตอนได้ง่าย เพื่อสื่อสารเข้าใจไปในทิศทางเดียวกันทั่วโลก โดยมีตัวอย่างสัญลักษณ์ที่สำคัญดังนี้

สัญลักษณ์	ชื่อเรียก	ความหมาย
	จุดเริ่มต้น (Start)/จุดสิ้นสุด (Stop)	แสดงจุดเริ่มต้นของกระบวนการ และจุดสิ้นสุดของกระบวนการ
	ขั้นตอนการทำงาน (Process)	แสดงการทำงานแต่ละขั้นตอน
	การรับข้อมูล (Input)	แสดงจุดรับข้อมูลหรือรับค่าตัวแปร
	การตัดสินใจ (Decision)	แสดงจุดที่ต้องตัดสินในในกระบวนการ
	เอกสาร (Document)	แสดงจุดเก็บเอกสารหรือแหล่งความรู้
	ลูกศร (Flow line)	แสดงทิศทางการทำงาน

รูปที่ 11 ตัวอย่างสัญลักษณ์ที่สำคัญของ Flow chart ในมาตรฐาน ANSI

ที่มา ANSI

สมมุติต้องการเขียนกระบวนการทำงานและกระบวนการตัดสินใจของอู่ซ่อมรถแห่งหนึ่ง เพื่อให้ทีมงานเข้าใจตรงกัน จะเขียนเป็นตัวอย่างได้ดังรูปที่ 12 นี้



รูปที่ 12 ตัวอย่างกระบวนการทำงานและกระบวนการตัดสินใจของอู่ซ่อมรถแห่งหนึ่ง

ความเกี่ยวข้องกับการวิจัย

การเขียนผังงาน (Flow chart) แสดงขั้นตอนการทำงานหรือกระบวนการตัดสินใจ จะนำมาใช้เป็นเครื่องมือสำคัญในการแสดงสัญลักษณ์ให้เห็นกระบวนการคิดอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์เมื่อค้นพบปัจจัยการไร้ตัวตนในเทคโนโลยีใดที่มีเทคนิคสามารถนำมาใช้ประกอบอาชญากรรมได้

2.11 แนวคิดศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์

ระบบศาลตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 3 บัญญัติว่า “อำนาจอธิปไตยเป็นของปวงชนชาวไทย พระมหากษัตริย์ผู้ทรงเป็นประมุข ทรงใช้อำนาจนั้นทางรัฐสภา คณะรัฐมนตรี และศาล ตามบทบัญญัติแห่งรัฐธรรมนูญ รัฐสภา คณะรัฐมนตรี ศาล องค์กรอิสระ และหน่วยงานของรัฐ ต้องปฏิบัติหน้าที่ให้เป็นไปตามรัฐธรรมนูญ กฎหมาย และหลักนิติธรรม เพื่อประโยชน์ส่วนรวมของประเทศชาติและความผาสุกของประชาชนโดยรวม”

บทบัญญัติดังกล่าวได้แบ่งอำนาจอธิปไตยออกเป็น 3 ทาง ในอำนาจตุลาการนั้นพระมหากษัตริย์ทรงทรงมอบให้ศาลเป็นผู้ใช้อำนาจตุลาการวินิจฉัยชี้ขาดข้อพิพาทที่เกิดขึ้นเป็นคดีมาสู่ศาลและเป็นหน้าที่ของศาลที่จะต้องปฏิบัติหน้าที่ดังกล่าวให้สำเร็จลุล่วงไปตามหลักนิติธรรม

รัฐธรรมนูญฯ กำหนดให้มี 4 ศาล คือ ศาลรัฐธรรมนูญ ศาลปกครอง ศาลทหาร และศาลยุติธรรม โดยศาลยุติธรรมตามบทบัญญัติตามพระธรรมนูญศาลยุติธรรม พ.ศ. 2543 ให้มีศาลยุติธรรมมีอยู่ทั่วราชอาณาจักร และระบบศาลยุติธรรมแบ่งออกเป็น 3 ชั้น คือ ศาลขั้นต้น ศาลอุทธรณ์ และศาลฎีกา

ศาลยุติธรรมมีพัฒนาการที่ต่อเนื่องในการเพิ่มประสิทธิภาพเพื่ออำนวยความยุติธรรมและการพิจารณาพิพากษาคดีดังปรากฏจากการเพิ่มจำนวนศาล เช่น การตั้งแผนกเพื่อพิจารณาพิพากษาคดีพิเศษขึ้นในศาล การจัดตั้งศาลชำนัญพิเศษ และศาลพิเศษ การนั่งพิจารณาคดีเป็นองค์คณะและการสนับสนุนให้มีการระงับข้อพิพาท การไกล่เกลี่ยข้อพิพาท การอนุญาโตตุลาการ เป็นต้น

ศาลพิเศษ และศาลชำนัญพิเศษ ในระบบกฎหมายไทย มีศาลพิเศษเพียง 1 ศาล คือ ศาลเยาวชนและครอบครัว ส่วนศาลชำนัญพิเศษ ปัจจุบันมีอยู่ 4 ศาล คือ ศาลภาษีอากรกลาง ศาลล้มละลายกลาง ศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง และศาลอุทธรณ์คดีชำนัญพิเศษ แบ่งออกเป็น 5 แผนก คือ แผนกคดีทรัพย์ทางปัญญาและการค้าระหว่างประเทศแผนกคดีภาษีอากร แผนกคดีแรงงาน แผนกคดีล้มละลาย และแผนกคดีเยาวชนและครอบครัว

ศาลชำนัญพิเศษ เป็นศาลที่จัดตั้งขึ้นตามพระราชบัญญัติเฉพาะศาลนั้น ด้วยเหตุผลที่คดีบางประเภทต้องอาศัยความรู้และความเชี่ยวชาญเฉพาะเรื่องแตกต่างจากคดีแพ่งและคดีอาญาทั่วไป ควรได้รับการพิจารณาโดยผู้พิพากษาที่มีความรู้และความชำนาญในคดีพิพาทเฉพาะเรื่องนั้นหรือมีบุคคลที่มีความรู้และ ความเข้าใจในคดีเฉพาะเรื่องนั้นมาเป็นผู้พิพากษาสมทบร่วมวินิจฉัยคดี

เดิมทีสหภาพโทรคมนาคมระหว่างประเทศหรือ International Telecommunication Union (Development) เป็นองค์กรชำนัญพิเศษแห่งสหประชาชาติที่คอยให้แนะนำแก่ประเทศสมาชิกในการกำกับดูแลกิจการสื่อสารของชาติ ได้ตั้งคณะทำงาน (Working group) ในเดือนพฤษภาคม ค.ศ. 2007 กำหนดวาระสำคัญระดับนานาชาติด้านอาชญากรรมไซเบอร์หรือ Global Cybercrime Agenda (GCA) และได้พัฒนามาเป็นคณะทำงานระดับโลกที่มีผู้เชี่ยวชาญทักษะสูงขึ้นหรือ High-Level Experts Group (HLEG) นับร้อยคนจากทั่วโลกมากำหนดยุทธศาสตร์ร่วมกันออกมาเป็นรายงาน Global Strategic Report ในปี ค.ศ. 2008 ว่าด้วยเรื่องความมั่นคงปลอดภัยไซเบอร์และกฎหมายอาชญากรรมไซเบอร์ (cybersecurity and cybercrime legislations)

องค์การสหประชาชาติได้ริเริ่มศึกษาผลกระทบจากอาชญากรรมไซเบอร์อย่างจริงจังในปี ค.ศ. 2010 ในการประชุม United Nations Congress on Criminal Prevention and Criminal Justice ครั้งที่ 12 ที่กรุงซัลวาดอร์ ประเทศบราซิล บรรลุผลเป็น Salvador Declaration Article 42 เพื่อเชื้อเชิญ คณะกรรมาธิการว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา (Commission on Crime Prevention and Criminal Justice) ซึ่งเป็นคณะกรรมาธิการภายใต้คณะมนตรีเศรษฐกิจและสังคม (Economic and Social Council – ECOSOC) ของสหประชาชาติ ให้เปิดประชุมคณะทำงานผู้เชี่ยวชาญที่มาจากแต่ละประเทศสมาชิกเพื่อศึกษาปัญหาของอาชญากรรมไซเบอร์และแนวทางในการเตรียมรับปัญหา และคำแนะนำ (Recommendations) ได้รับการยอมรับในการประชุมสมัชชาสหประชาชาติ (United Nations General Assembly) เรียกว่าเป็น resolution 65/230

องค์กรภาคเอกชนในนาม The EastWest Institute (EWI) เป็นกลุ่มผู้เชี่ยวชาญกฎหมายที่ไม่ใช่ตัวแทนภาครัฐ (Non-Govermment) ได้ตั้งคณะทำงานกฎหมายอาชญากรรมไซเบอร์ (Cybercrime Legal Working Group) โดยมีผู้พากษาชาวนอร์เวย์ สเติร์น สชโจลเบิร์ก (Stein Schjolberg) เป็นประธานคณะทำงาน ซึ่งคณะทำงานนี้ได้ทำงานเชิงรุกในการร่างพันธกรณีระหว่างประเทศและคำแนะนำ (Recommendations) ที่จะนำไปสู่กลไกกฎหมายที่มีศักยภาพให้ประเทศสมาชิกควรจะนำไปใช้ปฏิบัติในการรับมือความมั่นคงปลอดภัยไซเบอร์และอาชญากรรมไซเบอร์

สหรัฐอเมริกาและสหภาพยุโรปก็ได้ตั้งคณะทำงานขึ้นเช่นกันในเดือน พฤศจิกายน ค.ศ.2010 ชื่อคณะทำงาน Cybersecurity and Cybercrime at the EU-US คณะทำงานชุดนี้ได้ร่างแนว

ทางการประสานความร่วมมือในการแก้ไขปัญหาเรื่องความมั่นคงปลอดภัยไซเบอร์และอาชญากรรมไซเบอร์

สเติร์น สชโจลเบิร์ก (Stein Schjolberg[8], 2012) ได้ให้ความเห็นปัญหาสำคัญมากในทางปฏิบัติร่วมกันในการกำหนดนิยามตามกฎหมาย เพราะแต่ละเป็นมีระบบกฎหมายไม่เหมือนกันและกระบวนยุติธรรมไม่เหมือนกันบางประเทศเป็นกฎหมายลายลักษณ์อักษร (Civil law) และบางประเทศเป็นกฎหมายจารีตประเพณี (Common law) นอกจากนั้น สเติร์น สชโจลเบิร์ก เป็นผู้ริเริ่มเสนอแนวคิดการจัดตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ระหว่างประเทศ An International Criminal Tribunal for Cyberspace (ICTC) โดยให้หลักการและเหตุผลว่า อาชญากรไซเบอร์สามารถข้ามพรมแดนประเทศก่อคดีอาชญากรรมได้อย่างไร้ขอบเขต ขณะที่การสืบสวนและการดำเนินคดีข้ามพรมแดนระหว่างประเทศนั้นเป็นอุปสรรคใหญ่หลวง จึงควรจะมีพันธกรณีระหว่างประเทศเพื่อลงฉันทามติร่วมกันในการก่อตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ระหว่างประเทศ โดยเสนอให้มีสำนักงานอยู่ที่กรุงเฮก ประเทศเนเธอร์แลนด์หรือที่ประเทศสิงคโปร์หรือจะเป็นศาลชั่วคราวเฉพาะกิจจัดตั้งเป็นกรณี (ad-hoc) เป็นข้อเสนอทางเลือก

สเติร์น สชโจลเบิร์ก และคณะได้ร่างเป็นข้อเสนอพันธกรณีระหว่างประเทศในการจัดตั้งศาลอาญาระหว่างประเทศหรือศาลยุติธรรมไซเบอร์ (Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace) และได้แก้ไขร่างถึง 9 ครั้ง มีทั้งหมด 34 มาตรา โดยสาระสำคัญต้องการให้มีหลักกฎหมายอาชญากรรมไซเบอร์ระหว่างประเทศที่ควรจะนำไปใช้เป็นเป็นหลักปฏิบัติในการสืบสวนคดีอาญาและการดำเนินคดีอาญาระหว่างประเทศ

สเติร์น สชโจลเบิร์ก ได้ยกประเด็นเฉพาะเรื่อง Cloud computing ให้เห็นชัดว่า ข้อมูลในระบบ Cloud (ระบบที่เซิฟเวอร์มีการกระจายไว้หลายแห่งในแต่ละทวีปเพื่อสำรองข้อมูลและกระจายการให้บริการในพื้นที่ได้รวดเร็ว) จึงไม่สามารถระบุหลักดินแดน (เขตอำนาจศาล) ว่าเป็นอาชญากรรมที่เกิดขึ้นในประเทศใดได้ และปัญหานี้จะแก้ได้เมื่อทุกประเทศลงพันธะกรณีร่วมกันมอบอำนาจอธิปไตยบางส่วนมาใช้ดำเนินคดีแบบไร้พรมแดนเช่นเดียวกับอาชญากรรมไซเบอร์

ในระหว่างที่ประเทศสมาชิกในองค์การสหประชาชาติหรือองค์กรต่างๆยังไม่ได้ลงพันธกรณีจนเกิดการตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ระหว่างประเทศขึ้นมาเป็นทางการ แต่ละประเทศกลับมีข่าวการตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ในหลายประเทศ เช่น เว็บไซต์

[8] Judge Stein Schjolberg (2012). An International Criminal Tribunal for Cyberspace (ICTC). Recommendations for potential new global legal mechanisms against global cyber-attacks and other global cybercrimes. A paper for the East West Institute (EWI) Cybercrime Legal Working Group. Available from URL: https://www.cybercrimelaw.net/documents/ICTC.pdf

รัฐบาลอังกฤษได้เผยแพร่ Press release เรื่อง World-class fraud and cybercrime court approved for London's Fleetbank House site [9] ความว่า ประธานศาลสูงสุด (Lord Chancellor) ได้ประกาศจัดตั้งศาลชำนัญพิเศษเมื่อวันที่ 4 กรกฎาคม พ.ศ.2557 เพื่อพิจารณาคดีอาชญากรรมไซเบอร์ การฉ้อโกง และอาชญากรรมเศรษฐกิจ โดยอังกฤษเป็นผู้นำในการพัฒนาระบบกฎหมายของโลก

ประเทศฟิลิปปินส์ มีความก้าวหน้าด้านงานยุติธรรมในคดีอาชญากรรมไซเบอร์อย่างมากในอาเซียน ศาลสูง (Supreme court) ได้จัดตั้ง ศาลอาชญากรรมไซเบอร์ (Cybercrime court) อย่างเป็นทางการเมื่อ เดือนพฤศจิกายน พ.ศ.2559 โดยมีรากฐานมาจากพระราชบัญญัติ Cybercrime Prevention Act of 2012 ที่มีเจตนารมณ์ต้องการให้มีสถาบันที่ชำนัญเฉพาะทางการแก้ปัญหาอาชญากรรมไซเบอร์ในอนาคต

เจย์ แชนคาร์ (Jay Shankar, 2018) ได้เขียนบทความเรื่อง 'India may require special courts to try cybercrime cases'[10] ความว่า อาชญากรรมไซเบอร์ในอินเดียพุ่งสูงขึ้นตั้งแต่เรื่องความมั่นคงปลอดภัยไซเบอร์ไปจนการฉ้อโกงออนไลน์ในหลายรูปแบบ กระบวนการยุติธรรมยังอ่อนแอสำหรับการพิทักษ์ประชาชนจากอาชญากรรมไซเบอร์

ความเกี่ยวข้องกับการวิจัย

ปัญหาในการสืบสวนจับกุมและรวบรวมพยานหลักฐานเพื่อดำเนินคดีอาชญากรรมไซเบอร์ในทางปฏิบัติเป็นปัญหาเหมือนกันไปทั่วโลก โดยเฉพาะการก่ออาชญากรรมไซเบอร์ข้ามพรมแดน ความเกี่ยวข้องในการวิจัยนี้คือเรื่องการสืบสวนจับกุมและรวบรวมพยานหลักฐานเพื่อดำเนินคดีอาชญากรรมไซเบอร์อันเป็นปัจจัยการไร้ตัวตนที่ผู้วิจัยตั้งข้อสังเกตไว้ ดังนั้นแนวทางการแก้ไขปัญหากระบวนการยุติธรรมด้านอาชญากรรมไซเบอร์จึงมี 2 แนวทางคือ การลงพันธกรณีตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ระหว่างประเทศขึ้นและการตั้งศาลชำนัญพิเศษด้านอาชญากรรมไซเบอร์ในประเทศไทย

---

[9] Ministry of Justice and HM Courts & Tribunals Service (2018). World-class fraud and cybercrime court approved for London's Fleet bank House site. Published 4 July 2018. Available from URL : https://www.gov.uk/government/news/worldclass-fraud-and-cybercrime-court-approved-for-londons-fleetbank-house-site

[10] Jay Shankar (2018). India may require special courts to try cybercrime cases. The Hindu. SEPTEMBER 29, 2018. Available form URL : https://www.thehindu.com/business/india-may-require-special-courts-to-try-cybercrime-cases/article25083785.ece

2.12 บทความวิชาการเรื่อง การพบปรากฏการณ์ผลกระทบของการไร้ตัวตนในกฎหมายและการจัดระเบียบในโลกไซเบอร์ (Phenomenal exploration into impact of anonymity on law and order in cyberspace)

บทความนี้เขียนโดย ซิงกาน ลี (Xingan Li, 2014)[11] แห่ง Tallinn University Law School ประเทศ เอสโตเนีย ตีพิมพ์ในวารสาร Criminology & Social Integration: journal for criminology, penology and behaviour problems เมื่อวันที่ 28 พ.ย. 2557 ขณะที่ระบบเทคโนโลยีสารสนเทศกำลังจัดเตรียมความสะดวกสบายให้มนุษย์ก้าวเข้าสู่สังคมยุคใหม่ แต่ปัญหาหนึ่งที่สำคัญมากในการจัดระเบียบสังคม (Social order) นั่นก็คือ “การไร้ตัวตน” ในโลกไซเบอร์ (anonymity of cyberspace) ซึ่งนับวันเป็นปัญหาที่สำคัญมากขึ้นเรื่อยๆ ในการตรวจสอบค้นหาตัวตน (identity tracing) ผู้ที่สร้างปัญหา ทั้งในการสืบสวนและสอบสวน (detection and investigations)

การไร้ตัวตนในโลกไซเบอร์ (anonymity) เป็นปัญหาสำคัญที่สุดที่ทำให้เกิดแรงจูงใจในการก่ออาชญากรรม (Critical impacts on criminal motivation) และเกิดเป็นปรากฏการณ์รูปแบบใหม่ในการตกเป็นเหยื่อ (phenomena of victimization) ซึ่งการไร้ตัวตนเป็นปัญหาสำคัญมากในการบังคับใช้กฎหมายกับช่องว่างทางเทคโนโลยี

บทความวิชาการนี้ได้ชี้ให้เห็นถึง ศักยภาพของอาชญากรที่ไร้ตัวตนในโลกไซเบอร์ และผลกระทบของการไร้ตัวตนในโลกไซเบอร์ต่อกระบวนการทางกฎหมาย ผลกระทบต่อการจัดระเบียบสังคม ผลกระทบต่อสังคมข้อมูลข่าวสาร

ปัจจุบันมีประชากรโลกราว 3,000 ล้านคนหรือ 42% ของประชากรโลก (Internet World Stats 2014) เข้าร่วมเครือข่ายอินเทอร์เน็ตเพื่อใช้งานส่งและรับข้อมูลข่าวสารจำนวนมหาศาลมาก ซึ่งในนั้นมีทั้ง สแปม ที่ทำลายระบบและข้อมูล อีกทั้งข้อมูลส่วนบุคคลมีความเสี่ยงมากขึ้นที่ความเป็นส่วนตัวหายไป

แม้การไร้ตัวตนในโลกไซเบอร์ (anonymity) เป็นเรื่องที่ผู้ใช้ทั่วไปรู้สึกพึงพอใจ แต่ในด้านลบการไร้ตัวตนในโลกไซเบอร์ (anonymity) การมองไม่เห็นตัวตน (invisibility) และปัญหาการติดตามผู้ก่ออาชญากรรม (concealment of criminal traces) ยังคงเป็นปัญหาที่กลืนไม่เข้าคายไม่ออก

---

[11] Xingan Li (2014), Phenomenal exploration into impact of anonymity on law and order in cyberspace. Criminology & Social Integration: journal for criminology, penology and behavior problems. 28 November 2014.

อาชญากรรมไซเบอร์แตกต่างจากอาชญากรรมดั้งเดิม ทั้งการสร้างความเสียหายกว้างขวางมากขึ้น และซับซ้อนมากขึ้น ซึ่งองค์ประกอบสำคัญคือ การไร้ตัวตน การปกปิดซ่อนเร้น และการพรางตัวให้มองไม่เห็น เป็นปัญหาในการติดตามหาตัวตนผู้กระทำความผิด ซึ่งเป็นอุปสรรคสำคัญในการสืบสวน และการดำเนินคดี

ตัวอย่างเช่น สแปม (Spam) ในอีเมล์ ทั้งถูกใช้ในการทำตลาด และทางการเมือง สแปม เป็นการละเมิดความเป็นส่วนตัวที่เราไม่ต้องการรับข้อมูลข่าวสาร แต่ถูกส่งมาจากผู้ที่ไร้ตัวจน และไม่สามารถเอาผิดได้ สแปมไม่ได้มาทาง อีเมล์ ส่วนตัวเท่านั้น แต่รวมถึง อีเมล์ ขององค์กรหรือบริษัท หากมีปริมาณมหาศาลย่อมส่งผลกระทบต่อการใช้งานทำให้เกิดความเสียหาย

การก่อการร้ายทางไซเบอร์ (cyber terrorism) อย่างไรก็ตามการก่อการร้ายทางไซเบอร์ไม่ได้เกิดขึ้นจริงอย่างที่หลายคนกังวลในปลายศตวรรษที่ 20 แต่เหตุผลมากมายที่จะเป็นไปได้ในการเกิดการก่อการร้ายสมัยใหม่ (Weimann 2004: 6) เพราะต้นทุนถูกกว่า หลบซ่อนตัวตนให้รอดพ้นจากการสืบสวนจับกุมได้ดีกว่า และสร้างความเสียหายในวงกว้างระดับโลกได้มากกว่า การก่อการร้ายทางไซเบอร์ไม่มีกำแพงเมืองกั้น ไม่มีเส้นชายแดน

ขณะที่อาชญากรรมที่เกิดขึ้นจริง การคุกคามและการฆาตกรรม เกิดจากโลกไซเบอร์ ในปี 2005 กระทรวงความปลอดภัยสาธารณะของประเทศจีน (China Ministry of Public Security) สืบสวนพบว่า เหยื่อราว 1,000 คดี ถูกสังหารจากอาชญากรที่ติดตามเหยื่อจากอินเทอร์เน็ต (Yi 2006) โดยอาชญากรค้นหา ติดตาม สะกดรอยตามเหยื่อด้วยเทคโนโลยีอินเทอร์เน็ต และหลบซ่อนตัวให้ไร้ตัวตนจนเหยื่อไม่รู้ตัว

ในทางกลับกัน ยังคงเป็นที่ถกเถียงกันตลอดมาถึงสถานะทางกฎหมายกับการไร้ตัวตนในโลกไซเบอร์ (legal status of cyber anonymity) เพื่อเป็นการป้องกันอาชญากรรมสังคมควรมีทฤษฎีทางอาชญาวิทยามาช่วยอธิบายให้เห็นความสำคัญในการแก้ไขปัญหาการไร้ตัวตนในโลกไซเบอร์ ซึ่งนับวันภัยคุกคามจากการไร้ตัวตนในโลกไซเบอร์กำลังเผชิญหน้าสร้างความยุ่งยากให้กระบวนการยุติธรรมทางอาญาอย่างมาก

Xingan Li ยังชี้ให้เห็นว่า การไร้ตัวตนในโลกไซเบอร์เป็นสิ่งที่ผู้ใช้รู้สึกนิยมที่สุดในการใช้งานอินเทอร์เน็ต ในช่วงที่ผ่านมาผู้ใช้อินเทอร์เน็ตจำนวนมากมักเชื่อมต่ออินเทอร์เน็ตจาก ร้านอินเทอร์เน็ต และห้องสมุด (cyber cafés or libraries) ซึ่งทำให้พวกเขารู้สึกว่าสามารถเข้าไปใช้งานอินเทอร์เน็ตอย่างไร้ตัวตน (ไม่ใช่เลขหมาย IP ที่บ้านหรือจากโทรศัพท์เคลื่อนที่ของตน) โดยเปรียบเทียบให้เห็นว่าที่ประเทศจีน cyber cafés เกิดขึ้นจำนวนมากและเป็น Third space ของเด็กและเยาวชน นอกจากบ้านและโรงเรียน ซึ่งการใช้งานอินเทอร์เน็ตจากห้องสมุดโรงเรียนเป็นเรื่องที่ไม่

สะดวกสำหรับพวกเขา และคดีเจาะระบบ (Hacking) จำนวนมากที่เพิ่มขึ้น เมื่อสืบสวนพบว่ามาจาก cyber cafés

คดีเจาะระบบคอมพิวเตอร์ (Hacking) จำนวนมากที่ต้นทางมาจาก cyber cafés นั่นคือพฤติการณ์ที่อาชญากรไซเบอร์ต้องพยายามหลบซ่อนตัวตนให้ได้มากที่สุดก่อนก่ออาชญากรรม

ความเกี่ยวข้องกับการวิจัย

ชิงกาน ลี เห็นว่าการไร้ตัวตนในโลกไซเบอร์นับวันเป็นปัญหาที่สำคัญมากขึ้นเรื่อยๆ ในการตรวจสอบค้นหาตัวตนผู้ที่สร้างปัญหา ทั้งในการสืบสวนและสอบสวน (detection and investigations) เป็นความเห็นที่สอดคล้องกับการวิจัยและการไร้ตัวตนในโลกไซเบอร์เป็นปัญหาสำคัญที่สุดที่ทำให้เกิดแรงจูงใจในการก่ออาชญากรรมและเกิดเป็นปรากฏการณ์รูปแบบใหม่ในการตกเป็นเหยื่อ อีกทั้งการไร้ตัวตนเป็นปัญหาสำคัญมากในการบังคับใช้กฎหมายกับช่องว่างทางเทคโนโลยี

บทความวิชาการนี้ได้ชี้ให้เห็นถึง ศักยภาพของอาชญากรที่ไร้ตัวตนในโลกไซเบอร์และผลกระทบของการไร้ตัวตนในโลกไซเบอร์ต่อกระบวนการยุติธรรมทางอาญา ผลกระทบต่อการจัดระเบียบสังคมและผลกระทบต่อสังคมจากข้อมูลข่าวสาร

2.13 วิทยานิพนธ์เรื่อง การไร้ตัวตน อาชญากรรมไซเบอร์ และการเกี่ยวข้องกับการเงินดิจิทัล (Anonymity, Cybercrime and the Connection to Cryptocurrency)

วิทยานิพนธ์เรื่องนี้เขียนโดย เจสซี่ เบรย์ (Jesse, 2016)[12] แห่งมหาวิทยาลัย Eastern Kentucky University ประเทศสหรัฐอเมริกา ในปี ค.ศ. 2016 ได้ให้นิยาม Anonymity หมายถึงคุณภาพหรือสถานะภาพการเป็นผู้ที่คนส่วนมากไม่รู้จักตัวตน “the quality or state of being unknown to most people” (Anonymity, Merriam Webster, 2014)

องค์กรก่อการร้าย (terrorist organizations) แม้ยังไม่เปลี่ยนรูปแบบการก่อการร้ายจากวิธีการวางระเบิดหรือการใช้ความรุนแรง แต่การใช้เทคโนโลยีอินเทอร์เน็ตช่วยให้การติดต่อสื่อสารระหว่างเครือข่ายก่อการร้ายทำได้ง่ายดายขึ้นด้วยการไร้ตัวตนในโลกไซเบอร์ (Anonymity) อีกทั้งยังช่วยให้องค์กรก่อการร้ายประสบความสำเร็จอย่างสูงในการสร้างเครือข่าย องค์กรก่อการร้ายสร้างเว็บไซต์มากมายใช้โฆษณาชวนเชื่อ บอกเล่าเรื่องราวตั้งแต่ประวัติศาสตร์ขององค์กร ผู้ก่อการร้ายที่มี

[12] Jesse Bray (2016). Anonymity, Cybercrime and the Connection to Crypto currency. Eastern Kentucky University. August, 2016.

ชื่อเสียงขององค์กรหรือผู้ก่อตั้ง อุดมการณ์ และความสำเร็จที่ผ่านมา เพื่อใช้ประโยชน์ในการคัดเลือกคนเข้าร่วมองค์กร

กลุ่มก่อการร้าย Hezbollah และ Hamas มักใช้อินเทอร์เน็ตในการเผยแพร่ถกแถลงถึงผลงานการโจมตีเหยื่อเป้าหมาย และผลงานจำนวนศพการพลีชีพต่อจำนวนผลการเสียชีวิตของเหยื่อที่ถูกสังหาร

Dark-net และ deep-web (The Onion Router) คือเครื่องมือสำคัญที่องค์กรก่อการร้ายใช้โฆษณาชวนเชื่อ และคัดเลือกคนเข้าร่วมองค์กร เพราะช่วยปิดบังตัวตนเลขหมาย IP ของเจ้าของเว็บไซต์หรือองค์กรก่อการร้าย และปิดบังผู้เข้าเยี่ยมชมเว็บไซต์ เป็นการง่ายดายในการสร้างการไร้ตัวตนในโลกไซเบอร์ (Anonymity)

ใน deep web นอกจากเครือข่ายก่อการร้ายและสินค้าผิดกฎหมายมากมาย ยังมีบริการขายบริการ การไร้ตัวตนในโลกไซเบอร์ (Anonymity) ที่มีความซับซ้อนในการปิดบังตัวตนมากยิ่งขึ้นไปอีก (high degree of anonymity) ทำให้ผู้ใช้มั่นใจมากขึ้นในการสนทนาในเว็บบอร์ดหรือการสั่งสินค้าโดยจ่ายค่าบริการด้วย Bitcoins หรือ crypto currencies อื่น

Crypto currency โดยเฉพาะสกุล Bitcoin ดึงดูดให้ผู้ใช้ยาเสพติดเข้ามาซื้อขายใน deep web นอกจาก deep-web (The Onion Router) ช่วยให้เกิดการไร้ตัวตนในโลกไซเบอร์ (Anonymity) ในการท่องเว็บผิดกฎหมายแล้ว การทำธุรกรรมซื้อขายด้วย Bitcoin ยังช่วยปิดบังตัวตนและเส้นทางการเงินได้อีกด้วย ซึ่งระบบการเงินแบบเก่าทำไม่ได้

อีกทั้งไม่สามารถใช้กฎหมายการฟอกเงินกำกับดูแล Bitcoin ได้ เนื่องจากว่า Bitcoin ไม่ใช่เงินที่มีองค์ประกอบตามกฎหมายระบุ เมื่อไม่ใช่เงินก็ไม่เข้าหลักเกณฑ์ที่กฎหมายให้อำนาจไว้

ดังนั้นการไร้ตัวตนในโลกไซเบอร์ (Anonymity) เป็นภัยคุกคามจากอาชญากรรมออนไลน์ มิใช่เพียงแค่ปิดบังเลขหมาย IP ของเว็บไซต์ทำให้รัฐปิดกั้นไม่ได้ และไม่สามารถตรวจสอบเลขหมาย IP ของผู้เข้าชมเว็บไซต์ได้แล้ว ยังมีเส้นทางการเงิน Cryptocurrency ทั้งการก่อการร้ายและการค้าสินค้าผิดกฎหมายที่ไม่สามารถตรวจสอบที่มาที่ไปได้เป็นการไร้ตัวตนเส้นทางการเงินอาชญากรรมด้วยอีกเช่นกัน

ความเกี่ยวข้องกับการวิจัย

การไร้ตัวตนในโลกไซเบอร์ของวิทยานิพนธ์ดังกล่าวเกี่ยวข้องกับการวิจัยนี้ในเรื่องรูปแบบการก่ออาชญากรรมไซเบอร์รูปแบบใหม่ๆ ที่ไร้ตัวตนโดยเฉพาะการติดต่อสื่อสารผ่าน Darkweb

และเส้นทางการเงิน Cryptocurrency ทั้งการก่อการร้าย การค้ายาเสพติดและองค์กรอาชญากรรมข้ามชาติ

2.14 เอกสารวิชาการของ ศูนย์สงครามพิเศษทางไซเบอร์ องค์การนาโต้ ศูนย์เฉพาะกิจเมือง ทัลลิน ประเทศเอสโตเนีย (NATO Cooperative Cyber Defense Centre of Excellence) เรื่อง เทคนิคและภาพรวมกฎหมายของเครือข่ายการไร้ตัวตนแบบ TOR (Technical and Legal Overview of the Tor Anonymity Network)

บทความนี้เขียนโดย อิมิล โทมัส และ Anna (Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula (2015)[13] การไร้ตัวตนใน Deep web ด้วยระบบเครือข่าย Tor เป็นปรากฏการณ์ที่ทำให้เกิดปัญหาทางกฎหมายมากมาย รวมทั้งเป็นความท้าทายของรัฐที่จะต้องจัดการ สิทธิของผู้ที่ต้องการใช้ Tor ความน่าเชื่อถือของเนื้อหาที่ไร้ข้อจำกัด

ผู้ก่อตั้งโครงการ Tor Project เป็นองค์กรไม่แสวงหากำไรให้บริการทั้งสาธารณะ และองค์กรขนาดเล็ก ปัจจุบันเครือข่าย Tor เป็นเวอร์ชันรุ่นที่ 3 ของ Onion Router ซึ่งแต่เดิมเป็นโครงการวิจัยพัฒนาของกองทัพเรือ สหรัฐอเมริกา เพื่อที่จะปกป้องระบบการสื่อสารของรัฐบาล

รัฐบาลสหรัฐอเมริกา ได้เริ่มเป็นผู้สนับสนุนการเงินโครงการ ในปี พ.ศ. 2556 โดย U.S. Department of State และ U.S. Department of Defence เป็นเงินจำนวนถึง $1.8 ล้านดอลลาร์สหรัฐ เป็นรายได้ราว 60% ของโครงการ และได้เปิดรับการสนับสนุนจากภาคส่วนต่างๆ

Tor Browser ถูกรัฐบาลจีนปิดกั้น โดยกำหนดให้เป็นสิ่งผิดกฎหมายและบล็อกการเข้าใช้งาน รวมทั้ง ซาอุดี อาราเบีย สหรัฐ อาหรับเอมิเรต และอิรัค ต่างก็ปิดกั้นประชาชนไม่ให้เข้าใช้งานด้วยเช่นกัน

ทางด้านรัสเซียก็ได้ตระหนักถึงภัยคุกคามเรื่อง การไร้ตัวตน (Anonymity) ต่อความมั่นคงของชาติและความปลอดภัย จึงได้ตั้งรางวัลเป็นจำนวนเงิน $110,000 ดอลลาร์สหรัฐ ให้แก่ผู้ที่ทำการเจาะระบบ Tor ได้

ในบทความนี้ ได้สรุปสาระสำคัญด้านเทคนิคและข้อจำกัดทางกฎหมาย ที่ยังไม่สามารถกำกับดูแลอาชญากรรมที่เกิดจากการไร้ตัวตนด้วยเครือข่าย Tor ได้ นอกจากนั้นยังได้ตั้งข้อสังเกตเรื่องการ

[13] Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula (2015). Technical and Legal Overview of the Tor Anonymity Network. NATO Cooperative Cyber Defence Centre of Excellence. Tallin. 2015

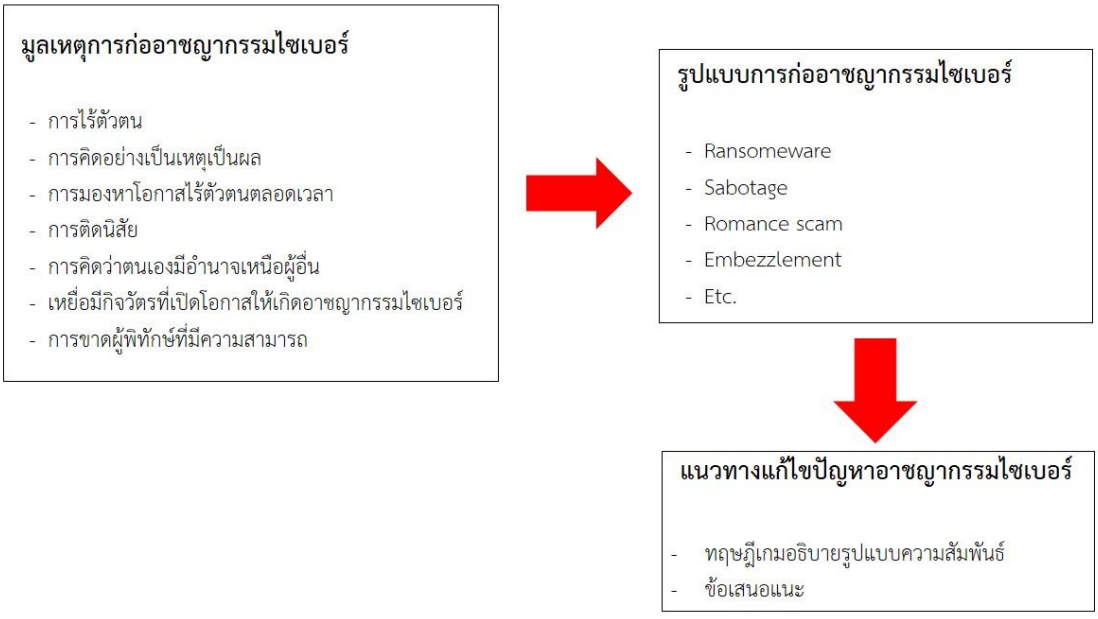
ปิดกั้น Tor ว่าจะเป็นการละเมิดสิทธิมนุษยชนหรือไม่ หากไปจำกัดเสรีภาพในการสื่อสารหรือแสดงความคิดเห็น

ความเกี่ยวข้องกับการวิจัย

บทความวิชาการนี้ได้เห็นลักษณะทางเทคนิคการไร้ตัวตนในเครือข่าย TOR และข้อจำกัดทางกฎหมายในการปิดกั้นการไร้ตัวตนในระบบ TOR เกรงว่าจะเป็นการละเมิดสิทธิประชาชนในการแสดงความคิดเห็น แต่ก็ยังมีหลายประเทศได้ปิดกั้นประชาชนไม่ให้เข้าใช้งานเครือข่าย ในการวิจัยนี้จะนำประเด็นดังกล่าวมาสรุปและเป็นข้อเสนอแนะในตอนบทสุดท้าย

2.15 กรอบแนวคิดในการศึกษาวิจัย

ดุษฎีนิพนธ์นี้ ได้ศึกษารวบรวมอาชญากรรมไซเบอร์ในหลายรูปแบบที่เคยเกิดขึ้นจากอดีตจนถึงปัจจุบัน จากนั้นใช้ทฤษฎีเกม และทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลเป็นเครื่องมือในการวิเคราะห์ความสัมพันธ์ระหว่างกระบวนการตัดสินใจของอาชญากรในการประกอบอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน ซึ่งจะช่วยให้สามารถทำนายอาชญากรรมไซเบอร์ใหม่ๆ ที่ยังไม่เคยเกิดขึ้นได้ เมื่อเข้าใจกระบวนการคิดอย่างเป็นเหตุเป็นผลของอาชญากร โดยได้กำหนดกรอบแนวคิดในการศึกษาวิจัยดังนี้



รูปที่ 13 กรอบแนวคิดการศึกษาวิจัย

บทที่ 3

ระเบียบวิธีวิจัย

การวิจัยในดุษฎีนิพนธ์นี้ เป็นการหาความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ โดยใช้กระบวนทัศน์ทางเลือกในการค้นหาความสัมพันธ์ มีระเบียบวิธีวิจัยดังนี้

3.1 รูปแบบการวิจัย

การศึกษาเรื่องนี้จะใช้วิธีการวิจัยแบบผสมผสาน (Mixed research method) มีทั้งการวิจัยเชิงปริมาณ (Qualitative research จากข้อมูลสถิติกับแบบสำรวจ (จากผู้ตอบแบบสอบถามออนไลน์ 35 ราย) และการวิจัยเชิงคุณภาพ (Qualitative research) โดยการจัดทำกรณีศึกษา (Case study) ด้วยการวิจัยเอกสาร (Documentary research) อาทิ ข่าว บทความ หนังสือชีวประวัติ เอกสารราชการ งานวิชาการ บทสัมภาษณ์ในสื่อต่างๆ และคำพิพากษา จำนวน 17 กรณี เพื่อศึกษารูปแบบในการกระทำความผิดของ อาชญากรรมไซเบอร์ และวิเคราะห์ถึงความเป็นเหตุเป็นผลในการตัดสินใจกระทำความผิด

ในการสัมภาษณ์เชิงลึก (In-depth Interview) เป็นการสัมภาษณ์จากผู้ให้ข้อมูลสำคัญ 1 ท่าน โดยไม่เคยพบตัวจริงและไม่ทราบชื่อจริง ทำการสัมภาษณ์ทางโทรศัพท์ ซึ่งเป็นอดีตแฮ็กเกอร์และปัจจุบันเป็นวิศวกรด้านความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดในกรณีศึกษาที่ 6)

โดยมีการกำหนดขั้นตอนการวิจัยดังนี้

3.1.1 การตั้งสมมุติฐานการวิจัย (Research hypothesis)

การตั้งสมมุติฐานการวิจัย ในดุษฎีนิพนธ์นี้คือ

“การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน”

โดย “การไร้ตัวตน” (Anonymity) ในดุษฎีนิพนธ์นี้ได้นิยามไว้ในข้อ 1.3 หมายถึงองค์ประกอบ 2 ปัจจัยหลัก (Anonymous Factors) ที่ช่วยให้อาชญากรรอดพ้นโทษอาญาได้ คือ

(ก.) การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective)

(ข.) การรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

การตั้งสมมุติฐานการวิจัยในดุษฎีนิพนธ์นี้ เกิดจากการสังเกตของผู้วิจัยต่อปรากฏการณ์อาชญากรรมไซเบอร์ในสังคมว่า อาชญากรรมไซเบอร์ทุกประเภทมีบางสิ่งที่สอดคล้องเหมือนกันนั่นคือ “ปัจจัยการไร้ตัวตน (Anonymous Factor)” เป็นสิ่งสำคัญที่ทำให้อาชญากรตัดสินใจประกอบอาชญากรรมไซเบอร์ เมื่ออาชญากรเชื่อว่าเขามีเทคโนโลยีช่วยให้หลบพ้นจากการสืบสวนจับกุมเขาจะลงมือทันที และถึงแม้เขาถูกจับกุมได้ หากแต่ว่าการรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีทำไม่ได้ อาชญากรก็ยังตัดสินใจลงมือประกอบอาชญากรรม

การวิจัยในดุษฎีนิพนธ์นี้ เกี่ยวกับกระบวนการตัดสินใจของอาชญากรไซเบอร์ในการตัดสินใจลงมือก่ออาชญากรรม โดยมีจุดเกาะเกี่ยวของเหตุผลเมื่อเทคโนโลยีไซเบอร์ใดก็ตาม มีปัจจัยการไร้ตัวตนอาชญากรจะตัดสินใจประกอบอาชญากรรมทันที ผู้วิจัยจึงเห็นว่า อาชญากรรมไซเบอร์กับการไร้ตัวตนมีความสัมพันธ์ต่อกัน ดังนั้นต้องหาเครื่องมือในการวิจัยมาอธิบายรูปแบบความสัมพันธ์ปรากฏการณ์ดังกล่าว

3.1.2 การศึกษารวบรวมข้อมูล

ผู้วิจัยทำการศึกษารวบรวมอาชญากรรมไซเบอร์ทุกประเภทตามการจัดหมวดหมู่ในรูปที่ 4 อาทิเช่น การทำลายข้อมูล เจาะระบบ ถอดรหัส ดักรับข้อมูล ก่อวินาศกรรมด้วยระบบคอมพิวเตอร์ การฉ้อโกง การคุกคาม การหมิ่นประมาท ตลอดจนการสร้างความเสียหายต่อระบบเศรษฐกิจ และโครงสร้างสังคม ดังนี้

ด้วยวิธีการศึกษาจากเอกสาร (Documentary study) จาก ข่าว บทความ ในนิตยสารที่มีความน่าเชื่อถือ และมีชื่อเสียงในโลก ศึกษาเอกสารจาก หนังสือชีวประวัติอาชญากรไซเบอร์ บทสัมภาษณ์ในสื่อต่างๆ ของอาชญากรไซเบอร์ เอกสารราชการ งานวิชาการ และคำพิพากษา โดยผู้วิจัยจะมุ่งไปที่ปรากฏการณ์อาชญากรรมไซเบอร์ที่มีประเด็นสำคัญ ยกมาเป็นกรณีศึกษาเด่นๆ ที่เห็นว่าปัจจัยการไร้ตัวตนมีความสัมพันธ์กับการเกิดอาชญากรรมไซเบอร์แต่ละประเภทนั้น โดยผู้วิจัยได้มีแนวทางเลือกกรณีศึกษาดังนี้

กรณีศึกษาแฮ็กเกอร์ จำนวน 5 กรณีศึกษา

จุดประสงค์ของการศึกษารวบรวมข้อมูลดังกล่าว เพื่อหาเหตุผลของแฮ็กเกอร์หรืออาชญากรไซเบอร์คดีสำคัญๆ ที่ให้คำสารภาพหรือบทสัมภาษณ์ ตลอดจนพฤติการณ์แห่งคดีที่ชี้ให้เห็นความเป็นเหตุเป็นผลของแฮ็กเกอร์แต่ละรายบุคคลอันเกี่ยวเนื่องกับการไร้ตัวตน

กรณีศึกษาฉ้อโกงออนไลน์ 2 กรณีศึกษา

2 กรณีศึกษาในการศึกษาของดุษฎีนิพนธ์นี้ ได้การยกตัวอย่างอาชญากรรมไซเบอร์ 2 ประเภท คือ คดี Romance scam และ แก๊งค์ คอลเซ็นเตอร์ ซึ่งความจริงมีเหตุเกิดขึ้นหลายคดี แต่จุดประสงค์ของการศึกษารวบรวมข้อมูลดังกล่าว เพื่อให้เห็นการไร้ตัวตนส่งผลกับการเพิ่ม และลดของอาชญากรรมไซเบอร์ 2 ประเภทนี้มีความสัมพันธ์กัน

กรณีศึกษาการจ้างสังหารออนไลน์ 1 กรณีศึกษา

ได้ยกรูปแบบอาชญากรรมไซเบอร์ประเภทการจ้างสังหารออนไลน์ ผ่าน Darkweb และจ่ายค่าจ้างวานฆ่าด้วย Crypto currency ขึ้นมา 1 คดี และได้ศึกษาค้นคว้ารวบรวมอีกหลายเว็บไซต์ที่เปิดให้บริการ เพื่อให้เข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมไซเบอร์ประเภทนี้อย่างสูง และเป็นแนวโน้มคดีสำคัญในอนาคตอันใกล้

กรณีศึกษาการค้ายาเสพติดผ่าน Darkweb 1 กรณีศึกษา

เป็นรูปแบบอาชญากรรมไซเบอร์ประเภท 1 ที่ส่งผลเสียร้ายแรงต่อสังคม ในการศึกษายกมา 2 กรณีคือ Silkroad และ Alphabay market เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมไซเบอร์ประเภทนี้ ซึ่งปัจจุบันมีหลายบริการและมีแนวโน้มเติบโตอย่างสูงในอนาคต

กรณีศึกษาการทำสงคราม โดยแฮ็กระบบเรดาร์กองทัพ 1 กรณีศึกษา

เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมไซเบอร์ประเภทนี้อย่างไรและรูปแบบการก่ออาชญากรรมไซเบอร์ที่รุนแรงเช่นนี้มีผลอย่างไร

กรณีศึกษาการโจมตีระบบเทคโนโลยีสารสนเทศของรัฐบาล 1 กรณีศึกษา

เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมไซเบอร์ประเภทนี้อย่างไร และรูปแบบการก่ออาชญากรรมไซเบอร์ที่รุนแรงเช่นนี้ที่ดูเหมือนการสร้างการจราจรกีดขวางการรับส่งข้อมูลคอมพิวเตอร์ให้หนาแน่นเหมือนไม่ใช่เทคโนโลยีที่ซับซ้อน แต่ส่งผลเสียหายรุนแรงระดับชาติอย่างไร

กรณีศึกษาการระดมทุนและเส้นทางการเงินการก่อการร้าย 1 กรณีศึกษา

เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับอาชญากรรมไซเบอร์ประเภทนี้อย่างไรและรูปแบบการเงินดิจิทัลจะส่งผลต่อการระดมทุนเพื่อการก่อการร้ายและเส้นทางการเงินของขบวนการก่อการร้ายมีแนวโน้มเติบโตอย่างไร

กรณีศึกษาช่องว่างกระบวนการยุติธรรมไทยกับการไร้ตัวตน 3 กรณีศึกษา

เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับกระบวนการยุติธรรมอาญาในการตัดสินคดีอาชญากรรมไซเบอร์ของไทยมีช่องว่างให้หลุดคดีอย่างไรและจะส่งผลต่อการอาชญากรไซเบอร์ในการตัดสินใจประกอบอาชญากรรมต่อไปอย่างไร

กรณีศึกษาการเปลี่ยนแปลงการปกครองในกลุ่มประเทศอาหรับ 1 กรณีศึกษา

เพื่อให้เห็นภาพเข้าใจว่าการไร้ตัวตนมีความสัมพันธ์กับการก่ออาชญากรรมไซเบอร์เพื่อละเมิดกฎหมายในการต่อต้านรัฐบาล จนนำไปสู่การเปลี่ยนแปลงการปกครองได้อย่างไร

กรณีศึกษาผู้ให้ข้อมูลสำคัญ (Key Informants) 1 กรณีศึกษา

ในการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลสำคัญ 1 กรณีศึกษาโดยไม่เคยพบตัวจริง ด้วยการสัมภาษณ์ทางโทรศัพท์ ซึ่งเป็นอดีตแฮ็กเกอร์ชาวไทย และปัจจุบันเป็นวิศวกรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเจาะลึกว่าการไร้ตัวตนตามนิยามในการวิจัยนี้ส่งผลต่อมูลเหตุจูงใจ กระบวนความคิด กระบวนการตัดสินใจ อย่างไร อันจะนำไปสู่การตีความทำความเข้าใจอาชญากรไซเบอร์ประเภทต่างๆ

3.2 จริยธรรมการวิจัย

ผู้วิจัยได้ยึดมั่นในการปฏิบัติตามจริยธรรมนักวิจัยของ สำนักงานคณะกรรมการการวิจัยแห่งชาติอย่างเคร่งครัดทั้ง 9 ประการ และหลักการของจริยธรรมการวิจัยในคนนั้นได้ปฏิบัติตามจริยธรรมขั้นพื้นฐาน 3 ประการ ในการวิจัยเกี่ยวกับคน คือ

ประการแรก การขอความยินยอมโดยให้ข้อมูลที่เพียงพอ

ประการที่สอง การรักษาความลับของแหล่งข้อมูล

ประการที่สาม การป้องกันผลกระทบที่อาจเกิดกับแหล่งข้อมูล

การป้องกันการกระทบต่อสิทธิผู้ให้ข้อมูลสำคัญโดยเฉพาะการปกปิดชื่อจริงและนามสกุล และการรักษาความลับเมื่อสัมภาษณ์ผู้ให้ข้อมูลสำคัญ ถือเป็นจรรยาบรรณสูงสุดของนักวิจัย ในการวิจัยนี้จึงได้ตัดปัญหาดังกล่าว โดยไม่ได้พบหน้า ไม่ขอทราบชื่อจริงและนามสกุลผู้ให้ข้อมูลสำคัญ ซึ่งมีนามสมมุติว่า “มอสแฮ็กเกอร์คุณธรรม” ผู้วิจัยได้หมายเลขโทรศัพท์จากผู้ช่วยอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยแห่งหนึ่ง ได้ประสานให้โทรศัพท์ไปสัมภาษณ์โดยมิได้พบตัวจริง ผู้ให้ข้อมูลสำคัญยินยอมให้ข้อมูลอย่างเพียงพอ เพราะทราบว่านำมาศึกษาวิจัยในดุษฎีนิพนธ์อันจะเป็นประโยชน์ต่อสังคม

เกณฑ์การคัดเลือกผู้ให้ข้อมูลสำคัญดังกล่าว ในครั้งแรกผู้วิจัยได้พิจารณาจะคัดเลือกผู้ให้ข้อมูลสำคัญ 3 คน คือ อาชญากรไซเบอร์ที่เคยก่ออาชญากรรม อาชญากรไซเบอร์ที่เลิกก่ออาชญากรรม และตำรวจไซเบอร์ที่เคยทำคดี

อาชญากรไซเบอร์ที่เคยก่ออาชญากรรม ที่ผู้วิจัยได้ทาบทามในครั้งแรกเป็นอดีตเพื่อนร่วมห้อง (Room mate) ของผู้วิจัยสมัยเป็นนักศึกษาและเคยมีชื่อเสียงในวงการคอมพิวเตอร์จากการแก้ปัญหา Y2K ในปี ค.ศ.1999 และมีประสบการณ์เป็นแฮ็กเกอร์มีความสามารถเจาะระบบถอดรหัสคอมพิวเตอร์ จนได้รับเชิญจากหน่วยงานความมั่นคงไปร่วมประชุมบ่อยครั้ง ปัจจุบันเป็นวิศวกรคอมพิวเตอร์บริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่รายใหญ่ สุดท้ายขอปฏิเสธการให้สัมภาษณ์ด้วยเหตุผลส่วนตัวต้องการรักษาความลับเพื่อใช้ชีวิตอย่างสงบ

ผู้ให้ข้อมูลสำคัญอีกรายที่ผู้วิจัยทาบทามของสัมภาษณ์เชิงลึก เป็นตำรวจที่เคยทำคดีอาชญากรรมไซเบอร์ ยศพันตำรวจโทปัจจุบันเป็นอาจารย์โรงเรียนนายร้อยตำรวจ ซึ่งผู้วิจัยเป็นอาจารย์พิเศษโรงเรียนนายร้อยตำรวจจึงได้รู้จัก แลกเปลี่ยนความรู้ ความเห็น ขอข้อมูลสถิติและขอทาบทามสัมภาษณ์เชิงลึกในการวิจัย สุดท้ายไม่ได้รับการตอบรับและผู้วิจัยเองเห็นว่า หากสัมภาษณ์เชิงลึกตำรวจที่เคยทำคดีอาจจะกลายเป็นเบาะแสให้อาชญากรได้เรียนรู้ จึงไม่ติดตามทวงถามเชิญมาสัมภาษณ์ต่อ

ผู้ให้ข้อมูลสำคัญที่ได้ คือ อาชญากรไซเบอร์ที่เลิกก่ออาชญากรรม ผู้วิจัยตั้งชื่อนามสมมุติว่า “มอสแฮ็กเกอร์คุณธรรม” เหตุผลที่เลือกคนนี้ เพราะได้ให้ข้อมูลเบื้องต้นผู้ช่วยอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยแห่งหนึ่งว่า ต้องการคนที่มีประสบการณ์เป็นแฮ็กเกอร์ตั้งแต่เด็ก แล้วกลับตัวมาเป็นคนดี และได้ดิบได้ดีในปัจจุบัน จึงได้รับการแนะนำ “มอส” ซึ่งในวงการแฮ็กเกอร์จะเรียก แฮ็กเกอร์ที่ไม่ได้ก่อคดีสร้างความเสียหายให้ผู้อื่น แต่คอยช่วยสอดส่องดูแลความปลอดภัยในโลกไซเบอร์ว่า White hat hacker หรือแฮ็กเกอร์หมวกขาวหรือแฮ็กเกอร์คุณธรรม ผู้วิจัยจึงตั้งชื่อนามสมมุติว่า “มอสแฮ็กเกอร์คุณธรรม”

นอกจากนั้นผู้วิจัยได้ทำแบบสอบถามออนไลน์ (google form) เพื่อสำรวจหญิงไทยที่เคยมีประสบการณ์ตกเป็นเหยื่ออาชญากรไซเบอร์ประเภท Romance scam ซึ่งเป็นสมาชิกในเฟซบุ๊ค กลุ่ม

“ภัยผู้หญิงในโลกออนไลน์” และมีผู้ตอบแบบสอบถามจำนวน 35 ราย โดยผู้ตอบไม่ต้องเปิดเผยชื่อจริงและนามสกุล มีเพียง E-mail ที่เป็นหลักฐานยืนยันตัวตน ซึ่งผู้วิจัยรักษาจรรยาบรรณไม่ได้เปิดเผยที่ใด

3.3 เครื่องมือในการวิเคราะห์ข้อมูล

ข้อมูลที่เก็บรวบรวมจากการสังเกตปรากฏการณ์อาชญากรรมไซเบอร์ที่มีความสัมพันธ์กับการไร้ตัวตน เครื่องมือสำคัญในการวิเคราะห์ข้อมูล คือ ทฤษฎีทางอาชญาวิทยา อาทิ ทฤษฎีการคิดอย่างเป็นเหตุเป็นผล (Rational choice theory) ทฤษฎีสามเหลี่ยมอาชญากรรม (Triangle of crime) และ ทฤษฎีเกม (Game theory)

ปัญหาสำคัญในการวิจัยนี้คือ สถิติอาชญากรรมไซเบอร์ไม่เพียงพอ อีกทั้งผู้วิจัยได้พบว่า การวิเคราะห์ข้อมูล แล้วทำนายปรากฏการณ์อาชญากรรมในอนาคตจากสถิติในอดีต หมายความว่าย่อมมีเหยื่อเคยเกิดขึ้นแล้ว แต่หน้าที่สำคัญของนักอาชญาวิทยาต้องป้องกันให้มีเหยื่อเกิดขึ้นอีกหรือไม่มีเหยื่อในอาชญากรรมประเภทใหม่เกิดขึ้นเลย

ดังนั้นจึงเลือกใช้ทฤษฎีเกม เป็นเครื่องมือสำคัญในการวิเคราะห์ข้อมูล และอธิบายกระบวนการตัดสินใจของอาชญากรไซเบอร์ โดยเอาทฤษฎีอาชญาวิทยามาเป็นพื้นฐานประกอบ ให้เห็นว่าการไร้ตัวตนมีความสัมพันธ์กับการก่ออาชญากรรมไซเบอร์อย่างไร

บทที่ 4

ผลการศึกษาและการอภิปรายผลการศึกษา

การศึกษาวิจัยตามวัตถุประสงค์ในดุษฎีนิพนธ์นี้ มีผลการวิจัยและอภิปรายผลดังนี้

4.1 **การศึกษาเชิงคุณภาพ (**17 **กรณีศึกษา)**

การศึกษาเชิงคุณภาพของอาชญากรรมไซเบอร์ 17 กรณีศึกษา ตามเกณฑ์ที่เลือกไว้ดังในบทที่ 3 ที่ครอบคลุมอาชญากรรมไซเบอร์ทุกรูปแบบและนำมาอภิปรายผลการศึกษาตามวัตถุประสงค์ของการวิจัย โดยเริ่มจาก

4.1.1 ศึกษาและรวบรวมรูปแบบการประกอบอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นจากอดีตมาจนถึงปัจจุบัน อันเป็นกรณีศึกษาเกี่ยวข้องกับการไร้ตัวตนเป็นปัจจัยสำคัญของการเกิดอาชญากรรม

4.1.2 ศึกษาความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตน (Anonymous Factor) อันเหตุให้รอดพ้นจากการสืบสวนจับกุม (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) กับการตัดสินใจก่ออาชญากรรมไซเบอร์ของอาชญากร

4.1.3 สร้างรูปแบบความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์

ได้ผลการศึกษาเชิงคุณภาพดังนี้

<u>กรณีศึกษาที่</u> 1 คำสารภาพของ เควิน มิตนิค (Kevin Mitnick) อดีตแฮ็กเกอร์มือหนึ่งของโลก

เควิน มิตนิค (Kevin Mitnick) ชาวสหรัฐอเมริกา และเคยได้ฉายาว่าเป็น "ซูเปอร์แฮกเกอร์" ขณะที่บางคนก็เรียกเขาว่าเป็น "แฮกเกอร์จากนรก" (Hacker from Hell) มิตนิกถูกจับ และถูกควบคุมตัวอยู่ในเรือนจำ Lompoc ของรัฐแคลิฟอร์เนีย นานถึง 59 เดือน ในคดี ที่ถูกกล่าวหาว่า เข้าไปเจาะข้อมูลจากเครือข่ายคอมพิวเตอร์ของบริษัทด้านเทคโนโลยีหลายแห่งโดยไม่ได้รับอนุญาต อาทิ เช่น Sun Micro-systems, Motorola และ Qualcomm สร้างความเสียหายให้กับบริษัทเหล่านั้นหลายร้อยล้านเหรียญสหรัฐ

รูปที่ 14 เควิน มิตนิค (Kevin Mitnick) แฮกเกอร์

ที่มา https://medium.com/@Genius50/kevin-david-mitnick-the-mischievous-hacker-9db11714ea2a

หนังสือเรื่อง “ตามล่ายอดแฮกเกอร์” (Ghost in the Wires, 2012) ที่เขาเขียนขึ้นมาเล่าเรื่องอัตชีวประวัติของเขา **ตลอดจนได้บอกเหตุผลและความคิด** ในขณะที่**ตัดสินใจ**ประกอบอาชญากรรมไซเบอร์อย่างละเอียด ช่วยให้ได้ข้อมูลเชิงคุณภาพเป็นอย่างดี

ในบทนำของหนังสือ เควิน เล่าเรื่องราวอันน่าตื่นเต้น เขาวางแผนจะเข้าไปยังศูนย์คอมพิวเตอร์ในบริษัทแห่งหนึ่ง ทำทีเป็นคนส่งจดหมายเดินถือไปให้พนักงานในบริษัทนั้น แท้จริงเขาเข้าไปสังเกตรูปแบบบัตรพนักงาน ติดรูปตรงไหน โทนสีอะไร ตัวอักษรแบบไหน แล้วเขาแวะเข้าร้านอินเทอร์เน็ตแถวนั้น ดาวน์โหลด โลโก้ ของบริษัทนั้น และใช้โปรแกรม Photoshop ตัดต่อภาพตัวเองลงบนบัตร แล้วพิมพ์ออกมาใส่ซองพลาสติกเป็นบัตรเหมือนของจริงทุกประการ

เขากลับไปที่บริษัทยักษ์ใหญ่นั้นอีกครั้ง เขาเดินตามกลุ่มพนักงานที่ออกมาสูบบุหรี่กำลังกลับเข้าไปยังตัวอาคารคนนำหน้าต้องใช้บัตร สแกน เปิดประตู เขาสวมรอยเดินตามเข้าไปอย่างมั่นใจว่าบัตรเขาไม่เป็นที่ผิดสังเกต ในที่สุดเขาก็หาห้องศูนย์คอมพิวเตอร์ในบริษัทแห่งนั้นพบ แล้วลักลอบเข้าไป ใส่ซีดี เพื่อโหลดโปรแกรมที่เป็นเครื่องมือของแฮกเกอร์ จากนั้นกลับมารอที่บ้านตอนเช้าเมื่อ แอดมิน ล็อคอินเข้าเครื่อง ข้อมูลทั้งหมดจะส่งผ่านอินเทอร์เน็ตเข้าสู่คอมพิวเตอร์ที่บ้านเขา รวมทั้งรหัสผ่านของ วิศวกร และพนักงานทุกคน โดยเฉพาะอย่างยิ่งข้อมูลบัตรเครดิตนับล้านๆ เลขหมาย

แต่เขาอ้างว่าเขาไม่ได้นำบัตรเครดิตไปใช้จ่าย เขาถูกว่าจ้างให้ทดลองเจาะระบบบริษัทดังกล่าว และนั่นคืองานประจำของเขา ซึ่งเขาหลงใหลงานเจาะระบบคอมพิวเตอร์และเทคโนโลยีการสื่อสารอย่างมาก

ในหนังสือของ เควิน เขาเล่าว่า เขาเป็นเด็กลูกคนเดียว พ่อทิ้งไปตั้งแต่สามขวบ แม่หาเลี้ยงด้วยการเป็นเด็กเสิร์ฟในร้านอาหาร เขาชอบหลบเลี่ยงระบบรักษาความปลอดภัยตั้งแต่ขวบกว่า โดยหาทางปีนหนีจากเปล คลานไปประตู มองหาทางหนีออกจากประตูตลอดเวลา

ช่วงที่เขาเติบโต แม่ของ เควิน มีสามีใหม่ 3 คน และมีเพื่อนชายนับไม่ถ้วน ผู้ชายบางคนทุบตีเขา บางคนล่วงละเมิดเขา ซึ่งแม่ของ เควิน ก็เลือกเขาก่อนเสมอ

ในวัยสิบกว่าขวบเขาได้รู้จักคนขับรถเมลล์คนหนึ่งเป็นนักวิทยุสมัครเล่นสาธิตให้ดูการโทรศัพท์ฟรีผ่านวิทยุสื่อสาร โดยใช้บริการ ‘ออโต้ แพด’ เขาบันทึกว่า เขาประทับใจอย่างสุดซึ้งและถอนตัวไม่ขึ้น หลังจากนั้นไม่กี่สัปดาห์เขาเรียนรู้วงจรอิเล็กทรอนิกส์ และสอบผ่านใบอนุญาตใช้วิทยุสมัครเล่น เขารู้สึกดีใจมาก เป็นความสำเร็จที่ยิ่งใหญ่เพราะเด็กรุ่นเดียวกับเขาน้อยคนนักจะมีใบอนุญาตแบบนี้ จากนั้นเขาอยากเรียนรู้กลไกระบบโทรศัพท์ให้แตกฉาน เขามีความสุขกับมายากลของเทคโนโลยี

เมื่ออายุ 13 ปี เขาเริ่มทำบัตรปลอมขึ้นรถเมล์ฟรี เจอหนังสือสอนเจาะระบบทะเบียนใบขับขี่ รายงานบัตรเครดิต หนังสือใต้ดินที่คนทั่วไปไม่ควรรู้ เขาจดจำอย่างขึ้นใจ ความรอบรู้เรื่องพิเศษคือสิ่งที่เขาชื่นชอบ และได้พบเครื่องมือสะเดาะกุญแจ เขาอยากจะลักลอบเข้าไปในสถานที่ต่างๆ และจากนั้นเขาได้รู้จักคอมพิวเตอร์ เขาชอบที่จะค้นหารหัสของครูสอนคอมพิวเตอร์

เด็กมัธยมอย่างเขาไปขอเรียนคอมพิวเตอร์ที่มหาวิทยาลัยแห่งหนึ่ง แต่ถูกปฏิเสธเพราะห้องคอมพิวเตอร์ให้ใช้ได้เฉพาะนักศึกษา แต่เขาทำทีว่าอยากเรียนแต่ห้องคอมพิวเตอร์ที่โรงเรียนปิดเร็ว หัวหน้าภาควิชาคอมพิวเตอร์เห็นใจจึงให้รหัสผ่านของเขาแก่เควินเข้าไปใช้งาน เควิน เรียนรู้การเขียนโปรแกรม ฟอร์แทรน และเบสิก ในไม่กี่สัปดาห์ เขาเขียนโปรแกรมขโมยรหัสผ่านฝังไว้ในระบบคอมพิวเตอร์ เมื่อนักศึกษาคนอื่นล็อคอิน เขาก็จะได้รหัสผ่านไป เขานึกขันในใจใครจะเชื่อว่าเด็กมัธยมเขียนโปรแกรมขโมยรหัสผ่านได้ เขาไม่มีแผนชั่วร้ายอะไรทำไปเพราะความรู้สึกสนุก รู้สึกมีพลังอำนาจ แต่แล้วเขาก็ถูกมหาวิทยาลัยและตำรวจจับ

เขาเติบโตมาพร้อมความรู้สึกตื่นเต้นท้าทาย และมีพลังอำนาจจากการมีเทคโนโลยีเหนือคนอื่น เมื่อเข้าไปในระบบคอมพิวเตอร์คนอื่น ในระบบเครือข่ายการสื่อสารขนาดใหญ่ ระบบข้อมูลธุรกิจ เขาเสพติดการเจาะระบบ และในที่สุดถูกจับกุมคุมขังในเรือนจำ

เควิน ได้อธิบายความรู้สึกในการถูกจับกุมตอนนั้นทำนองว่า *‘แฮ็กเกอร์อย่างเขาเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นเพื่อความสนุกเท่านั้น มันคล้ายๆ กับเด็กที่แอบปีนเข้าบ้านร้าง มันสนุกมันตื่นเต้นท้าทายก็แค่นั้นเอง เขาไม่ได้หยิบอะไรติดมือมา เขาไม่เคยใช้บัตรเครดิตที่ขโมยข้อมูลมา’*

เควิน หายตัวล่องหนปิดบังตัวตนทั้งข้อมูลการใช้อินเทอร์เน็ต และโทรศัพท์เคลื่อนที่เพื่อหลบหนี FBI อยู่ได้นานถึง 2 ปี จนถูกจับกุม และถูกศาลสั่งขังเดี่ยวด้วยเกรงว่าเขาอาจจะหาทางแฮ็กระบบนิวเคลียร์

เควิน (2557,น.493) เอฟบีไอ ค้นพบฐานข้อมูลของ Netcom ที่มีข้อมูลบัตรเครดิตของลูกค้ามากกว่า 20,000 ใบในคอมพิวเตอร์ของ เควิน แต่เขาไม่เคยใช้สักครั้ง และอัยการไม่สามารถหาพยานหลักฐานฟ้องร้องเขาได้ เขาบอกว่าการใช้ข้อมูลบัตรเครดิตผู้อื่นมันเป็นความชั่วร้าย ถ้วยรางวัลที่เขาได้รับคือ ฐานข้อมูลของ Netcom เท่านั้น เควิน หลบหนีอยู่สองปี ย้ายที่นอนไปเรื่อย ปิดโทรศัพท์เคลื่อนที่ และอำพรางตัวตลอดเวลา

เควิน เล่าว่าเขาเข้าใจดีถึงปัญหาที่ผู้ที่จับกุมเขาจะไม่สามารถเข้าใจแรงจูงใจพิเศษของเขาได้ เขามองว่าเป็นเพียงเกมประลองทักษะ และหากคนทั่วไปมีข้อมูลบัตรเครดิตมากกว่า 20,000 ใบ คงอดทนไม่ใช้ได้แน่ๆ

เควิน ไม่ได้สนใจการแสวงหาประโยชน์อันเป็นตัวเงิน คำกล่าวของผู้ช่วยอัยการกล่าวว่า “เขาเข้าถึงข้อมูลความลับทางการค้านับพันล้านดอลลาร์ เขาไม่ใช้ ไม่ขาย แล้วเนื้อแท้ของอาชญากรรมอยู่ที่ใด?”

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 1

เมื่อศึกษา การใช้ชีวิต ความคิด และการตัดสินใจ ของ เควิน มิตนิค แล้ว อาจจะยังไม่สามารถหาทฤษฎีทางอาชญาวิทยามาอธิบายปรากฏการณ์การก่ออาชญากรรมไซเบอร์ของเขาได้ เพราะอาชญากรไซเบอร์มีความแตกต่างจากการจัดประเภทอาชญากรตามทฤษฎีที่เคยปรากฏ อาชญากรประเภทอื่นอาจจะทำร้ายร่างกาย ฆาตกรรม ชิงทรัพย์ หรือก่อการร้าย ต่อหน้าเหยื่อหรือตำรวจ แต่อาชญากรไซเบอร์จะไม่ปรากฏตัว ความลับถือเป็นหัวใจสำคัญ และพวกเขาเป็นอาชญากรที่มีความรู้ และความฉลาด

เควิน มิตนิค ได้เขียนในหนังสือของเขาว่า แม้เขาได้เข้าถึงข้อมูลบัตรเครดิตนับแสนๆ ใบ แต่ไม่ได้ใช้มาหาประโยชน์แก่ตนเลย ทำเพื่อตอบสนองความท้าทายเท่านั้น

ทฤษฎี Rational Choice Theory ของนักวิชาการหลายๆ คนได้เสนอความเห็นตรงกันว่ามนุษย์รู้ในทุกทางเลือก และตัดสินใจเลือกอย่างเป็นเหตุเป็นผลว่าทางเลือกใดที่ให้อรรถประโยชน์ (Utility) สูงสุดแก่ตน แม้มนุษย์มีเหตุมีผลในการตัดสินใจอย่างเป็นเหตุเป็นผล แต่ จอห์น เอลสเตอร์ (ไชยันต์, 2561) ได้ให้เหตุผลว่าความพึงพอใจ (Preference) ก็เป็นอรรถประโยชน์ของมนุษย์ในการตัดสินใจเลือกอย่างเป็นเหตุเป็นผล

เควิน มิตนิค ไม่ได้รับอรรถประโยชน์จากการก่ออาชญากรรมไซเบอร์ในบางครั้ง นอกจากความพึงพอใจ เขาต้องการตอบสนองสิ่งท้าทายด้วยความรู้สึกตื่นเต้นเร้าใจ ด้วยความเชื่อว่าจะไม่ถูกจับได้ เขารู้สึกถึงพลังวิเศษที่จะบุกรุกล่องหนหายตัวเข้าไปยังเครือข่ายคอมพิวเตอร์ขององค์กรชั้นนำที่มีระบบรักษาความปลอดภัยแน่นหนา และจะไม่ถูกจับได้ ซึ่งอาจจะเป็นมุมมองทางด้านจิตวิทยา (Psychology) สาเหตุการเกิดของการก่ออาชญากรรม ทำให้เขารู้สึกเบิกบานใจ (exhilaration) เพียงเพราะต้องการมีประสบการณ์ที่ทำให้รู้สึกตื่นเต้นเร้าใจ (solely for the thrill of the experience)

<u>กรณีศึกษาที่</u> 2 คำสารภาพของ มาร์คัส ฮัตชินส์ (Marcus Hutchins) ฮีโร่ ผู้กลายเป็นอาชญากรไซเบอร์

นิตยสาร Wired เป็นนิตยสารด้านไซเบอร์เทคโนโลยีชั้นนำของโลก ฉบับเดือน มิถุนายน 2020 ได้ขึ้นปก มาร์คัส ฮัตชินส์ พร้อมพาดหัวว่า The ~~Hero Hacker~~ Who Saved The Internet

ราวปี ค.ศ. 2017 มัลแวร์เรียกค่าไถ่ (Ransomware) ที่รู้จักกันในนาม WannaCry ระบาดไปทั่วโลก คอมพิวเตอร์นับแสนเครื่องได้รับความเสียหาย สื่อหลายแห่งเกิดความกังวลว่าโลกอินเทอร์เน็ตอาจถึงคราวสิ้นสุดลง

มาร์คัส ฮัตชินส์ วัย 22 ปี คือผู้ที่พบวิธีปิดการทำงานของ WannaCry และหยุดยั้งภัยคุกคามได้สำเร็จ จึงได้รับการยกย่องว่าเป็น ฮีโร่ ผู้รักษาโลกอินเทอร์เน็ตไว้ได้

เขาได้รับเชิญเป็น VIP ร่วมงาน hacker party มากมาย ได้รับสิทธิดื่มฟรีตลอดชีวิตใน Defcon (การประชุม แฮ็กเกอร์ใหญ่ที่สุดของโลกงานหนึ่ง) ได้รับเชิญร่วมรับประทานอาหารค่ำกับนักเขียนมากมาย และยังมีแฟนคลับจำนวนมากขอถ่ายรูปด้วย

กันยายน ค.ศ. 2017 ประมาณ 3 เดือนต่อมา หลังจากเสร็จสิ้นการประชุม Defcon ที่ลาสเวกัส มาร์คัส ฮัตชินส์ ได้ถูกทาง FBI จับกุมที่สนามบินขณะกำลังจะเดินทางกลับบ้านที่ลอนดอน ด้วยข้อหาเป็นหนึ่งในผู้สร้างมัลแวร์ Kronos ออกขายด้วยราคาที่สูงถึง $3,000 หรือราว ๆ 105,000 บาท ขายให้อาชญากรไซเบอร์นำไปขโมยข้อมูลบัญชีธนาคารและบัตรเครดิตในเดือนกรกฎาคม ปี 2014 และในเดือนกุมภาพันธ์ 2015 ทาง มาร์คัส ฮัตชินส์ ยังได้ทำการอัปเดตมัลแวร์ Kronos อีกด้วย และ FBI เชื่อว่า นอกจาก มาร์คัส ฮัตชินส์ แล้ว ยังมีผู้ร่วมขบวนการอีกที่ไม่เปิดเผยชื่อ

Andy Greenber คอลัมนิสต์อาวุโสจากนิตยสาร Wired ได้เขียนบทความเชิงสืบสวนสอบสวน อาชญากรไซเบอร์เป็นบทความชื่อ The Confessions of Marcus Hutchins, the Hacker

Who Saved the Internet[14] ได้ให้สัมภาษณ์ มาร์คัส ฮัตชินส์ และคุณแม่ของเขา เจเน็ต ฮัตชินส์ บอกเล่าเรื่องราวอย่างละเอียด และคำสารภาพของเขาสรุปย่อดังนี้

มาร์คัส ฮัตชินส์ เติบโตในฟาร์มเมือง Devon ห่างไกล ในประเทศอังกฤษ คุณแม่เจเน็ต ฮัตชินส์เป็นพยาบาล และคุณพ่อแดสมอนด์ ฮัตชินส์ เป็นเจ้าหน้าที่ดับเพลิงที่จาไมก้า

ในวัย 6 ขวบ มาร์คัส ฮัตชินส์ เข้ากับเด็กในละแวกนั้นไม่ค่อยได้ เขาตัวสูงใหญ่กว่าคนอื่น และมีผมที่หยิกฟูเหมือนไม้ถูพื้น เขาเฝ้าดูแม่ใช้คอมพิวเตอร์ของครอบรัวในระบบปฏิบัติการ Window95 อย่างหลงใหล

มาร์คัส ฮัตชินส์ เรียนรู้คุณลักษณะของ HTML อันพื้นฐานของเว็บไซต์ และเริ่มเขียนสคริปต์ด้วยภาษา เบสิก เข้าไปโพสต์ข้อความว่า “Hello world” ในเว็บไซต์ที่เขาเข้าไปท่อง

ในวิชาคอมพิวเตอร์ที่โรงเรียน ใช้โปรแกรม Word พิมพ์เอกสารทำให้เขาเบื่อมาก และระบบคอมพิวเตอร์ในโรงเรียนมีการป้องการการลงโปรแกรมกมส์คอมพิวเตอร์ และจำกัดเว็บไซต์ที่ให้เข้าได้

มาร์คัส ฮัตชินส์ จึงใช้โปรแกรม Word เขียนสคริปต์ด้วยภาษา Visual Basic ที่เขาค้นพบเทคนิคในการลงโปรแกรมเกมส์ Counterstrike and Call of Duty ในระบบคอมพิวเตอร์ของโรงเรียน และท่องเว็บไซต์ที่โรงเรียนปิดกั้นได้ด้วย

ในวันเกิดอายุครบ 13 ปี ครอบครัวของเขามีความเห็นว่าจะซื้อคอมพิวเตอร์ตัวแรกให้เขา แต่เขาซื้อแบบแยกชิ้นส่วนมาประกอบเองและทำให้เขาใช้ชีวิตอย่างหนักกับคอมพิวเตอร์ ทั้งเล่นเกมและฝึกทักษะการเขียนโปรแกรม จนแม่ของเขาเป็นกังวลมากอยากให้ลูกได้ใช้ชีวิตร่าเริงในชนบท จนต้องลงโปรแกรมสำหรับควบคุมการใช้คอมพิวเตอร์สำหรับครอบครัว (Parental controls) ในคอมพิวเตอร์ของ มาร์คัส ซึ่ง มาร์คัส ก็แก้ไขอย่างง่ายดายหรือแม่ของเขาพยายามจำกัดการเข้าใช้ Router WiFi เขาก็สามารถแก้ไขให้กลับมาตั้งค่าเดิมที่มาจากโรงงานได้เหมือนเดิม แม่ของเขายอมรับว่า ไม่มีทางที่จะห้ามหรือเฝ้าระวังการใช้อินเทอร์เน็ตของ มาร์คัสได้

1 ปีที่ได้มีคอมพิวเตอร์ส่วนตัว มาร์คัส สามารถ แฮ็ก เว็บไซต์ฟอร์รัมต่างๆ ได้ และยังสร้างนวัตกรรมมัลแวร์ของตนด้วยการซ่อนมัลแวร์ล่องหนแฝงไปในไฟล์รูป JPEG และส่งไปทาง messaging platform MSN บัญชีเพื่อนๆ ผู้ใดเปิดไฟล์ก็จะตกเป็นเหยื่อทันที

อายุ 14 ปี มาร์คัส ฮัตชินส์ โพสต์ใน ฟอร์รัม การขโมยพาสเวิร์ดอย่างง่าย ด้วยการติดตั้งโปรแกรมลงในเครื่องคอมพิวเตอร์ของเหยื่อ เมื่อเหยื่อใช้ บราวส์เซอร์ เข้าชมเว็บไซต์ และมัลแวร์ของ

[14] Andy Greenber (2020). The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet. Cited on December 5, 2020. Available from URL: https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/?fbclid=IwAR3gDfsXqek5YpGNOpESlVDZALezYnvOCOEtimuKXmD2e4NEnPiMCVZqRK4

เขาได้รับการยอมรับจากฟอร์รัมทำให้เขาดีใจอย่างยิ่ง และได้เริ่มต้นอาชีพ แฮ็กเกอร์ ซึ่งนั่นไม่ทำให้มาร์คัส รู้ตัวเลยว่ากำลังเข้าสู่วงการอาชญากรรมไซเบอร์ เป็นการกระทำผิดกฎหมายอาญา

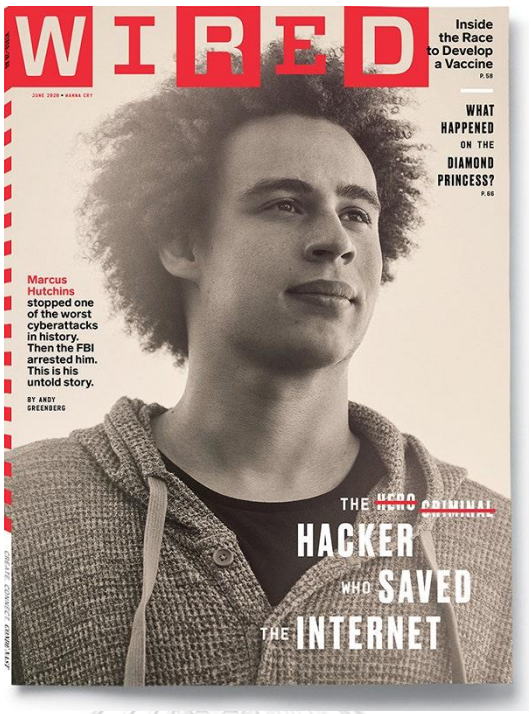
ทุกเย็นเขาจะรีบกลับมาอยู่หน้าคอมพิวเตอร์ กินข้าวหน้าคอมพิวเตอร์ และแกล้งนอนหลับแต่หัวค่ำ หลังจากพ่อกับแม่เช็คว่าปิดไฟนอนแล้วเขาจะลุกขึ้นมาอยู่กับคอมพิวเตอร์จนกระทั่งเช้า และเข้านอนก่อนแม่ตื่นสักครึ่งชั่วโมง และในที่สุดแม่เขาก็พบความจริงเมื่อต้องพาเขาไม่หาหมอเพราะเขาเป็นโรคพักผ่อนไม่เพียงพอ

อายุ 15 ปี เขาถูกโรงเรียนจำกัดบัญชีการเข้าสู่ระบบคอมพิวเตอร์ และตั้งข้อสงสัยว่า มาร์คัส โจมตีระบบคอมพิวเตอร์ของโรงเรียน เจาระบบแม่ข่าย และแก้ไขอะไรบางอย่าง แต่ มาร์คัส ปฏิเสธทุกอย่าง และถามหาหลักฐาน (เขามั่นใจว่าไม่ทิ้งร่องรอยใดไว้) แต่ผู้บริหารระบบ (แอดมิน) ไม่เปิดเผยให้ดู มาร์คัส กล่าวว่าเขาเป็นแพะรับบาป แต่แม่ของเขาไม่เชื่อ และบอกว่า มาร์คัส เป็นคนโกหกไม่เก่ง แม่ของเขาเชื่อว่าลูกชายเป็นคนทำแน่ๆ

สองสัปดาห์หลังถูกคาดโทษ มาร์คัส ถูกห้ามใช้ระบบคอมพิวเตอร์ของโรงเรียนตลอดไป เขานอนหลับในห้องเรียน และเริ่มโดดเรียน ทำให้แม่กลุ้มใจมากขึ้น

ครอบครัว ฮัตชินส์ ย้ายออกจากฟาร์มไปบ้านใหม่ มาร์คัส ได้เริ่มธุรกิจอาชญากรรมไซเบอร์จริงจัง ตั้งแต่ขโมยพาสเวิร์ด เฟซบุ๊ค ยึดคอมพิวเตอร์ผู้อื่น โจมตีระบบด้วย DDoS สร้าง Botnet และมัลแวร์เขาได้ โพสต์ Code ตัวอย่างใน HackForums ซึ่งสมาชิกต่างก็ชื่นชมความสามารถ และร้องขอให้ช่วยตรวจสอบวิธีเอาชนะโปรแกรม Antivirus ต่างๆ

อายุ 16 ปี มาร์คัส มีชื่อเสียงมากในวงการ แฮ็กเกอร์ เขาได้รับฉายาว่า Malware ghostwriter และเขาได้ถูกทาบทามจากลูกค้านิรนามคนหนึ่งมีนามสมมุติว่า วินนี่ (Vinny) ให้ทำธุรกิจจริงจัง โดยวินนี่จะนำเครื่องมือ (Code) ต่างๆ ของ มาร์คัส ไปขายให้แฮ็กเกอร์มืออาชีพใน Hacker marketplaces ซึ่งเป็นตลาดใหญ่กว่า HackForums เสียอีก และแบ่งรายได้คนละครึ่ง ชุดเครื่องมือแฮ็กเกอร์ชุดแรกที่ มาร์คัส พัฒนาเรียกว่า UPAS Kit



รูปที่ 15 มาร์คัส ฮัตชินส์ (Marcus Hutchins)

ที่มา ปกนิตยสาร WIRED (Photograph: Ramona Rosales, 2020)

มาร์คัส ไม่เคยพบตัวจริงของ วินนี่ เขาสนทนาผ่านการส่งข้อความ เขารู้สึกว่า วินนี่ แตกต่างจากแฮ็กเกอร์อื่นๆ มีความเป็นมืออาชีพมาก ไม่คุยโม้เกินจริง ไม่เลียนแบบคนอื่น และเก็บความลับยอดเยี่ยม เขาทั้งสองจะไม่ทิ้งหลักฐานการสนทนาไว้เลย ลบทิ้งทุกครั้ง วินนี่ ล่องหนหายตัวในโลกออนไลน์ลึกลับที่สุด ลบ Routing การเชื่อมต่ออินเทอร์เน็ตหรือเชื่อมต่ออินเทอร์เน็ตผ่าน Multiple proxy servers และไม่เคยคุยเรื่องส่วนตัวเลย และเขาไม่เคยถามวินนี่ด้วยซ้ำว่าขาย UPAS Kit ให้ใครใน HackForums เพียงแค่โอนเงินมาให้ มาร์คัส เป็นพันดอลลาร์ เขาก็พอใจแล้ว ซึ่งทำให้เขานำเงินมาซื้อคอมพิวเตอร์ที่แรงขึ้นได้อีก

UPAS Kit เวอร์ชันที่ 2 จึงได้ถูกพัฒนาขึ้นมีลูกเล่นใหม่ๆ ที่ฝังไปกับเว็บไซต์ที่เหยื่อกดเข้ามาชม เช่น Keylogger (จำแป้นพิมพ์ใดบ้างที่ถูกกดรหัส) และได้แชร์ Code ให้ วินนี่ พิจารณา แต่ วินนี่บอกมาร์คัส ให้ร่วมงานกับโปรแกรมเมอร์ อีกสองคนจะพัฒนาเป็น มัลแวร์ เพื่อโจมตีสถาบันการเงิน ซึ่ง มาร์คัส ไม่เห็นด้วย เพราะเขาพัฒนา Code เสร็จแล้ว ซึ่ง วินนี่ ก็ได้ทุกอย่างไปอยู่ในมือแล้ว มาร์คัส รู้สึกว่าตกหลุมพรางของ วินนี่ เข้าแล้ว วินนี่ จึงนำไปพัฒนาต่อเอง แต่ก็ยังส่งส่วนแบ่งการขายมาให้ มาร์คัส เสมอ มาร์คัส เครียดเริ่มสั่ง แอมเฟ็ตตามีน (amphetamines) จากเว็บมืด SilkRoad มาเสพเพื่อให้ได้นอน และเขาไม่ติดต่อกับ วินนี่ อีกเลย

ปี ค.ศ. 2014 เครื่องมือแฮ็กเกอร์ถูกพัฒนาเสร็จ วินนี่ วางขายใน cybercriminal marketplaces อาทิ Exploit.in and Dark0de. ต่อมาได้วางขายในเว็บไซต์มืดค้ายาเสพติดที่ใหญ่ที่สุด AlphaBay และเปลี่ยนชื่อแบรนด์ใหม่เป็น Kronos โทรจันสำหรับโจมตีธนาคาร (Banking Trojans) ที่สร้างความเสียหายสูงสุดในประวัติศาสตร์อาชญากรรมไซเบอร์

นี่จึงเป็นสาเหตุที่ FBI ดำเนินการจับกุมดำเนินคดี มาร์คัส ฮัตชินส์ ในปี 2017 และมีหลักฐานที่เกี่ยวข้องกับตัวเขาว่าเป็นผู้ริเริ่มเขียน Code โทรจัน Kronos ขึ้นมา แต่ ดร.โอริน เคอร์ (Orin Kerr) อาจารย์ มหาวิทยาลัยจอร์จ วอชิงตัน และผู้เชี่ยวชาญด้านอาชญากรรมไซเบอร์ ให้ความเห็นคดีนี้ว่า

“การสร้างมัลแวร์ไม่เป็นความผิดอาญา การขายก็ไม่เป็นความผิด แต่จะเป็นความผิดต่อเมื่อนำไปใช้กระทำความผิด เนื้อหาตามคำบรรยายฟ้องนั้นยังไม่เพียงพอ” อธิบายเพิ่มเติมได้ว่า แม้ มาร์คัส ฮัตชินส์ เป็นผู้ริเริ่มเขียน Code โทรจัน Kronos ขึ้นมา แต่ขาดองค์ประกอบความผิดอาญา ทั้งเจตนา และการกระทำ

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 2

จากคำสารภาพโดยละเอียด มาร์คัส ฮัตชินส์ มีความพึงพอใจอย่างสูงเมื่อปิดบังอำพรางมัลแวร์ของตน ซ่อนส่งไปให้เป้าหมายอย่างที่ไม่มีใครมองเห็น จึงอาจเป็นแรงบันดาลใจให้เขาพัฒนาทักษะด้านนี้มาเรื่อย เพราะทำให้รู้สึกว่าตนมีความพิเศษที่ล่องหนหายตัวไปควบคุมคอมพิวเตอร์ผู้อื่นได้

มาร์คัส ฮัตชินส์ ในปี 2017 มีชื่อเสียงโด่งดังจากการหยุดยั้งภัยคุกคามของ WannaCry ได้สำเร็จ จึงทำให้ตัวตนของเขาปรากฏขึ้นมาในสังคม และหลายคนที่สนใจก็สืบค้นเรื่องราวผลงานต่างๆ ของเขาออกมาจนในที่สุดก็พบหลักฐานเกี่ยวข้องกับการซื้อขายเครื่องมือแฮ็กเกอร์ (Code) อย่าง UPAS Kit อันเป็นที่มาของ Kronos ในการขายให้อาชญากรนำไปประกอบอาชญากรรมไซเบอร์ แม้ยังไม่พบหลักฐานว่าเขาได้ร่วมก่ออาชญากรรมด้วยก็ตาม

แต่กรณี วินนี่ ผู้ไร้ตัวตนล่องหนหายตัวอย่างไม่มีเบาะแส แม้แต่ มาร์คัส ฮัตชินส์ แฮ็กเกอร์ระดับต้นของโลกยังไม่สามารถค้นหาตัวตนของ วินนี่ ได้ ความเป็นมืออาชีพในการบิดบังอำพรางตัวตนทุกมิติของ วินนี่ ทั้งการไม่พูดคุยเรื่องส่วนตัว ไม่ให้เบาะแสใดๆ ปิดบัง IP address ชั้นลึก อาจทำให้เขามั่นว่าจะไม่มีวันถูกจับกุม จึงกล้าที่จะตัดสินใจลงมือก่ออาชญากรรมไซเบอร์ต่อไปเรื่อยๆ

<u>กรณีศึกษาที่</u> 3 คำสารภาพของ เอเดรียน ลาโม่ (Adrian Lamo) แฮ็กเกอร์ไร้บ้าน

เอเดรียน ลาโม่ เป็นแฮ็กเกอร์ที่มีประวัติน่าสนใจที่สุดของสหรัฐอเมริกาคนหนึ่ง ประวัติเขาถูกนำไปสร้างสารคดี และภาพยนตร์ เขาประกาศตัวเป็นแฮ็กเกอร์สีเทา (Grey Hat) เข้าไปบุกรุกเครือข่ายคอมพิวเตอร์องค์กรใหญ่ อาทิเช่น ซิสโก้ ไมโครซอฟต์ แบงค์ออฟอเมริกา นิวยอร์ค ไทม์ ยาฮู และเวิร์ลคอม เป็นต้น แต่เขาบุกรุกเพื่อแจ้งให้ทราบถึงช่องโหว่และให้แก้ไข ไม่ได้เข้าไปสร้างความเสียหายใดๆ โดยเขาหวังที่จะได้รับค่าจ้างในการสอดส่องดูแลความปลอดภัยของระบบ แต่นั่นเป็นการกระทำความผิดอาญาเขาจึงถูก FBI จับกุมดำเนินคดี เขารับสารภาพในข้อกล่าวหา และถูกศาลพิพากษาตัดสินจำคุก 2 ปี โดยเปลี่ยนโทษจำคุกเป็นถูกกักขังที่บ้านแทนเป็นเวลา 6 เดือน และได้รับคำสั่งให้ชดใช้ค่าเสียหาย 65,000 เหรียญสหรัฐ ในปี ค.ศ. 2004

ลาโม่ ใช้ชีวิตตัวคนเดียว เขาไม่มีบ้านหรืออพาร์ตเม้นต์เป็นหลักแหล่ง เขาจึงมีฉายาแฮ็กเกอร์ไร้บ้าน (Homeless Hacker) ลาโม่ สารภาพให้รายละเอียดแก่ Jennifer Kahn นักเขียนจากนิตยสาร Wired ได้เขียนบทความเรื่อง The Homeless Hacker v. The New York Times[15] ว่าเขาจะอาศัยหรือนอนไม่เป็นหลักแหล่ง โดยนอนบนโซฟาในบริษัทที่เขาทำงานรักษาความปลอดภัยระบบคอมพิวเตอร์ เขาแอบไปอยู่ในอาคารร้าง สถานที่ก่อสร้าง ในแต่ละที่ ลาโม่จะไม่นอนที่ใดเกินสองคืน และใช้ WiFi ฟรีจากสถานที่ต่างๆ ในบริเวณนั้น หรืออาจจะใช้ของร้านกาแฟหรือห้องสมุดสาธารณะหรือมหาวิทยาลัย เป็นการอำพรางตัว

ต่อมา เอเดรียน ลาโม่ ทำงานเป็นนักข่าวและนักพูด เกี่ยวกับวงการ Hacker และได้รับรางวัลนักข่าวยอดเยี่ยม

ปี ค.ศ. 2009 เว็บไซต์ WikiLeaks ได้เผยรายชื่อผู้บริจาคนิรนามให้แก่เว็บไซต์ WikiLeaks และมีชื่อของ ลาโม่ อยู่ในนั้นด้วย ทำให้เขาไม่พอใจว่า เว็บไซต์ WikiLeaks ทำเช่นนั้นเพื่ออะไร

ปี ค.ศ. 2010 เขาจึงได้รายงานต่อ ผู้บังคับบัญชากองสืบสวนอาชญากรรมในกองทัพสหรัฐ (Army's Criminal Investigation Division) ว่า แบรดเลย์ แมนนิ่ง (Bradley Manning) วัย 22 ปี นักวิเคราะห์ข่าวกรอง กองทัพอเมริกันที่อยู่ในสงครามอิรัค เป็นแฮ็กเกอร์ กำลังจารกรรมข้อมูลรัฐกว่า 260,000 รายการส่งต่อข้อมูลลับให้แก่เว็บไซต์ WikiLeaks โดยเฉพาะวิดีโอการโจมตีกรุงแบกแดดทางอากาศ แบรดเลย์ แมนนิ่ง ถูกพิพากษาให้จำคุกเป็นเวลา 35 ปี เป็นภัยร้ายแรงต่อความมั่นคงสหรัฐฯ

[15]Jennifer Kahn (2004). The Homeless Hacker v. The New York Times. Cited on January 4, 2004 Available from URL: https://www.wired.com/2004/04/hacker-5/

ต่อมาในปี ค.ศ. 2017 เขาสามารถขออภัยโทษได้ภายหลังถูกจำคุกไปแล้วแปดปี หลังพ้นโทษเขาได้เปลี่ยนชื่อเป็น เชลซี แมนนิ่ง (Chelsea Manning) และแปลงเพศ เป็นเคลื่อนไหวเพื่อความเป็นธรรมในสหรัฐฯ (American activist and whistleblower)

รูปที่ 16 เชลซี แมนนิ่ง (ซ้าย) และเอเดรียน ลาโม่ (ขวา)

ที่มา Washington post และ the guardian

ลาโม่ ถูกประณามจากหลายฝ่ายทั้งจาก WikiLeaks และกลุ่มแฮ็กเกอร์ต่างๆ ลาโม่ ใช้ชีวิตหลบๆ ซ่อนๆ เร่ร่อนไปทั่วสหรัฐอเมริกา และเสพยาเสพติด เขาเสียชีวิตปริศนาใน วันที่ 14 มีนาคม ค.ศ. 2018 หลายเดือนหลังการชันสูตรศพแพทย์นิติเวชไม่อาจยืนยันสาเหตุการตายได้ แต่สถานที่พบศพมียาเสพติด และพืชกระท่อม

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 3

เอเดรียน ลาโม่ บุกรุกเครือข่ายคอมพิวเตอร์ขององค์กรใหญ่ๆ แล้วมาเปิดเผยตัวตน หวังจะมีรายได้จากการชี้ช่องโหว่ความปลอดภัย แต่เป็นการกระทำความผิดกฎหมายอาญาสมบูรณ์แล้ว เมื่อเปิดเผยตัวตนก็ต้องได้รับโทษ กรณีนี้ชี้ให้เห็นว่าเมื่ออาชญากรไซเบอร์เปิดเผยตัวตนเมื่อใด จะถูกจับกุม และถูกตัดสินดำเนินคดี เขาจะไม่ก่ออาชญากรรมไซเบอร์ประเภทนั้นอีก

แต่อาจจะไม่ใช่ว่า เอเดรียน ลาโม่ จะไม่ก่ออาชญากรรมไซเบอร์ หากแต่อาจจะไม่เปิดเผยตัวตน เพราะเขาใช้ชีวิตพเนจรไปกับคอมพิวเตอร์ หลบซ่อนทั้งการถูกคุกคาม และใช้อินเทอร์เน็ตสาธารณะเพื่อไม่ให้สามารถหาร่องรอยการเชื่อมต่ออินเทอร์เน็ตได้ เพราะอย่างไรชีวิตของเขาอยู่กับคอมพิวเตอร์ตลอดเวลา นั่นย่อมแสดงว่าเขายังคงอาจจะยังบุกรุกเครือข่ายคอมพิวเตอร์แห่งอื่นอยู่ และเชื่อมั่นว่าจะไม่ถูกจับกุมอีกเพราะอำพรางตนหลบซ่อนตัวอย่างดีที่สุด

เชลซี แมนนิ่ง หลบซ่อนอำพรางตนอยู่ในกองทัพสหรัฐ จารกรรมข้อมูลสำคัญของกองทัพและรัฐบาลจำนวนมหาศาลเผยแพร่ออกไป เป็นการก่ออาชญากรรมทางไซเบอร์ต่อความมั่นคง และเมื่อตัวตนของเขาถูกเปิดเผย อาชญากรรไซเบอร์ประเภทนี้จึงยุติทันที

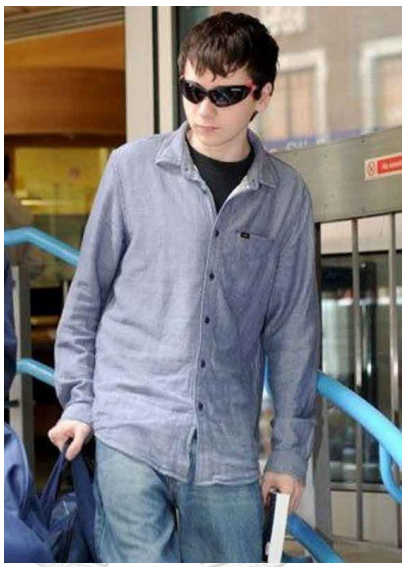
กรณีศึกษาที่ 4 คำสารภาพของ โจนาธาน เจมส์ (Jonathan James) แฮ็กเกอร์เยาวชนวัย 15 ปี

โจนาธาน เจมส์ เป็นเยาวชนคนแรกของสหรัฐอเมริกาที่ถูกดำเนินคดีอาชญากรรมไซเบอร์และมีผลงานก่ออาชญากรรมไซเบอร์ที่ได้รับการยกย่องว่ายิ่งใหญ่ที่สุดคนหนึ่ง มีนามแฝงในวงการแฮ็กเกอร์คือ ‘c0mrade’

ในปี ค.ศ.1999 โจนาธาน เจมส์ ในวัยเพียง 15 ปี เริ่มต้นก่ออาชญากรรมไซเบอร์คดีแรกด้วยการเจาะระบบ และเอาข้อมูลของบริษัท BellSouth ผู้ให้บริการโทรศัพท์เคลื่อนที่รายใหญ่ของสหรัฐอเมริกา เพื่อที่ให้ตนเองได้ใช้โทรศัพท์โทรไปไหนก็ได้แบบฟรีๆ ต่อมาเจาะระบบคอมพิวเตอร์เข้าไปยังหน่วยงาน DTRA (Defense Threat Reduction Agency) ของกระทรวงกลาโหมสหรัฐฯ เพื่อเข้าไปอ่านและดักฟังการสนทนาแบบลับๆ ทางการทหาร ต่อมาเขาแอบติดตั้ง Backdoors ซึ่งเป็นไวรัสคอมพิวเตอร์ชนิดหนึ่งลงในซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ขององค์การบริหารการบินและอวกาศแห่งชาติสหรัฐฯ หรือนาซ่า (NASA) เพื่อที่จะเข้าไปล้วงข้อมูลลับเกี่ยวกับโครงการทางอวกาศต่างๆ และเขายังสามารถขโมยโปรแกรม proprietary environmental control software เป็นโปรแกรมควบคุมอุณหภูมิ และความชื้น ในการใช้ชีวิตบนสถานีอวกาศ

ซึ่งการแฮ็กระบบคอมพิวเตอร์ของนาซ่าในครั้งนั้น สร้างความเสียหายมากถึง 1.7 ล้านดอลลาร์สหรัฐ หรือประมาณ 59 ล้านบาท ทำให้นาซาต้องปิดปรับปรุงระบบคอมพิวเตอร์ทั้งหมดนานถึง 21 วัน และเมื่อ โจนาธาน เจมส์ ถูกจับกุมเขาสารภาพต่อหน้าศาลว่าที่ตนแฮ็กระบบคอมพิวเตอร์ของหน่วยงานต่างๆ นั้น ก็เพื่อที่จะขโมยโปรแกรมเหล่านั้นมาฝึกการเขียนโปรแกรมภาษา C ของตัวเองให้ดีขึ้นเท่านั้น แต่ไม่นึกว่าโปรแกรมที่ขโมยมาได้นั้นจะแย่มาก (ห่วยแตก) และมีราคาแพงถึงเพียงนี้! โจนาธาน เจมส์ ถูกตัดสินจำคุก 6 เดือน แต่เปลี่ยนเป็นกักบริเวณ ให้เขียนจดหมายขอโทษหน่วยงานที่ได้รับความเสียหาย ห้ามแตะต้องคอมพิวเตอร์ในยามพักผ่อน และทำทัณฑ์บนไว้จนกว่าจะอายุ 18 ปี

โจนาธาน เจมส์ ละเมิดทัณฑ์บน เขาถูกตรวจพบว่าเสพยา จึงถูกนำไปคุมขังที่ อลาบาม่า เป็นเวลา 6 เดือน



รูปที่ 17 Jonathan Joseph James แฮ็กเกอร์เยาวชน

ที่มา https://www.pinterest.com/pin/692850723907288323/

ปี ค.ศ.2007 ห้างสรรพสินค้า TJX ถูกขโมยข้อมูลเลขบัตรเครดิตของลูกค้านับล้านราย โดยแฮ็กเกอร์ กลุ่มหนึ่ง และยังโจมตีทางไซเบอร์ร้านค้าปลีกหลายรายในสหรัฐอเมริกา อาทิ BJ's Wholesale Club, Boston Market, Barnes & Noble, Sports Authority, Forever 21, DSW, OfficeMax, and Dave & Buster's แฮ็กเกอร์กลุ่มนี้มี 13 คน โดยมีหัวหน้ากลุ่มแฮ็กเกอร์ชื่อ Albert Gonzalez ต่อมา Gonzalez ถูกจับในเดือนกันยายน และมีการซัดทอดเปิดเผยรายชื่อกลุ่มแฮ็กเกอร์หนึ่งในนั้นมีชื่อ Christopher Scott และเขาเป็นเพื่อนสนิทกับ โจนาธาน เจมส์

เจ้าหน้าที่สืบราชการลับ บุกเคาะประตูบ้าน เจมส์ และตั้งข้อสงสัยว่า โจนาธาน เจมส์ อาจมีส่วนเกี่ยวข้อง เพราะมีแฮ็กเกอร์ในกลุ่มนี้ใช้นามแฝงว่า J.J. โจนาธาน เจมส์ ปฏิเสธว่าไม่ได้เป็นคนทำและไม่มีหลักฐานเกี่ยวข้องกับเขาและเขา เริ่มป่วยซึมเศร้า

โจนาธาน เจมส์ ในวัย 24 ปี ตัดสินใจฆ่าตัวตาย เมื่อวันที่ 18 ตุลาคม ค.ศ. 2008 เนื่องจากเขาถูกใส่ร้ายว่าเกี่ยวข้องกับการแฮ็กระบบคอมพิวเตอร์ปล้นเงินบริษัทบัตรเครดิตแห่งหนึ่ง โดยโจนาธาน เจมส์ ได้ทิ้งจดหมายลาตายเอาไว้ เนื้อหาในจดหมายระบุว่า

‘ผมไม่เชื่อในกระบวนการยุติธรรม บางทีการตายของผมจะสามารถช่วยให้ผู้คนแข็งแกร่งขึ้น ผมไม่สามารถควบคุมสถานการณ์เหล่านี้ได้อีกแล้ว นี่เป็นวิธีเดียวที่จะทำให้ผมได้กลับมาควบคุมตัวเองได้อีกอย่างแท้จริง’

เควิน พอลเซ่น (Kevin Poulsen) แฮ็กเกอร์ และนักเขียนชื่อดังใน นิตยสาร Wired ได้สัมภาษณ์คุณพ่อของ โจนาธาน เจมส์ ชื่อ โรเบิร์ต เจมส์ และเขียนเป็นบทความชื่อว่า Former Teen Hacker's Suicide Linked to TJX Probe[16] มีสาระสำคัญว่า

โรเบิร์ต เจมส์ เป็นโปรแกรมเมอร์ แต่เขาไม่ได้สนิทสนมกับลูกชายมากนัก แต่เขาก็ภูมิใจลึกๆ ว่าลูกชายเป็นคนฉลาดมาก โจนาธาน เจมส์ เล่นคอมพิวเตอร์ตั้งแต่ 6 ขวบ เก่งทั้ง Windows และ Linux พ่อและแม่ของโจนาธาน เจมส์ จะทะเลาะกับลูกเสมอในเรื่องการใช้คอมพิวเตอร์ในตอนกลางคืน

และเขากลับเชื่อว่าแฮ็กเกอร์ในกลุ่มที่ปล้นข้อมูลการเงินห้างสรรพสินค้าในครั้งนั้น ที่ใช้นามแฝงว่า J.J. เป็นลูกชายของเขา

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 4

โจนาธาน เจมส์ ได้รับบทเรียนอย่างหนักหน่วงในวัยที่ยังเป็นเยาวชน จากการศึกษาประวัติของเขาผู้วิจัยเห็นว่า การถูกจับในครั้งแรกๆ นั้น เขาน่าจะไม่มีทักษะในการบิดบังอำพรางตนเท่าที่ควรมีเพียงความรู้ที่เข้าถึงระบบอย่างตรงไปตรงมาและบทเรียนในครั้งนั้นทำให้เขารู้แล้วว่าการบิดบังอำพรางให้ไร้ตัวตนเป็นเรื่องสำคัญของแฮ็กเกอร์

แฮ็กเกอร์ อาจจะเป็นอาชญากรติดนิสัย และเป็นอาชญากรครั้งคราว ต้องฝึกฝนทดสอบตนเองตลอดเวลา เพื่อหาโอกาสเป็นครั้งคราว เป็นไปได้ว่า โจนาธาน เจมส์ ล่องหนหายตัวไร้ตัวตนได้มาหลายปีหลังถูกจับครั้งแรกและถ้าหากมีส่วนร่วมกับการขโมยข้อมูลบัตรเครดิตครั้งใหญ่กับกลุ่มของ Albert Gonzalez จริง การล่องหนหายตัวอย่างไร้ตัวตนของ โจนาธาน เจมส์ หายไป ก็จะต้องถูกจับกุมดำเนินคดีอีกครั้ง และเขาเชื่อว่าคงถูกจับแน่ จึงเป็นชนวนสำคัญที่อาจทำให้ตัดสินใจฆ่าตัวตาย

<u>กรณีศึกษาที่</u> 5 ทวีทรัพย์ ลลิตศศิวิมล สื่อมวลชนขนานนามว่าแฮ็กเกอร์มือหนึ่งของไทย

คดีหมายเลขดำที่ : อ2863/2550 วันที่ฟ้อง : 07/08/2550 และคดีหมายเลขแดงที่ : อ 4948/2551 วันที่ออกแดง : 22/12/2551

[16] Kevin Poulsen (2009). Former Teen Hacker's Suicide Linked to TJX Probe. Cited on September 4, 2009 Available from URL: https://www.wired.com/2009/07/hacker-3/

สิงหาคม 2548 บริษัท ทรูมูฟ จำกัด หรือ บริษัท ที.เอ.ออเร้นจ์ จำกัด ในขณะนั้น ได้แจ้งความว่า มีผู้ลักลอบเจาะเข้าฐานข้อมูลของบริษัท ทำให้สูญเสียเงินไปหลายร้อยล้านบาท จนกระทั่งในวันที่ 26 สิงหาคม 2548 เจ้าหน้าที่ตำรวจก็สามารถจับกุมผู้ต้องหาทั้งหมดได้ นำโดย นายทวีทรัพย์ ลลิตศศิวิมล[17] จำเลยที่ 1 กับพวก สื่อมวลชนกล่าวว่าเขาคือ “แฮ็กเกอร์อันดับ1”ของไทย ติดอันดับ “ปล้นเหยียบเมฆ” ของโลก

นายทวีทรัพย์ ลลิตศศิวิมล จำเลยที่ 1 กับพวก ได้ร่วมกันใช้ข้อมูลรหัส ชื่อผู้ใช้ (user name) และรหัสผ่าน (pass word) ของพนักงานผู้เสียหาย และพนักงาน บริษัท อัลคาเทล ซี. ไอ. ที. จำกัด อันเป็นบัตรอิเล็กทรอนิกส์ เข้าถึงระบบคอมพิวเตอร์ที่บันทึกข้อมูลโทรศัพท์เคลื่อนที่ระบบเติมเงินของบริษัท ที.เอ.ออ เร้นท์ จำกัด ผู้เสียหาย โดยมิชอบ แล้วทำการแก้ไขข้อมูล ตัวเลขจำนวนเงินในบัญชีลูกค้าผู้ใช้บริการโทรศัพท์เคลื่อนที่ในระบบเติมเงินของผู้เสียหายโดยการหลอกลวงดังกล่าวทำให้ผู้เสียหายหลงเชื่อว่ามีการเติมเงินเข้าไปในบัญชีหมายเลขโทรศัพท์เคลื่อนที่ของลูกค้าผู้เสียหายตามจำนวนเงินที่มีการแก้ไขนั้น และมีผลทำให้จำเลยที่ 1 และจำเลยที่ 2 กับพวกได้ไปซึ่งสิทธิและประโยชน์ในการใช้บริการโทรศัพท์เคลื่อนที่ ในระบบเติมเงินของบริษัท ที.เอ.ออเร้นจ์ จำกัด ผู้เสียหาย มีมูลค่าสูงถึง 105 ล้านบาท และได้นำออกไปจำหน่าย 12 ล้านบาทเศษ

ระหว่างประกันตัวออกมาสู้คดี นายทวีทรัพย์ ลลิตศศิวิมล ได้ก่อคดีทำนองเดียวกันเพิ่ม[18] คือ กลางเดือน เม.ย.2550 กองปราบปรามได้รับการร้องเรียนจากเอไอเอสว่า ทางบริษัทน่าจะถูกนักเจาะระบบ(แฮ็กเกอร์) โจรกรรมรหัสผ่านเข้าไปในระบบคอมพิวเตอร์ของบริษัทเพื่อเข้าไปทำการสร้างข้อมูลเกี่ยวกับบัตรเติมเงินมูลค่าต่างๆขึ้นมาใหม่เนื่องจากเจ้าหน้าที่ตรวจสอบพบว่ารหัสสินค้าประเภทบัตรเติมเงินเป็นจำนวนมากไม่ได้ลงทะเบียนในสาระบบและมีการใช้ในวงเงินที่มีมูลค่าสูงขึ้นกว่ามูลค่าเงินเดิมที่ได้ลงทะเบียนไว้ในระบบ

ตัวอย่างเช่น เดิมบริษัทบันทึกในระบบว่ามีบัตรเติมเงินราคา 100 บาทจำนวน 100 ใบก็จะถูกคนร้ายเข้าไปแก้ไขเพิ่มเติมเข้าไปอีก 20 ใบโดยชุดบัตรเติมเงินที่เพิ่มเข้าไปนั้นก็จะถูกคนร้ายแก้ไขเพิ่มวงเงินการใช้จากเดิม 100 บาท เป็น 1,000 บาท ซึ่งบริษัทได้ตรวจสอบพบข้อมูลบัตรเติมเงินที่ผิดปกติย้อนหลังไปถึง 3 เดือนมูลค่าความเสียหายประมาณ 100 ล้านบาท

ส่วนข้อมูลบัตรเติมเงินที่ถูกแก้ไขแล้วนั้น นายทวีทรัพย์จะนำไปลงประกาศผ่านทางอินเตอร์เน็ต โดยเฉพาะการโฆษณาแบบ “ป๊อปอัพแอด” ทางหน้าเว็บไซต์ต่างๆ ประกาศขายบัตรเติม

---

[17] ศาลฎีกาสั่งจำคุก 50 ปีแฮกเกอร์แก้ไขระบบเติมเงินทรูมูฟกว่า 105 ล้านบาท. Thai PBS. 13 กรกฎาคม 2558. Available from URL : https://news.thaipbs.or.th/content/3504

[18] จับแฮกเกอร์มือ 1 ล้วงตับ AIS ทำบัตรเติมเงินโกยร้อยล้าน. ผู้จัดการออนไลน์. 15 พ.ค. 2550. Available from URL: https://mgronline.com/daily/detail/9500000055824

เงินในราคา 100 บาท สามารถโทรได้ 1,000 บาท หากเป็นบัตรราคา 1,000 บาทก็จะสามารถโทรได้ในมูลค่า 10,000 บาท เป็นต้น ผู้ที่สนใจก็จะโอนเงินเข้าบัญชีธนาคารที่เปิดไว้เมื่อได้เงินแล้วก็จะส่งข้อมูลรหัสผ่านมาให้ ซึ่งเจ้าหน้าที่ตำรวจจะได้ตรวจ สอบบัญชีธนาคารต่างๆอีกครั้งว่ามีการแอบอ้างชื่อบุคคลอื่นหรือมีการกระทำผิดเรื่องเอกสารการขอเปิดบัญชีหรือไม่ ส่วนลูกค้าที่ซื้อบริการจากนายทวีทรัพย์นั้นน่าจะมีด้วยกัน 2 ส่วน คือ ลูกค้าทั่วไปที่ทราบข่าวจากโฆษณาและบอกกันปากต่อปาก อีกส่วนหนึ่งเป็นกลุ่มผู้แทนจำหน่ายบัตรเติมเงินที่ไปตั้งโต๊ะขายตามที่ต่างๆ ทั้งในกรุงเทพฯ และต่างจังหวัด

คนร้ายได้หลอกล่อให้เจ้าหน้าที่เชื่อว่าเป็นการใช้คอมพิวเตอร์จากร้านอินเตอร์เน็ตคาเฟ่หลายแห่ง ทำให้เจ้าหน้าที่เชื่อว่าคนร้ายรายนี้ต้องมีความเชี่ยวชาญด้านคอมพิวเตอร์และอินเทอร์เน็ตเป็นอย่างมากจึงเริ่มสืบค้นประวัติอาชญากรคอมพิวเตอร์หลายๆรายที่เคยถูกจับกุม ประกอบกับการใช้วิธีการสืบสวนทางเทคโนโลยีต่างๆเข้ามาร่วมตรวจสอบจนได้ข้อมูลที่เชื่อมโยงกันว่าเป็นฝีมือของนายทวีทรัพย์ อดีตผู้ต้องหาเจาะระบบบริษัท ทรูคอร์ปอเรชั่น จำกัด (มหาชน) ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ ที.เอ.ออเร้นจ์ จำกัด (ปัจจุบันคือทรูมูฟ) ด้วยวิธีการเดียวกันคือเข้าไปแก้ไขวงเงินในบัตรเติมเงิน จึงรวบรวมหลักฐานขออนุมัติหมายจับและหมายค้นห้องพักจากศาล

ขณะนี้ คดีแรก (เจาะระบบ บริษัท ที.เอ.ออเร้นจ์ จำกัด) ถึงที่สุดแล้ว โดยศาลอาญาได้อ่านคำพิพากษาศาลฎีกา เมื่อวันที่ 29 มิถุนายน 2558 ให้ จำคุกจำเลยที่ 1 ฐานร่วมกันปลอมบัตรอิเล็กทรอนิกส์และกระทำความผิดฐานร่วมกันจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม รวม 48 กรรม จำคุกกระทงละ 2 ปี เป็นจำคุก 96 ปี ลดโทษให้ 1 ใน 3 แล้วจำคุก 64 ปี แต่ให้ลงโทษจำคุก 50 ปี ตามที่กฎหมายกำหนด

จำคุกจำเลยที่ 2 ฐานเป็นผู้สนับสนุนความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ และกระทำความผิดฐานร่วมกันจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม รวม 16 กรรม จำคุกกระทงละ 2 ปี เป็นจำคุก 32 ปีลดโทษให้ 1 ใน 3 แล้วจำคุก 21 ปี 4 เดือน จำเลยที่ 3 กระทำความผิดฐานร่วมกันจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม รวม 4 กรรม จำคุกกระทงละ 2 ปี เป็นจำคุก 8 ปี ลดโทษให้ 1 ใน 3 แล้วจำคุก 5 ปี 4 เดือน

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 5

แท้จริงแล้ว จากการค้นคว้าของผู้วิจัยไม่พบว่า เจ้าหน้าที่ตำรวจใช้เทคนิคการสืบสวนใด จนนำไปสู่การจับกุมด้วยเทคโนโลยีใด และจากการศึกษาคำฟ้อง/คำพิพากษา ไม่พบว่าฟ้องคดีเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ แต่เป็นการฟ้องให้ลงโทษ ข้อหา “ร่วมกันใช้บัตร

อิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ร่วมกันปลอมบัตรอิเล็กทรอนิกส์ มีไว้เพื่อจำหน่ายบัตรอิเล็กทรอนิกส์ปลอม ร่วมกันฉ้อโกง”

ดังนั้น คดีนี้จำเลยอาจจะไม่ใช่แฮ็กเกอร์ที่เจาะระบบคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต แต่เป็นการเข้าถึง (user name) และรหัสผ่าน (pass word) ของพนักงานด้วยวิธีการอื่น และการสืบสวนจับกุมจึงไม่น่าจะใช้เทคโนโลยีในการตามหาตัวตนจำเลยได้พบ หากแต่อาจจะเป็นการสืบสวนทางอื่นโดยอ้อม เช่น จากคู่ค้าบัตรเติมเงินหรือบัญชีธนาคาร

จึงยังคงทำให้จำเลยมั่นใจว่า หากยังประกอบอาชญากรรมไซเบอร์ด้วยเทคโนโลยีเดิมก็คงไม่ถูกจับกุมได้แน่นอน เพราะไร้ตัวตน (Anonymity) ไร้ร่องรอย เมื่อประกันตัวออกมาสู้คดีจึงยังประกอบอาชญากรรมแบบเดิม และเจ้าหน้าที่ตำรวจสืบจากประวัติอาชญากรที่มีลักษณะเดียวกันและมีเพียงรายเดียว จึงง่ายในการสืบสวนจับกุมขยายผลดังกล่าว

การไร้ตัวตน (Anonymity) ของเทคโนโลยีที่จำเลยใช้ประกอบอาชญากรรม ทำให้จำเลยยังเชื่อมั่นว่า เขาจะไม่ถูกจับกุมได้ เทคโนโลยีที่ปิดบังซ่อนเร้นตัวตนยังใช้ได้ดี จึงเป็นแรงจูงใจให้ชั่งน้ำหนักตัดสินใจเลือกประกอบอาชญากรรมไซเบอร์ซ้ำสองอีกครั้งหนึ่ง

<u>กรณีศึกษาที่</u> 6 แฮ็กเกอร์คุณธรรม มอส นามสมมุติ

ผู้วิจัยได้สัมภาษณ์เชิงลึก “มอส” นามสมมุติ แฮกเกอร์คุณธรรม (White hat) โดยไม่เคยพบตัวจริงมาก่อน ได้รับการติดต่อผ่านจาก ผู้ช่วยอาจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยแห่งหนึ่งแนะนำให้ และผู้วิจัยได้โทรศัพท์ไปบอกกล่าวขอบเขตการสัมภาษณ์เพื่อการศึกษาวิจัยให้ทราบก่อน หากยินยอมให้โทรกลับมาแจ้งว่าอนุญาตให้สัมภาษณ์จริงอีกครั้ง จึงจะเริ่มต้นสัมภาษณ์ ในระหว่างสัมภาษณ์ทางโทรศัพท์ได้ขออนุญาตเปิดลำโพงและบันทึกเสียงไว้เป็นหลักฐานทางวิชาการ (รายละเอียดการถอดความสนทนาในภาคผนวก)

เหตุผลที่ผู้วิจัยเลือกมอสเป็นผู้ให้ข้อมูลสำคัญ ด้วยในเบื้องต้นได้ติดต่อไปยังผู้ช่วยอาจารย์ท่านดังกล่าว ซึ่งนอกจากเป็นผู้ช่วยสอนวิศวกรรมคอมพิวเตอร์แล้ว ยังเป็นวิศวกรคอมพิวเตอร์ที่อยู่ในวงการวิศวกรรมคอมพิวเตอร์ จึงขอให้แนะนำผู้ให้ข้อมูลสำคัญที่ยินดีให้สัมภาษณ์ทางโทรศัพท์ โดยต้องการคนที่เคยทำความผิดเกี่ยวกับคอมพิวเตอร์และกลับตัวใช้ความรู้ความสามารถของตนมาเป็นประโยชน์กับตนและสังคมในปัจจุบัน

จึงได้รับการแนะนำให้รู้จักกับ มอส (นามสมมุติ) อายุ 28 ปี จบการศึกษาระดับปริญญาโทวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยชั้นนำของไทย มีความสนใจคอมพิวเตอร์ตั้งแต่อายุ 4-5 ขวบ แต่

เพื่อเล่นเกมส์คอมพิวเตอร์ ยังไม่ได้สนใจเรื่อง Cyber security จนกระทั่งอยู่ชั้นมัธยมปีที่ 1-2 ผู้วิจัยได้ถอดบทสัมภาษณ์ออกมาสรุปเป็นข้อความดังนี้

มอส ในวัย ม.1 - ม.2 โรงเรียนที่มอสเรียนอยู่จะจำกัดเว็บไซต์ที่อนุญาตนักเรียนเข้าได้ โดยตั้งค่าจากรหัส login ใช้ WiFi ของโรงเรียน มอส จึงรู้สึกท้าทายความสามารถของเขาและเด็กนักเรียนหลายคนก็รู้สึกเช่นนั้น มอสเริ่มศึกษาด้วยตนเองว่าจะแก้ไขระบบอย่างไรให้เข้าเว็บไซต์ที่ถูกจำกัดได้ แล้วมอสได้ไปพบหนังสือ โปรแกรมคอมพิวเตอร์ ภาษา ซี ในเล่มมีบทที่สอนเขียนโปรแกรม Key logger (โปรแกรมขโมยพาสเวิร์ดจากเหยื่อเป้าหมาย เมื่อลงโปรแกรมในเครื่องนั้นแล้วจะบันทึกความจำการกดแป้นพิมพ์ไว้ทำให้รู้รหัสผ่าน) แล้วเขาจึงเขียนโปรแกรม Key logger ตามหนังสือ แล้วเอาไปไปฝังไว้ในเครื่องคอมพิวเตอร์ของอาจารย์ เมื่อถึงเวลาอาจารย์เปิดคอมพิวเตอร์พิมพ์ ก็จะส่งทั้ง Username และ Password ของอาจารย์กลับมาให้ มอส ทำให้เขาเข้าอินเทอร์เน็ตและระบบคอมพิวเตอร์ของโรงเรียนได้อย่างไม่มีข้อจำกัด มอส เล่าว่าเขารู้สึกดีใจตื่นเต้นมาก เพราะเริ่มฝ่าฝืนกฎระเบียบครั้งแรกแล้วสำเร็จเลย

ในประเด็นนี้ผู้วิจัยได้สังเกตจากการศึกษาหลายๆ กรณี พบว่าเหล่าแฮ็กเกอร์ล้วนถือกำเนิดจากการถูกจำกัดการเข้าเว็บไซต์หรือจำกัดเวลาในการใช้คอมพิวเตอร์ในวัยเด็กแทบทั้งสิ้น ทั้งจากโรงเรียนและผู้ปกครองที่บ้านที่ลงทุนซื้อซอฟต์แวร์จำกัดเวลาการใช้คอมพิวเตอร์ ไม่ว่าจะเป็น เควิน มิตนิก และ มาร์คัส ฮัตชินส์ เป็นต้น รวมถึงมอส มุมมองผ่านสายตาผู้วิจัยสัมผัสได้ถึงความรู้สึกน้ำเสียงของมอสจากการสนทนาว่านั่นคือความรู้สึกภาคภูมิใจอย่างยิ่งกับประสบการณ์ชีวิตวัยเด็กครั้งนั้นและเมื่อหวนกลับไปนึกถึงความคิดความรู้สึกของตัวผู้วิจัยเองสมัยเป็นนักศึกษาวิศวกรรมศาสตร์เมื่อเข้าห้องปฏิบัติการคอมพิวเตอร์ของมหาวิทยาลัยแล้ว ทุกคนจะพยายามแสวงหาสิ่งใหม่หรือเทคนิคการใช้คอมพิวเตอร์ใหม่ๆ ตลอดเวลา โดยเฉพาะการเข้าเว็บไซต์แปลกๆ ที่ถูกจำกัดจะได้รับการยกย่องจากเพื่อนๆที่มามุงล้อมดู และเมื่อมองผ่านสายตาแฮ็กเกอร์ชื่อดังของโลกที่สามารถเอาชนะระบบที่จำกัดสิทธิการใช้คอมพิวเตอร์ของพวกเขาได้ ผู้วิจัยเชื่อว่าเขาจะรู้สึกมีอำนาจเหนือการถูกควบคุมและมีแรงผลักดันให้ทำอะไรที่วิเศษกว่านั้นได้ยิ่งขึ้นไปอีก

ต่อมาอาจารย์ทราบว่ามอสขโมยพาสเวิร์ดอาจารย์ไปได้และเข้าเว็บไซต์ที่ถูกจำกัดไว้ได้ เป็นการก่ออาชญากรรมคอมพิวเตอร์ที่มีโทษร้ายแรงและผิดวินัยโรงเรียน แต่อาจารย์กลับไม่ตำหนิอะไรและรู้ว่า มอส มีความสามารถทางด้านนี้มาก เลยสนับสนุนส่งเสริมไปแข่งขันทักษะวิชาการ นั่นคือจุดเริ่มต้นความสนใจด้านความปลอดภัยไซเบอร์จนได้เรียนจบถึงปริญญาโทวิศวกรรมคอมพิวเตอร์และได้มีงานที่ดีทำ ในประเด็นนี้เป็นข้อแตกต่างของอาชญากรคอมพิวเตอร์ชื่อดังหลายๆคน เพราะเมื่อถูกจับได้ครั้งแรกในวัยเด็กทั้ง เควิน มิตนิก และมาร์คัส ฮัตชินส์ กลับถูกลงโทษรุนแรงเสียใจจน

บอบช้ำและพวกเขาก็พัฒนาขีดความสามารถของตนให้ร้ายกาจยิ่งขึ้นไปอีก ในทางกลับกันถ้ามอสถูกลงโทษรุนแรงชีวิตอาจจะเปลี่ยนไปในอีกทางหนึ่งก็เป็นได้

จากนั้น มอส มีความรู้และทักษะในการ Hack เจาะระบบคอมพิวเตอร์มากขึ้น เริ่มเปลี่ยนหน้าเว็บเพจ ของโรงเรียนตนเอง โรงเรียนอื่นๆ และหน่วยงานต่างๆ เขาคิดว่าไม่ได้สร้างความเสียหายอะไรมาก เป็นเรื่องสนุกเพราะไม่ชอบโรงเรียนนั้นไม่ชอบองค์กรนี้ มอส ให้ความเห็นว่าแท้จริงแล้วเขายังไม่ได้ใช้ความสามารถอะไรมาก เพียงแต่ผู้ดูแลระบบเหล่านั้นตั้ง Password อ่อนแอ เช่นตั้ง ตั้ง Password ว่า Password เป็นการเดา Password อย่างง่าย (เรียกว่า Brute force attack)

จากประสบการณ์ของผู้วิจัยที่เคยหัดเขียนเว็บไซต์ราวปี พ.ศ.2548-2549 (ก่อนมี พรบ. คอมพิวเตอร์บังคับใช้) ทำให้ทราบว่า เว็บไซต์ปกติทั่วไปผู้ดูแลเว็บไซต์จะ Login เข้าระบบผ่านหน้าเว็บไซต์ด้วยเพิ่มท้าย URL ชื่อเว็บไซต์ว่า “/admin” เช่น เว็บไซต์ xxx.com ผู้ดูแลระบบจะพิมพ์ว่า xxx.com/admin ซึ่งในอดีตหน่วยราชการห้างร้านเมื่อจ้างทำเว็บไซต์แล้วส่งมอบงาน เขาจะให้ผู้ว่าจ้างเปลี่ยนพาสเวิร์ดเอง โดยมี username เริ่มต้นคำว่า admin หรือคำว่า username ทับศัพท์กันลืม ส่วน password นิยมเป็น 1234 หรือคำว่า password อย่างที่มอสกล่าวไว้ แต่แล้วหน่วยราชการห้างร้านก็ไม่ได้เปลี่ยน username กับ password ทำให้แฮ็กเกอร์ยึดเว็บเพจไปได้ง่ายดาย

ตัวอย่าง การเข้าหน้าเว็บไซต์องค์การบริหารส่วนตำบลแห่งหนึ่ง

ผู้วิจัยได้ลองคำนึงถึงบริบทปัจจุบัน องค์กรใหญ่ๆหรือหน่วยราชการคงมีประสบการณ์มากแล้วและมีบุคคลากรที่เชี่ยวชาญมารับผิดชอบ จึงตั้งสมมติฐานในใจว่าหน่วยราชการย่อยๆ เช่น สถานีตำรวจภูธร และองค์การบริหารส่วนตำบลเริ่มมีเว็บไซต์กันมากขึ้น ซึ่งผู้วิจัยเชื่อว่าหน่วยงานย่อยเหล่านั้นน่าจะขาดผู้เชี่ยวชาญมาดูแลเว็บไซต์และหลังการส่งมอบงานเขียนเว็บไซต์ก็ยังคงพิมพ์ “/admin” ต่อหลัง URL แล้วเข้าสู่หน้า Login ของ Admin ได้ จึงทดลองเข้าเว็บไซต์ขององค์การบริหารส่วนตำบลแห่งหนึ่งและก็เป็นดังที่คาดไว้เข้าสู่หน้า Login ของ Admin ได้อย่างง่ายดาย

รูปที่ 18 ตัวอย่างการเข้าสู่หน้า Login ของ Admin เว็บไซต์องค์การบริหารส่วนตำบลแห่งหนึ่ง

ผู้วิจัยได้ตั้งถามคำถามสำคัญกับมอสว่า “ตอนเป็นเด็กมั่นใจได้แค่ไหนว่า...เขาสืบหาเราไม่ได้หรือจับเราไม่ได้?” มอส ตอบว่ามั่นใจมาก เพราะ แฮ็ก ระบบผ่าน Tor Browser จะเปลี่ยนเลขหมาย IP ของเขาไปเรื่อยๆ เป็นประเทศอื่นที่ ไม่ใช่ประเทศไทย นอกจากนั้นยังทำการ Brute Force เอาตัว Password WiFi ข้างบ้านมาใช้ WiFi ถึงจับได้ก็มั่นใจว่า ไม่มีหลักฐานดำเนินคดีกับเขาได้อยู่ดี

ผู้วิจัยได้ถามคำถามสุดท้ายว่า “เป็นคนหาโอกาสตลอดเวลาเห็นช่องว่างแล้วค่อยลงมือหรือไม่?” มอส ตอบสวนทันทีไม่คิดนาน ว่าเขามองหาตลอดเวลา ทุกครั้งที่มีระบบใหม่ขึ้นมา เขาจะสงสัยว่าระบบใหม่มีช่องโหว่อยู่หรือไม่ หรือถ้าเข้าสามารถแฮ็กระบบที่ไม่เคยมีใครเจาะได้จะภูมิใจมาก ซึ่งในวงการแฮ็กเกอร์ ถ้าใครเจาะระบบไหนได้ แล้วยังไม่เคยมีมีใครเจาะช่องโหว่นั้นได้ คนนั้นจะได้หมายเลข CVE ตามด้วยชื่อหรือนามสมมุติของแฮ็กเกอร์คนนั้น มอส ให้ข้อมูลว่ากลุ่มแฮ็กเกอร์มีการแลกเปลี่ยนข้อมูลใน Dark web เข้าผ่าน TOR

ในมุมมองผ่านสายตาผู้วิจัย แฮ็กเกอร์เป็นอาชญากรติดนิสัย ดังเช่นที่ผู้วิจัยยกตัวอย่างการพิมพ์ “/admin” ต่อหลัง URL เมื่อพบเว็บไซต์ใหม่หรือประเมินจากองค์กรหรือเจ้าของเว็บแล้วว่าน่าจะหละหลวมในมาตรการป้องกันอันเป็นกิจวัตรและขาดผู้พิทักษ์ดูแล แฮ็กเกอร์จะติดนิสัยพิมพ์ “/admin” ต่อหลัง URL เมื่อเข้าสู่หน้า Login ของ Admin ได้จะทดลองเดา username กับ password อย่างง่ายทันที

มอสให้ข้อมูลประสบการณ์ว่าแม้แต่ธนาคารเขาก็ยังเคยเข้ายึด เพราะมาตรการรักษาความปลอดภัยเว็บไซต์หละหลวมให้เดา username กับ password ง่ายดาย ซึ่งเขาไม่ได้ใช้ความสามารถหรือเขียนซอฟต์แวร์มาเจาะระบบ

มอสให้ข้อมูลเพิ่มเติมว่า การปิดบังตัวตนเป็นหัวใจสำคัญของแฮ็กเกอร์และไม่ไว้ใจกัน แฮ็กเกอร์มีชุมชนใน Dark web แลกเปลี่ยนความรู้และศึกษาพัฒนาตัวเองตลอดเวลา แต่ขณะเดียวกันจะไม่คลิก Link ที่มีใครส่งมาให้เพราะอาจจะเป็น Script มัลแวร์ก็เป็นได้

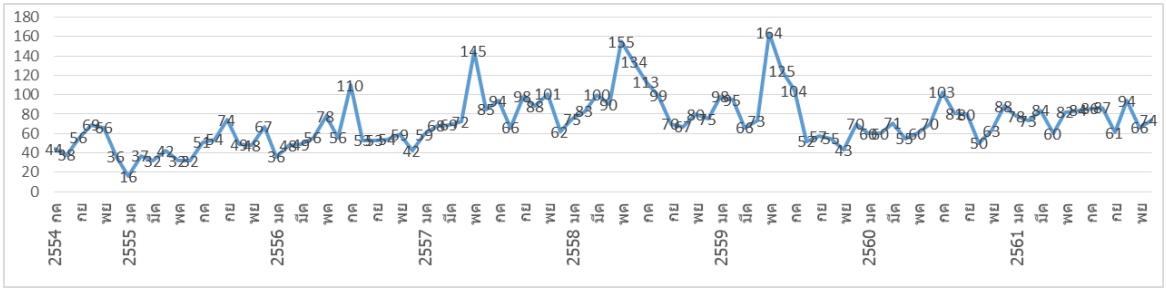
ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 6

มอส แฮ็กเกอร์ มีแรงจูงใจในวัยเด็กอยากได้ Password ของอาจารย์ เป็นสิ่งที่ท้าทายให้เขาพัฒนาความสามารถในการเขียนโปรแกรมด้วยตัวเองจนเก่งขึ้น เพื่อที่จะได้ท่องเว็บที่นอกเหนือจากที่โรงเรียนจำกัดไว้ แม้การเข้าถึงมาตรการรักษาความปลอดภัยระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเขาก็ไม่ได้คำนึงถึงโทษอาญา และตกเป็นอาชญากร หรือถูกลงโทษจากอาจารย์

แต่อาชญากรคอมพิวเตอร์ส่วนใหญ่ แตกต่างจากอาชญากรในคดีอาญาอื่นๆ ตรงที่อาชญากรทั่วไป ต้องการหาประโยชน์ให้ตนบนความเสียหายของผู้อื่น แต่อาชญากรคอมพิวเตอร์หลายคนที่มีจุดเริ่มต้นในวัยเด็กล้วนต้องการเพียงความสนุกหรือทำสิ่งที่ท้าทายความสามารถ ไม่ได้มุ่งสร้างความเสียหายแก่ผู้อื่น และมอสก็เช่นกัน ขาดเจตนาร้ายกับผู้อื่น แต่ลักษณะความเป็นอาชญากรในตัวของเขาที่ได้ทราบจากการสัมภาษณ์นั้นก็คือ การมุ่งหาแสวงหาโอกาสตลอดเวลา เป็นอาชญากรติดนิสัย (Habitual Criminal) และทันทีที่เขาพบโอกาสที่ทำให้มั่นใจว่า จะไม่มีใครรู้ว่าเขาเป็นใคร (สืบหาไม่ได้) และมั่นใจว่าไม่สามารถดำเนินคดีกับเขาได้ (ใช้ WiFi ข้างบ้าน) เขาจะลงมือเจาะระบบนั้นทันที

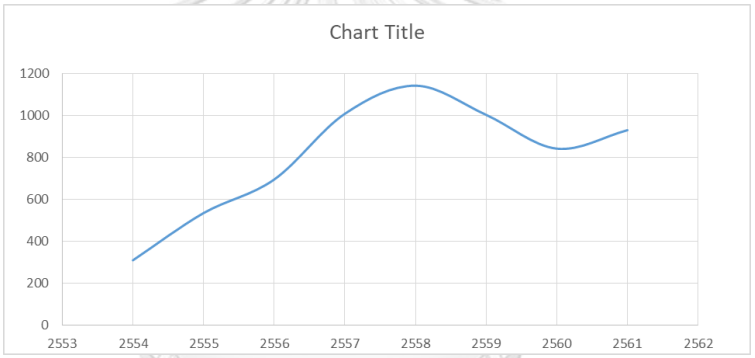
<u>กรณีศึกษาที่</u> 7 อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ แบบ แก๊งคอลเซ็นเตอร์

อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) ในประเทศไทย มี 3 ชนิดหลักๆ คือ คดีแก๊งคอลเซ็นเตอร์ คดี Romance Scam และคดี Digital Asset Scam



รูปที่ 19 กราฟเชิงเส้นอาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) ในประเทศไทย จากข้อมูลสถิติรายเดือนตั้งแต่ปี พ.ศ.2554-2561

ที่มา ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.)



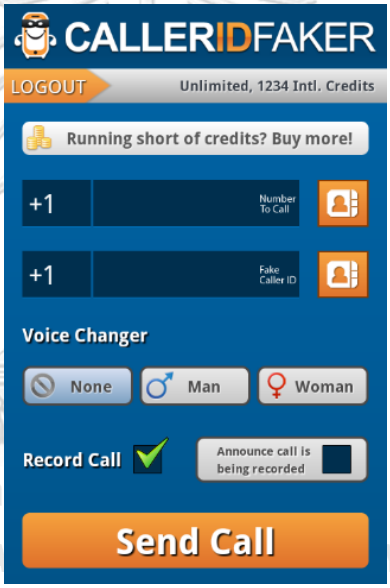
รูปที่ 20 การทำให้เป็นกราฟเชิงเส้นของ อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) ในประเทศไทย จากข้อมูลสถิติรายปี พ.ศ.2554-2561

ที่มา ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.)

ทวีป (2555) คดีแก๊งค์คอลเซ็นเตอร์ คือ การฉ้อโกงออนไลน์ โดยใช้เทคโนโลยี Voice over Internet Protocol (VoIP) เป็นเทคโนโลยีที่ใช้การติดต่อโทรศัพท์ผ่านทางเครือข่ายอินเทอร์เน็ตแทนการใช้เครือข่ายโทรศัพท์ปกติ เพื่อปิดบังตัวตนให้พ้นจากการถูกจับกุม

จากการค้นคว้าข่าวพบว่า คดีแก๊งค์คอลเซ็นเตอร์ ได้ก่ออาชญากรรมฉ้อโกงออนไลน์ในประเทศไทยเริ่มต้นขึ้นเมื่อปี พ.ศ.2552[19] และเมื่อค้นคว้าจากข่าวพบว่าได้มีจำนวนคดีเพิ่มมากขึ้นในปี พ.ศ. 2553[20] และ พ.ศ. 2554 ตามลำดับ

5 ธ.ค. 2560 ผู้จัดการออนไลน์ ได้นำเสนอข่าวในหัวข้อ “อย่าวางใจเบอร์โทร.เข้า! แอปฯ โชว์เบอร์ปลอมมีเพียบ “แก๊งคอลเซ็นเตอร์” นำไปใช้หลอกเหยื่อ”[21] แก๊งคอลเซ็นเตอร์ นอกจากใช้เทคโนโลยี Voice over Internet Protocol (VoIP) อาชญากรยังพัฒนาเทคนิคการก่ออาชญากรรมมาใช้แอพพลิเคชัน (Application) ที่เรียกว่า Fake Caller ID หรือ Caller ID Maker สามารถปลอมเบอร์โทรเข้า โดยแสดงหมายเลขเป็นหมายเลขโทรศัพท์ของหน่วยราชการหรือสถาบันการเงิน เพื่อทำให้เหยื่อหลงเชื่อสนิทใจ



รูปที่ 21 แอพพลิเคชัน (Application) Fake Caller ID หรือ Caller ID Maker

ที่มา https://www.getjar.com/categories/all-games/multiplayer-games/Caller-ID-Faker-35339

---

[19] จำคุก 20 ปี! แก๊งคอลเซ็นเตอร์ไต้หวันหลอกโอน 2 ล้าน. ผู้จัดการออนไลน์ 31 มี.ค. 2554. Available from URL: https://mgronline.com/crime/detail/9540000040829

[20] แฉกลฮิต รวมมุกเด็ด แก๊งคอลเซ็นเตอร์ ก่อนตกเป็นเหยื่อ ตุ๋นหลอกโอนเงิน.ไทยรัฐออนไลน์ เผยแพร่เมื่อ 13 พ.ย. 2560 05:30 น. Available from URL: https://www.thairath.co.th/scoop/1122724 และปอศ.จับแก๊งค์คอลเซ็นเตอร์อ้างตัวเป็นพนักงานธปท. หลอกเงินคนไทยกว่า 20 ล้านบาท. ไทยพีบีเอส เผยแพร่เมื่อ 21 มิถุนายน 2556. Available from URL: http://news.thaipbs.or.th/content/178597

[21] อย่าวางใจเบอร์โทร.เข้า! แอปฯ โชว์เบอร์ปลอมมีเพียบ “แก๊งคอลเซ็นเตอร์” นำไปใช้หลอกเหยื่อ.5 ธ.ค. 2560 ผู้จัดการออนไลน์. Available from URL: https://mgronline.com/onlinesection/detail/9600000122700

ในปี 2555 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน หลอกลวงทางโทรศัพท์ (แก๊งคอลเซ็นเตอร์) เป็นจำนวน **679** ราย

ในปี 2556 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงินการหลอกลวงทางโทรศัพท์ จำนวน **603** เรื่อง หลอกลวงทาง E-mail/Social media อีก 104 เรื่อง

ในปี 2557 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน การหลอกลวงทางโทรศัพท์ จำนวน **374** เรื่อง โดยแอบอ้างเป็น ธปท. หรือ ปปง. แจ้งว่าต้องอายัดบัญชีเนื่องจากพบว่ามีเงินทุนหมุนเวียนในบัญชีผิดปกติหรือสงสัยว่าบัญชีจะเกี่ยวข้องกับการค้ายาเสพติด รองลงมาเป็นการหลอกลวงทาง e-mail และSocial Media เช่น Facebook จำนวน **151** เรื่อง โดยหลอกว่าจะได้รับเงินจากต่างประเทศ แต่ต้องโอนเงินค่าธรรมเนียมไปชำระก่อน

สันนิษฐานว่ามีการจับกุมแก๊ง คอลเซ็นเตอร์ ครั้งแรก[22] เมื่อ พ.ศ.2557 เจ้าหน้าที่ตำรวจฝ่ายสืบสวน สน.ทองหล่อ พร้อมนำหมายค้น ศาลอาญากรุงเทพใต้ เลขที่ 64/2557 ลงวันที่ 13 พ.ค.57 เข้าตรวจค้น บ้านเลขที่267/1 ซอยสุขุมวิท 31ถนนสุขุมวิท แขวงคลองตันเหนือ เขตวัฒนา กทม. มีการลักลอบตั้งแก๊งคอลเซ็นเตอร์เครือข่ายชาวจีน

ภายในบ้านหลังดังกล่าวเป็นลักษณะบ้านเดี่ยวหรูสูง 3 ชั้น เนื้อที่ประมาณ 50 ตร.วา มีรั้วรอบขอบชิด เปิดเป็นสำนักงานคอลเซ็นเตอร์ และมีห้องสำหรับพักอาศัยเป็นสัดส่วน รวมทั้งมีการเตรียมเสบียงอาหารไว้เป็นจำนวนมาก ซึ่งภายในพบผู้ต้องหาชาวจีนจำนวน 21 คน เป็นชาย 14 คน เป็นหญิง 7คน พร้อมของกลาง โทรศัพท์บ้าน โทรศัพท์มือถือ โน๊ตบุ๊ค โมเด็มอินเตอร์เน็ต วิทยุสื่อสาร จำนวนมาก

ในปี 2558 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย รายงานสถิติรับเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงินการถูกหลอกลวงทางโทรศัพท์ มีจำนวน **238** ราย

---

[22] ทลายแก๊งคอลเซ็นเตอร์ชาวจีน เสียหายร้อยล้าน.กรุงเทพธุรกิจ. 13 พฤษภาคม 2557 (https://www.bangkokbiznews.com/news/detail/582188)

ในปี 2559 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย รายงานสถิติเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงินการถูกหลอกลวงทางโทรศัพท์ มีจำนวน **987** รายการ

ในการดำเนินคดีภายหลังการสืบสวนจับกุม เจ้าหน้าที่สามารถรวบรวมพยานหลักฐานดิจิทัลเพื่อพิสูจน์ความผิดจำเลยไปจนถึงชั้นฎีกา ศาลสั่งให้ลงโทษอาญา ประเมินว่าเป็นครั้งแรก

ย่อคำพิพากษาศาลฎีกาที่ 831/2559

การแสดงข้อความอันเป็นเท็จต่อประชาชนในความผิดฐานฉ้อโกงประชาชนตาม ป.อ. มาตรา 343 ถือเอาเจตนาแสดงข้อความอันเป็นเท็จต่อประชาชนเป็นสำคัญ โดยจะเห็นได้จากวิธีการหลอกลวง เมื่อจำเลยทั้งสี่กับพวกจัดตั้งระบบอุปกรณ์โทรศัพท์และระบบคอมพิวเตอร์ในรูปสำนักงานเครือข่ายโทรศัพท์ ขึ้นในต่างประเทศ และใช้การสื่อสารทางเสียงผ่านโครงข่าย**อินเตอร์เน็ต** การกระทำของจำเลยทั้งสี่ตามฟ้องจึงเป็นการร่วมกันฉ้อโกงประชาชน

ในปี 2560 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียน และรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน การหลอกลวงทางโทรศัพท์ จำนวน **357** ราย

ในปี 2561 ศูนย์เฝ้าระวังช่วยเหลือประชาชนไม่ตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์ สำนักงาน ปปง. ได้รายงานข้อมูลรับแจ้งเหตุ ตั้งแต่วันที่ 15 พฤศจิกายน 2560 จนถึง 3 กรกฎาคม 2561 มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน **387** ราย รวมมูลค่าความเสียหายประมาณ 172,915,325.86 บาท สามารถยับยั้งและ ช่วยเหลือได้จำนวน 93 ราย มูลค่ารวม 37,716,707.15 บาท

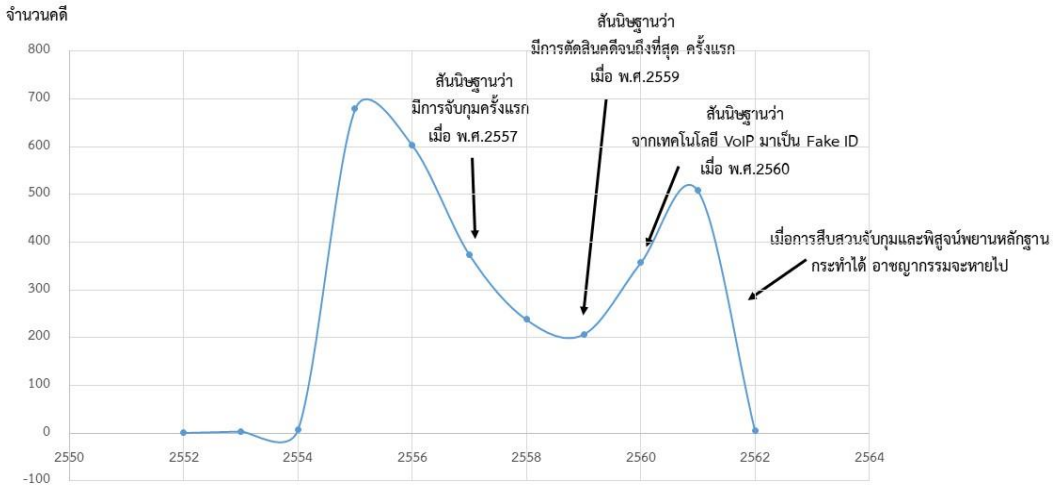
ในปี 2562 ข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) สรุปผลคดีแก๊งคอลเซ็นเตอร์ จากปี พ.ศ. 2561 ถึง 31 พฤษภาคม 2562 ทั้งหมด **514** เรื่อง เสร็จสิ้น 497 เรื่อง คงเหลือ 17 เรื่อง ความเสียหาย 260,437,332 บาท หมายจับเดิม 674 หมาย หมายมีคุณภาพ 595 ราย หมายไม่มีคุณภาพ 79 ราย

สรุปปี พ.ศ. 2562 รับแจ้ง 6 คดี เสียหาย 730,700 บาท

รูปที่ 22 ภาพการแถลงข่าวสำนักงานป้องกันและปราบปรามการฟอกเงิน และสายด่วน 1155 ของสำนักงานตำรวจแห่งชาติ ร่วมกับธนาคารกสิกรไทย ธนาคารไทยพาณิชย์ ธนาคารกรุงเทพ และธนาคารกรุงศรีอยุธยา

ที่มา ไทยรัฐออนไลน์ (thairath.co.th)

21 เม.ย. 2561 สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานตำรวจแห่งชาติ ร่วมกับธนาคารกสิกรไทย ธนาคารไทยพาณิชย์ ธนาคารกรุงเทพ และธนาคารกรุงศรีอยุธยา แถลงข่าวคดีแก๊งคอลเซ็นเตอร์ ตั้งแต่1 เม.ย.61-19 เม.ย.61 มีแนวโน้มลดลงอย่างต่อเนื่องอย่างรวดเร็ว



ที่มา : ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

รูปที่ 23 การสังเกตปรากฏการณ์ แก๊งคอลเซ็นเตอร์ ในประเทศไทย

ที่มา ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.)

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 7

การตีความปรากฏการณ์ที่เกิดขึ้นตามรูปที่ 19 พบว่าอาชญากรรมไซเบอร์แบบ แก๊งค์ คอลเซ็นเตอร์ ในช่วงเริ่มต้นปิดบังซ่อนเร้นหรืออำพรางหมายเลขโทรศัพท์หรือหมายเลข IP Address ได้ดี ทำให้การสืบสวนสอบสวนทางดิจิทัลไม่สามารถดำเนินการจับกุมได้ คดีประเภทนี้จึงเพิ่มสูงขึ้นอย่างรวดเร็วในปี พ.ศ. 2554 แลเมื่อเจ้าหน้าที่กดดันอย่างหนักจนสามารถหาตัวตนจับกุมได้ในปี พ.ศ.2557 และถูกศาลพิพากษาคดีถึงที่สุดได้ในปี พ.ศ.2558 คดีประเภทนี้จึงลดลงอย่างรวดเร็ว

แต่แล้วในปี พ.ศ.2559 ได้มีเทคโนโลยีใหม่มาช่วยปิดบังอำพรางตัวตน อย่างเช่น แอพพลิเคชัน (Application) Fake Caller ID ทำให้คดีประเภทนี้พุ่งสูงขึ้นอย่างมากอีกครั้ง และในที่สุดเจ้าหน้าที่สามารถหาตัวตนจับกุมได้ในปลายปี พ.ศ.25562 คดีประเภทนี้จึงลดลงจนหายไปในที่สุด

อาจเป็นไปได้ว่า การบิดบังอำพรางตัวตน (Anonymity) เพื่อให้หลบพ้นการสืบสวนทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เป็นเหตุเป็นผลต่อการตัดสินใจก่ออาชญากรรมของกลุ่มอาชญากร ส่งผลให้อัตราการเกิดอาชญากรรมไซเบอร์ประเภทคดีแก๊งคอลเซ็นเตอร์ลดลงจนแทบจะหมดสิ้นไปในที่สุด

<u>กรณีศึกษาที่</u> 8 อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ แบบ Romance scam

ลักษณะของอาชญากรรมไซเบอร์ประเภท Romance scam หรือ Scammer หรือ “อาชญากรหลอกให้รัก”เป็นการกระทำอาชญากรรมไซเบอร์ต่อจิตใจบุคคล ด้วยการปฏิบัติการทางจิตวิทยาของอาชญากร อาชญากรจะขโมยรูปภาพผู้ที่มีเสน่ห์ดึงดูด หน้าตาดี หรือมีชื่อเสียง (โดยเฉพาะชาวต่างประเทศ) มาสร้าง Facebook หรือ Social Media อื่นมาสร้างเพจเขียน Profile ให้น่าสนใจ ตลอดจนการสมัครหาคู่รักออนไลน์ในบริการ Dating websites แล้วทำความรู้จักกัน

อาชญากรรมไซเบอร์ประเภทนี้บางครั้งถูกเรียกวิธีว่า Catfishing และอาชญากรจะลงภาพสร้างเรื่องราว Lifestyle ในชีวิตประจำวันอย่างต่อเนื่องเพื่อสร้างตัวตนขึ้นมาเสมือนว่ามีอยู่จริง

จากนั้นอาชญากรจะเริ่มทักทาย ส่งข้อความติดต่อสื่อสารกับเหยื่อ จนเริ่มรู้จักใช้เทคนิคสร้างความสนิทสนมคุ้นเคยขึ้นเรื่อยๆ และในที่สุดอาชญากรจะบอกเหยื่อว่า “ตกหลุมรักเหยื่อเข้าแล้ว” จนอยากจะแต่งงานกับคุณ และมีอนาคตร่วมกัน ในที่สุดก็จะออกอุบายมีสาเหตุให้เสียทรัพย์ ไปจนเสียตัว และถูกล่อลวงเข้าไปทำงานให้องค์กรอาชญากรรม

ผู้วิจัยได้ค้นคว้าวิจัยจริง และสัมภาษณ์เหยื่อพบว่า นับวันคดีเหล่านี้ที่เกิดในประเทศไทยหนักขึ้นเรื่อยๆ ข่าวสาวชาวไทยถูก Romance Scam เลยเถิดจนต้องโทษประหารชีวิตที่มาเลเซียถึง 7 คน และอยู่ระหว่างพิจารณาคดีอีกหลายสิบคน


www.komchadluek.net/news/local/124604

คมชัดลึก

14-20 พ.ย. 59 ราคาเพียง 39,900.-

ข่าวเด่นวันนี้ | บันเทิง | กีฬา | รายงานพิเศษ | ไลฟ์สไตล์ | คลิปเด็ด | ดูดวง

ภูมิภาคทั่วไทย : 5 มิ.ย. 2555

7สาวไทยรอประหารที่มาเลเซีย

สาวไทยรอประหารที่มาเลเซีย - เตือนคิดให้ดีก่อนทำงานผิดกฎหมาย

สาวไทยถูกจับที่ประเทศมาเลเซียรอประหารชีวิต 7 คน ขณะที่รอศาลตัดสินโทษเดียวกันอีก 10 คน ซึ่งทางการประเทศมาเลเซียประกาศเอาจริง แรงงานผิดกฎหมาย พร้อมกวาดล้างทุกวันอย่างต่อเนื่องเพื่อรักษาภาพลักษณ์ของเมือง หลวงคือกรุงกัวลาลัมเปอร์ และเมืองอื่นๆ

นายสมพงษ์ กางทอง อัครราชทูตที่ปรึกษา สถานเอกอัครราชทูต ณ กรุงกัวลาลัมเปอร์ ขณะนี้ทางการประเทศมาเลเซียประกาศเอาจริงจับแรงงานต่างด้าว และการทำผิดกฎหมายในประเทศอย่างจริงจัง ซึ่งขณะนี้คนไทยที่ทำความผิดและถูกจับในประเทศนี้ ด้วยเรื่องยาเสพติด มากเป็นอันดับ 2 รองจากประเทศไนจีเรีย ล่าสุด ศาลได้ตัดสินประหารชีวิตแล้ว 7 คน เป็นผู้หญิงทั้งหมด และยังรอศาลชั้นต้นตัดสินอีก 29 คน ในเขตกัวลาลัมเปอร์ ส่วนในเขตปีนัง ศาลตัดสินประหารชีวิตแล้ว 4 คน รอคำตัดสินอีก 10 คน ถ้ารวมนักโทษที่ต้องโทษประหารชีวิตทั้งหมดในขณะนี้ ประเทศไทยมีสูงมากเป็นอันดับหนึ่ง

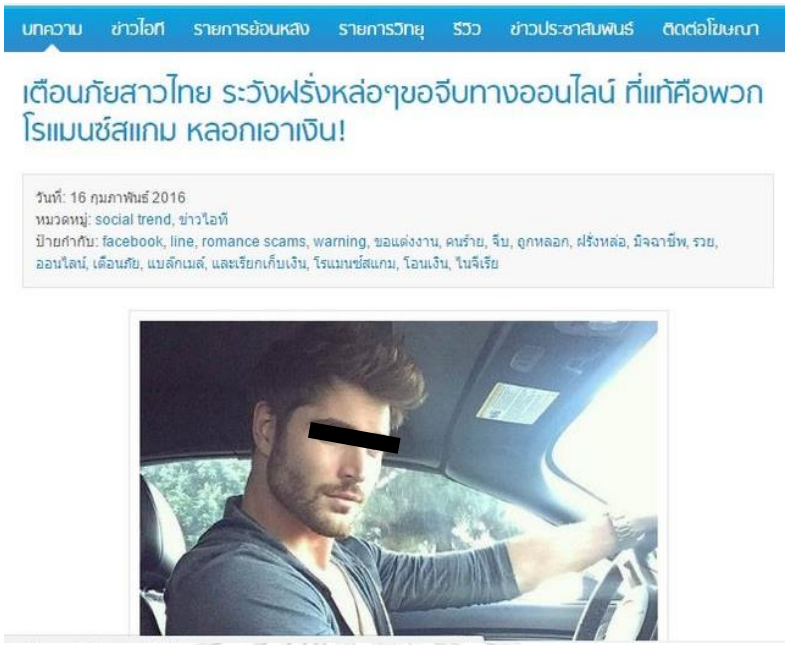
รูปที่ 24 ภาพข่าวจาก คมชัดลึก 5 มีนาคม 2555

ที่มา คมชัดลึก (komchadluek.net)

อาชญากร Romance scam หรือ Scammer ในที่นี้ผู้วิจัยขอเรียกทับศัพท์ ลักษณะการประกอบอาชญากรรม คือ อาชญากรจะขโมยรูปภาพผู้ที่มีเสน่ห์ดึงดูด หน้าตาดี หรือมีชื่อเสียง (โดยเฉพาะในต่างประเทศ) มาสร้าง Facebook เขียน Profile หรือสร้างเพจใน Social medias ต่างๆ หรือ E-mail ตลอดจนการสมัครหาคู่รักออนไลน์ในบริการ Dating websites

ศัพท์เทคนิคทาง Cyber crime เรียกวิธีนี้ว่า Catfishing[23] และพวกเขาจะลงภาพ Lifestyle ที่หรูหราในชีวิตประจำวันอย่างต่อเนื่องเพื่อสร้างตัวตนขึ้นมาเสมือนว่ามีอยู่จริง

[23] David McClellan. What Is Catfishing Online: History, Meaning, Psychology and Everything Else About Catfish Scams. Cited on March 5, 2019. Available from URL: https://socialcatfish.com/blog/what-is-catfishing-online-dating/



รูปที่ 25 ภาพข่าวจากสื่อต่างๆ เกี่ยวกับคดี Romance scam

ที่มา https://petmaya.com/scammer-warning

รูปที่ 26 ภาพข่าวจากสื่อต่างๆ เกี่ยวกับคดี Romance scam

ที่มา tv5.co.th

พฤติการณ์แห่งคดี

อาชญากรส่วนใหญ่เป็น ชาวไนจีเรีย ซึ่งอาชญากรชาวไนจีเรียก่อคดีฉ้อโกงไปทั่วโลก FBI เรียกว่า Nigeria 419 เพราะเป็นมาตรากฎหมายอาญาของ ไนจีเรีย

อาชญากรชาวไนจีเรีย สร้างสื่อ Social media ปลอม โดยเฉพาะ facebook โดยใช้ภาพที่ขโมยมาเป็นชาวฝรั่งผิวขาวมีทั้งหน้าตาดี และหน้าตาธรรมดา เพื่อเลือกให้เหมาะสมกับเหยื่อ อีกทั้งสร้างเรื่องราวว่าตนเองเป็นทั้งคนจนหรือคนรวยเพื่อเลือกให้เหมาะสมกับเหยื่อ บางกรณีปลอมเป็นเจ้าชายตะวันออกกลางผู้สูงศักดิ์ บางครั้งปลอมเป็นทหารอเมริกันภรรยาเสียชีวิตไปนานแล้ว อาศัยอยู่กับแม่และลูกชาย

อาชญากรจะใช้ภาษาอังกฤษในการสนทนา ซึ่งเหยื่อย่อมเป็นคนมีการศึกษา และมีฐานะ จากการวิจัยได้ทราบว่ามีทั้ง หมอ นักธุรกิจ อาจารย์มหาวิทยาลัย ตกเป็นเหยื่อ หญิงไทยบางรายไม่ได้มีฐานะ แต่อาชญากรไนจีเรียเอาไว้ใช้ประโยชน์ เช่น มีลูกด้วยเพื่อจะได้สิทธิในการอยู่ในประเทศไทย หรือใช้เป็นนางนกต่อ เช่น หลอกว่าเป็นเลขา หลอกว่าเป็นเจ้าหน้าที่ศุลกากร และใช้บัญชีธนาคารพวกเธอรับเงิน

จากนั้นอาชญากรจะเริ่มทักทาย ส่งข้อความติดต่อสื่อสารกับเหยื่อ จนสนิทสนมคุ้นเคยขึ้นเรื่อยๆ และอาชญากรจะบอกเหยื่อว่า.... “ตกหลุมรักเหยื่อเข้าแล้ว” จนอยากจะแต่งงานกับคุณ และมีอนาคตร่วมกัน

ในกรณีที่อาชญากรอ้างเป็นชาวต่างชาติ จะออกอุบายว่าเดินทางจะมาพบเหยื่อ แต่เกิดเหตุสุดวิสัยขึ้น เช่น กระเป๋าตังค์หาย เกิดอุบัติเหตุ เป็นต้น ให้เหยื่อโอนเงินมาให้ยืมช่วยเหลือ แล้วจะคืนให้ภายหลังเมื่อไปพบกันแล้ว

“สรุป คือ หลอกให้รัก หาอุบายยืมเงิน แล้วหนี”

ซึ่งแก๊งค์ต้มตุ๋นที่โด่งดังที่สุดในโลกไซเบอร์ก็คือ กลุ่ม อาชญากรไซเบอร์ ชาวไนจีเรีย ที่ชาวโลกขนานนามว่า Nigerian 419

ตัวเลข 419 ก็คือ กฎหมายอาญา มาตรา 419 ของประเทศไนจีเรีย ซึ่งบัญญัติความผิดว่าด้วยการฉ้อโกง (Advance-Fee Frauds) เป็นกฎหมายสำคัญที่แก๊งค์ต้มตุ๋นชาวไนจีเรีย จำนวนมากต้องโทษคดี และทวีจำนวนผู้กระทำความผิดมากขึ้นเรื่อยๆ

ในยุคแรกของอินเทอร์เน็ตนั้น พวกเขาใช้ E-mail ในการหลอกลวงต้มตุ๋น อย่างที่เชื่อว่าหลายคนเคยเจอ คือ อี เมลล์ ที่แจ้งว่า “คุณได้รับรางวัลหรือมรดกจำนวนมหาศาล แต่ต้องโอนเงินค่าภาษีหรือค่าธรรมเนียมไปให้เขาก่อน” หรืออุบายอื่นๆ

เว็บไซต์ FBI จะใช้คำว่า 419 เข้าใจความหมายทันทีว่าเป็นแก๊งค์ต้มตุ๋นทางอินเทอร์เน็ตของชาวไนจีเรีย กลายเป็นคำสากลในอาชญากรรมไซเบอร์ไปแล้ว

หญิงไทยจำนวนมาก โดยเฉพาะสาวต่างจังหวัด นิยมชื่นชมฝรั่งต่างด้าว อยากได้เป็นสามี เพราะดูดีมีความศิวิไลซ์ บางคนสร้างภาพมีการศึกษา มีการงานดี มีฐานะ เป็นคนดี

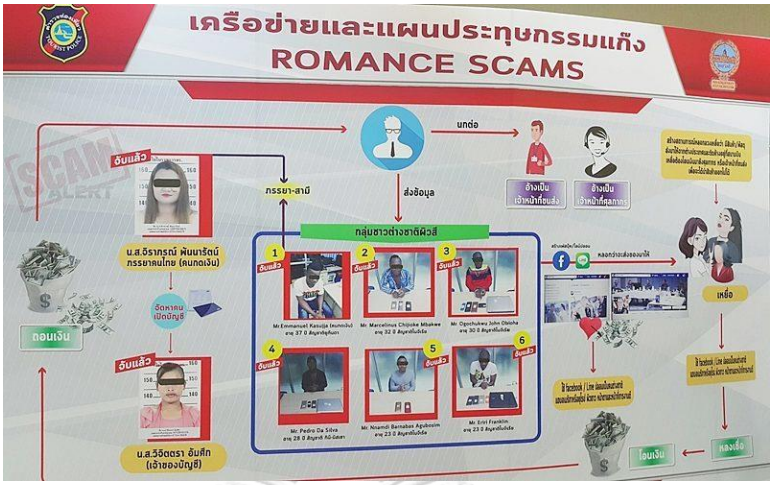
แต่ความจริงกลับกลายเป็นชายชาวแอฟริกันตัวดำผมหยิกยากจนจากไนจีเรีย สร้าง facebook ปลอมขึ้นมา แล้วใช้รูปฝรั่งผิวขาวรูปหล่อขับรถสปอร์ตหรูดูดี มีชีวิตหรูหราในทุกวันเข้ามาตีสนิทกับพวกเธอ เช่น เขาเอารูปจาก facebook ใครสักคนที่ดูดีอีกซีกโลกหนึ่งมาสร้างตัวตนให้เธอเห็น และเริ่มทักทายมาเป็นภาษาอังกฤษ เธอก็รู้สึกตื่นเต้นมากเมื่อชายออนไลน์ที่หมายปองทักทายมาเรื่อยๆ จนเธอต้องเริ่มฝึกภาษาอังกฤษ ตอบไปอย่างกระท่อนกระแท่น วันคืนผ่านไปในที่สุดชายหนุ่มก็สารภาพว่าหลงรักเธออย่างไร้เหตุผลและไม่มีเงื่อนไข เขาจะไม่มีชีวิตอยู่ได้หากไม่มีเธอข้างกาย และแน่นอนเขาจะบินข้ามฟ้ามาหาเธอเพื่อขอแต่งงานให้ได้

เขาลาเธอ บอกว่ากำลังจะเดินทางจากดินแดนอันศิวิไลซ์ห่างไกลโพ้นจะมาหาเธออีกไม่นานและอาจจะขอเธอแต่งงาน เธอเฝ้ารอด้วยหัวใจคับพองอิ่มเอมชีวิตดังความฝันกำลังจะเป็นความจริง

แต่เวลาแห่งการเดินทางของคนรักเริ่มช้าผิดปกติ ในที่สุดเธอได้รับข้อความว่าชายคนรักของเธอประสบอุบัติเหตุถ้าไม่รีบโอนเงินมาเป็นค่าประกันการผ่าตัด ชายคนรักของเธอต้องตายแน่ๆ เพราะทางโรงพยาบาลติดต่อใครไม่ได้ เจ้าหน้าที่จึงขออภัยที่ต้องเปิดดูข้อความในมือถือของเขาและคิดว่าเธอเป็นแฟน

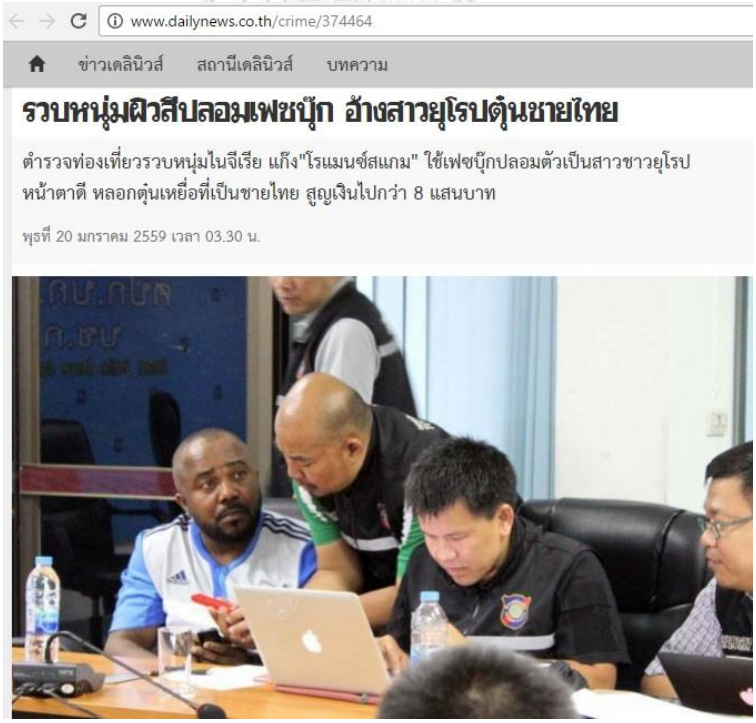
หรือบางครั้ง เขาส่งข้อความมาบอกเองว่า กระเป๋าเงินหายตกเครื่องขณะ transit อยู่ที่ไหนสักแห่ง การเดินทางที่แสนจะมีขวากหนามเพื่อไปหาเธอเจ้าหญิงของเขาน่าเห็นใจยิ่งนัก เขาหาทางออกไม่ได้นอกจากจะขอยืมเงินเธอก่อน โอนมาให้เจ้าหน้าที่ขายบัตรโดยสารเลยก็แล้วกัน อย่างไรก็ตามเขาก็มาหาเธอที่เมืองไทยอยู่ดี แล้วจะคืนให้

ชาวไนจีเรียหลายคนก่อคดี Romance Scams กับสาวไทยนับร้อยๆ ราย เป็นองค์กรอาชญากรรมข้ามชาติ ผู้วิจัยทราบเบื้องต้นในกรุงเทพมหานครมีชาวไนจีเรียเข้ามาสร้างกลุ่มอาศัยอยู่ร่วมกันหลายพันคนย่านรามคำแหง (พ.ศ.2562) แต่ไม่สามารถเข้าไปในทำวิจัยในพื้นที่ได้ เนื่องจากว่าได้รับคำเตือนเกรงว่าผู้วิจัยจะมีอันตราย เพราะผู้วิจัยได้ทำคลิปวิดีโอเตือนภัย คดี Romance scam ที่มีผู้รับชมนับหมื่นคน ทำให้อาชญากรจำใบหน้าได้



รูปที่ 27 ผังผู้ร่วมขบวนการก่อคดี Romance scam[24]

ที่มา สำนักพิมพ์ข่าวสด



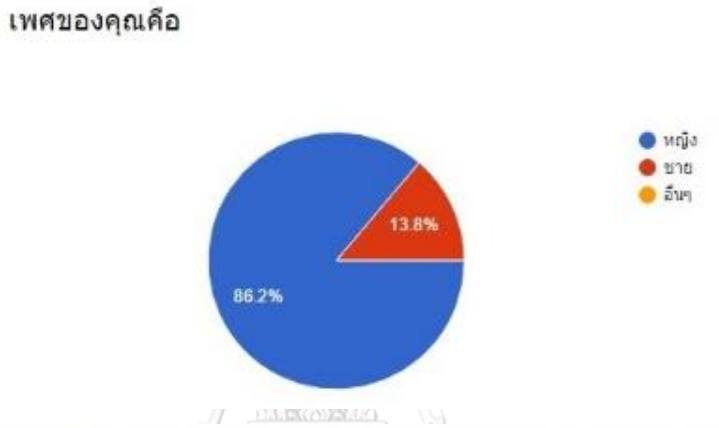
รูปที่ 28 ภาพข่าวจากสำนักพิมพ์เดลินิวส์ ผู้ต้องหาชาวไนจีเรียคดี Romance scam

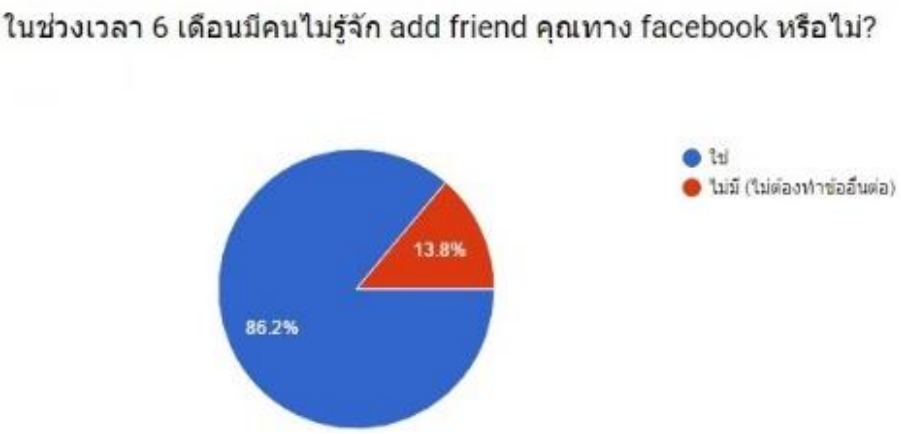
ที่มา dailynews.co.th

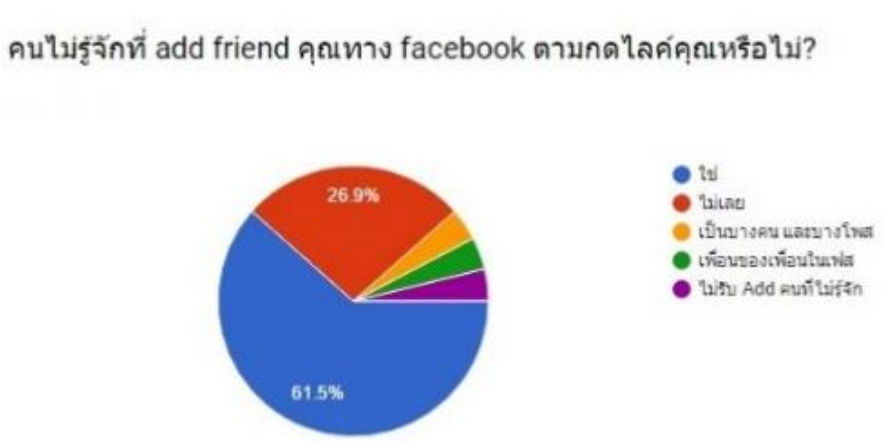
---

[24] ข่าวสด. ‘บิ๊กโจ๊ก’ แถลงจับแก๊งโรแมนซ์สแกม ตุ๋นเหยื่อโอนเงิน แฉกลลวงเตือนภัย!. Cited 2 มิถุนายน 2561; Available from URL: https://www.khaosod.co.th/breaking-news/news_1162267

ผู้วิจัยได้ทำแบบสอบถามออนไลน์ (google form) โดยผู้ตอบไม่ต้องเปิดเผยชื่อจริง แล้วโพสต์ไว้ใน facebook กลุ่ม “ภัยผู้หญิงในโลกออนไลน์” สำรวจหญิงไทยที่ตกเป็นเหยื่อ จำนวน 35 ราย ซึ่งเป็นสมาชิกในเฟซบุ๊ค ได้ผลสำรวจที่น่าสนใจคือ กลุ่มสตรีที่มีโอกาสตกเป็นเหยื่อ 85.7% ไม่ได้เคยพบตัวจริงอาชญากร (Anonymity) แต่ปัจจุบันกลุ่มอาชญากรไซเบอร์ชาวไนจีเรียเข้ามาอาศัยในประเทศไทยเพื่อประกอบอาชญากรรมประเภทนี้กันอย่างมาก เมื่อเหยื่อตกหลุมรักอย่างหนัก อาชญากรจะเปิดเผยตัวตน และมาพบเหยื่อด้วยตัวเอง ผลสำรวจได้ข้อมูลดังนี้

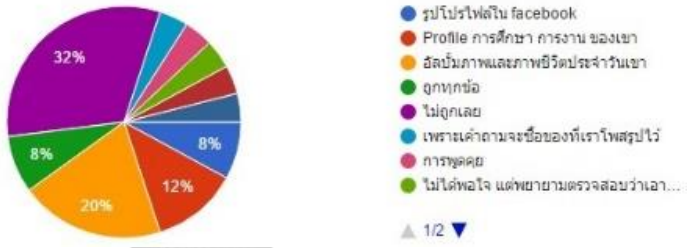




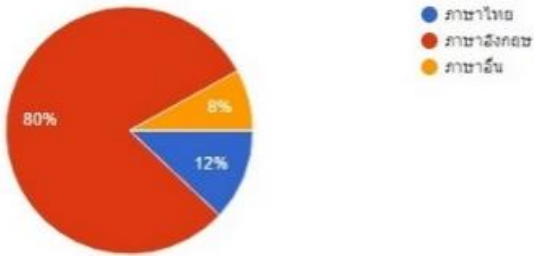


คนไม่รู้จักที่ add friend คุณทาง facebook เริ่มส่งข้อความมาทักคุณหลังจากรับ Add แล้วกี่เดือน?

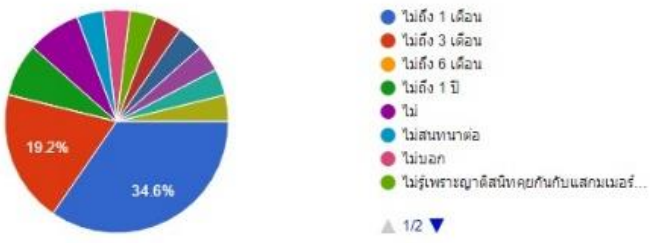
คุณพอใจเขาในระดับหนึ่งถึงคุยด้วยเพราะ?

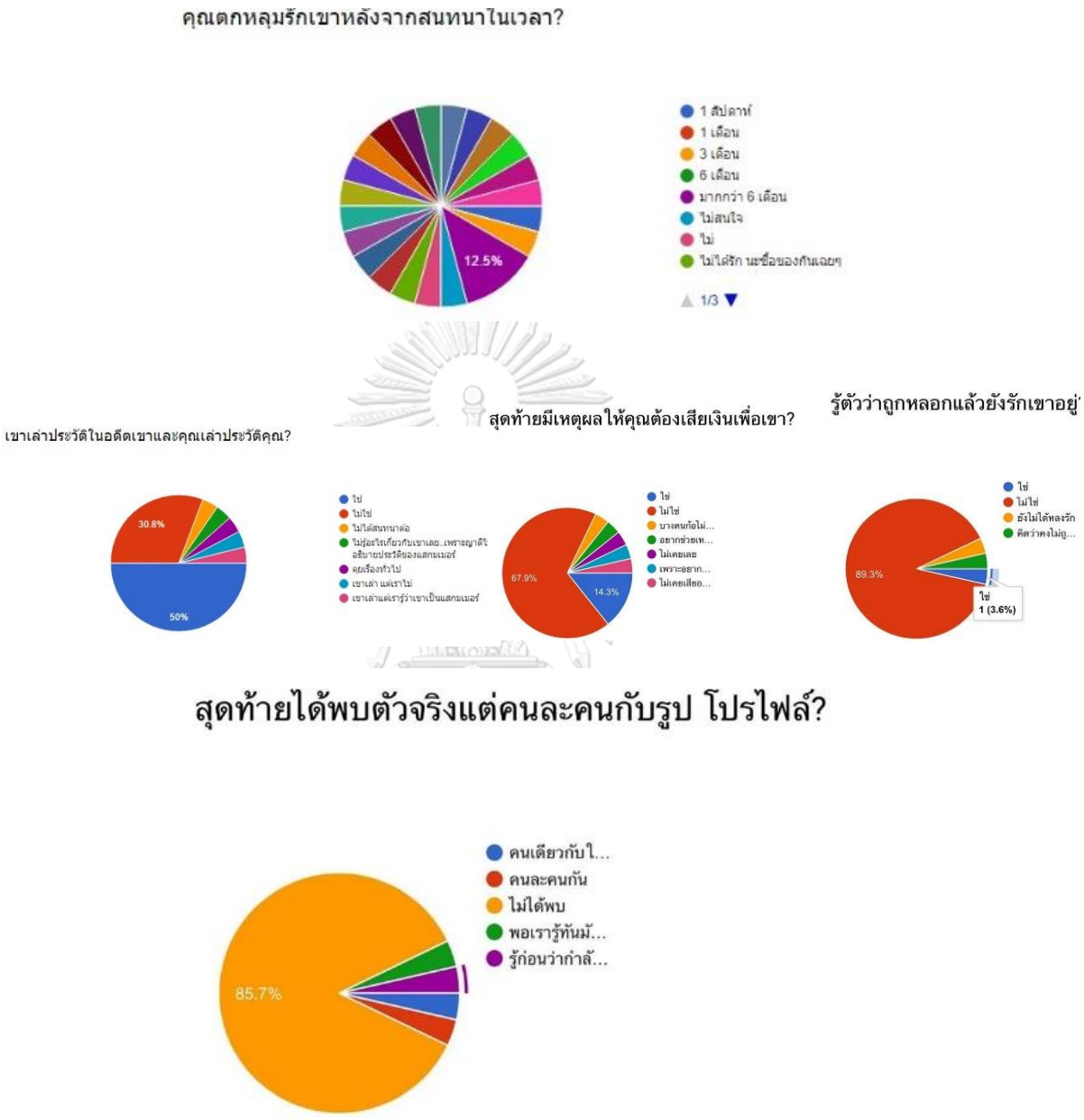


เขาพูดภาษาอะไรกับคุณ



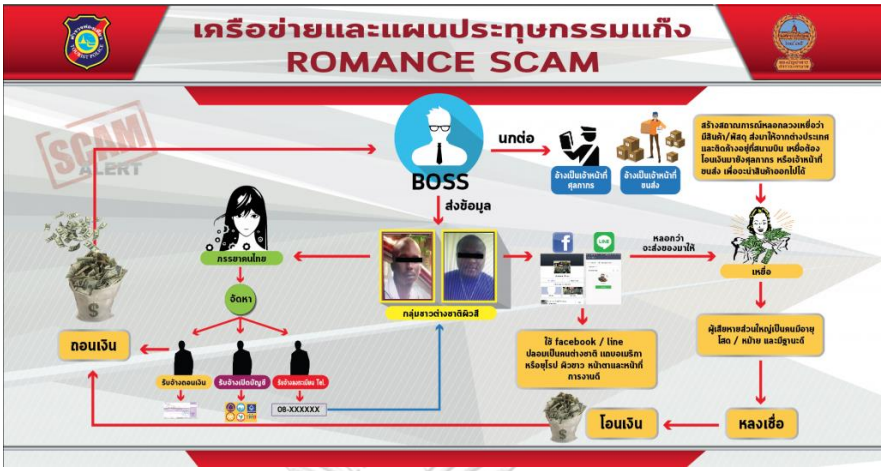
เขาบอกว่าอยากใช้ชีวิตร่วมกับคุณหลังจากรู้จักได้?





รูปที่ 29 ผลสำรวจ จำนวน 35 ราย ในกลุ่ม facebook “ภัยผู้หญิงในโลกออนไลน์”

85.7% อาชญากรล่องหนหายตัว (Anonymity) แต่หญิงไทยหลายรายแม้รู้ว่าถูกหลอกก็ยังหลงรักอยู่ถูกอาชญากรไนจีเรียพาเข้าร่วมองค์กรอาชญากรรมข้ามชาติ ทั้งการค้ามนุษย์ ค้ายาเสพติด จนต้องโทษอาญาในมาเลเซียหลายราย



รูปที่ 30 ผังเครือข่ายและแผนประทุษกรรมคดี Romance scam

ที่มา ตำรวจท่องเที่ยว

ปี 2555 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ profile และอีเมล์ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **47** ราย

ปี 2556 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ E-mail/Social media ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **104** ราย

ปี 2557 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ E-mail/Social media ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **151** ราย

ปี 2558 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ E-mail/Social media ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **126** ราย

ปี 2558[25] พ.ต.อ.ภาณุวัฒน์ ร่วมรักษ์ รองผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (รอง ผบก.ปอท.) ระบุว่า ที่ผ่านมาเฉพาะคดีเกี่ยวกับโรแมนซ์ส

[25] "โรแมนซ์สแกม" เมื่อคนรักออนไลน์กลายเป็นโจร!.อินทรชัย พาณิชกุล. โพสต์ ทูเดย์. 14 ก.พ. 2559. (https://www.posttoday.com/politic/report/416010)

แกมถูกร้องเรียนเข้ามาถึง **80** คดี มูลค่าความเสียหาย 150 ล้านบาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก เหยื่อส่วนใหญ่เป็นหญิงโสดอายุ 40-60 ปี การศึกษาดี หน้าที่การงานมั่นคง

ปี 2559 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ E-mail/Social media ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **35** ราย

ปี 2560 ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย ได้รับเรื่องร้องเรียนและรับแจ้งเบาะแสที่เกี่ยวกับภัยทางการเงิน โดยใช้ E-mail/Social media ปลอม (สันนิษฐานว่าเป็น Romance Scam) เพื่อหลอกให้โอนเงิน **71** ราย

31 พฤษภาคม พ.ศ. 2562[26] สำนักงาน ปปง.จัดตั้งศูนย์ประสานงานเพื่อปฏิบัติการตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน (ศปก.ปปง.) ขึ้นเมื่อวันที่ 21 มิ.ย.61 ถึงวันที่ 31 พ.ค.62 สถิติการรับเรื่องคดี Romance Scam มีผู้เสียหายหลงเชื่อและโอนเงิน จำนวน **332** ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท

4 เม.ย. 2562[27] สถิติคดี Romance Scam ของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) ตั้งแต่วันที่ 22 มิ.ย.61 ถึงวันที่ 26 มี.ค.62 รวมระยะเวลา 9 เดือน ได้รับแจ้งเหตุจำนวน **296** คดี มีผู้ตกเป็นเหยื่อโดนหลอกให้โอนเงิน มูลค่าความเสียหายรวม 157,926,842 บาท

ในปี 2562 ณ วันที่ 31 พฤษภาคม ข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) สรุปรับแจ้ง **62** คดี เสียหาย 36,402,858 บาท หมายจับเดิม 314 หมาย หมายมีคุณภาพ 309 หมายไม่มีคุณภาพ 5 หมาย

[26] ปปง.เผยตั้งศปก.ปปง.1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน. ข่าวสด. 31 พฤษภาคม พ.ศ. 2562 (https://www.naewna.com/local/417058)

[27] ชำแหละแก๊งโรแมนซ์สแกม รู้ทันไม่มีวันตกเป็นเหยื่อ. ไทยรัฐออนไลน์. 4 เม.ย. 2562. (https://www.thairath.co.th/news/local/1536313)

รูปที่ 31 การจับกุมผู้ต้องหาคดี Romance scam ครั้งแรกเมื่อ 3 ธ.ค. 2558

ที่มา https://mgronline.com/crime/detail/9580000133789

จากการค้นคว้าข่าวใน google.co.th ด้วยคำค้นว่า “จับโรแมนซ์สแกม 2555” ซึ่งเป็นปีแรกที่เกิดคดีนี้ขึ้นในประเทศไทยเท่าที่ค้นข้อมูลสถิติมาได้ โดยผู้ต้องหาถูกจับกุมเมื่อวันที่ 3 ธ.ค. 2558 กองปราบปราม แถลงข่าวจับกุม นายเอ็มเบ็นกา โอยาจูลู โอโคชุกวู อายุ 35 ปี สัญชาติไนจีเรีย

พล.ต.ต.ชาญ วิมลศรี รอง ผบช.ก.รักษาราชการแทน ผบก.ป. กล่าวต่อว่า จากการตรวจสอบโทรศัพท์มือถือของผู้ต้องหาพบว่ามีการใช้งานแอปพลิเคชัน ไลน์ อ้างตัวเป็นชายหนุ่มชาวยุโรป ผิวขาวหน้าตาดี มีชื่อว่า หลุยส์ มาร์ก “Luis Mark” ติดต่อพูดคุยกับสาวไทยหลายคนในเชิงชู้สาว จากนั้นก็จะพยายามตีสนิทก่อนจะหลอกลวงว่าจะนำเงินมาให้ แต่เงินที่ใส่ไว้ในกระเป๋าเดินทางเข้ามาประเทศไทยถูกเจ้าหน้าที่ที่ทางการไทยยึดไว้ หากจะนำเงินดังกล่าวออกมาต้องเสียเงินค่าดำเนินการก่อนจะขอให้ผู้เสียหายโอนเงินมาให้ ที่ผ่านมามีผู้หญิงไทย 2 รายที่ตกเป็นเหยื่อสูญเงินไป 99,800 บาท นอกจากนี้ยังปลอมตัวเป็นหญิงสาวชาวอังกฤษใช้ชื่อว่า เชียนนา แอดดิสัน “Gianna Addison” พูดคุยกับชายชาวไทยซึ่งเป็น ผอ.โรงเรียนแห่งหนึ่งในภาคอีสาน แล้วหลอกผู้เสียหายให้โอนเงินให้ 150,000 บาท

สอบสวนนายเอ็มเบ็นการับสารภาพว่า เข้ามาก่อคดีในประเทศไทยตั้งแต่ปี 2555 สมัครแอปพลิเคชัน ไลน์ ปลอมตัวเป็นชายหนุ่มชาวยุโรปผิวขาวหน้าตาดี ใช้ชื่อและรูปถ่ายปลอมเป็นโปรไฟล์ มีตำแหน่งหน้าที่การงานมั่นคง ก่อนจะติดต่อพูดคุยกับหญิงไทย จากนั้นจึงออกอุบายว่าต้องการคบหาด้วยและมีเงินจะนำมาให้แต่ติดปัญหาด้านศุลกากร มีค่าใช้จ่ายที่จำเป็นต้องขอให้เหยื่อโอนเงินผ่านบัญชีธนาคารมาให้ ซึ่งในขั้นตอนดังกล่าวมีหญิงสาวชาวไทยอีกคนอ้างตัวเป็นเจ้าหน้าที่ศุลกากรร่วม

หลอกลวงเหยื่อ ที่ผ่านมาได้ก่อเหตุมาแล้วหลายราย ใช้เวลาในการหลอกลวงเหยื่อรายละประมาณ 1-2 สัปดาห์ ได้เงินแต่ละครั้งประมาณ 10,000-400,000 บาท สำหรับเงินที่ได้มานั้นก็จะนำมาแบ่งกับเพื่อนก่อนจะโอนกลับไปยังประเทศบ้านเกิด โดยรวมแล้วได้เงินจากการกระทำการลักษณะดังกล่าวมาแล้วไม่ต่ำกว่า 1 ล้านบาท

รูปที่ 32 สำนักงานตำรวจแห่งชาติ จัดตั้งศูนย์ปรามปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) โดยได้ทำการสืบสวนและปราบปรามจนนำไปสู่การจับกุมผู้กระทำความผิดอย่างต่อเนื่อง

ที่มา ศปอส.ตร

พล.ต.อ.จักรทิพย์ ชัยจินดา ผบ.ตร. ได้จัดตั้งศูนย์ปรามปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) โดยได้ทำการสืบสวนและปราบปรามจนนำไปสู่การจับกุมผู้กระทำความผิดอย่างต่อเนื่องดังนี้[28]

23 ม.ค.2562 พล.ต.ท.สุรเชษฐ์ หักพาล ผบช.สตม./รองผอ.ศปอส.ตร. หน.ชุดปราบปรามพร้อมคณะทำงาน ได้บุกเข้าปฏิบัติการจับกุมผู้ต้องหาใน 7 จุด ในย่านที่พักอาศัย กลางกรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย (จับกุมผู้ต้องหารวม 14 ราย เป็นบุคคลสัญชาติไทย 4 ราย และสัญชาติไนจีเรีย 10 ราย) และอีก 3 จุด ในประเทศไทย (จับกุมผู้ต้องหารวม 4 ราย เป็นบุคคลสัญชาติ

[28] เจ้าหน้าที่ตำรวจจับตัวผู้ต้องหาแก๊งโรแมนซ์สแกมจำนวน 10 คน จากประเทศมาเลเซีย. สำนักข่าวสมาคมตำรวจ. 8 ก.พ.62 (http://www.rtpanews.com/32747/)

ไทย 3 ราย และสัญชาติไนจีเรีย 1 ราย) รวมปฏิบัติการพร้อมกัน 2 ประเทศ สามารถจับกุมผู้ต้องหาได้ทั้งหมด **18** ราย (บุคคลสัญชาติไทย 7 ราย และสัญชาติไนจีเรีย 11 ราย)

7 ก.พ.62 เวลาประมาณ 20.00 น. ทางประเทศมาเลเซียได้ประสานส่งตัวผู้ต้องหาซึ่งมีหมายจับ ศาลจังหวัดเชียงใหม่ ในข้อหา “ร่วมกันฉ้อโกงประชาชนโดยแสดงตนเป็นคนอื่น และมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ” จำนวน **10** คน ที่บริเวณด่านตรวจคนเข้าเมืองสะเดา จ.สงขลา เจ้าหน้าที่ตำรวจจึงได้รับตัวผู้ต้องหา นำส่งพนักงานสอบสวนดำเนินคดีตามกฎหมาย

8 ก.พ.62 เจ้าหน้าที่ตำรวจ พร้อมชุดปฏิบัติการสยบไพรี ได้นำตัวผู้ต้องหาทั้ง 10 คน มาตรวจร่างกาย และจัดเก็บสารพันธุกรรม โดยแพทย์จากโรงพยาบาลตำรวจ และสอบปากคำผู้ต้องหาที่ ศปอส.ตร.

การร่วมปราบปรามอาชญากรรมข้ามชาติของชุดปฏิบัติการ ศปอส.ตร. ตามแนวทาง “One World One Team หรือ ตำรวจเป็นหนึ่งเดียวกันทั่วโลก” สรุปผลการประสานงานความร่วมมือปราบปรามอาชญากรรมไซเบอร์คดี Romance Scam ระหว่างประเทศ จำนวน 10 ครั้ง / 7ประเทศ ดังนี้

ครั้งที่ 1 ประเทศมาเลเซีย เมื่อวันที่ 26 ม.ค.2561 จับกุมผู้ต้องหา จำนวน 5 คน เป็นคนไต้หวัน จำนวน 3 คน คนมาเลเซีย 2 คน

ครั้งที่ 2 ประเทศกัมพูชา เมื่อวันที่ 16 ก.พ.2561 จับกุมผู้ต้องหา จำนวน 37 คน เป็นคนไต้หวัน 6 คน คนไทย 26 คน และคนกัมพูชา 5 คน

ครั้งที่ 3 ประเทศมาเลเซีย เมื่อวันที่ 20 ก.พ.2561 จับกุมผู้ต้องหา จำนวน 16 คน เป็นคนไต้หวัน 5 คน และคนไทย 11 คน

ครั้งที่ 4 ประเทศสหรัฐอาหรับเอมิเรตส์ เมืองดูไบ เมื่อวันที่ 19 มี.ค.2561 จับผู้ต้องหา จำนวน 24 คน เป็นคนไต้หวัน 1 คน และคนไทย 23 คน

ครั้งที่ 5 ประเทศสาธารณรัฐประชาชนจีน มณฑลฝูเจี้ยน เมื่อวันที่ 27 มี.ค.2561 จับกุมผู้ต้องหา จำนวน 7 คน เป็นคนไต้หวัน 1 คน และคนไทย 6 คน

ครั้งที่ 6 ไต้หวัน เมืองไถ่หนาน เมื่อวันที่ 24 พ.ค.2561 จับผู้ต้องหา จำนวน 21 คน เป็นคนไต้หวันทั้งหมด 21 คน

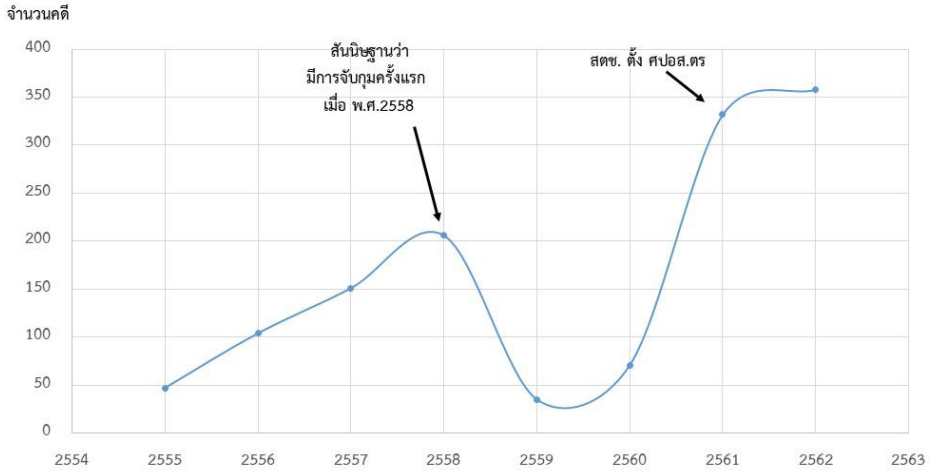
ครั้งที่ 7 ประเทศมาเลเซีย เมื่อวันที่ 5 มิ.ย. 2561 จับผู้ต้องหา จำนวน 12 คน เป็นคนไต้หวัน 2 คน และคนไทย 10 คน

ครั้งที่ 8 ประเทศฟิลิปปินส์ เมื่อวันที่ 14 มิ.ย. 2561 จับผู้ต้องหา จำนวน 19 คน เป็นคนไต้หวัน 3 คน และคนไทย 16 คน

ครั้งที่ 9 ประเทศเวียดนาม เมื่อวันที่ 24 ส.ค.2561 จับผู้ต้องหา จำนวน 19 คน เป็นคนไต้หวัน 2 คน และคนไทย 17 คน

ครั้งที่ 10 ประเทศมาเลเซีย เมื่อวันที่ 23 ม.ค. 2562 จับผู้ต้องหา จำนวน 14 คน เป็นคนไนจีเรีย 10 คน และคนไทย 4 คน

รวมจับกุมผู้ต้องหา ทั้งสิ้น 174 คน เป็นคนไต้หวัน 44 คน คนไทย 113 คน คนมาเลเซีย 2 คน คนกัมพูชา 5 คน และคนไนจีเรีย 10 คน



ที่มา : ประมาณการจากข้อมูลของ
ศูนย์ประสานงานเพื่อปฏิบัติการตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน (ศปก.ปปง.)
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย
ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

รูปที่ 33 การสังเกตปรากฏการณ์ คดี Romance Scam ในประเทศไทย

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 8

จากรูปที่ 33 ตีความว่า การสืบสวนสอบสวนทางดิจิทัล (Digital Detective) เพื่อหาตัวตนอาชญากรมาดำเนินคดีสามารถกระทำได้และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic)

เพื่อดำเนินคดีกระทำได้ ดังนั้นสัดส่วนระหว่างจำนวนคดีที่เกิดขึ้นกับการสืบสวนจับกุมจึงลดลง ในปี พ.ศ. 2559

แต่เมื่อมีการปรับรูปแบบการก่ออาชญากรรมให้หลากหลายซับซ้อน ส่งผลให้อัตราการเกิดอาชญากรรมไซเบอร์ ประเภทคดี Romance Scam เพิ่มขึ้น แม้ สตช. ได้ตั้งชุดปฏิบัติการ ศปอส.ตร. จับกุมอาชญากรอย่างต่อเนื่องและจำนวนมากแต่จำนวนคดียังมีอัตราที่สูงอยู่

อาจเป็นไปได้ว่า การบิดบังอำพรางตัวตน (Anonymity) เพื่อให้หลบพ้นการสืบสวนทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เป็นเหตุเป็นผลต่อการตัดสินใจก่ออาชญากรรมของกลุ่มอาชญากรไซเบอร์ประเภทคดี Romance Scam

<u>กรณีศึกษาที่</u> 9 การจ้างสังหารออนไลน์ผ่าน TOR และจ่ายค่าจ้างด้วย Crypto currency

การใช้ไซเบอร์เทคโนโลยีประกอบอาชญากรรม (Criminal Cyber Technology) ไปประกอบอาชญากรรมประเภทต่างๆ อาทิ การค้ายาเสพติดด้วยการใช้เครือข่าย Tor network และเงินเสมือน (Crypto currency) การจ้างสังหารด้วยการใช้เครือข่าย Tor network และเงินเสมือน (Crypto currency) ตลอดจนการใช้โดรน (Drone) ติดอาวุธเดินทางผ่านเครือข่าย 3G/4G/5G และค้นหาใบหน้าเหยื่อด้วยเทคโนโลยี Face recognition เพื่อสังหาร และเส้นทางการเงินก่อการร้ายด้วยการใช้เงินเสมือน (Crypto currency) เป็นต้น

เนื่องด้วยเป็นอาชญากรรมร้ายแรงยากต่อการเก็บรวบรวมสถิติเชิงปริมาณทั้งหมด จึงใช้วิธีการสืบสวนหาความจริงจากเนื้อหา (Content Investigation) ด้วยวิธีวิจัยเชิงสืบสวน (Investigative social research) จากเบาะแสในโลกออนไลน์ ตามวิธีของ แจ๊ค ดั๊กลาส (Jack Douglas, 1976) มาเป็นกรอบการวิจัยเพื่อเข้าหาความจริง ดังนี้

13 พฤศจิกายน 2016 พบศพนาง Amy allwine วัย 44 ปี คุณแม่ลูก 1 เสียชีวิตถูกยิงที่ศีรษะในบ้านอันแสนสงบที่ปกคลุมไปด้วยหิมะ ราวกับเธอฆ่าตัวตาย

รูปที่ 34 ที่เกิดเหตุบ้านของครอบครัว Allwine ใน Minnesota

ที่มา https://www.dailymail.co.uk/news/article-4133592/Man-charged-slaying-wife-pretending-killed-self.html

2 เดือนต่อมาเจ้าหน้าที่เห็นว่านั่นไม่ใช่การฆ่าตัวตาย จึงจับกุมตัวผู้ต้องสงสัยคือ นาย Stephen allwine สามีวัย 43 ปี มีอาชีพเป็น IT specialist ไปสอบสวน

นาย Stephen สารภาพว่าเขาต้องการให้เธอตายจริงๆ แต่เขาไม่ได้ลงมือสังหารเธอเอง หากเป็นนักฆ่าคนใดสักคนใน dark web ชื่อเว็บไซต์ Besa mafia ที่ให้บริการรับจ้างสังหารหรือทำร้ายคน โดยเขา order สังหารภรรยาตนเอง และจ่ายค่าจ้างเป็น bitcoin ตำรวจตั้งข้อหาเขาจ้างวานฆ่า

นอกจากนั้นนาย Stephen ได้จ้างให้สังหารลูกชายด้วย โดยให้ข้อมูล GPS ที่ติดตัวใน Smartwatch ของลูกชายเพื่อให้คนร้ายเลือกเวลาเหมาะสมลงมือสังหาร

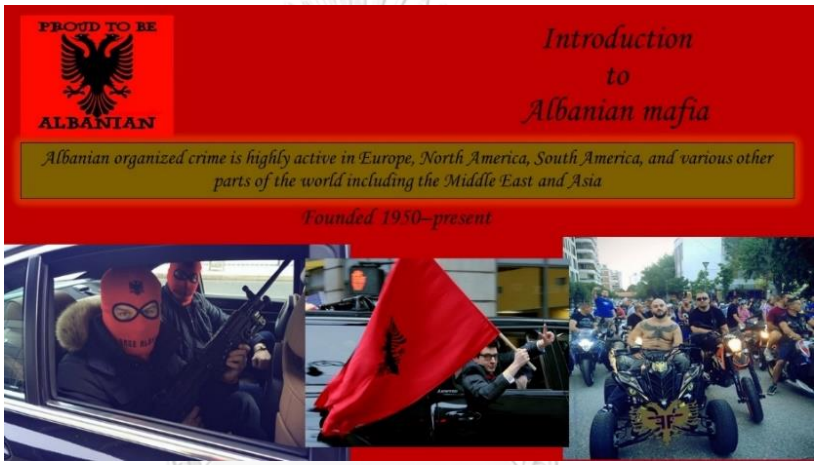
ไคล์ สเวนสัน[29] (Swenson, 2018) นักเขียนออนไลน์เว็บไซต์ชั้นนำของโลก วอชิงตันโพสต์ บรรยายว่า Stephen กับ Amy พบรักกันในโบสถ์ทั้งคู่เคร่งศาสนา จากนั้นไม่นานเขาก็ขอเธอแต่งงาน แต่เหตุการณ์ฆาตกรรม Amy แท้จริงเกิดจากการที่นาย Stephen หักหลังภรรยาตนด้วยการมองหาแฟนใหม่ โดยเขาพบรักกับใครสักคนจากเว็บไซต์หาคู่ชื่อดัง Ashley Madison และการหย่าเป็นเรื่องที่ขัดกับศรัทธาของทั้ง Stephen กับ Amy จึงเป็นเรื่องที่เป็นไปไม่ได้ ดังนั้นวิธีเดียวที่ Stephen จะแยกทางกับ Amy ได้คือ เธอต้องตาย

ผู้ใช้นามว่า “Dogdaygod” คือผู้ที่จ่าย Bitcoin จ้างสังหาร Amy ในเว็บไซต์ Besa Mafia อาจจะเป็นหลักฐานที่ชวนเชื่อหลอกลวง แต่แท้จริงแล้ว Stephen อาจจะเป็นคนลงมือสังหารเอง

[29] Kyle Swenson. A church elder’s Ashley Madison affairs led him to the dark Web and murder, police say. The Washington post. Cited January 25, 2018; Available from URL: https://www.washingtonpost.com/news/morning-mix/wp/2018/01/25/a-church-elders-ashley-madison-affairs-led-him-to-the-dark-web-and-murder-police-say/

“Besa Mafia” จึงกลายเป็นข่าวโด่งดังกล่าวขานไปทั่วในแวดวงผู้สนใจเทคโนโลยีสมัยใหม่ เกี่ยวกับ อาชญากรรมไซเบอร์สายพันธ์ใหม่ (New breed of Cybercrime) องค์กรรับจ้างสังหารออนไลน์ผ่าน Tor browser และจ่ายค่าจ้างด้วยเงินดิจิทัล (Crypto Currency)

การรวบรวมพยานหลักฐานทางดิจิทัลหรือการดำเนินคดีกับมือสังหารหรือหลักฐานการจ้างวานฆ่าแทบเป็นไปไม่ได้เลย เพราะความเป็น Anonymous (ไร้ตัวตน) ทั้งเจ้าของเว็บไซต์ที่ใช้งานผ่าน Tor browser เป็น Virtual network ปกปิดเลขหมาย IP Server เว็บไซต์ และปิดบัง IP ผู้ใช้งาน อีกทั้งการจ่ายเงินด้วย bitcoin ก็ไร้การตรวจสอบเส้นทางการเงินว่าผู้ใดเป็นเจ้าของบัญชีหรือแม้แต่หากสารภาพศาลจะเชื่อพยานหลักฐานหรือไม่ ก็สุดที่จะคาดเดาเพราะเป็นคดีแรกในประวัติศาสตร์



รูปที่ 35 Besa mafia กลุ่มอันธพาลชาวอัลบาเนียใน สหรัฐอเมริกา

ที่มา https://www.gotoknow.org/posts/643649

Besa mafia จากกลุ่มอันธพาลชาวอัลบาเนียข้างถนนใน สหรัฐอเมริกา เติบโตอย่างรวดเร็วจากธุรกิจผิดกฎหมาย และเริ่มต้นธุรกิจลอบสังหารผ่าน dark web ในปี ค.ศ. 2014-2016 จึงเกิดการรวมกลุ่มอันธพาลจากย่านต่างๆ เข้ามาเสนอตัวรับงานในเว็บไซต์จนกลายมาเป็นเฟียกลุ่มใหญ่ทรงอิทธิพลกลุ่มหนึ่งใน สหรัฐ อเมริกา ขยายบริการสังหารและทำร้ายร่างกายอย่างรวดเร็วไปถึงยุโรปและเอเชีย

Besa Mafia พื้นเพเป็นชาวอัลบาเนียที่รวมกลุ่มเป็นมาเฟียทำธุรกิจผิดกฎมายทุกประเภทหรือเป็นองค์กรอาชญากรรมใน สหรัฐอเมริกา กลุ่มใหม่ที่กำลังมีอิทธิพลขึ้นเรื่อยๆ

มาเฟียชาว อัลบาเนีย แตกต่างจากมาเฟียกลุ่มอื่นในอเมริกาตรงที่ไม่มีหัวหน้าใหญ่เป็นการบริหารองค์กรแบบ Flat management แบ่งเป็นหัวหน้ากลุ่มเล็กๆ ที่สามัคคีกัน

Besa หมายถึงความไว้ใจกันและเป็นสัญลักษณ์แห่งเกียรติ ความภักดี และรักกันแบบครอบครัว Besa Mafia เป็นองค์กรอาชญากรรมที่ประกอบธุรกิจผิดกฎหมาย อาทิ ค้ายาเสพติด ค้า

อาวุธ โสเภณี เรียกค่าไถ่ การพนัน ค้ามนุษย์ ค้าอวัยวะมนุษย์ รับจ้างทำร้ายร่างกาย และรับจ้างสังหาร มีเครือข่ายกว้างขวางไปถึงยุโรป และเอเชีย มีสมาชิกในองค์กรนับแสนคน กลายเป็นองค์กรอาชญากรรมขนาดใหญ่

Besa Mafia ถูกใช้นำมาเรียกชื่อเว็บไซต์รับจ้างสังหารใน Dark web เข้าใช้บริการผ่าน Tor browser โดยมี URL คือ http://oiiuv2gwl2jhvg3j.onion และจ่ายค่าจ้างด้วย Bitcoin

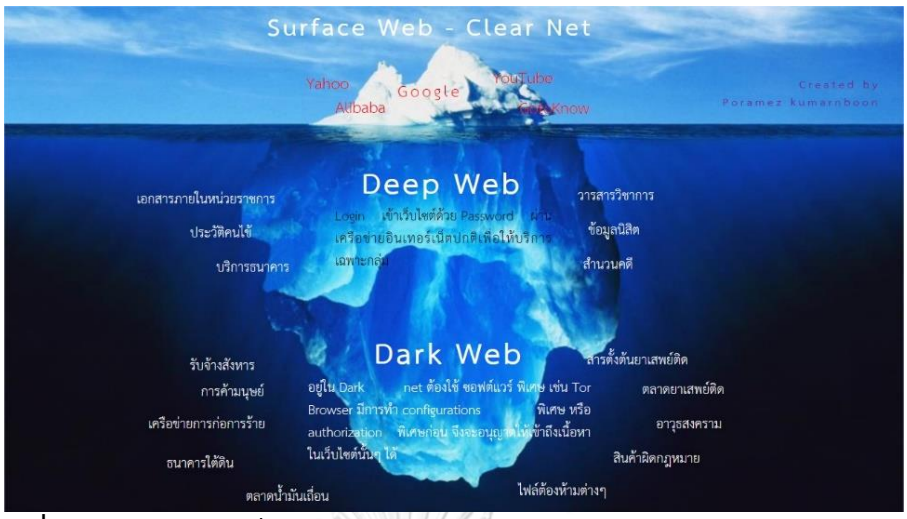
FBI เปิดเผยว่า ด้วยความที่นาย Stephen เป็น IT specialist เขาจึงมีทักษะในการเรียนรู้เทคโนโลยีใหม่ๆ อย่างรวดเร็ว และได้เข้าไปท่อง Dark web เพียงไม่นานเขาก็สั่งยากล่อมประสาทชื่อว่า scopolamine จาก dark web แห่งหนึ่งมาเสพมากมายจนประสาทหลอน อาจนำมาซึ่งเหตุสลดดังกล่าว

องค์กรอาชญากรรมนั้นเป้าหมายหลักคือทำธุรกิจผิดกฎหมายและหาเงินจำนวนมาก Business model ใหม่ของธุรกิจลอบสังหารอย่าง Besa Mafia จึงอาจจะเชื่อได้ว่าเป็นธุรกิจจ้างสังหารแห่งศตวรรษที่ 21 Dark web and Crypto currencies เมื่อการฆ่าคนจะง่ายดายเพียงปลายนิ้วและไร้หลักฐาน

Dark web

หากเปรียบประเภทของเว็บไซต์เป็นดังก้อนน้ำแข็ง Iceberg ที่ลอยอยู่ในมหาสมุทร ดังในรูปที่ 29 ส่วนที่ลอยพ้นผิวน้ำทะเลก็คือ เว็บไซต์ปกติเรียกว่า Surface Web หรือ Clear Net เป็นเว็บไซต์สะอาดไม่ผิดกฎหมาย ไม่มีเนื้อหาอะไรที่ต้องการปิดบังไม่ให้รัฐตรวจสอบ สามารถใช้ Browser ปกติ เช่น Safari Chrome แล้วกรอก URL หรือค้นใน Search engine ก็เข้าถึงเว็บไซต์ทันที

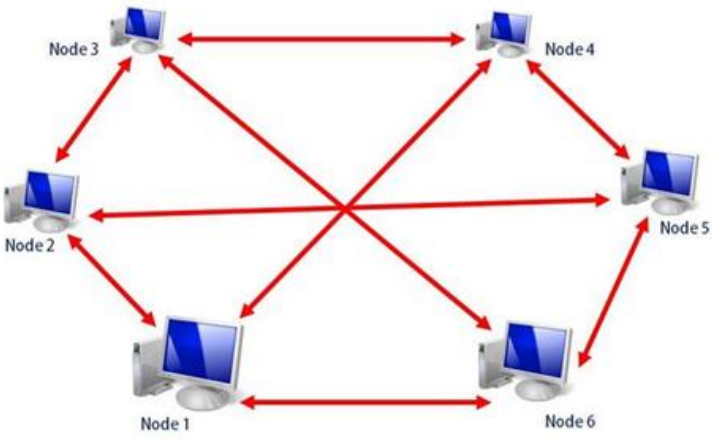
Deep Web คือเว็บไซต์ปกติหรือบางเว็บไซต์ URL อาจจะเป็นคำที่สะกดภาษาไม่ได้ความหมาย ต้องส่ง Link ให้เฉพาะหรือมีปราการ Firewall ให้ซ่อนตัวอยู่และต้องกรอกรหัสลับ (Password) จึงจะเข้าถึงเนื้อหาในเว็บไซต์นั้นได้ เช่น เว็บบริการบทความวิชาการ ฐานข้อมูลราชการ บริการธนาคาร เป็นต้น ผู้วิจัยได้วาดภาพให้เข้าใจดังนี้



รูปที่ 36 ประเภทของเว็บไซต์แบ่งตามระดับความยากในการเข้าถึง

แต่เว็บที่อยู่ชั้นในลึกสุดเรียกว่าเว็บมืด (Dark webX ไม่สามารถกรอก URL ผ่าน Browser ปกติหรือใส่รหัสผ่านแล้วเข้าเว็บไซต์ได้ แต่เป็นการเข้าเว็บที่มีความซับซ้อนชั้นลึกกว่าปกติ

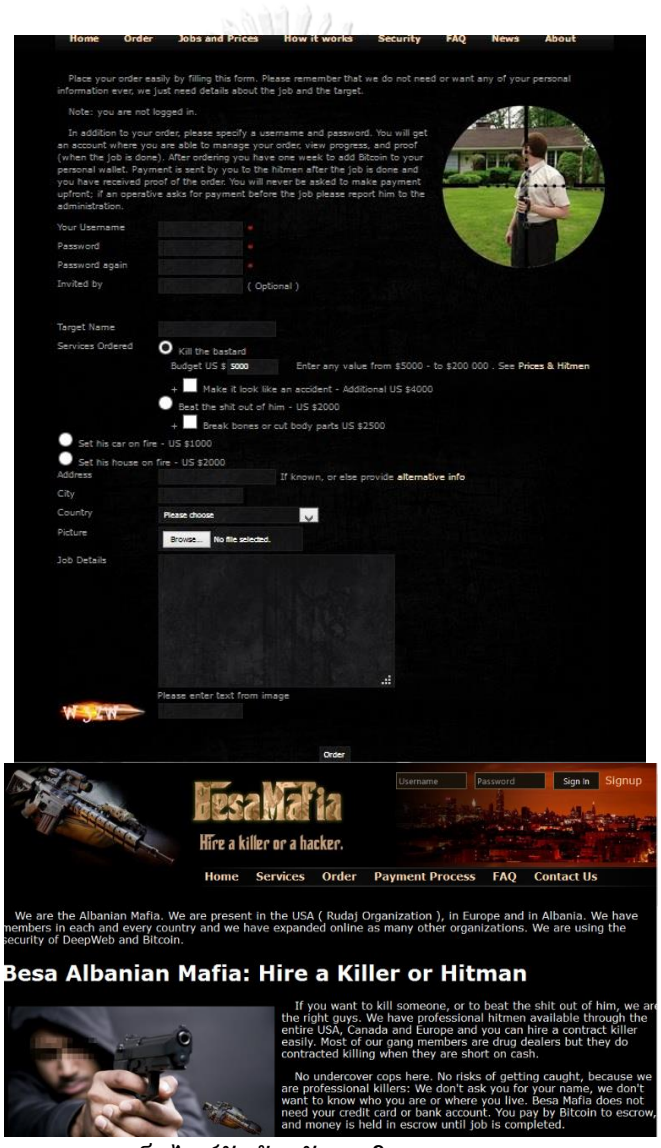
ผู้ใช้งานต้องส่ง Link URL เฉพาะกลุ่ม และเข้าเว็บผ่าน Browser พิเศษชื่อ TOR ซึ่งเป็น Browser ปกปิดตัวตนสำหรับผู้ที่ login เข้าใช้งานในเว็บมืด โดยมีระบบ Virtual Private Network (VPN) ที่เป็นโครงข่ายแบบไร้ศูนย์กลาง (Distributed Network) โดยสมาชิกในกลุ่มนำคอมพิวเตอร์มาเชื่อมต่อกันนับหมื่นเครื่องแล้ว โยนข้อมูลกันไปมาตลอดเวลา และมี Proxy ถึง 3 ชั้น ทำให้ไม่ทราบที่ตั้ง Server เว็บไซต์ และช่วยปิดบัง IP address ของผู้เข้าใช้งานในเว็บไซต์ มีให้ดาวน์โหลดฟรีที่ torproject.org



รูปที่ 37 สมาชิกเครือข่าย Tor จะโยนข้อมูลกันไปมาตลอดเวลาทำให้ไม่ทราบที่ตั้ง Server เว็บไซต์ และปกปิดตัวตนผู้เข้าใช้บริการ Browser เว็บมืด

Bitcoin

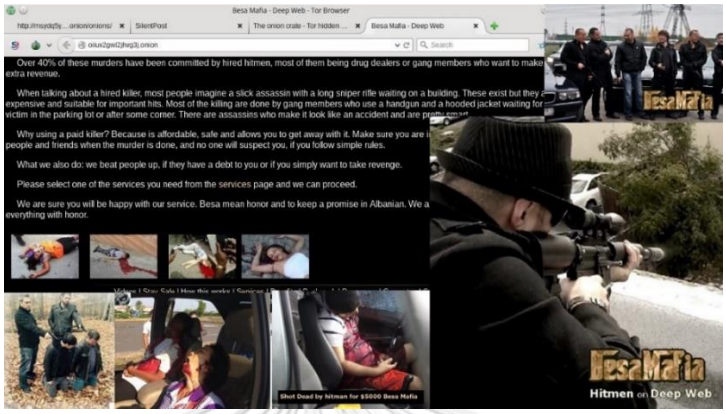
Bitcoin เป็นเงินดิจิทัลที่มีความต้องการสูงสุด เป็นโปรแกรมคอมพิวเตอร์ที่เขียนให้ทำงานในเทคโนโลยี Blockchain ซึ่งเป็นเครือข่ายที่ไม่มีศูนย์กลางการเก็บข้อมูลทั้ง Server หรือ Data centre คล้ายหลักการทำงานของ Tor network เปิดบัญชีโดยไม่ต้องแสดงตัวตนเพราะไม่มีคนกลางอย่างธนาคารคอยตรวจสอบ ระบบถูกสร้างให้ทำงานอัตโนมัติต่อเนื่องไม่สามารถแก้ไขทำลาย จึงได้รับความเชื่อถือว่าปลอดภัย เพียงได้ที่อยู่กระเป๋าเงิน (Bitcoin address) เช่น 1N2VwcfGTXA1J9FGNG3uit3VYA4D6zMoP2 ก็สามารถแลกเปลี่ยนเงินตราได้จากทั่วโลกโดยไร้ตัวตน เป็น Criminal Financial network ที่เหล่าอาชญากรปรารถนา



รูปที่ 38 Besa Mafia เว็บไซต์รับจ้างสังหารใน Dark web

ที่มา http://oiiuv2gwl2jhvg3j.onion (เข้าผ่าน Tor browser)

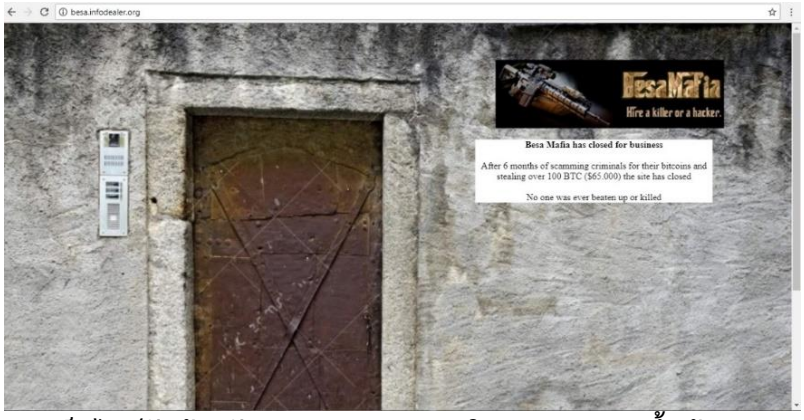
เว็บไซต์รับจ้างสังหาร Besa Mafia มี Package ให้เลือกความต้องการว่าจะทำร้ายเหยื่อระดับใด มีค่าจ้างเท่าใด อยู่ที่ความยากในการสังหารเหยื่อหากเป็นนักการเมืองก็จะแพงขึ้นเป็นลำดับ ค่าจ้างตั้งแต่ 5,000-200,000 ดอลลาร์ สหรัฐ พร้อมภาพ และคลิปวิดีโอประกอบผลงานที่ผ่านมา



รูปที่ 39 ผลงานที่อ้างว่ารับจ้างสังหารที่ผ่านมา

ที่มา http://oiiuv2gwl2jhvg3j.onion (เข้าผ่าน Tor browser)

หลังจากคดีโด่งดัง ปัจจุบัน ณ วันที่ 28 ธันวาคม 2560 ผู้วิจัยได้เข้าไปค้นหาข้อมูลพบว่าเว็บไซต์ Besa Mafia ซึ่งมี URL เป็น http://oiiuv2gwl2jhvg3j.onion ได้ปิดให้บริการแล้ว และมีข้อความขึ้นว่า “Besa Mafia ปิดเพื่อธุรกิจ หลังจากเหล่าอาชญากรเปิดให้บริการมา 6 เดือน เพื่อหลอกลวง และ Bitcoin ได้ถูกขโมยไปกว่า 100 เหรียญ (ปัจจุบัน 1 Bitcoin ประมาณ 510,000 บาท) เว็บไซต์ได้ถูกปิดแล้ว และไม่มีใครเคยถูกทำร้ายหรือถูกฆ่าจากบริการของเว็บนี้”



รูปที่ 40 เว็บไซต์รับจ้างสังหาร Besa Mafia ใน Dark web ขึ้นข้อความว่า “ถูกปิด ไม่เคยก่อมีคดีใดมาก่อน เป็นเว็บต้มตุ๋น และ Bitcoin ถูกขโมยไปแล้ว”

ที่มา http://oiiuv2gwl2jhvg3j.onion (เข้าผ่าน Tor browser)

ร่องรอยหลักฐานผู้ให้บริการจ้างวานฆ่า Besa Mafia

ผู้วิจัยได้พยายามค้นคว้าร่องรอยหลักฐานจากบันทึกใน Blog ที่เชื่อว่าน่าจะเกิดจากบุคคลที่อาจจะมีตัวตนจริงเป็นผู้เขียนขึ้น มิใช่เกิดจากนักเขียนบทความ มีตัวอย่างดังนี้

กรณี maryrhamilton65

บันทึกใน blog จากผู้ใช้นามว่า maryrhamilton65[30] เมื่อวันที่ 17 มีนาคม 2016 เรื่อง Besa Mafia true story: How I did murder ผู้เขียนมีทำนองการเขียนเป็นหญิง เธอต้องการเล่าประสบการณชีวิตในการเป็นฆาตกรของเธอ และเธอเขียนโดยใช้ Tor browser ปิดบัง IP เธอเล่าว่า

วันที่ 24 กุมภาพันธ์ เพื่อนสาวของเธอถูกเพื่อนร่วมงานคนหนึ่งชื่อ Giovanni ทำร้ายและข่มขืนในที่ทำงาน เพื่อนของเธอร้องไห้ไม่หยุดและไม่อยากจะไปแจ้งความ เธอเจ็บปวดอยากจะแก้แค้นแต่เธอไม่รู้เรื่องวิธีการที่จะต่อสู้กับใครได้ และเธอก็เกรงว่า Giovanni จะกลับมา blackmail หรือทำร้ายเพื่อนเธออีก

วันที่ 26 กุมภาพันธ์ เธอใช้ google ค้นหาบริการรับจ้างทำร้าย จนมาพบ Besa Mafia ที่มีราคาค่าจ้างเริ่มต้นที่ $5000 เธอศึกษาวิธีการเข้าใช้งานใน Dark web และวิธีสมัครสมาชิก จากนั้นเธอเริ่มส่งข้อความไปยัง Admin เว็บไซต์ Besa Mafia เพื่อสอบถามว่ารับงานที่ Ohio หรือไม่

Admin เว็บไซต์ Besa Mafia ตอบข้อความกลับมาว่าทำได้และขอรายละเอียดเหยื่อ สถานที่พร้อมภาพถ่าย จากนั้น 2 วันต่อมาเธอศึกษาวิธีซื้อ Bitcoin และโอนไปยังบัญชีของ Admin เว็บไซต์ Besa Mafia และสนทนาเลือกวันลงมือสังหารเป็นวันที่ 7 มีนาคม 2016 เนื่องจากเธอจะออกนอกเมืองไปสังสรรค์กับเพื่อนสมัยมัธยม หากมีการสืบสวนจากตำรวจมาถึงตัวเธอจะได้มีข้ออ้าง

วันที่ 7 มีนาคม 2016 Admin เว็บไซต์ Besa Mafia ส่งข้อความมาให้เธอ เป็นภาพ Giovanni ถูกยิงตายในรถของเขา เธอตกใจมาก และสงสัยว่าเป็นเรื่องจริงหรือไม่? จนกระทั่งชั่วโมงต่อมาเธอได้เห็นข่าวว่า Giovanni ถูกยิงเสียชีวิตในรถ ตามข่าวนี้

[30] ไม่ปรากฏนามผู้เขียน. Besa Mafia true story: How I did murder.
Cited 2017 May; Available from URL: https://besamafiastories.wordpress.com/

รูปที่ 41 ภาพที่อ้างว่าเหยื่อถูกสังหารจากบริการของเว็บไซต์ Besa Mafia

ที่มา https://www.news5cleveland.com/news/local-news/oh-summit/akron-man-found-shot-dead-in-his-car

maryrhamilton65 บันทึกว่าเธอรู้สึกประทับใจกับบริการจ้างสังหารนี้มาก มันไร้ตัวตนจนเธอไม่รู้สึกกลัวตำรวจ แม้แต่การเขียนบันทึกนี้ก็เช่นกันก็ไม่สามารถสืบสวนมาถึงเธอได้

กรณี บุรุษนิรนามจ้างวานฆ่าลูกนอกสมรส Besa Mafia

จากบันทึกเรื่อง Besa Mafia my experience with them ของบุรุษนิรนาม[31] เขาได้ค้นหาบริการจ้างสังหารเพื่อฆ่าลูกนอกสมรสจนมาเจอ Besa mafia และได้ซื้อ Bitcoin จากเว็บ coinbase.com จากนั้นเขาได้ว่าจ้างในราคา $5000 แล้วส่งภาพถ่ายพิกัดสถานที่นัดวันเวลา เขาตื่นเต้นรอคอยทั้งวันจนตกเย็น Admin เว็บไซต์ Besa Mafia ส่งข้อความมาให้เป็นภาพลูกนอกสมรสของเขาที่ถูกสังหาร เขารู้สึกพอใจในบริการมาก มันไร้ตัวตนจนเขาไม่รู้สึกกลัวตำรวจ แม้แต่การเขียนบันทึกนี้ก็เช่นกันก็ไม่สามารถสืบสวนมาถึงเขาได้ และเขาได้โพสต์ link ไว้ http://oiiuv2gwl2jhvg3j.onion และ http://oiiuv2gwl2jhvg3j.onion.link

รูปแบบการประกอบธุรกิจรับจ้างสังหารผ่าน Dark web และจ่ายค่าจ้างด้วย Bitcoin จากเรื่องราว Besa Mafia นั้น นับว่าเป็น Business model ในอุดมคติขององค์กรอาชญากรรมและองค์กรอาชญากรรมข้ามชาติที่ต้องการความไร้ตัวตนและรวดเร็ว ซึ่งก็คือการสื่อสารที่ไม่สามารถตรวจสอบได้และเส้นทางการเงินที่ไม่สามารถระบุตัวตนได้

[31] ไม่ปรากฏนามผู้เขียน. Besa Mafia my experience with them.
Cited ไม่ปรากฏวันที่; Available from URL: https://sites.google.com/site/besamafiarealstory/

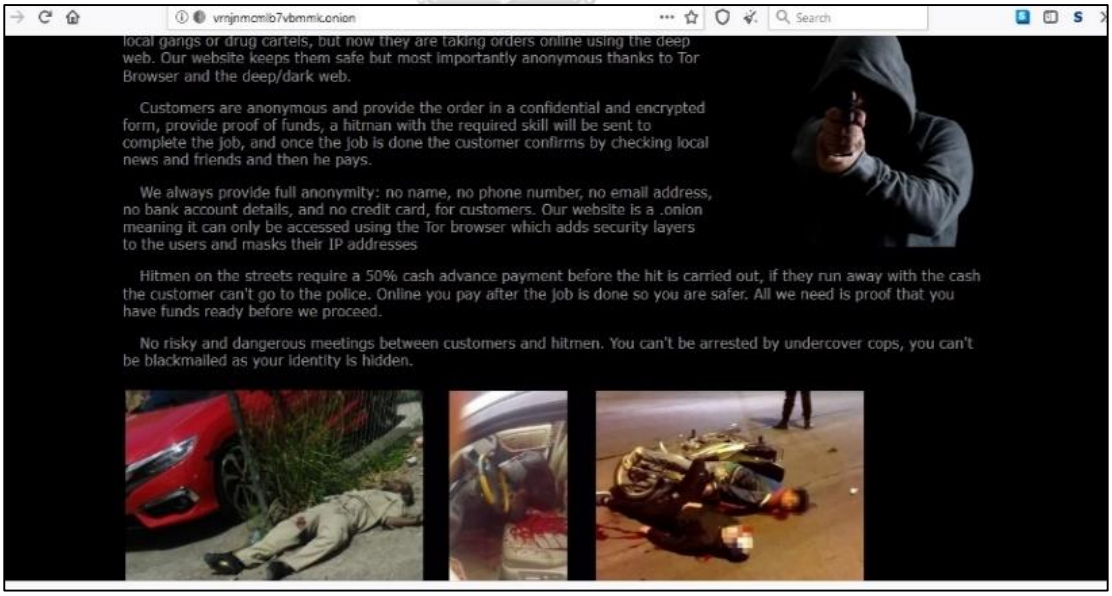
แม้เว็บมืด Besa Mafia ปิดตัวหลบหนีไปแล้ว แต่ผลกระทบจาก Business model ใหม่ของธุรกิจลอบสังหาร Besa Mafia องค์กรอาชญากรรมกลุ่มอื่นได้ลอกเลียนแบบมากมาย ได้เกิดเว็บมืดรับจ้างทำร้ายและสังหารหลายเว็บในปัจจุบัน (พ.ศ.2562)

ผลการวิจัยเชิงสืบสวนสังหารหลายเว็บใน TOR

ผู้วิจัยได้ทำการรวบรวมข้อมูลและเนื้อหาต่าง ๆ ที่ปรากฏในสื่ออินเทอร์เน็ต ทั้งยังมีการเข้าไปสำรวจเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดผ่าน Tor Network ได้ผลมาทำการวิจัยเชิงสืบสวนจากเบาะแสในโลกออนไลน์ (Investigative social research) ดังนี้

1. Internet Killers, Tor URL : http://vrnjnmcmlb7vbmmk.onion/

เป็นเว็บมืดรับจ้างสังหารใน Tor network อัตราค่าจ้างสังหารประมาณ $10 000 - $15 000 ระยะเวลาปิดงาน 7-14 วัน ก่อตั้งมาแล้ว 4 ปี ความน่าเชื่อถือในอินเทอร์เน็ตสูงมาก เพราะไม่ต้องวางเงินมัดจำ และไม่เคยมีการร้องเรียนหรือเปิดเผยในชุมชนใดว่าเป็นเว็บหลอกลวง



รูปที่ 42 เว็บไซต์ Internet Killers

ที่มา http://vrnjnmcmlb7vbmmk.onion (เข้าผ่าน Tor browser)

2. Sinaloa Mexican Hitmen, Tor Url: http://zrbxuw7ur46pno4y.onion

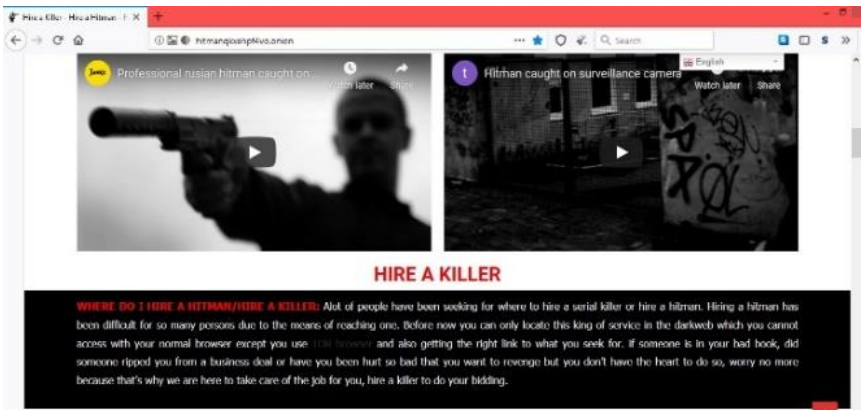
เป็นเว็บมืดรับจ้างสังหารใน Tor network อัตราค่าจ้างสังหารประมาณ $4,000 - $10,000 ก่อตั้งมาแล้ว 3 ปี ให้บริการใน Europe, Canada, Australia, Japan, China, India, Pakistan และ South American

รูปที่ที่ 43 เว็บไซต์ Sinaloa Mexican Hitmen

ที่มา http://zrbxuw7ur46pno4y.onion (เข้าผ่าน Tor browser)

3. Hire a Killer, Tor Url: https://hireakiller.io

เป็นเว็บมืดรับจ้างสังหารใน Tor network อัตราค่าจ้างสังหารประมาณ $15,000 มีชื่อเสียงและอยู่ในอันดับดี (เรตติ้งดี) ไม่มีการวางมัดจำ ก่อตั้งมาประมาณ 1 ปี และติดต่อผ่าน Encrypted E-mail

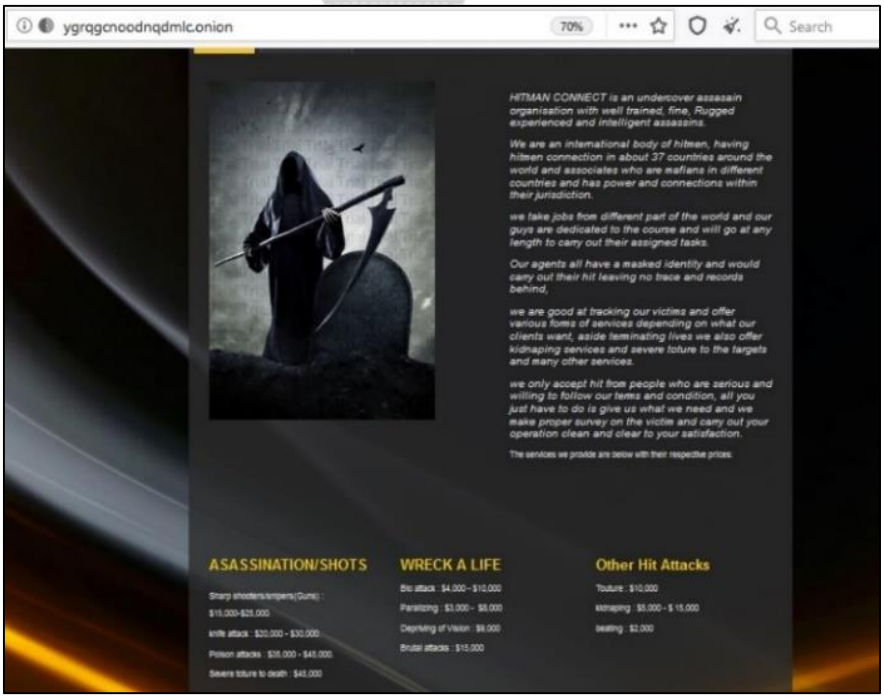


รูปที่ 44 เว็บไซต์ Hire a Killer

ที่มา https://hireakiller.io (เข้าผ่าน Tor browser)

4. Hitman Connect, Tor URl: http://ygrqgcnoodnqdmlc.onion

เป็นเว็บมืดที่รับจ้างสังหารใน Tor network อัตราค่าจ้างสังหารประมาณ $15,000 - $20,000 ชื่อเสียงไม่ค่อยดี ก่อตั้งมาประมาณ 2 ปี



รูปที่ 45 เว็บไซต์ Hitman Connect

ที่มา http://ygrqgcnoodnqdmlc.onion (เข้าผ่าน Tor browser)

5. เว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืด อื่น ๆ

ผู้วิจัยได้สำรวจเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดมากมาย และขอยกตัวอย่าง URL ไว้เพื่อการศึกษา ณ วันที่ 15 กันยายน พ.ศ. 2563 ไว้เบื้องต้นดังนี้

5.1 http://camorrau23edy436.onion	ชื่อ Camorra Hitmen
5.5.2 http://vrnjnmcmlb7vbmmk.onion.onion	ชื่อ Hydra Hitmen
5.5.3 http://h4gca3vb6v37awux.onion	ชื่อ 18th Street Gang Hitmen
5.5.4 http://idomquol7lannf22.onion	ชื่อ The Mechanic
5.5.5 http://assassinec3wumxw.onion	ชื่อ The Assassins
5.5.6 http://yo4jmu6dsfaeekt3.onion	ชื่อ VeniceMan Killer Hitman
5.5.7 http://dtt6tdtgroj63iud.onion	ชื่อ Torminator
5.5.8 http://zy3dkytcaubkq2y3.onion	ชื่อ Hitman

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 9

จากวิจัยเชิงสืบสวนเบาะแสในโลกไซเบอร์ พบว่ามีเบาะแสเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดจำนวนมาก มีรายละเอียดวิธีการ ตลอดจนข้อคิดเห็นประสบการณ์จากผู้เคยใช้บริการมาบอกต่อ

เมื่อคำนึงถึงบริบทเทคโนโลยีปัจจุบัน จึงประเมินได้ว่า การจ้างสังหารออนไลน์อย่างไร้ตัวตนผ่าน TOR และจ่ายค่าจ้างด้วย Crypto currency มีความเป็นไปได้อย่างสมบูรณ์ ไร้ตัวตนทั้งผู้จ้างและผู้รับจ้าง เหตุผลที่สนับสนุนว่ามีการจ้างสังหารออนไลน์ผ่าน TOR และจ่ายค่าจ้างด้วย Crypto currency เป็นคดีฆาตกรรมมาแล้ว และไม่เคยมีการต้มตุ๋นหลอกลวงเอาเหรียญ Crypto currency เพราะไม่เคยมีผู้เสียหายออกมาเปิดเผยหรือร้องเรียน

ผู้วิจัยจึงได้นำมาวิเคราะห์ เพื่อทำนายปรากฏการณ์ว่าเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืด และจ่ายค่าจ้างวานฆ่าด้วย Crypto currency ได้ผลดังนี้

Tor network เป็น Decentralized network ไม่มี Server ศูนย์กลางเก็บข้อมูลเว็บไซต์และผู้เข้าใช้งาน ใช้วิธีกระจายข้อมูลไปสู่คอมพิวเตอร์ของโครงข่าย ซึ่งไม่สามารถระบุตัวตน (IP

Address) เจ้าของเว็บไซต์ ผู้รับจ้างวานฆ่า และผู้สั่งจ้างวานฆ่าได้ อีกทั้งหากมีการจ่ายค่าจ้างวานฆ่าด้วย Crypto currency ก็ไม่สามารถทราบได้ว่าเจ้าของบัญชีเป็นผู้ใด รูปแบบเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดเป็นจริง และปัจจุบันมีเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดจำนวนมาก แต่ก็มีการต้มตุ๋นหลอกลวง (Scam) ในบางเว็บไซต์เช่นกัน โดยให้วางเงินมัดจำก่อน อย่างไรก็ตามเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดที่มีชื่อเสียง กลับไม่มีการวางเงินมัดจำจ่ายค่าจ้างเมื่อเสร็จงาน จึงไม่มีเหตุผลว่าจะหลอกลวงได้อย่างไร จึงสรุปได้ว่าเว็บไซต์จ้างสังหารออนไลน์อย่างไร้ตัวตนในเว็บมืดมีอยู่จริง

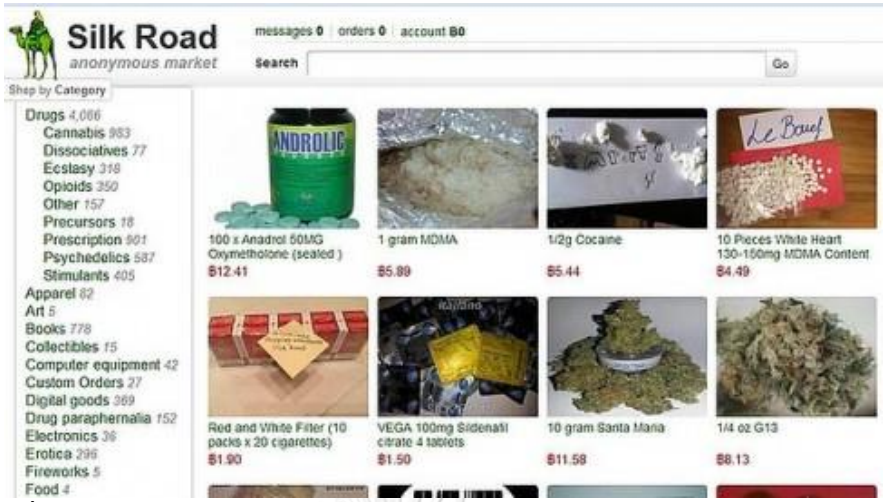
จากต้นแบบการประกอบธุรกิจจ้างสังหารของ Besa Mafia เป็น Business model ในอุดมคติขององค์กรอาชญากรรม และองค์กรอาชญากรรมข้ามชาติที่ต้องการความไร้ตัวตนให้รอดพ้นจากการสืบสวนจับกุมและไร้ร่องรอยหลักฐานการดำเนินคดี

จะเห็นได้ว่าอาชญากรมี 2 ปัจจัยการไร้ตัวตนครบถ้วน (Anonymous Factors) ทั้ง การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

แม้เว็บมืด Besa Mafia ปิดตัวหลบหนีไปแล้ว แต่ผลกระทบจาก Business model ใหม่ของ Besa Mafia ส่งผลให้องค์กรอาชญากรรมกลุ่มอื่นได้ลอกเลียนแบบมากมาย เกิดเว็บมืดรับจ้างทำร้ายและสังหารผ่าน TOR และจ่ายค่าจ้างด้วย Crypto currency หลายเว็บในปัจจุบัน (พ.ศ.2564) รวมทั้งประเทศไทย จึงคาดการณ์ได้จากปัจจัยการไร้ตัวตนที่ครบถ้วนนี้จะทำให้อาชญากรรมไซเบอร์ประเภทนี้เติบโตขึ้นอย่างรวดเร็ว

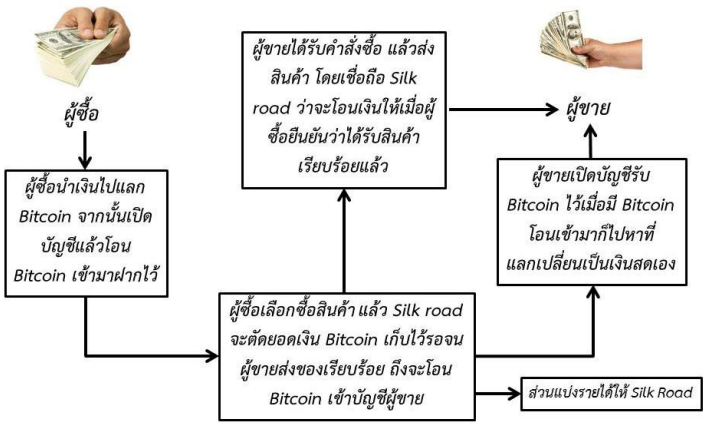
<u>กรณีศึกษาที่</u> 10 เว็บไซต์ค้ายาเสพติดใน TOR Network และชำระเงินด้วย Crypto currency

Silk Road เป็นต้นแบบเว็บไซต์ค้ายาเสพติดและขายของผิดกฎหมายที่มีชื่อเสียงที่สุดในยุคแรก เป็นต้นแบบขององค์กรอาชญากรรมไซเบอร์ยุคใหม่ โดยจำหน่าย ยาเสพติด สารตั้งต้นยาเสพติด คู่มือการผลิตยาเสพติด และอาวุธ ฯลฯ จ่ายเงินด้วย Bitcoin ทำให้รูปแบบเส้นทางการเงินและ Business Model ของอาชญากรและองค์กรอาชญากรรมเปลี่ยนแปลงไป ธุรกิจจำหน่ายของผิดกฎหมายทุกประเภทสามารถอยู่ได้ และเติบโตอย่างรวดเร็วมีสมาชิกและรายการสินค้านับแสนรายการ บริการค้าขายได้ทั่วโลก



รูปที่ 46 ตัวอย่างหน้าเว็บไซต์ Silk road

ที่มา http://silk4rd6h4qdy3wvz2urxvwx66l7ektov5wmpkoptmgwuldaefc55yyd.onion/ (เข้าผ่าน Tor browser)



รูปที่ 47 ผังวิธีการซื้อของผิดกฎหมายในเว็บไซต์ Silk road ผ่าน TOR จ่ายเงินด้วย Bitcoin

วิธีการซื้อขายยาเสพติดและของผิดกฎหมายในเว็บไซต์ Silk road ด้วย Bitcoin โดยที่ Silk road มีรายได้จากการหักค่าธรรมเนียมจากการให้บริการซื้อขาย และกำไรจากมูลค่าการถือครอง Bitcoin ที่เพิ่มขึ้นในช่วงเวลานั้นๆ Silk road ทำรายได้มากกว่า 100 ล้านบาทต่อปี (โดยประมาณ)

จากการเป็นต้นแบบของเว็บไซต์ขายของผิดกฎหมายค้าขายทั่วโลก ซึ่งขบวนการอาชญากรรมต่างๆ เอาเยี่ยงอย่างเดินตามมาอีกมากมาย แม้ว่าในราวปี ค.ศ. 2013 FBI สามารถจับกุมตัว นาย Ross William Ulbricht เจ้าของเว็บไซต์ Silk road ได้ ซึ่งทางการได้ติดตามสืบสวนมายาวนาน

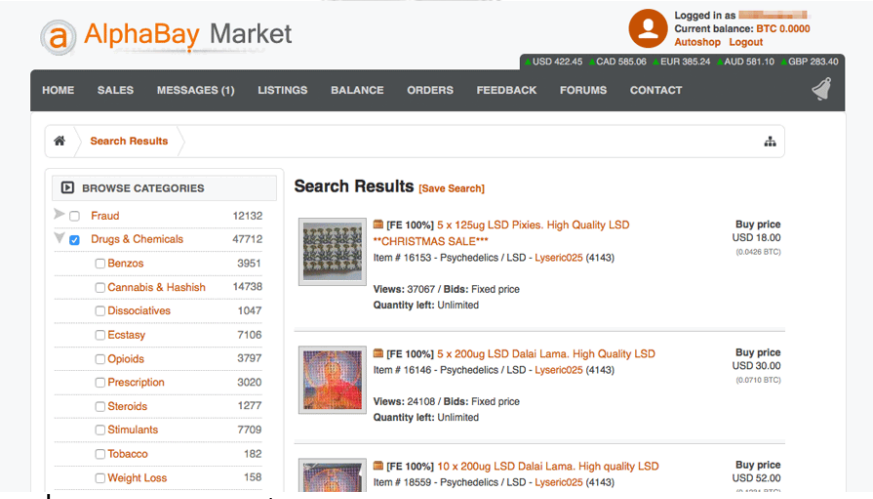
จากการค้นคว้าของผู้วิจัยพบว่า FBI ไม่ได้สืบสวนจนสามารถจับกุมได้จากเว็บไซต์หรือเส้นทางการเงินของ Bitcoin แต่เกิดจากการสับเพร่าของนาย Ulbricht เอง ที่ไปโพสต์ E-mail ตัวเองตอบคำถามในเว็บบอร์ดแห่งหนึ่งที่ถามหาการซื้อขายยาเสพติด ทำให้เจ้าหน้าที่ค้นหา E-mail และ Facebook เจอจนรวบรวมหลักฐานจับกุมตัวได้ในที่สุด

ปัจจุบันขณะที่นาย Ulbricht เจ้าของเว็บไซต์ถูกคุมขังอยู่ เขาถูกตัดสินจำคุกตลอดชีวิต นอกจากคดียาเสพติด ยังมีคดีจ้างสังหารออนไลน์ร่วมด้วย แต่เว็บไซต์ Silk Road ได้กลับมาเปิดให้บริการอีกครั้งในเวอร์ชัน Silk Road 3.0 ให้บริการใน Dark web เข้าซื้อสินค้าผ่าน Browser TOR ได้เหมือนเดิม นับเป็นปรากฏการณ์สำคัญต่อวงการอาชญาวิทยาอย่างยิ่ง

Business Model วิธีการซื้อขายยาเสพติดและของผิดกฎหมายในเว็บไซต์ Dark web ผ่าน Tor ด้วยการใช้เงิน Bitcoin ทำให้กลายเป็นองค์กรอาชญากรรมข้ามชาติขนาดใหญ่ที่สุด

อดีตเว็บไซต์ค้าเสพติดใหญ่ที่สุดในโลก คือ AlphaBay Market จากประเทศไทย

AlphaBay ก่อตั้งขึ้นในปี 2014 โดยนาย Alexandre Cazes (อาเล็กซองเดร คาเซส) ชาวแคนาดาหนุ่มวัย 26 IT Specialist อาศัยอยู่ภูเก็ต ประเทศไทย AlphaBay เป็นเว็บไซต์ที่จำหน่ายยาเสพติด อาวุธปืนและสิ่งผิดกฎหมายทุกชนิด มีลูกค้าเป็นสมาชิกในเว็บไซต์มากกว่า 200,000 ราย



รูปที่ 48 ตัวอย่างหน้าเว็บไซต์ AlphaBay Market

ที่มา https://darkweblink.com/alphabay/

AlphaBay Market เข้าเว็บไซต์ผ่าน Dark web เช่นกัน ผู้ใช้งานต้องเข้าเว็บผ่าน TOR ซึ่งเป็น Browser ปกปิดตัวตนของผู้ที่ login เข้าเว็บไซต์มืด และซื้อขายด้วย Bitcoin ต้องมีสมาชิกในเครือข่ายแนะนำเข้ามา

นาย Alexandre Cazes เจ้าของเว็บ AlphaBay Market[32] ถูกจับกุมตัวตั้งแต่เมื่อวันที่ 5 กรกฎาคม พ.ศ.2560 ด้วยปฏิบัติการ Bayonet ตั้งแต่ช่วงระหว่างเดือนพฤษภาคม พ.ศ. 2560 นำโดยเอฟบีไอ หน่วยงานปราบปรามยาเสพติดสหรัฐ อเมริกา หรือดีอีเอ สำนักงานตำรวจแห่งชาติเนเธอร์แลนด์ สหราชอาณาจักร ฝรั่งเศส และลิทัวเนีย ก่อนที่จะประสานกับตำรวจไทยเข้าจับกุมได้สำเร็จ

เจ้าหน้าที่ได้ค้นพบ E-mail ส่วนตัวของนาย Alexandre Cazes ซึ่งเคยถูกระบุไว้ในหัวจดหมาย (E-mail) ต้อนรับผู้ใช้งานรายใหม่ที่สมัครเข้ามาใน AlphaBay หลังการยืนยันการสมัครสมาชิกเสร็จสมบูรณ์ ในช่วงที่ AlphaBay เพิ่งเปิดให้บริการได้ไม่นาน โดย E-mail นั้นใช้ชื่อ Pimp_Alex_91@hotmail.com

จากเบาะแส E-mail ดังกล่าว เจ้าหน้าที่ได้สืบทราบว่า เมื่อวันที่ 3 ธันวาคม พ.ศ. 2551 มีผู้ใช้ชื่อ Alpha02 ตอบกระทู้ออนไลน์บนเว็บไซต์ www.commentcamarche.com เกี่ยวกับวิธีการกำจัดไวรัสจากภาพถ่ายดิจิทัลอย่างถูกวิธี โดยที่ใต้ข้อความดังกล่าวมีการลงท้ายว่า Alexandre Cazes พร้อมกับ E-mail นี้ จึงได้สืบค้นต่อไปในเว็บไซต์ LinkedIn ซึ่งพบว่าว่าเขามีอาชีพนักออกแบบเว็บไซต์อิสระ และระบุได้ว่านาย Cazes อาศัยอยู่ในประเทศไทย

ต่อมาวันที่ 12 ก.ค.60 ช่วงระหว่างเวลา 07.00 น. ถึง 07.30น ก่อนถูกส่งตัวไปดำเนินคดียังสหรัฐ อเมริกา นาย Alexandre Cazes ได้ใช้ผ้าเช็ดตัวผูกคอตัวเองภายในห้องน้ำเสียชีวิต[33]

รูปที่ 49 ภาพข่าวการเสียชีวิตของ Alexandre Cazes

ที่มา https://thehackernews.com/2017/07/alphabay-darkweb-alexandre-cazes.html

[32] BBC News Thai. ตร.ไทย เปิดเบื้องหลังการจับกุม AlphaBay เว็บค้าสิ่งผิดกม.ใหญ่ที่สุดในโลก.
Cited on 24 2017. Available from URL: https://www.bbc.com/thai/international-40702712

[33] Jeff Parsons. Dark web fugitive found hanged in prison cell after being arrested in Thailand. Cited 14 July 2017. Available from URL: https://www.mirror.co.uk/tech/alleged-founder-notorious-dark-web-10795471

เว็บไซต์ Hackread.com[34] ให้ข้อมูลว่า นาย Alexandre Cazes มีสินทรัพย์ดิจิทัลดังนี้ จำนวน bitcoins 1,605.05 btc (1 btc มูลค่า 2.1 ล้านบาท ณ วันที่ 14 เม.ย. 64) หรือประมาณ 3,300 ล้านบาทโดยประมาณ เหรียญ Ethereum 8,309.27 Eth (1 Eth มูลค่า 7.7 หมื่นบาท ณ วันที่ 14 เม.ย. 64) และ 3,691.98 zcash ขณะที่เหรียญ Monero ไม่ทราบจำนวน นอกจากนั้น ตำรวจยังยึดทรัพย์สินมูลค่าหลักล้านได้หลายรายการ รวมถึงอสังหาริมทรัพย์ 3 แห่ง และรถยนต์ลัมโบกินี 4 คัน

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 10

เว็บไซต์ค้ายาเสพติดใน TOR Network และชำระเงินด้วย Crypto currency อย่าง Silk Road และ AlphaBay Market เป็นต้นแบบเว็บไซต์ค้ายาเสพติดและขายของผิดกฎหมายที่มีชื่อเสียงที่สุดในยุคแรก เป็น Business model ในอุดมคติขององค์กรอาชญากรรมและองค์กรอาชญากรรมข้ามชาติที่ต้องการความไร้ตัวตนให้รอดพ้นจากการสืบสวนจับกุมและไร้ร่องรอยหลักฐานการดำเนินคดีอยู่แล้ว มี 2 ปัจจัยการไร้ตัวตนครบถ้วน (Anonymous Factors) ทั้ง การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

แต่เหตุที่แท้จริงของทั้งเจ้าของ Silk Road และ AlphaBay Market ถูกจับกุมนั้น ไม่ได้เกิดจากการสืบสวนทางดิจิทัลแต่อย่างใด แต่เกิดจากการสับเพร่าของทั้งคู่ในการใช้ E-mail จริงของทั้งคู่ในการตอบลูกค้า จึงทำให้สืบสวนจับกุมได้อย่างง่ายดายเพียงค้นใน google เท่านั้นเอง ไม่ได้ใช้วิธีสืบสวนจากเส้นทางดิจิทัลแต่อย่างใด

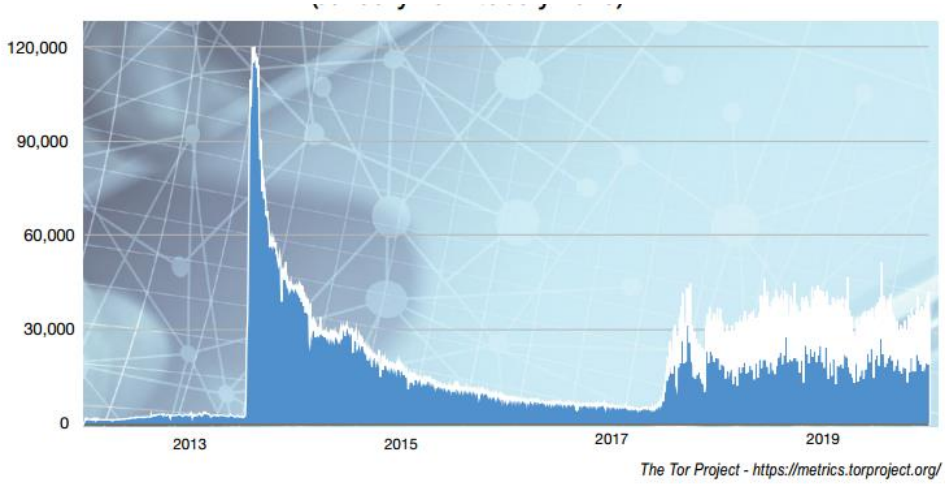
โดยเฉพาะอย่างยิ่งแม้หากตอนจับกุมตัวนาย Ross William Ulbricht เจ้าของเว็บไซต์ Silk road ได้ถ้าหากเขาไม่สารภาพไม่ยอมบอกพาสเวิร์ดคอมพิวเตอร์ก็ย่อมไม่สามารถเอาผิดดำเนินคดีได้แต่อย่างใด แต่การจับกุมครั้งนี้เจ้าหน้าที่ FBI วางแผนมาอย่างดี รอให้นาย Ross William Ulbricht เข้าไปนั่งในห้องสมุด แล้วเปิดคอมพิวเตอร์โน๊ตบุ๊ค เจ้าหน้าที่ส่วนหนึ่งก็จับตัว เจ้าหน้าที่ส่วนหนึ่งก็ยกคอมพิวเตอร์ไปตรวจค้นขณะเครื่องยังเปิดอยู่

ส่วนนาย Alexandre Cazes เจ้าของ AlphaBay Market นั้น หากไม่สารภาพการรวบรวมพยานหลักฐานดิจิทัลย่อมเป็นไปได้ยาก จึงไม่น่าเชื่อว่าจะเป็นเหตุให้ตัดสินใจฆ่าตัวตายอย่างง่ายดาย

---

[34] Carolina. Dark Web: US court seizes assets and properties of deceased AlphaBay operator. Cited on 18 September 2018. Available from URL: https://www.hackread.com/dark-web-us-court-seizes-assets-alphabay-operator/

อย่างไรก็ตาม ต้นแบบเว็บไซต์ค้ายาเสพติดใน TOR Network และจ่ายเงินด้วย Crypto currency มี 2 ปัจจัยการไร้ตัวตนครบถ้วนให้รอดพ้นจากการสืบสวนจับกุมและไร้ร่องรอยหลักฐานการดำเนินคดี อาจเป็นเหตุเป็นผลทำให้อาชญากรตัดสินใจลงมือก่ออาชญากรรมไซเบอร์ในรูปแบบประเภทนี้จนเติบโตอย่างรวดเร็วในปัจจุบันนับร้อยเว็บไซต์



รูปที่ 50 ผู้ใช้บริการเชื่อมต่อ Tor Browser จากประเทศไทย (January 2012 to July 2020)

ที่มา https://metrics.torproject.org/

จากเอกสารงานวิจัยของ United Nations Office on Drugs and Crime (UNODC) เรื่อง Darknet Cybercrime Threats to Southeast Asia 2020[35] ผู้ใช้บริการเชื่อมต่อ Tor Browser จากประเทศไทยลดลงอย่างมากนับตั้งแต่ Silkroad ถูกปิด และกลับมาได้รับความนิยมเพิ่มขึ้นในช่วงปลายปี 2561 อีกครั้ง มีผู้ใช้บริการเฉลี่ย 4,000 รายต่อวัน และลดลงเหลือ 250 รายต่อวันในปี 2563 ด้วยเปลี่ยนไปใช้บริการอื่น เช่น I2P โครงการอินเทอร์เน็ตล่องหน (ผู้วิจัยแปล) หรือสมัครบริการ VPN อื่นที่มีค่าบริการ

[35] United Nations Office on Drugs and Crime (2020). Darknet Cybercrime Threats to Southeast Asia. 2020.

<u>กรณีศึกษาที่</u> 11 การแฮ็กเรดาร์ตรวจจับเครื่องบินรบของกองทัพซีเรียก่อนถูกถล่มอย่างไร้ตัวตน

6 กันยายน 2550[36] ราวเที่ยงคืนเศษ ฝูงบินรบเก่าจาก อิสราเอล ที่ไม่ใช่เครื่องบินหลบเรดาร์ (non-stealthy warplanes) บินจากทางตอนเหนือ ทะลุผ่านการตรวจจับระบบเรดาร์ของกองทัพซีเรีย ซึ่งใช้เทคโนโลยีของรัสเซีย

ริชาร์ด และ โรเบิร์ต[37] (Richard and Robert, 2012) สงครามไซเบอร์ (Cyber war) ได้อุบัติขึ้นครั้งแรก เมื่อเครือข่ายเทคโนโลยีสารสนเทศระบบป้องกันภัยทางอากาศมูลค่ามหาศาลหลายพันล้านดอลลาร์สหรัฐของประเทศซีเรีย ที่สั่งซื้อจากรัสเซียถูกแฮ๊ค (Hack) ระบบไปครอบครอง โดยสายลับอิสราเอล หน้าจอเรดาร์แสดงความว่างเปล่าไม่ปรากฏวัตถุใดในน่านฟ้า ขณะที่ฝูงบิน F-15 Eagle และ F-16 Falcon บินข้ามพรมแดงมุ่งหน้าสู่เมืองหลวง กรุงดามัสกัส เมื่อถึงเป้าหมายที่ต้องสงสัยว่าเป็นโรงงานอาวุธนิวเคลียร์ ก็ทิ้งระเบิดจนสว่างวาบไปทั่วท้องฟ้าราวกับกลางวัน กลุ่มอาคารเป้าหมายพังพาบราบคาบไปในพริบตา จากนั้นฝูงบินดังกล่าววกกลับไปอย่างง่ายดายไร้การตอบโต้แต่อย่างใด

ต่อมาสื่อต่างๆ ได้เผยแพร่เหตุการณ์ดังกล่าวรวมทั้งภาพถ่ายจากดาวเทียม กล่าวว่าอิสราเอลได้เคยเจรจากับซีเรียซึ่งมีพรมแดนติดกับอิสราเอลด้วยข้อสงสัยว่า ซีเรียกำลังพยายามสร้างโรงงานผลิตอาวุธนิวเคลียร์โดยร่วมมือกับเกาหลีเหนือ แต่ซีเรียได้ปฏิเสธมาตลอด

ฝูงบิน F-15 Eagle และ F-16 Falcon เป็นฝูงบินรบเก่าที่ถูกสร้างขึ้นในทศวรรษที่ 1970 ไม่ใช่เครื่องบินสมัยใหม่ที่หลบเรดาร์ได้ โครงสร้างทำจากไทแทเนียม และเหล็กกล้า พร้อมติดระเบิดและจรวดนำวิถีครบครัน อาจเป็นความจงใจสร้างประวัติศาสตร์สงครามไซเบอร์ในการบินอย่างไร้ตัวตนข้ามน่านฟ้ามาถล่มถึงเมืองหลวง ภาพจอเรดาร์ที่ปรากฏแต่ความว่างเปล่า จรวดนำวิถีต่อต้านอากาศยานของกองทัพซีเรียไม่สามารถยิงขึ้นไปได้เพราะมองไม่เห็นเป้าหมาย อีกทั้งฝูงบินรบกองทัพอากาศซีเรียจำเป็นต้องมีระบบควบคุมภาคพื้นดินที่ต้องสร้างเส้นสมมุติลากไปยังเครื่องบินเป้าหมายก่อนปล่อยขึ้นบิน ก็ไม่สามารถทำได้ เพราะศัตรูไร้ตัวตนบนจอเรดาร์

[36] David A. Fulghum and Douglas Barrie (2007). Israel used electronic attack in air strike against Syrian mystery target. ABC News. Cited on 8 October 2007. Available from URL: https://abcnews.go.com/Technology/story?id=3702807&page=1

[37] Richard A. Clarke and Robert Knake. Cyber War: The Next Threat to National Security and What to Do about It. West Point New York. Army Cyber Institute. April 10 2012.

รูปที่ 51 เป้าหมายก่อนและหลังโจมตี

ที่มา https://www.aljazeera.com/news/2018/3/21/israel-confirms-bombing-syria-nuclear-reactor-in-2007

นี่คือสงครามไซเบอร์ครั้งแรกที่รัฐชาติหนึ่งแทรกซึมเครือข่ายคอมพิวเตอร์ของรัฐชาติอีกแห่งหนึ่งที่เป็นปรปักษ์ก่อนบุกถล่มแบบสายฟ้าแลบ โดยไม่ได้ทำลายระบบรักษาความปลอดภัยทางอากาศของกองทัพเหมือนการรบในอดีต เครือข่ายคอมพิวเตอร์และไฟเบอร์ออปติกของระบบรักษาความปลอดภัยทางอากาศของซีเรียทำงานผิดพลาด แต่แสดงอาการปกติประหนึ่งว่าไม่มีอะไรเกิดขึ้นและระบบไม่ได้เสียหาย อิสราเอลวางแผนอย่างไร้ที่ติและเก็บเป็นความลับว่าใช้วิธีการใดในการครอบครองระบบเครือข่ายคอมพิวเตอร์เพื่อความมั่นคงของซีเรีย

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 11

การแฮ็กเรดาร์ของระบบการป้องกันภัยทางอากาศไม่ให้สามารถตรวจจับเครื่องบินรบเป็นเรื่องใหญ่ที่สุด เมื่อฝูงบินข้าศึกหลบพ้นระบบเทคโนโลยีสารสนเทศของเรดาร์เข้ามาทิ้งระเบิดถล่มเป้าหมายได้ เมื่อไม่สามารถตรวจจับเครื่องบินข้าศึกได้ก็ไม่สามารถส่งฝูงบินขึ้นไปต่อต้านได้ และถ้าหากเลยเถิดถล่มทั้งเมืองย่อมเกิดการสูญเสีย ชีวิต ทรัพย์สินพลเรือนอย่างมหาศาล และถึงขั้นสูญเสียอธิปไตยก็เป็นได้

จากกรณีศึกษาที่ 11 จะเห็นได้ว่าฝูงบินข้าศึกมี 2 ปัจจัยการไร้ตัวตนครบถ้วน (Anonymous Factors) ทั้ง การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีหรือเอาผิดทำไม่ได้

หากประเทศใดหรือกลุ่มก่อการร้ายหรืออาชญากรเปิดเผยตัวตนมาทิ้งระเบิดในประเทศซีเรีย ย่อมถูกประกาศสงคราม หรือถูกคว่ำบาตรจากนานาประเทศ แต่ความมั่นใจว่าปฏิบัติการดังกล่าวจะมีเทคโนโลยีที่ปิดบังอำพรางอย่างไร้ตัวตนจนเป้าหมายตรวจจับไม่ได้ อาจเป็นเหตุเป็นผลที่สำคัญที่ทำให้อาชญากรตัดสินใจ

เทคโนโลยีที่ช่วยให้อาชญากรไร้ตัวตนหรือล่องหนได้ ทำให้ซีเรียไม่อาจทราบตั้งแต่การบุกรุกเข้ามา หรือจะทราบได้ว่าเป็นการกระทำของผู้ใด และไม่ปรากฏหลักฐานในการเอาผิดร้องทุกข์กล่าวโทษผู้ใดได้ในเวทีนานาชาติ ในทางกลับกันหากเหล่าอาชญากรหรือฝูงบินข้าศึก ทราบว่าซีเรียสามารถสืบสวนจับกุมทางดิจิทัลได้ และการรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีได้ ย่อมไม่กล้าบุกรุกเข้ามาแน่ เพราะจะเป็นการประกาศสงครามอันจะนำมาซึ่งการต่อต้านจากนานาชาติ

กรณีศึกษานี้เกิดคำศัพท์ทางอาชญากรรมไซเบอร์ใหม่ที่ฉายให้เห็นภาพการก่อการร้ายหรือสงครามยุคใหม่เช่นคำว่า Cyber espionage, Cyber Sabotage และ Cyber warfare เป็นต้น ซึ่งปัญหาการไร้ตัวตนในการใช้เทคโนโลยีไซเบอร์ก่ออาชญากรรมดังกล่าว จะเป็นภัยคุกคามความมั่นคงของชาติอย่างใหญ่หลวงต่อไป

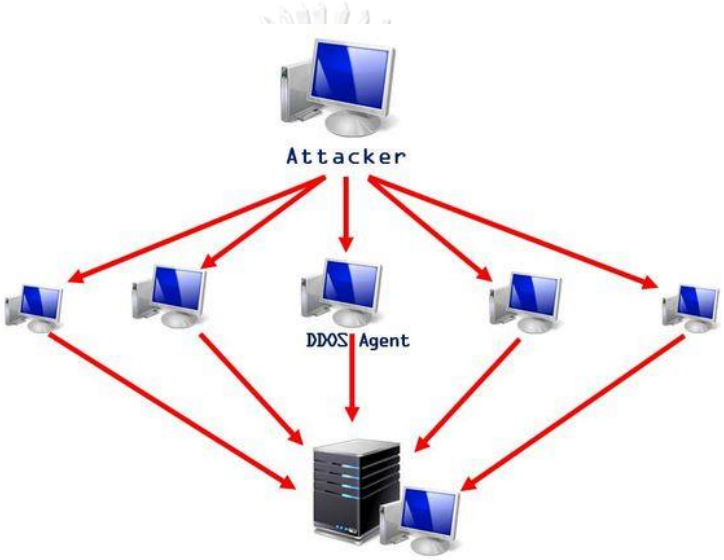
<u>กรณีศึกษาที่</u> 12 โจมตีรัฐบาลด้วย DDoS ครั้งใหญ่ที่สุดในประวัติศาสตร์โลก

การแฮ็กหรือเจาะระบบเครือข่ายคอมพิวเตอร์เพื่อครอบครองหรือทำลายเป็นเรื่องที่เข้าใจทั่วไปง่ายสำหรับคนทั่งไปในปัจจุบัน แต่อาชญากรรมไซเบอร์อีกประเภทที่สร้างความเสียหายใหญ่หลวง และทวีความรุนแรง มากขึ้นเรื่อยๆ กลับกลายเป็น DDoS

DDoS Attack หรือ Denial-of-service (DoS) Attack เป็นการก่ออาชญากรรมไซเบอร์ในรูปแบบ “การโจมตีไปยัง Server ของเหยื่อหรือเป้าหมายให้ใช้บริการไม่ได้หรือเชื่อมต่ออินเทอร์เน็ตไม่ได้อย่างชั่วคราวหรือถาวร” ด้วยวิธีการส่งข้อมูลจำนวนมหาศาลไปยัง Server ของเหยื่อเป้าหมายจนปริมาณ Traffic data ในการรับส่งใช้เวลาการทำงานนานมากจนไม่สามารถให้บริการได้ อาทิเช่น การส่ง E-mail ขยะจำนวนมหาศาลนับล้านๆ ฉบับมายัง Server ของเหยื่อเป้าหมายหรือการส่ง TCP Syn Flood DOS Attack ทำให้ Server ของเหยื่อต้องใช้หน่วยความจำในการรอจำนวนมากเพื่อหน่วงเวลาการทำงานให้ไม่ปกติหรือการส่ง Ping of Death แพ็กเก็ตขนาดใหญ่เข้ามาเรื่อยๆ จน Server ของเหยื่อเป้าหมายจนรองรับไม่ไหว

อาชญากรไซเบอร์จะโจมตี Server เหยื่อหรือองค์กรเป้าหมายด้วยการแฮ็คคอมพิวเตอร์หลายๆเครื่องช่วยในการโจมตีหรืออาจจะใช้ Malware ควบคุมเครื่องเหล่านั้น เพื่อยืมมือในการช่วยโจมตีเหยื่อเป้าหมาย เรียกเครื่องที่ถูกควบคุมเหล่านั้นว่า Zombie หรือ Botnet หรือ DDoS Agent

หรือบางครั้ง DDoS Agent ไม่ได้ถูกควบคุมแต่ร่วมมือกันช่วยถล่ม Server ของเหยื่อที่ตกเป็นเป้าหมาย ซึ่งบางครั้งการโจมตีเว็บไซต์ขององค์กรที่ตกเป็นเหยื่อเหล่านั้นไม่ได้เกิดความเสียหายอะไร แต่เกิดการถูกชะลอการให้บริการช้าลงหรือเข้าเว็บไซต์ไม่ได้ชั่วขณะ เนื่องด้วยมีปริมาณข้อมูลผ่านเข้าออก Server มากกว่าปกติ



รูปที่ 52 อาชญากรรมไซเบอร์ในแบบ DDoS Attack

วิธีการโจมตีแบบ DDoS Attack ที่ง่ายที่สุดคือ การใช้วิธีการนัดหมายเข้าเว็บไซต์เหยื่อเป้าหมายพร้อมกันแล้วกดปุ่ม F5 บนคีย์บอร์ดคอมพิวเตอร์ของตนรัวๆ การกด F5 บนหน้าเว็บไซต์คือการกด Refresh เมื่อกด Refresh รัวๆ พร้อมๆ กันหลายคน ก็เป็นการร้องขอ (Request to send) ให้ Server ของเหยื่อส่งข้อมูลกลับมา เมื่อเกิดการร้องขอและส่งข้อมูลในเวลาเดียวกันมากๆ เว็บไซต์ก็เกิดการทำงานไม่ปกติจนไม่สามารถให้บริการได้ชั่วคราว

บางครั้งเหยื่อเป้าหมายเป็นเว็บไซต์หน่วยงานราชการหรือหน่วยงานความมั่นคง เมื่อข่าวแพร่ออกไปก็จะเกิดมวลชนตามเข้ามาดูเว็บไซต์ของเหยื่อเป้าหมาย ซึ่งก็จะทำให้ Server เกิดการชะลอ

เวลาการให้บริการช้าลงหรือเข้าเว็บไซต์ไม่ได้ชั่วขณะ เนื่องด้วยมีปริมาณข้อมูลผ่านเข้าออก Server มากกว่าปกติ แต่เมื่อปริมาณคนเข้าชมน้อยลงหรือ Traffic data คล่องตัวขึ้นเว็บไซต์ดังกล่าวก็ใช้งานได้ตามปกติ มิได้เกิดความเสียหายแต่อย่างใด มิได้เกิดการแฮ๊คอย่างที่ประกาศไว้

ริชาร์ด และ โรเบิร์ต (Richard and Robert, 2012) เมือง ทัลลินน์ (Tallinn) มีประชากรราว 400,000 คน เป็นเมืองหลวงของประเทศ เอสโตเนีย ที่ได้แยกตัวออกมาเป็นอิสระภายหลังจากการล่มสลายของโซเวียต

ช่วงปี ค.ศ. 1941-1944 เอสโตเนีย ถูกยึดครองโดยนาซีเยอรมัน และเมื่อสิ้นสงครามโลกครั้งที่ 2 สหภาพโซเวียตมีชัยเหนือกองทัพนาซี เอสโตเนียจึงถูกยึดครองและผนวกเข้าเป็นส่วนหนึ่งของสหภาพโซเวียต

สหภาพโซเวียตจึงสร้างอนุสาวรีย์รูปปั้นสำริดทหารกองทัพแดง (Red Army) แห่งพรรคคอมมิวนิสต์ (Bronze Soldier of Tallinn) เพื่อไม่ให้ชาวเอสโตเนียลืมความเสียสละของเหล่าทหารกองทัพแดงที่ปลดปล่อยเอสโตเนียจากนาซี ตั้งอยู่ที่สุสานทหารแห่งทัลลินน์ (Defence Forces Cemetery of Tallinn)

รูปที่ 53 อนุสาวรีย์รูปปั้นสำริดทหารกองทัพแดง (Red Army) แห่งพรรคคอมมิวนิสต์ (Bronze Soldier of Tallinn)

ที่มา https://www.shutterstock.com/th/image-photo/bronze-soldier-tallinn-84239659

แต่เมื่อเอสโตเนียประกาศตัวเป็นอิสระอีกครั้ง ความขัดแย้งระหว่างชาวเอสโตเนียเดิมกับชาวรัสเซียที่มาอาศัยอยู่ในเอสโตเนียก็ปะทุขึ้น เมื่อคนส่วนใหญ่ในเอสโตเนียพยายามลบล้างสัญลักษณ์ใดๆ ที่บ่งบอกถึงการตกเป็นเมืองขึ้นรัสเซียอื่นออกไป

ในอดีตก่อนที่จะตกเป็นเมืองขึ้นของรัสเซีย สุสานทหารแห่งทัลลินน์ เป็นที่ฝังศพทหารชาวเอสโตเนียที่ต่อสู้เพื่ออิสรภาพมาก่อนในสงคราม Estonian War of Independence และมีอนุสาวรีย์ทหารชาวเอสโตเนีย แต่มาถูกผู้มีอำนาจของรัสเซียทำลาย และนำรูปปั้นสำริดทหารกองทัพแดงโซเวียตมาแทนหลังสงครามโลกครั้งที่ 2 ทำให้ชาวเอสโตเนียขุ่นข้องหมองใจมายาวนาน

รัฐบาลเอสโตเนียออกกฎหมาย[38] การอนุรักษ์หลุมฝังศพทหารจากสงคราม ซึ่งต้องการปกป้องหลุมฝังศพวีรบุรุษของชาติ และมรดกทางประวัติศาสตร์ ส่งผลให้สิ่งปลูกสร้างที่มีลักษณะต้องห้าม รูปปั้นสำริดทหารกองทัพแดงโซเวียตจะต้องถูกรื้อถอน และศพทหารโซเวียตจะต้องถูกเคลื่อนย้ายจากสุสานทหารเอสโตเนีย

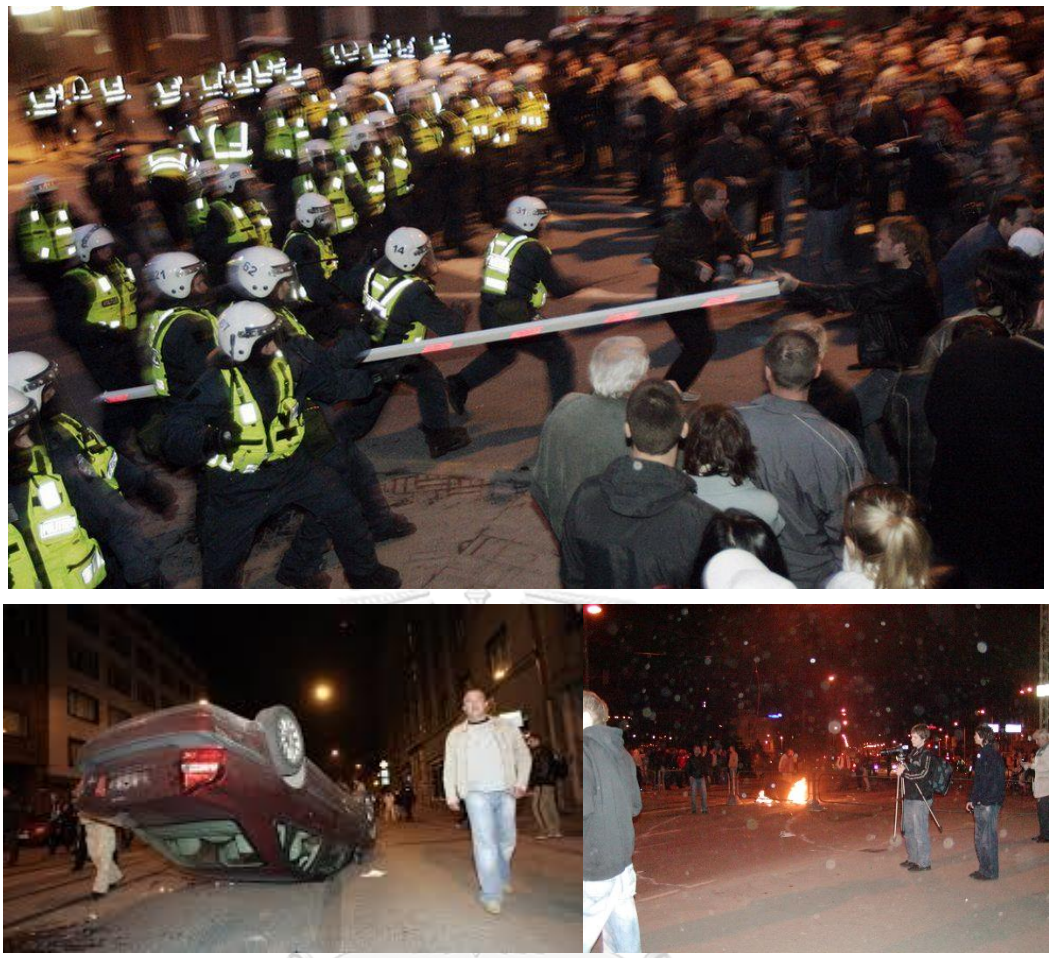
ทางการรัสเซียประณามการเคลื่อนย้ายรูปปั้นสำริดทหารกองทัพแดงโซเวียต และศพทหารโซเวียตเป็นการทำลายเกียรติยศทหารที่สละชีพ ประธานาธิบดี เอสโตเนียใช้อำนาจวีโต้กับกฎหมายฉบับนี้ทันที

แต่กาลกลับเป็นกลุ่มคนเชื้อสายรัสเซียคัดค้านการย้ายรูปปั้นสำริดทหารกองทัพแดงโซเวียตรวมตัวมากขึ้นเรื่อยๆ และฝ่ายตรงข้ามคือกลุ่มชาตินิยมเอสโตเนียก็เริ่มรวมตัวกันและขู่จะทำลายรูปปั้นสำริดทหารกองทัพแดง ความขัดแย้งลุกลามอย่างรวดเร็วกลายเป็นกองกำลังพร้อมต่อสู้กันทำลายกัน

ค่ำวันที่ 27 เมษายน 2550 สื่อทั่วโลกเรียกว่า “Bronze Night” เกิดจลาจลระหว่างฝ่ายคัดค้านการย้ายรูปปั้นสำริดทหารกองทัพแดงและฝ่ายสนับสนุนการย้าย เกิดการตะลุมบอนกันจนมีผู้เสียชีวิต

---

[38] Protection of War Graves Act. Passed 10 January 2007. Estonia. Available from URL : http://www.melaproject.org/sites/default/files/2019-07/Protection%20of%20War%20Graves%20Act.pdf



รูปที่ 54 “Bronze Night” เกิดจลาจลรุนแรงก่อนนำไปสู่ Cyber attack ในวันรุ่งขึ้น

ที่มา https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia

รัฐบาลเอสโตเนียรีบเคลื่อนย้ายรูปปั้นสำริดทหารกองทัพแดงออกจากสุสานทหารเอสโตเนียไปที่ใหม่ทันที จนต้องมีการส่งทหารมาอารักขารูปปั้น และเหตุการณ์บนถนนก็สงบลง แต่ย้ายการปะทะมาบนโลกไซเบอร์

เอสโตเนียได้รับเอกราชเพียง 25 ปี แต่ประเทศที่เกิดใหม่จากเถ้าถ่านแห่งนี้ ได้รับการยกย่องว่าเป็นสังคมเศรษฐกิจดิจิทัลที่ก้าวหน้าที่สุดแห่งหนึ่งของโลก ความสำเร็จต่างๆ ถูกกล่าวขานถึงทั้ง e-Society, e-Government, e-Residency, e-Voting, etc.

บริการออนไลน์ของภาครัฐ และภาคเอกชนครอบคลุมแทบทุกมิติของชีวิตประชากรชาวเอสโตเนีย การจ่ายภาษีออนไลน์ การทำธุรกรรมธนาคารออนไลน์ บัตรประชาชนอิเล็กทรอนิกส์ ข้อมูลด้านสุขภาพของประชาชนถูกจัดเก็บไว้อย่างเป็นระบบบนคลาวด์ ฯลฯ

ไม่กี่วันหลังจาก “Bronze Night” บรรดา Server ของบริการต่างๆ ในเอสโตเนียถูกคำขอเข้าสู่หน้าเว็บ (Request to send) จำนวนมหาศาลจนทำให้ Server ล่ม หลายบริการปิดตัวลง และบาง Server ได้รับคำสั่ง ping เข้ามามากจนค้างไม่สามารถให้บริการได้อีกต่อไป รวมทั้งระบบรัฐบาลอิเล็กทรอนิกส์ไม่สามารถให้บริการได้ สิ่งเหล่านี้คือการโจมตีที่เรียกว่า DDoS Attack

DDoS Attack ดูเหมือนแค่เรื่องก่อกวนเล็กน้อยไม่ซับซ้อนสำหรับชาวโลกมันไม่ใช่อาวุธหนักสำหรับการทำสงครามไซเบอร์และคนส่วนใหญ่ก็คิดเช่นนั้น แต่ในครั้งนั้นรัฐบาลเอสโตเนียมองว่า DDoS Attack มาเป็นกองทัพมหาศาลทั้ง Zombie และ Botnet จากคอมพิวเตอร์นับหมื่นนับแสนเครื่องโจมตีต่อเนื่องจากคำสั่งยาวนานนับสัปดาห์ ซึ่งเจ้าของเครื่องคอมพิวเตอร์ไม่มีทางทราบได้เลยว่าตนตกเป็นเหยื่อ Zombie หรือ Botnet คอมพิวเตอร์

เอสโตเนีย ถูกโจมตีด้วย DDoS ครั้งใหญ่ที่สุดในประวัติศาสตร์โลก ไม่ใช่แค่ Server เว็บไซต์แต่รวมถึง Server ของเครือข่ายโทรศัพท์เคลื่อนที่ ระบบการสื่อสาร หนังสือพิมพ์ ธนาคารออนไลน์และระบบพาณิชอิเล็กทรอนิกส์ของรัฐบาลล่มทันที

เอสโตเนียนำเรื่องนี้ขึ้นสู่สภาความร่วมมือแอตแลนติกเหนือ (North Atlantic Cooperation Council) องค์กรสูงสุดกลุ่มประเทศพันธมิตรทางทหารนาโต้

ผู้เชี่ยวชาญด้าน Cyber security จากยุโรป และอเมริกา เดินทางไปช่วยเหลือทันที และผู้เชี่ยวชาญได้ทำการแกะรอย Track back ย้อนรอยคำสั่ง ping ว่ามาจากที่ใดพบว่ามาจากรัสเซีย

รัฐบาลรัสเซียแถลงอย่างเกรี้ยวกราดปฏิเสธว่ามิได้อยู่เบื้องหลังการโจมตีทางไซเบอร์กับเอสโตเนีย และยังปฏิเสธคำร้องขอทางการทูตอย่างเป็นทางการในการให้ความช่วยเหลือแกะรอยผู้ควบคุมการโจมตีครั้งนี้แม้มีความตกลงทวิภาคีที่ระบุว่ารัสเซียต้องให้ความร่วมมืออยู่ก็ตาม

ริชาร์ด และ โรเบิร์ต (Richard and Robert, 2012) เชื่อว่าเป็น “กลุ่มรัสเซียรักชาติ” กลุ่มชาตินิยมรัสเซียรุ่นใหม่เหล่าอันธพาลวัยรุ่นคลั่งชาติ และเป็นกลุ่มแฮ๊คเกอร์ที่ชำนาญที่สุดในรัสเซีย ส่วนใหญ่คนเหล่านี้ทำงานให้องค์กรอาชญากรรม

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 12

การโจมตีเอสโตเนียด้วย DDoS กับหน่วยงานรัฐบาลครั้งใหญ่ที่สุดในประวัติศาสตร์โลก จะเห็นได้ว่าเหล่าอาชญากรมี 2 ปัจจัยการไร้ตัวตนครบถ้วน (Anonymous Factors) ทั้ง การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

โดยเฉพาะการดำเนินคดีอาญากับอาชญากร ผู้วิจัยได้ตั้งข้อสังเกตว่า “การไร้ตัวตน” ศาลจะมีแนวโน้มยกฟ้องในหลายประเด็น อาทิเช่น เจตนาขาดตอนหรือไม่ครบองค์ประกอบความผิด เจตนาภายนอก และเจตนาภายใน เพราะอาชญากรไซเบอร์ส่ง Malware ไปฝังไว้ยังเครื่องคอมพิวเตอร์ Agent ทั้งหลายเพื่อยืมมือในการช่วยโจมตีแบบ DDoS เหยื่อเป้าหมาย เรียกว่า Zombie หรือ Botnet ซึ่งทั้งตัวเจ้าของ คอมพิวเตอร์เองหรือตัวอาชญากรเองไม่ได้สั่งการทุกครั้งให้โจมตี Server เหยื่อเป้าหมาย แต่เครื่องคอมพิวเตอร์ Agent เหล่านั้นทำงานอัตโนมัติหรือมีปัญญาประดิษฐ์คิดเองได้ว่าเมื่อใดจะเหมาะสม

เทคโนโลยีการไร้ตัวตนไม่ได้ช่วยเพียงให้อาชญากรล่องหนได้ แต่กลายเป็นไม่เคยมีตัวตนหรือเป็นคนขึ้นมาก่อนเลย ทำให้ไม่ทราบได้ว่าเป็นการกระทำของผู้ใด และไม่ปรากฏหลักฐานในการเอาผิดร้องทุกข์กล่าวโทษผู้ใดได้

ในทางกลับกันหากเหล่าอาชญากร ทราบว่าเอสโตเนียมีความสามารถสืบสวนจับกุมทางดิจิทัลได้ และการรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีได้ ย่อมไม่กล้าโจมตีแน่เช่นกัน

แต่ในกรณีนี้จะเห็นว่า เบาะแสที่ผู้เชี่ยวชาญด้าน Cyber security จากยุโรป และอเมริกาเดินทางไปช่วยเหลือเอสโตเนีย แกะรอยว่าการโจมตีเอสโตเนียด้วย DDoS มาจากทิศทางประเทศรัสเซีย แม้การรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีทำไม่ได้ แต่การสืบสวนทางดิจิทัลทำได้เพียงบางส่วน

การโจมตีแบบ DDoS กลายเป็นปัญหาใหญ่ในอาชญากรรมไซเบอร์ปัจจุบันแม้ไม่ได้มีเทคโนโลยีซับซ้อน อาชญากรไซเบอร์ส่ง Malware แพร่กระจายอัตโนมัติไปฝังไว้ยังเครื่องคอมพิวเตอร์ Agent ทั้งหลายให้กลายเป็น Zombie หรือ Botnet รวมถึงกล้องวงจรปิด IP Camera เพื่อนำมาสร้าง Traffic data โจมตี Server เหยื่อเป้าหมายเพื่อทำลายหรือเรียกค่าไถ่จำนวนมาก และมีแนวโน้มสูงขึ้นทุกวัน

<u>กรณีศึกษาที่</u> 13 กลุ่มก่อการร้าย ISIS ระดมทุนถล่มกรุงปารีสด้วย Bitcoin

คืนวันศุกร์ที่ 13 พฤศจิกายน พ.ศ. 2558 เกิดเหตุก่อการร้ายด้วยหลายกรณีทั้ง การกราดยิงผู้คน 6 จุด การระเบิดฆ่าตัวตาย 4 จุด และการจับตัวประกันในกรุงปารีส และเมืองแซ็ง-เดอนี (ย่านชานกรุงปารีสทางทิศเหนือ) ประเทศฝรั่งเศส รวมถึงที่บริเวณใกล้กับสนามกีฬาแห่งชาติ ซึ่งกำลังมีการแข่งขันฟุตบอลนัดกระชับมิตรระหว่างทีมชาติฝรั่งเศสกับทีมชาติเยอรมนี การโจมตีทำให้มีผู้เสียชีวิตอย่างน้อย 153 คน

ประชาชนเสียชีวิตมากที่สุดอยู่ที่โรงละคร บาตากล็อง (Bataclan) ผู้ก่อการร้ายได้จับผู้ชมคอนเสิร์ตเป็นตัวประกันและเผชิญหน้ากับตำรวจจนสิ้นสุดลงเมื่อเวลา 00:58 น. ของวันที่ 14 พฤศจิกายน ครั้งนี้เป็นการโจมตีที่ร้ายแรงที่สุดที่เกิดกับฝรั่งเศสนับตั้งแต่สงครามโลกครั้งที่ 2

27 พฤศจิกายน 2558 เว็บไซต์ ข่าวไทยพีบีเอส[39] นำเสนอข่าวเรื่อง “เยอรมนีจับพ่อค้าอาวุธปืนให้ผู้ก่อการร้ายปารีส” ทางการเยอรมนีจับกุมตัวผู้ต้องสงสัยค้าอาวุธปืนให้กลุ่มก่อการร้ายในกรุงปารีส ประเทศฝรั่งเศส พบหลักฐานเป็น E-mail ในโทรศัพท์มือถือที่ใช้ติดต่อกลุ่มชาวอาหรับ อาวุธปืนที่อยู่ในรายการซื้อขายประกอบด้วย ปืนเอเค-47 ผลิตในจีนจำนวน 2 กระบอก และปืนซาสตาวา เอ็ม 70 ผลิตในยูโกสลาเวีย อีก 2 กระบอก โดยช่วงเวลาขายอาวุธปืนคือ 7 พ.ย. 2558 ซึ่งไม่ถึง 1 สัปดาห์ ก่อนเกิดเหตุก่อการร้ายในกรุงปารีส

อัยการฝรั่งเศสเชื่อว่าอาวุธปืนทั้ง 4 กระบอกเป็นส่วนหนึ่งของอาวุธที่กลุ่มผู้ก่อการร้ายใช้ในการก่อเหตุ แต่อัยการเยอรมนีเผยว่า ตำรวจเยอรมนีจับกุมผู้ต้องสงสัยค้าอาวุธจริง แต่ยังไม่แสดงความเห็นว่าผู้ต้องสงสัยคนดังกล่าวขายอาวุธปืนให้แก่กลุ่มก่อการร้ายจริงหรือไม่

6 กุมภาพันธ์ 2561 เว็บไซต์ คมชัดลึก[40] นำเสนอข่าวเรื่อง “มือถล่มปารีสปิดปากสนิทขึ้นศาลเบลเยียม” ใจความว่า นายซาเลาะห์ อับเดลสลาม ผู้ต้องสงสัยก่อการร้ายโจมตีกรุงปารีสที่ยังมีชีวิตอยู่เพียงคนเดียวถูกนำตัวจากเรือนจำใกล้เมืองหลวงฝรั่งเศส ไปขึ้นศาลเบลเยียมในกรุงบรัสเซลส์

อับเดลสลาม วัย 28 ปี ถือสัญชาติฝรั่งเศสแต่เกิดในเบลเยียมและมีเชื้อสายโมร็อกโก ถูกแจ้งข้อหาพยายามฆ่าตำรวจและมีอาวุธต้องห้ามในครอบครอง อับเดลสลามยิงต่อสู้กับตำรวจในเขตฟอเรสต์ของกรุงบรัสเซลส์เมื่อ 15 มีนาคม 2559 ซึ่งไม่ยอมปริปากพูดกับพนักงานสอบสวนมาตั้งแต่ถูกจับกุมในเดือนมีนาคม 2559 แสดงท่าทีขัดขืนทันที ด้วยการไม่ลุกขึ้นยืนเมื่อผู้พิพากษาขอให้ยืนยันตัวตน ผู้ต้องสงสัยเพียงรายเดียวก็ดับความหวังของอัยการเพราะยังปิดปากเงียบต่อไป

พฤษภาคม 2017 The Centre for a New American Security (CNAS) ได้ตีพิมพ์วารสาร ENERGY, ECONOMICS & SECURITY เรื่อง “TERRORIST USE OF VIRTUAL CURRENCIES” ความตอนหนึ่งว่า

ได้พบหลักฐานการใช้เงินดิจิทัลของผู้ก่อการร้ายใน Gaza Strip และสมาชิกในกลุ่ม ISIS บางคนได้ใช้เงินดิจิทัลใน อินโดนีเซีย และสหรัฐ อเมริกา

---

[39] ข่าวไทยพีบีเอส. เยอรมนีจับพ่อค้าอาวุธปืนให้ผู้ก่อการร้ายปารีส. Cited 27 พฤศจิกายน 2558.
Available from URL: https://news.thaipbs.or.th/content/6339

[40] คมชัดลึก. มือถล่มปารีสปิดปากสนิทขึ้นศาลเบลเยียม. Cited 6 กุมภาพันธ์ 2561.
Available from URL: http://www.komchadluek.net/news/foreign/312180

แต่ผู้ก่อการร้ายในกลุ่มอื่นยังคงใช้ระบบการเงินแบบดั้งเดิม โดยเฉพาะแบบ Hawala ทั้งใน Sub-Saharan Africa Yemen และ Horn of Africa

จากการวิจัยพบว่าเงินดิจิทัลได้ถูกใช้อย่างกว้างขวางในบรรดาองค์กรอาชญากรรม แต่ในกลุ่มผู้ก่อการร้ายยังไม่ได้รับความนิยมเท่าที่ควรเพราะว่า

รูปที่ 55 ภาพข่าวจากสื่อต่างๆ ที่นำเสนอการระดมทุนถล่มกรุงปารีสด้วย Bitcoin ของ ISIS

ที่มา https://thehackernews.com/2015/11/paris-attacks-isis-funding.html

ผู้ก่อการร้ายส่วนใหญ่อยู่ในพื้นที่ห่างไกล ไม่มีโครงข่ายโทรคมนาคมที่มีประสิทธิภาพ ไม่มีเครื่องมือสื่อสารที่ดี และไม่มีความรู้การใช้เทคโนโลยีสมัยใหม่เท่าที่ควร อาทิเช่น อัลเคด้า อยู่ใน Islamic Maghreb (AQIM) ที่ Sahel และ อัลเคด้า ใน Arabian Peninsula (AQAP) อยู่ที่ Yemen และ ISIS อีกในหลายพื้นที่อยู่ ในอิรัก และซีเรีย รายงานดังกล่าวระบุว่าหากกลุ่มผู้ก่อการร้ายรู้จักนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้คงจะเติบโตเข้มแข็งมากขึ้น แต่การที่มีสมาชิกผู้ก่อการร้ายบางคนเริ่มใช้เงินดิจิทัลนั่นเป็นเพียงปฏิบัติการแบบ “Lone wolf”

กลุ่มแฮ็กเกอร์คุณธรรมที่มีนามว่ากลุ่ม Ghost Security Group (GSG) ได้อ้างว่ากลุ่มผู้ก่อการร้าย ISIS ได้ระดมทุนด้วยระบบเงินดิจิทัลสกุล Bitcoin ได้ราว 3,000,000 เหรียญ สหรัฐ

หรือประมาณเกือบ 90 ล้านบาท เพื่อปฏิบัติการถล่มกรุงปารีสหรือ Paris Attack เมื่อ พฤศจิกายน 2015

สอดคล้องกับที่นาย Faisal Tayeb หัวหน้าหน่วยสืบสวนคดีพิเศษ Detachment 88 ของอินโดนีเซียให้ข่าวว่า มีชาวอินโดนิเซียราวพันคนให้การสนับสนุน ISIS ด้วยการบริจาค Bitcoin แต่อย่างไรก็ตามเขากล่าวว่ามีการปลอม Bitcoin address ของ ISIS เพื่อหลอกเอาเงินผู้ให้การสนับสนุน

ผู้วิจัยได้ลองเข้า กูเกิล พิมพ์คำว่า ISIS Bitcoin address ก็พบว่าปัจจุบันมีปลอมจำนวนมาก คาดว่าน่าจะเป็นคนหัวหมอเอา Bitcoin address ตนเองไปโพสต์ไว้เผื่อมีผู้ร่วมอุดมการณ์หลงเชื่อ

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 13

การที่ ISIS ระดมทุนถล่มกรุงปารีสด้วย Bitcoin เป็นกรณีศึกษาอาชญากรรมการก่อการร้ายที่น่ากังวลมาก เพราะเส้นทางการเงินขององค์กรก่อการร้ายข้ามชาติเป็นเรื่องสำคัญที่สุด แม้การปราบปรามกลุ่มก่อการร้ายจนเสียชีวิต 7 ศพ และจับกุมดำเนินคดีผู้ต้องสงสัยได้เพียงรายเดียวซึ่งไม่ยอมให้การใดๆ

หากวิเคราะห์จากข่าว[41] จะเห็นข้อมูลว่าแม้พบหลักฐานชาวเยอรมนีผู้ต้องสงสัยขายอาวุธให้ผู้ก่อการร้ายเป็น E-mail ในโทรศัพท์มือถือที่ใช้ติดต่อกลุ่มชาวอาหรับ แต่อัยการกรุงปารีส ฟรองซัวส์ มูแลงส์ ให้ข่าวผ่านสื่อในเรื่องข้อสงสัยว่า “หาแหล่งเงินทุนอย่างไร” ในไทยรัฐออนไลน์ หัวข้อข่าวเรื่อง “อัยการฝรั่งเศสชี้ คนร้ายถล่มปารีสมี 3 ทีม-เบลเยียมรวบผู้ต้องสงสัยเอี่ยวโจมตี” เมื่อวันที่ 15 พฤศจิกายน 2558

จะเห็นได้ว่าในการรวบรวมพยานหลักฐานการดำเนินคดีไม่สามารถหาหลักฐานการจ่ายเงินให้กับพ่อค้าอาวุธได้ ซึ่งจะเป็นหลักฐานชัดเจนในการมัดผู้ต้องสงสัยหรือชี้ความเชื่อมโยงการก่อการร้าย ดังนั้นจะเห็นได้ว่าหากผู้ก่อการร้ายใช้ Bitcoin อย่างที่ CNAS และแหล่งข่าวอื่นๆ รายงานไว้ ย่อมเป็นไปได้ยากที่จะดำเนินคดีกับผู้ต้องสงสัยได้เพราะบัญชี Bitcoin ไม่มีหลักฐานว่าผู้ใดเป็นเจ้าของบัญชีไม่ต้องใช้บัตรประชาชนมาเปิดบัญชี

คณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force หรือ FATF) คือ องค์กรระหว่างรัฐบาล ซึ่งก่อตั้งขึ้นโดยที่ประชุมสุดยอด G7 เมื่อ

[41] ไทยรัฐออนไลน์. อัยการฝรั่งเศสชี้ คนร้ายถล่มปารีสมี 3 ทีม-เบลเยียมรวบผู้ต้องสงสัยเอี่ยวโจมตี. Cited 15 พ.ย. 2558. Available from URL: https://www.thairath.co.th/content/539503

ปี 2531 ให้ความสำคัญเรื่องการต่อต้านการให้การสนับสนุนทางการเงินแก่ผู้ก่อการร้าย (Counter Financing Terrorism: CFT) เป็นหลัก โดยเฉพาะเรื่องกฎหมายการฟอกเงินที่ทั่วโลกต้องปฏิบัติตาม

หากกลุ่มก่อการร้ายสามารถขนย้ายเส้นทางการเงินข้ามพรมแดนได้อย่างไร้ตัวตนการตรวจสอบสะกัดกั้นใดๆ การก่อการร้ายจะเติบโตอย่างสูง อีกทั้งการระดมทุนด้วย Bitcoin หรือการใช้เส้นทางการเงินข้ามพรมแดนด้วย Bitcoin หรือ Crypto currency มี 2 ปัจจัยการไร้ตัวตนครบถ้วน (Anonymous Factors) ทั้ง การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

ดังนั้นการระดมทุนการก่อการร้ายด้วย Bitcoin หรือ Crypto currency หรือการใช้เส้นทางการเงินด้วย Bitcoin หรือ Crypto currency จะทำให้การก่อการร้ายมีโอกาสเติบโตสูง

<u>กรณีศึกษาที่</u> 14 นายสุรภักดิ์ ภูไชยแสง (พิสูจน์ตัวตนว่าไม่ได้เป็นผู้กระทำความผิดจากการใช้ E-mail)

จะยกกรณีศึกษาของ นายสุรภักดิ์ ภูไชยแสง โปรแกรมเมอร์ ผู้ต้องหาคดีกระทำความผิดกฎหมายอาญามาตรา 112 ผ่านสื่อสังคมออนไลน์ ซึ่งเจ้าหน้าที่ตำรวจได้ติดตามพฤติกรรมมายาวนานได้หลักฐานครบถ้วน แต่ศาลยกฟ้องทั้งสามศาลจนถึงชั้นฎีกา โดยใช้ฐานข้อมูลคดีในเว็บไซต์ iLaw Freedom (https://freedom.ilaw.or.th/case/176)

นายสุรภักดิ์ ภูไชยแสง โปรแกรมเมอร์ ผู้ต้องหาคดีกระทำความผิดกฎหมายอาญามาตรา 112 หมิ่นประมาทหรืออาฆาตมาดร้ายต่อองค์พระมหากษัตริย์ ผ่านสื่อสังคมออนไลน์ facebook และ E-mail

ในช่วงสิบปีที่ผ่านมาเกิดการบิดเบือนความจริงและให้ร้ายสถาบันพระมหากษัตริย์พอสมควร เช่น ยุยงปลุกปั่นว่า สถาบันพระมหากษัตริย์ไม่สามารถวิพากษ์ (Criticize) วิจารณ์ (Comment) ได้ เป็นการจำกัดสิทธิเสรีภาพในการแสดงความคิดเห็นของประชาชน แต่ความจริงแล้วประชาชนชาวไทยไม่ได้ถูกจำกัดสิทธิดังกล่าว หากแต่เราไม่สามารถหมิ่นประมาท (Defamation) ได้ และบิดเบือนความจริงว่าสามารถถูกนำไปใช้กลั่นแกล้งทางการเมืองได้ง่าย

การขาดความรู้ของประชาชนในการแยกแยะความแตกต่างระหว่างวิพากษ์ (Criticize) วิจารณ์ (Comment) และหมิ่นประมาท (Defamation) ถูกนำมาสร้างเป็นเงื่อนไขให้เกิดอาชญากรรมแห่งความเกลียดชัง (Hate crime) กฎหมายอาญามาตรา 112 จึงอยู่ในหมวดความมั่นคง

หมิ่นประมาท (Defamation) นั้น หลักกฎหมายอาญาวางหลักไว้ว่า ห้ามมิให้ใส่ความให้บุคคลใดถูกเกลียดชัง ส่วนหลักกฎหมายแพ่งหมิ่นประมาทหมายความว่า การใส่ความเท็จให้ผู้อื่น

เสียหาย กล่าวคือ หากพิสูจน์ว่าเป็นความจริงมักยกฟ้อง ดังนั้นหมิ่นประมาทเป็นความชั่วร้ายใส่มนุษย์ไม่มีสิทธิทำความชั่วร้าย

หมิ่นประมาท (Defamation) คนละความหมายกับวิพากษ์ (Criticize) วิจารณ์ (Comment) ซึ่งกระทำบนเจตนาบริสุทธิ์บนพื้นฐานความจริงที่พิสูจน์ได้

กฎหมายอาญามาตรา 112 หมิ่นประมาท “อาฆาตมาดร้ายต่อองค์พระมหากษัตริย์” จึงถูกบิดเบือนความเข้าใจต่อประชาชน และบุคคลกลุ่มหนึ่งพยายามสร้างความเท็จ กุเรื่องที่พิสูจน์ไม่ได้ ใส่ความหมิ่นประมาทหรืออาฆาตมาดร้ายต่อองค์พระมหากษัตริย์จนคนจำนวนหนึ่งหลงเชื่อคล้อยตาม

นายสุรภักดิ์ ภูไชยแสง ถูกจับกุมและดำเนินคดีตกเป็นผู้ต้องหากระทำความผิดกฎหมายอาญามาตรา 112 หมิ่นประมาทหรืออาฆาตมาดร้ายต่อองค์พระมหากษัตริย์ และมาตรา 14(3) พ.ร.บ. คอมพิวเตอร์ฯ หมายจับ 1408/2554

รายละเอียดการกระทำตามข้อกล่าวหาระบุว่า สุรภักดิ์ ถูกกล่าวหาว่าเป็นเจ้าของ E-mail หนึ่ง และเป็นผู้ใช้ facebook ที่ตั้งชื่อว่า “เราจะครองแผ่นดินโดย xxx” ได้เขียนข้อความหมิ่นประมาท ดูหมิ่น ใส่ความ แสดงความอาฆาตมาดร้ายพระมหากษัตริย์ เผยแพร่ทาง facebook จำนวน 5 ข้อความต่างวันและเวลา อันเป็นความผิด 5 กรรม

ต่อมาตำรวจ ปอท. เข้าจับกุมนายสุรภักดิ์ ยึดคอมพิวเตอร์ไปตรวจพิสูจน์หลักฐาน และพบว่าคอมพิวเตอร์ดังกล่าวมีร่องรอยการเข้าใช้ facebook ในฐานะเจ้าของบัญชี “เราจะครองแผ่นดินโดย xxx”

คำขอท้ายคำฟ้องระบุว่า ขอให้ลงโทษจำเลยตามประมวลกฎหมายอาญามาตรา 112 มาตรา 91 มาตรา 33 พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 6) พ.ศ.2526 มาตรา 4 คำสั่งของคณะปฏิรูปการปกครองแผ่นดินฉบับที่ 41 ลงวันที่ 21 ตุลาคม 2519 ข้อ 1 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 3 มาตรา 14 มาตรา 17 และขอให้ศาลสั่งริบของกลาง ส่วนท้ายของคำฟ้องที่ร่างโดย นายชลัมพร เพ็ชรรัตน์ พนักงานอัยการสำนักงานอัยการสูงสุด เขียนไว้ว่า

"อนึ่ง จำเลยเป็นคนไทย อาศัยอยู่บนผืนแผ่นดินไทย อันมีพระมหากษัตริย์ทรงเป็นประมุข ทรงมีพระมหากรุณาธิคุณต่อชาติบ้านเมือง และพสกนิกรเป็นล้นพ้น จำเลยนอกจากไม่สำนักในพระมหากรุณาธิคุณทรงมีต่อพสกนิกรเสมอมาแล้ว ยังบังอาจแสดงความอาฆาตมาดร้าย มุ่งล้มล้างสถาบันพระมหากษัตริย์อันเป็นที่เคารพสักการะของปวงชนชาวไทย เป็นภัยต่อความมั่นคงของชาติที่ประชาชนชาวไทยไม่อาจยอมรับได้ พฤติการณ์ของจำเลยไม่มีเหตุอันควรปราณีไม่ว่าในทางใด สมควรได้รับโทษสถานหนัก

จำเลยกระทำผิดร้ายแรงอันเป็นภัยต่อความมั่นคงแห่งราชอาณาจักร หากจำเลยได้รับการปล่อยชั่วคราว อาจหลบหนีหรือไปยุ่งเหยิงกับพยานหลักฐาน หรือก่อภัยในลักษณะดังกล่าวขึ้นมาอีก หากจำเลยขอปล่อยตัวชั่วคราว โจทก์ขอคัดค้านการปล่อยตัวชั่วคราวของจำเลย"

สุรภักดิ์ ถูกจับกุมเมื่อวันที่ 2 กันยายน 2554 เวลาประมาณ 13.30 โดย พ.ต.อ.พิสิษฐ์ เปาอินทร์ รองผู้บัญชาการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) เป็นผู้นำกำลังพร้อมหมายค้นศาลอาญาที่ 233/2554 เข้าตรวจค้นที่ห้องพักย่านลาดพร้าว

ขณะเข้าตรวจค้นจำเลยอยู่ที่ห้องดังกล่าว จึงเป็นผู้นำตรวจค้นเอง เจ้าหน้าที่ได้ตรวจค้นและยึดของกลาง ได้แก่ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค 1 เครื่อง แอร์การ์ด 1 อัน ซิมการ์ดของบริษัททูมูฟ 2 อัน ซิมการ์ดวันทูคอล 1 อัน แผ่นซีดีบรรจุในกระเป๋าซีดี 52 แผ่น โมเด็มเร้าท์เตอร์ 1 เครื่อง คอมพิวเตอร์ตั้งโต๊ะ 1 เครื่อง แผงวงจรไฟฟ้า 1 ตัว ในชั้นจับกุมและชั้นสอบสวนจำเลยให้การปฏิเสธ สุรภักดิ์ ถูกควบคุมตัวอยู่ที่เรือนจำพิเศษกรุงเทพฯ โดยไม่เคยได้รับอนุญาตให้ประกันตัว

31 ตุลาคม 2555 ศาลพิพากษายกฟ้อง เพราะพยานหลักฐานที่โจทก์นำสืบยังมีความสงสัยว่าโจทก์ทำความผิดตามฟ้องหรือไม่ จึงยกประโยชน์แห่งความสงสัยให้จำเลย

25 มกราคม 2556 อัยการสำนักงานอัยการสูงสุด ยื่นอุทธรณ์ต่อศาลอุทธรณ์ สรุปสาระสำคัญได้ว่า โจทก์เห็นว่าศาลชั้นต้น หยิบยกข้อเท็จจริงด้านเทคนิคเกี่ยวกับคอมพิวเตอร์ จากคำเบิกความของจำเลย และพยานจำเลย โดยคลาดเคลื่อนจากความเป็นจริงอย่างมาก ดังจะกล่าวต่อไปนี้

1. การที่พบว่ามีคนเข้าใช้งานอีเมล์ dorkao@hotmail.com ในขณะที่จำเลยยังถูกควบคุมตัวอยู่ ก็ไม่ใช่เหตุที่จะฟังได้ว่าจำเลยไม่ใช่เจ้าของอีเมล์ เพราะจำเลยสามารถสร้างพยานหลักฐานเพื่อให้ตัวเองพ้นผิดได้โดยการให้รหัสผ่านแก่บุคคลอื่นเพื่อเข้าใช้อีเมล์ดังกล่าวได้

2. พยานหลักฐานของโจทก์ในคดีนี้ชี้ให้เห็นได้ว่า จำเลยเป็นเจ้าของอีเมล์ dorkao@hotmail.com และ facebook “เราจะครองแผ่นดินโดยxxx” การตรวจไม่พบประวัติการเข้าใช้งานในช่วงเวลากระทำความผิดตามฟ้องก็ไม่ใช่เรื่องผิดปกติแต่อย่างใด เพราะปกติแล้วผู้กระทำความผิดย่อมจะไม่ใช้เครื่องคอมพิวเตอร์ของตัวเอง หรือจะต้องพยายามปิดบังซ่อนเร้นเป็นอย่างดี

3. การตรวจพบข้อมูลการใช้งานอีเมล์และ facebook ในพาร์ทิชั่นที่สองไม่ใช่เรื่องผิดปกติ เพราะผู้ใช้งานคอมพิวเตอร์สามารถตั้งวินโดว์ให้ไปอยู่ในพาร์ทิชั่นที่สองหรือพาร์ทิชั่นอื่นได้ ซึ่งเครื่องคอมพิวเตอร์ของกลางปรากฏการติดตั้ง VM ware ในพาร์ทิชั่นที่สองซึ่งการเข้าใช้งานอินเทอร์เน็ตผ่านโปรแกรมนี้ ข้อมูลการใช้งานอินเทอร์เน็ตก็จะไปอยู่ในพาร์ทิชั่นที่สองได้

4. ไฟล์ที่ตรวจพบในเครื่องคอมพิวเตอร์ของกลาง ที่มีเวลาที่สร้าง (create) เวลาที่เข้าถึง (Access) และเวลาที่เปลี่ยนแปลง (Modify) เป็นเวลาเดียวกันนั้น ก็เป็นเรื่องปกติ การที่พยานจำเลยเบิกความว่าไฟล์ที่ตรวจพบมีความผิดปกติเพราะเวลาที่สร้างขึ้นและลบเป็นเวลาเดียวกันนั้น ที่จริงแล้วรายงานการตรวจพิสูจน์ไม่ได้บ่งบอกเรื่องเวลาที่ทำการลบไฟล์เลย จึงเป็นคำเบิกความที่คลาดเคลื่อน

5. การตรวจพบประวัติการใช้ facebook ไม่ใช่สิ่งที่ไม่สามารถเกิดขึ้นได้อย่างที่จำเลยอธิบาย เพราะโปรแกรมสืบค้นอินเทอร์เน็ต (Browser) จะทำการเขียนไฟล์หรือบันทึกเองเพื่อประโยชน์ในการใช้งานอยู่แล้ว การสาธิตของจำเลยเป็นคนละเรื่องกับการทำงานของ Browser ทำให้เกิดความสับสน

6. การที่จำเลยเบิกความว่า facebook มีระบบป้องกันไม่ให้เกิดร่องรอยการใช้งาน ไม่ใช่ความจริง เพราะการเข้าใช้งานเว็บไซต์อย่างไรเสียก็ต้องปรากฏร่องรอยเพราะการเข้าใช้งานไม่ใช่ความลับ กรณีจะเป็นความลับได้ก็ เช่น ประวัติการโพสข้อความ และคำกล่าวอ้างของจำเลยเป็นคำกล่าวอ้างลอยๆ ไม่มีการนำสืบผู้ก่อตั้ง facebook หรือผู้พัฒนาเว็บไซต์

7. การที่จำเลยกล่าวอ้างว่ามีการเปิดเครื่องคอมพิวเตอร์ของกลางขณะที่เครื่องคอมพิวเตอร์ถูกยึดแล้วนั้น จำเลยไม่ได้ซักค้านพยานผู้เชี่ยวชาญของโจทก์ให้ประจักษ์ชัด การรับฟังพยานหลักฐานของจำเลยในข้อนี้จึงยังไม่มีข้อยุติ

8. วิธีการปลอมแปลงไฟล์ที่จำเลยสาธิตนั้น เป็นเพียงวิธีการบันทึกหน้าเว็บเพจแล้วเปลี่ยนแปลงชื่อไฟล์ เป็นคนละเรื่องกับไฟล์ที่ตรวจพบ และเป็นไฟล์ที่อยู่คนละตำแหน่งกับไฟล์ที่ตรวจพบ การจะทำให้ปรากฏไฟล์แบบที่ตรวจพบเป็นเรื่องยากมาก และไฟล์ที่ตรวจพบนั้นก็พบว่าเวลาในการสร้างข้อมูล เวลาที่แก้ไข และเวลาที่เข้าถึงครั้งสุดท้าย ไม่ตรงกับวันเวลาที่มีการเปิดใช้เครื่องคอมพิวเตอร์ของกลาง

คดีนี้เป็นคดีที่ใช้เทคโนโลยีด้านคอมพิวเตอร์กระทำความผิด และจำเลยเป็นผู้มีความรู้ความสามารถสูง การค้นหาพยานหลักฐานให้ได้ประจักษ์ย่อมเป็นการยาก การดำเนินคดีจึงจำเป็นต้องอาศัยความช่วยเหลือจากพลเมืองดีที่เป็นผู้แจ้งเบาะแส คดีนี้ไม่ปรากฏว่าเจ้าหน้าที่หรือบุคคลที่เกี่ยวข้องในคดี รู้จักหรือมีมูลเหตุจูงใจจะต้องกลั่นแกล้งจำเลย หรือหากจะมีผู้ใดกลั่นแกล้ง ก็คงไม่สร้างพยานหลักฐานให้ไปปรากฏในพาร์ติชั่นที่สอง หรือจงใจให้ปรากฏหลักฐานการเข้าใจอีเมล์และ facebook ในช่วงเวลาที่ไม่ใช่วันกระทำความผิด

พยานหลักฐานในคดีนี้เป็นพยานหลักฐานที่เกิดขึ้นจริงจากการใช้งานในเครื่องคอมพิวเตอร์ของจำเลย และมีความพยายามจะซ่อนเร้นหลักฐาน แต่เกิดความผิดพลาดไม่อาจซ่อนเร้นได้ทั้งหมด

พยานหลักฐานของโจทก์มีน้ำหนักให้ลงโทษจำเลยได้ ขอศาลอุทธรณ์กลับคำพิพากษาศาลชั้นต้นและลงโทษจำเลยตามฟ้องด้วย

26 มีนาคม 2557 เวลา 9.30 น. ที่ห้องพิจารณาคดี 911 ศาลอาญารัชดาศาลอุทธรณ์มีคำพิพากษายืน ให้ยกฟ้องสุรภักดิ์ เพราะพยานหลักฐานของโจทก์มีพิรุธ ว่าอาจเป็นการปรักปรำจำเลย และไม่อาจพิสูจน์จนสิ้นสงสัยว่าจำเลยทำความผิดจริง จึงต้องยกประโยชน์แห่งความสงสัยให้จำเลย ศาลอุทธรณ์ยังมีคำสั่งให้คืนคอมพิวเตอร์ของกลางของจำเลยด้วย

หลังฟังคำพิพากษา สุรภักดิ์ ให้สัมภาษณ์กับผู้สื่อข่าวที่มารออยู่บริเวณหน้าศาลเป็นจำนวนมาก โดยสุรภักดิ์หวังว่าคำพิพากษาอุทธรณ์ในคดีนี้ น่าจะสร้างบรรทัดฐานที่ดีให้กับการพิจารณาคดีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในอนาคต

13 สิงหาคม 2558 เวลา 9.30 น. ห้องพิจารณาคดี 805 ศาลอาญา ศาลฎีกานัดฟังคำพิพากษาคดีของสุรภักดิ์

ศาลอ่านคำพิพากษาโดยอ่านเพียงข้อหา และคำพิพากษาของศาลฎีกาที่พิพากษายืนตามศาลอุทธรณ์ กระบวนการทั้งหมดใช้เวลาประมาณ 1 - 2 นาที เท่านั้น โดยศาลฎีกาพิพากษายืนตามศาลอุทธรณ์ ให้ยกฟ้องจำเลย สำหรับคำพิพากษาศาลอุทธรณ์ที่ให้คืนคอมพิวเตอร์ของกลางนั้น สุรภักดิ์บอกกับผู้สื่อข่าวว่าตนยังไม่ได้รับคืนเนื่องจากก่อนหน้านี้คดียังไม่ถึงที่สุด

รูปที่ 56 สุรภักดิ์ ภูไชยแสง ผู้ต้องหากระทำความผิดกฎหมายอาญามาตรา 112 ด้วย Facebook และมาตรา 14(3) พ.ร.บ. คอมพิวเตอร์ฯ

ที่มา โพสต์ทูเดย์

บันทึกการสังเกตการณ์คดี

พ.ต.อ.พิสิษฐ์ เบิกความว่า ตนได้ให้เจ้าหน้าที่ไปเฝ้าดูพฤติกรรมของผู้ต้องสงสัย ที่อพารต์เมนต์ ก็ได้พบบุคคลชื่อนายสุรศักดิ์หรือสุรภักดิ์เช่าอยู่จริง จึงได้ติดต่อแม่บ้านผู้ดูแล ได้ทราบว่านายสุรภักดิ์พักอยู่ห้องไหน และเมื่อพบบุคคลดังกล่าวมีตัวตนจริง จึงได้ขอหมายค้นจากศาล

พ.ต.อ.พิสิษฐ์เบิกความว่า ในวันที่ 2 กันยายน 2554 ได้นำกำลังไปตรวจค้นที่อพาร์ตเมนต์ พบนายสุรภักดิ์อยู่ชั้นล่าง จึงได้แจ้งให้เขาพาไปที่ห้องพัก โดยมีแม่บ้านของอพาร์ตเมนต์ไปด้วย ตัวจำเลยเป็นผู้นำตรวจค้น จากการสอบถามแม่บ้านและตรวจค้น ทราบว่าจำเลยอาศัยอยู่คนเดียว และมีคอมพิวเตอร์โน้ตบุ๊ก 1 เครื่อง คอมพิวเตอร์ตั้งโต๊ะ 1 เครื่อง ขณะเข้าไปค้นโน้ตบุ๊กยังออนไลน์อยู่ และจำเลยได้เข้าไปที่เครื่องคอมพิวเตอร์เพื่อดึงแอร์การ์ดที่เสียบอยู่ออก พนักงานสอบสวนจึงยึดแอร์การ์ดไว้

พ.ต.อ.พิสิษฐ์เบิกความว่า ขณะจับกุม จำเลยยอมรับว่าเป็นเจ้าของบัญชี “เราจะครอง xxx” โดยเป็นเจ้าของอีเมล์ dorkao@hotmail.com จำเลยได้เขียน username และ password ในกระดาษด้วยลายมือตัวเองไว้ในท้ายบันทึกการตรวจค้นด้วย

จากการสอบถามมูลเหตุจูงใจ จำเลยมีความเชื่อว่า ในการรัฐประหารเมื่อวันที่ 19 กันยายน 2549 พระมหากษัตริย์อยู่เบื้องหลังการทำรัฐประหารครั้งนั้น จึงมีความโกรธแค้น โพสต์ข้อความเพื่อระบายความรู้สึกตัวเอง โดยมีเพื่อนใน facebook ของจำเลยได้เห็นข้อความนี้เป็นจำนวนมากด้วย

นายสุรภักดิ์ ก่อนถูกจับ ประกอบอาชีพเป็นเจ้าของบริษัทพัฒนาซอฟท์แวร์คอมพิวเตอร์ เป็นผู้เชี่ยวชาญด้านเทคโนโลยี รับดูแลระบบฐานข้อมูล (data base) ให้กับบริษัทต่างๆ เช่น ทรู โรงงานไทยซัมมิตออโต้พาส และหน่วยงานราชการต่างๆ เช่น การประปานครหลวง การไฟฟ้าส่วนภูมิภาค และเคยทำระบบสืบค้นข้อมูลอาชญากรรมที่สถานีตำรวจนครบาลสายไหมให้กับสำนักงานตำรวจแห่งชาติ

ทนายความถามว่า ที่ถูกฟ้องว่าเป็นผู้ใช้เฟซบุ๊กชื่อ “เราจะครองxxx” และเป็นผู้ใช้อีเมล์ dorkao@hotmail.com นั้นเป็นความจริงหรือไม่ สุรภักดิ์ ตอบว่า **“ไม่เป็นความจริง”** ส่วนหน้า facebook ดังกล่าวนั้น ตนเพิ่งเคยเห็นตอนที่ถูกฟ้องต่อศาล ก่อนหน้านี้ไม่เคยเห็นมาก่อน

สุรภักดิ์เบิกความว่า ตนมี facebook เป็นของตัวเองใช้ชื่อว่า เรารัก ออราเคิล ซึ่งเป็นชื่อของโปรแกรมบริหารฐานข้อมูล และมีอีเมล์เป็นของตัวเอง ใช้ชื่อว่า surapak_phuchaisang@hotmail.com ซึ่งใช้สมัคร facebook และเป็นอีเมล์ที่ใช้ติดต่อนายสุรภักดิ์ เบิกความว่า ปัจจุบันอายุ 41 ปี ก่อนถูกจับ ประกอบอาชีพเป็นเจ้าของบริษัทพัฒนาซอฟท์แวร์คอมพิวเตอร์ เป็นผู้เชี่ยวชาญด้านเทคโนโลยี รับดูแลระบบฐานข้อมูล (data base) ให้กับบริษัทต่างๆ

เช่น ทรู โรงงานไทยซัมมิตออโต้พาส และหน่วยงานราชการต่างๆ เช่น การประปานครหลวง การไฟฟ้าส่วนภูมิภาค และเคยทำระบบสืบค้นข้อมูลอาชญากรรมที่สถานีตำรวจนครบาลสายไหมให้กับสำนักงานตำรวจแห่งชาติ

สุรภักดิ์เบิกความต่อว่า ที่พนักงานสอบสวนเบิกความว่า จำเลยไปดึงแอร์การ์ดออกนั้นไม่เป็นความจริง เนื่องจากตนเข้าใจว่า ถูกแจ้งข้อหาตามพ.ร.บ.คอมพิวเตอร์ฯ และจะถูกยึดเครื่องคอมพิวเตอร์ จึงเดินไปหยิบเครื่องคอมพิวเตอร์และถอดสายชาร์ตกับแอร์การ์ดออกพร้อมกันเพื่อยกไปให้เจ้าหน้าที่ตรวจ ซึ่งคอมพิวเตอร์เครื่องนี้ใช้ระบบ Hypernet หรือระบบจำศีล ถ้าหากพับฝาเครื่องลง หน้าจอจะค้างสถานะที่ทำงานอยู่ แต่เครื่องจะปิดการทำงาน (shut down) ซึ่งคอมพิวเตอร์เครื่องนี้ตั้งรหัสผ่านแบบไบออส (bios) ไว้ สำหรับเข้าถึงก่อนที่คอมพิวเตอร์จะทำงาน ไม่ใช่รหัสผ่านของวินโดวส์

สุรภักดิ์ เล่าต่อว่า เจ้าหน้าที่ตำรวจเข้าใจผิดคิดว่าตนจะทำลายหลักฐาน จึงไม่ยอมให้ตนแตะต้องคอมพิวเตอร์และเมื่อเปิดเครื่องขึ้นมาเห็นว่าต้องใช้รหัสผ่าน จึงข่มขู่ให้ตนให้รหัสผ่าน ซึ่งตนก็บอกไป จึงสามารถเปิดเครื่องคอมพิวเตอร์และเข้าไปทำอะไรข้างในได้ ซึ่งรหัสผ่านตัวนี้นอกจากจะใช้กับเครื่องคอมพิวเตอร์แล้วยังเป็นรหัสผ่านของ facebook และอีเมล์ที่ตนใช้ด้วย เจ้าหน้าที่คนที่จดรหัสจากตนไปคือ พ.ต.อ.พิสิษฐ์ เปาอินทร์

สุรภักดิ์ เล่าว่า หลังจากที่เข้าสู่เครื่องคอมพิวเตอร์ได้แล้ว เจ้าหน้าที่ข่มขู่ให้รับสารภาพ เมื่อเจ้าหน้าที่บอกให้เขียนรหัสผ่านบนหน้าเฟซบุ๊ก “เราจะครองxxx” ก็เลยเขียนให้ ตามที่มีลายมือปรากฏในสำนวน ตามเอกสารหมาย จ.11

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 14

ทนายความของนายสุรภักดิ์ ภูไชยแสง โปรแกรมเมอร์ ผู้ต้องหาคดีกระทำความผิดกฎหมายอาญามาตรา 112 หมิ่นประมาทหรืออาฆาตมาดร้ายต่อองค์พระมหากษัตริย์ ผ่านสื่อสังคมออนไลน์ facebook และ E-mail ไม่ได้สู้คดีบนหลักกฎหมายว่า ได้หมิ่นประมาท (Defamation) หรือไม่

แต่ได้สู้คดีในเรื่องการ**พิสูจน์ตัวตน** ว่า จำเลยเป็นเจ้าของ E-mail และ Facebook จริงหรือไม่ อีกทั้งการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล (Digital forensic) เป็นไปถูกต้องหรือไม่

การพิสูจน์ตัวตน เป็นประเด็นที่การไต่สวนคดีมีเหตุให้ไม่สิ้นสงสัยว่าจำเลยกระทำความผิดจริง ตามประมวลวิธีพิจารณาความอาญา มาตรา 227 หากไม่สิ้นสงสัยยกประโยชน์ให้จำเลย คดียกฟ้องเป็นพับตกไป

ดังนั้นการไร้ตัวตน (Anonymity) มิใช่เพียงการปิดบังอำพรางซ่อนเร้นหลักฐานการระบุว่าผู้ใดคือจำเลยหรืออาชญากรไซเบอร์ แต่การพิสูจน์ไม่ได้ว่าตัวตนจำเลยผู้นั้นเป็นผู้เดียวที่กระทำความผิดเป็นผู้อื่นไปไม่ได้ ก็เป็นเหตุให้เอาผิดลงโทษไม่ได้เช่นกัน

กรณีศึกษาที่ 15 คดี สงคราม ฉิมเฉิด (พิสูจน์ไม่ได้ว่าเป็นผู้ส่ง E-mail)

คดีที่อัยการเป็นโจทก์ฟ้อง นายสงคราม ฉิมเฉิด[42] พนักงานจัดส่งแก๊ส สาขาสมุทรสาคร บริษัท ไทยอินดัสเตรียลแก๊ส จำกัด (มหาชน) (ทีไอจี) ซึ่งเป็นอนุกรรมการสหภาพฯ ในข้อหานำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตามมาตรา 14 (Reeves) ของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

โดยคดีดังกล่าว เป็นคดีที่นางปาริชาติ พลพละ ผู้จัดการสาขาของบริษัทไทยอินดัสเตรียลแก๊ส จำกัด (มหาชน) (ทีไอจี) ฟ้องนายสงคราม ในข้อหาหมิ่นประมาทผู้อื่นโดยการโฆษณา ตามประมวลกฎหมายอาญามาตรา 326, 328 และ พ.ร.บ.แก้ไขเพิ่มเติมประมวลกฎหมายอาญา(ฉบับที่ 11) พ.ศ. 2535 มาตรา 3,4 รวมถึงข้อหานำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตาม พ.ร.บ.คอมพิวเตอร์ มาตรา 14 เนื่องจากมีการส่งอีเมลหนังสือร้องเรียน ซึ่งมีเนื้อหาหมิ่นประมาทไปยังองค์กรต่างๆ ซึ่งที่สุด หลังการเจรจาไกล่เกลี่ย นายจ้างได้ยอมความโดยถอนฟ้องไป แต่ยังคงเหลือข้อหาตาม พ.ร.บ.คอมพิวเตอร์ เพราะเป็นอาญาแผ่นดิน ไม่อาจยอมความได้ ทำให้ต้องต่อสู้คดีต่อไป

โดยในการสืบพยาน ฝ่ายโจทก์นำสืบพยาน 6 ปากได้แก่ นางปาริชาต พนักงานบริษัท 3 คน ผู้แปลเอกสาร 1 คน และพนักงานสอบสวน 1 คน ขณะที่ฝ่ายจำเลย นำสืบเพียงจำเลย

25 พ.ค.55 ศาลจังหวัดสมุทรปราการ พิพากษายกฟ้อง โดยศาลเห็นว่าแม้ข้อเท็จจริงจำเลยจะเป็นผู้ทำหนังสือร้องเรียนไปยังกรรมการผู้จัดการ แต่โจทก์ไม่มีพยานหลักฐานใดมาชี้ให้เห็นว่าจำเลยคือผู้ส่งอีเมล์ และไม่ปรากฏว่ามีการตรวจสอบกับผู้ให้บริการอีเมล์และเครือข่ายคอมพิวเตอร์ถึงแหล่งที่มาของอีเมล์ว่าเป็นของผู้ใด แม้คดีได้ความว่าจำเลยระบุสำเนาเรียนถึงบุคคลต่างๆ ในหนังสือร้องเรียน แต่พฤติการณ์เพียงเท่านี้ไม่อาจชี้ได้ว่าจำเลยเป็นผู้กระทำผิด พยานหลักฐานที่โจทก์นำสืบจึงไม่เพียงพอ พิพากษายกฟ้อง

---

[42]ยกฟ้อง! คดีแรก คนงานถูกฟ้อง พ.ร.บ.คอมพิวเตอร์. นักสื่อสารแรงงาน. 25 พ.ค.55 Available from URL: https://voicelabour.org/%E0%B8%A2%E0%B8%81%E0%B8%9F%E0%B9%89%E0%B8%AD%E0%B8%87-%E0%B8%84%E0%B8%94%E0%B8%B5%E0%B9%81%E0%B8%A3%E0%B8%81-%E0%B8%84%E0%B8%99%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%96%E0%B8%B9%E0%B8%81%E0%B8%9F/

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 15

คดีดังกล่าวนี้ จากการส่ง อีเมลล์ ถูกฟ้องหมิ่นประมาท (ออนไลน์) ยังฟ้องความผิดเกี่ยวคอมพิวเตอร์ โดยนำเข้าข้อมูลอันเป็นเท็จ และฝ่ายจำเลยมีเพียงจำเลยผู้เดียวนำสืบ วิเคราะห์พฤติการณ์ได้ว่า จำเลยไม่ได้มีความพยายามจะสู้คดีด้วยทนายความมืออาชีพเท่าใดนัก

แต่ศาลได้ลงลึกในประเด็นเรื่องการ**พิสูจน์ตัวตน** ว่า จำเลยเป็นผู้ส่ง อีเมลล์ จริงหรือไม่? ราวกับคดียิงผู้อื่นตายโจทก์ต้องนำสืบว่า จำเลยยิงให้ผู้อื่นตายอย่างไร ดังนั้นศาลจึงวางหลักว่าโจทก์ต้องทำให้ศาลเชื่อได้ว่า จำเลยคือคนกด Send ส่งอีเมลล์จริงๆ จึงจะสิ้นสงสัย และโจทก์ไม่ได้มีการตรวจสอบหาหลักฐานมายืนยันตัวตนว่า จำเลยเป็นเจ้าของ อีเมลล์ จริงหรือไม่ เหตุผลดังกล่าวสอดคล้องตามประมวลวิธีพิจารณาความอาญา มาตรา 227 หากไม่สิ้นสงสัยต้องยกประโยชน์ให้จำเลย

ดังนั้นการไร้ตัวตน (Anonymity) มิใช่เพียงการปิดบังอำพรางซ่อนเร้นหลักฐานการระบุตัวตนว่าผู้ใดคือจำเลยหรืออาชญากรไซเบอร์ แต่การพิสูจน์ไม่ได้ว่าตัวตนจำเลยเป็นผู้ลงมือกระทำความผิดจนสำเร็จ ก็เป็นเหตุให้เอาผิดลงโทษไม่ได้เช่นกัน

<u>กรณีศึกษาที่</u> 16 คดี นพวรรณ ตั้งอุดมสุข โพสต์ประชาไทหมิ่นเบื้องสูง (พิสูจน์ตัวตนว่าเป็นผู้กระทำความผิดไม่ได้ เพราะ IP Address เป็นชื่อแม่)

20 ต.ค. 58 ที่ห้องพิจารณา 807 ศาลอาญา ถ.รัชดาภิเษก ศาลอ่านคำพิพากษาศาลฎีกา คดีหมายเลขดำ อ.1257/2552 ที่พนักงานอัยการฝ่ายคดีอาญา 8 เป็นโจทก์ ยื่นฟ้อง น.ส.นพวรรณ ตั้งอุดมสุข[43] เป็นจำเลย ในความผิดฐาน หมิ่นประมาท ดูหมิ่น พระมหากษัตริย์ พระราชินี หรือรัชทายาท ตามประมวลกฎหมายอาญา มาตรา 112 และ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีเมื่อวันที่ 15 ต.ค. 51 มีการโพสต์ข้อความลงในเว็บไซต์ประชาไท จำเลยให้การปฏิเสธตลอดข้อกล่าวหา

โดยศาลชั้นต้น มีคำพิพากษา เมื่อวันที่ 31 ม.ค. 54 ให้ยกฟ้อง เนื่องจากเห็นว่า **พยานหลักฐานที่เป็นหมายเลข IP Address** ซึ่งใช้โพสต์ข้อความและเบอร์โทรศัพท์ สำหรับใช้ต่ออินเทอร์เน็ต ไม่อาจชี้ชัดได้ว่า จำเลยเป็นผู้โพสต์ข้อความดังกล่าว

---

[43] ศาลฎีกายกฟ้อง'นพวรรณ ตั้งอุดมสุข' โพสต์ประชาไทหมิ่นเบื้องสูง. กรุงเทพธุรกิจ. 20 ตุลาคม 2558. Available from URL: https://www.bangkokbiznews.com/news/detail/670846

อัยการโจทก์ ยื่นอุทธรณ์ ซึ่งศาลอ่านคำพิพากษาอุทธรณ์ เมื่อวันที่ 2 ต.ค. 56 เห็นว่าแม้ไม่มีประจักษ์พยาน แต่เจ้าหน้าที่รัฐ พยานโจทก์เบิกความยืนยันว่า หมายเลข IP Address ในเครื่องคอมพิวเตอร์แต่ละเครื่องไม่สามารถปลอมแปลงได้ และในการโพสต์ข้อความจำเป็นต้องใช้ชื่อและรหัสผ่านด้วย หากรหัสผ่านไม่ตรงกับข้อมูลของจำเลย ก็ไม่สามารถเข้าสู่ระบบได้ **จึงพิพากษากลับ** ให้จำคุก 5 ปี ตามประมวลกฎหมายอาญา ม.112 ซึ่งเป็นบทหนักสุด และให้ยึดเอกสารข้อความการกระทำผิด

ต่อมาจำเลย ยื่นฎีกาต่อสู้คดี โดยระหว่างฎีกา น.ส.นพวรรณ จำเลย ได้ประกันตัวไปวงเงิน 1 ล้านบาท โดยวันที่ 11 ก.ย.ที่ผ่านมา ศาลนัดอ่านคำพิพากษาศาลฎีกา แต่ น.ส.นพวรรณ จำเลยไม่เดินทางมาฟังคำพิพากษา ศาลอาญาจึงให้ออกหมายจับ และปรับนายประกัน 1 ล้านบาท

และวันที่ 20 ต.ค. 58 ทนายความ และบิดาของ น.ส.นพวรรณ ซึ่งเป็นนายประกันจำเลย เดินทางมาศาลพร้อมแถลงต่อศาลว่า ยังไม่สามารถติดตามจำเลยได้ ศาลจึงอ่านคำพิพากษาลับหลังจำเลย

ขณะที่ศาลฎีกาตรวจสำนวนประชุมปรึกษาหารือกันแล้ว ข้อเท็จจริงรับฟังได้ว่า คำเบิกความของผู้จัดการฝ่ายบริการลูกค้า ซึ่งให้บริการเชื่อมต่ออินเทอร์เน็ต พยานโจทก์ รับฟังได้ว่า ตรวจสอบข้อมูลหมายเลข IP Address ที่โพสต์ข้อความในวันที่ 15 ต.ค. 51 พบว่า เป็นรหัสของนางธนาวรรณ ตั้งอุดมสุข เชื่อมต่อกับหมายเลขโทรศัพท์ และ IP Address มีชื่อ นางธนาวรรณ ตั้งอุดมสุข เป็นลูกค้า ไม่ใช่จำเลย เนื่องจาก username เป็นคนละชื่อกับใบสมัครของจำเลย

นอกจากนี้ ยังได้ความจากเจ้าหน้าที่คณะวิทยาศาสตร์กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ว่า พยานได้ตรวจพิสูจน์เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์เก็บข้อมูลของกลาง ไม่พบการเปลี่ยนข้อความเมื่อวันที่ 15 ต.ค. 51 แต่กลับพบข้อความในคอมพิวเตอร์ของกลางมีการติดต่อกับเว็บไซต์ประชาไท ทั้งก่อนเกิดเหตุและหลังเกิดเหตุหลายครั้ง

เห็นว่าโจทก์ มีแต่ IP Address เป็นพยานแวดล้อม ซึ่งไม่อาจบ่งชี้ได้แน่ชัดว่า จำเลยมีส่วนเกี่ยวข้องกับการโพสต์ข้อความ ทั้งพยานโจทก์ ต่างเบิกความไม่สอดคล้องกัน ประกอบกับจำเลยให้การปฏิเสธตลอด พยานหลักฐานโจทก์จึงมีความสงสัยพอสมควรให้ยกประโยชน์แห่งความสงสัยให้จำเลย ฎีกาจำเลยฟังขึ้น พิพากษากลับให้ยกฟ้อง

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 16

คดีดังกล่าวนี้ จำเลยโพสต์ข้อความลงในเว็บไซต์ ในความผิดฐานหมิ่นสถาบันและความผิดเกี่ยวกับคอมพิวเตอร์ แม้คดีนี้มีการตรวจพิสูจน์พยานหลักฐานดิจิทัลจากผู้เชี่ยวชาญอย่างรัดกุมแน่น

หนา และจำเลยหนีประกัน แต่ศาลได้วางหลักไว้ว่า แม้จะทราบ หมายเลขโทรศัพท์ และ IP Address แต่มีชื่อ นางธนาวรรณ ตั้งอุดมสุข ไม่ใช่ชื่อจำเลย (อาจจะเป็นแม่ลูกหรือญาติอาศัยในบ้านหลังเดียวกัน) และนางธนาวรรณไม่ได้ถูกฟ้อง แต่ฟ้องนางสาวนพวรรณ คนละคนกัน โจทก์ไม่มีหลักฐานว่าจำเลยเป็นคนโพสต์ด้วยตนเองจริง (อาจจะเป็นผู้อื่นก็ได้) ศาลจึงยกฟ้อง

คดีนี้แม้ไม่ได้ใช้เทคโนโลยีชั้นสูงในการปิดบังตัวตนแต่ประการใด แต่กลายเป็นบรรทัดฐานแนวทางการสู้คดีอื่นๆ ของทนายความต่อไป และไม่มีคำตอบว่า จะพิสูจน์ตัวตนคนโพสต์อย่างไร ดังนั้นการไร้ตัวตน (Anonymity) มิใช่เพียงการปิดบังอำพรางซ่อนเร้นหลักฐานการระบุตัวตนว่าผู้ใดคือจำเลยหรืออาชญากรไซเบอร์ แต่การพิสูจน์ไม่ได้ว่าตัวตนจำเลยเป็นผู้ลงมือกระทำความผิดเองจนสำเร็จ ก็เป็นเหตุให้เอาผิดลงโทษไม่ได้เช่นกัน

<u>กรณีศึกษาที่</u> 17 ปรากฏการณ์ Arab Spring เปลี่ยนแปลงการปกครองในตะวันออกกลาง

เนื้อหา หรือ Content บนอินเทอร์เน็ต ได้สร้างการเปลี่ยนแปลงทางการเมืองการปกครองในโลกอาหรับที่ปิดกั้นเสรีภาพ ถูกสื่อมวลชนเรียกว่าปรากฏการณ์ “อาหรับ สปริง” (Arab Spring) แม้จะเป็นการโค่นล้มอำนาจผู้นำเผด็จการต่างๆ นำไปสู่การเปลี่ยนแปลงที่เกิดผลดี แต่บางประเทศก็ย่ำแย่กว่าเดิมอย่าง ซีเรีย ที่ยังเผชิญปัญหาความมั่นคงของชาติอย่างต่อเนื่องจากอาชญากรรมไซเบอร์

เนื้อหา หรือ Content บนอินเทอร์เน็ตที่ละเมิดกฎหมายอาญาเป็นอาชญากรรมไซเบอร์อีกประเภทหนึ่ง เมื่อถูกตราเป็นกฎหมายมีบทกำหนดโทษอาญา ผู้ขัดขืนกฎหมายอาญาก็เกิดอาชญากรรมไซเบอร์ และกลายเป็นอาชญากรไซเบอร์อีกประเภทหนึ่ง

ปรากฏการณ์ “อาหรับ สปริง” เริ่มขึ้นเมื่อปี ค.ศ. 2009[44] มีการรวมตัวแสดงความคิดเห็นของชาวอิหร่านผ่าน facebook และ twitter ไม่เห็นด้วยกับผลการเลือกตั้ง และในที่สุดประชาชนจำนวนมากก็ออกมาเดินขบวนต่อต้าน แต่แล้วรัฐบาลอิหร่านก็ใช้ความรุนแรงจนมีการบันทึกวิดีโอหญิงสาวผู้หนึ่งถูกฆาตกรรมขณะที่มาประท้วง วิดีโอนั้นเผยแพร่ทาง facebook อย่างรวดเร็วจนอิหร่านเกิดจลาจลในที่สุด

วันที่ 17 ธันวาคม 2010 ที่ประเทศ ตูนิเซีย[45] นายโมฮาเหม็ด บูอาซีซี คนขายผลไม้ วัย 26 ปี จุดไฟเผาตัวเองเพื่อประท้วงรัฐบาลบนถนนเมืองซิดีบูซิด จากนั้นประชาชนได้ส่งข้อมูลข่าวสารผ่าน

[44] Ian Black and Saeed Kamali Dehghan. Iran uprising turns bloody. The Guardian. Cited on 16 Jun 2009; Available from URL: https://www.theguardian.com/world/2009/jun/15/iran-elections-protests-mousavi-attacks

[45] Bilal Randeree. Protests continue in Tunisia. Al Jazeera. Cited on 26 Dec 2010; Available from URL: https://www.aljazeera.com/news/africa/2010/12/201012268243375190 4.html

โซเชียลมีเดียต่างๆ วิพากษ์วิจารณ์เรื่องนี้มากมาย ให้ข้อมูลด้านลบโจมตีรัฐบาลสร้างความเกลียดชังรุนแรงขึ้นเรื่อยๆ

ล่วงเข้าสู่ปี ค.ศ. 2011 เนื้อหา ความคิดเห็น วาทกรรม ตลอดจนวิธีปฏิบัติการจิตวิทยาเคลื่อนที่ผ่านสื่ออินเทอร์เน็ต facebook และ Blog นักเคลื่อนไหวต่างๆ เข้าถึงผู้คนอย่างรวดเร็ว ก่อให้เกิดการออกสู่ถนนปฏิวัติตูนิเซียนับแสนคน แต่แล้วการต่อสู่ทางการเมืองมิได้เกิดขึ้นแค่บนถนน การต่อสู้ทางไซเบอร์ก็เกิดขึ้น

เจ้าหน้าที่รัฐของตูนิเซียกระทำการจารกรรมออนไลน์ (Hack) ขโมย User name และ password ของนักข่าว นักวิจารณ์การเมืองไม่ให้สามารถ login เข้า facebook, twitter และ blog ของพวกเขาได้ อีกทั้งบรรดา เว็บไซต์ที่วิพากษ์รัฐบาลถูกปิด

กลุ่มนักเคลื่อนไหวนิรนามหรือแฮ็กเกอร์นิรนามจากต่างประเทศ (The Anonymous) โจมตีแบบ DDoS สู่ server บริษัทต่างๆ ที่ร่วมมือกับรัฐปิดกั้นเสรีภาพประชาชน[46]

ชาว ตูนิเซีย หลายคนส่ง E-mail ถึง facebook และ google ให้หาทางช่วยสื่อมวลชนเหล่านั้นเข้าถึง facebook และเว็บไซต์ของพวกเขาเหล่านั้นให้ได้ ในที่สุดระบอบอำนาจนิยมสิ้นสุดลง ประธานาธิบดี เบน อาลี ออกนอกประเทศในวันที่ 14 มกราคม 2011

เดือนต่อมาวันที่ 11 กุมภาพันธ์ 2011 ณ ประเทศอียิปต์[47] ระบอบการปกครองของประธานาธิบดี มูบารัก สิ้นสุดลงเป็นผลพวงจากความเปลี่ยนแปลงจากตูนิเซียที่แพร่หลายในสื่ออินเทอร์เน็ต

ไม่กี่วันต่อมา เมื่อถึงวันวาเลนไทน์ 14 กุมภาพันธ์ 2011 ข่าวสารการปฏิวัติระบอบการปกครองเก่าจากตูนิเซียสู่อียิปต์มาถึง เยเมน ผู้ประท้วงออนไลน์ออกสู่ถนนหลายแสนคนเรียกร้องให้ประธานาธิบดีเยเมน อะลี อับดุลลอฮ์ ศอเลียะห์ ลาออกจากตำแหน่ง มีการรายงานข่าวบนสื่ออินเทอร์เน็ตอย่างต่อเนื่องตลอดเวลา และการประท้วงก็บานปลายรุนแรงขึ้นในที่สุด

เหตุการณ์ที่ เยเมน[48] ลุกลามอย่างรวดเร็วสู่ประชาชนชาว บาห์เรน ในวันเดียวกัน 14 กุมภาพันธ์ 2011 พวกเขาเห็นว่าเป็นไปได้ที่จะเปลี่ยนแปลง จึงเริ่มออกมาประท้วง รัฐบาลใช้ความรุนแรงในการปราบปรามและปฏิบัติการจิตวิทยาให้ข่าวว่าผู้ประท้วงพยายามก่อความไม่สงบและ

---

[46] Yasmine Ryan. Tunisia's bitter cyberwar. Al Jazeera. Cited on 6 Jan 2011; Available from URL: https://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html

[47] John M. Cunningham. Egypt Uprising of 2011. Encyclopaedia Britannica. Cited on January 18 2019; Available from URL: https://www.britannica.com/event/Egypt-Uprising-of-2011

[48] Ian Black. Arrests and deaths as Egypt protest spreads across Middle East. Cited on 14 Feb 2011; Available from URL: https://www.theguardian.com/world/2011/feb/14/middle-east-iran-bahrain-yemen

พยายามใช้ความรุนแรง ประชาชนอย่าออกมาร่วมสมทบ แต่มีผู้สื่อข่าวสาวเห็นว่าไม่เป็นความจริงเธอจึงรายงานตรงไปตรงมาผ่านสื่อออนไลน์จนประชาชนออกมาสนับสนุนนับแสน

ถัดมาวันที่ 15 กุมภาพันธ์ 2011 ประชาชน ลิเบีย ได้ขยายตัวเริ่มต้นลุกฮือขึ้นทั่วประเทศเพื่อที่จะโค่นล้ม กัดดาฟี และจัดการเลือกตั้งอย่างเป็นประชาธิปไตย รัฐบาลก็ใช้ความรุนแรงปราบปรามความวุ่นวายต่อเนื่องไปนานและมีการรายงานข่าวออนไลน์ตลอดเวลา ส่วนรัฐบาลก็พยายามต่อต้านข่าว

เดือนต่อมา วันที่ 15 มีนาคม 2011 ข่าวสารใน ตูนิเซีย อียิปต์ เยเมน บาห์เรน และ ลิเบีย แพร่กระจายผ่านโลกออนไลน์อย่างรวดเร็วสู่ประชาชนชาว ซีเรีย จึงลุกขึ้นประท้วงเรียกร้องการปฏิรูปทางการเมืองในประเทศ เหตุการณ์ลุกลามบานปลายจนเป็นสงครามกลางเมืองบ้านเมืองเสียหายรุนแรงจนปัจจุบันนี้ยังไม่สิ้นสุด[49]

จากเหตุการณ์ ‘อาหรับสปริง’ เมื่อปี 2011 ประชาชนลุกฮือขึ้นปฏิวัติและโค่นล้มระบอบเผด็จการครั้งใหญ่ที่สุดในโลกอาหรับจนมาถึง ซีเรีย ซึ่งถูกปกครองด้วยรัฐบาลเผด็จการของประธานาธิบดีบาชาร์ อัล-อัสซาด (Bashar al-Assad) ที่รับช่วงการปกครองประเทศต่อจากพ่อของเขา ที่ปกครองซีเรียมานานเกือบ 30 ปี

บาชาร์ อัล-อัสซาด ลงสมัครรับเลือกตั้งประธานาธิบดี ที่เป็นไปในแนวของ “การลงประชามติ” ยึดเสียงข้างมาก บาชาร์ อัล-อัสซาดได้รับคะแนนจากประชาชนอย่างท่วมท้นกว่า 97%

Content อาหรับสปริง ทำให้เกิดอาชญากรรมแห่งความเกลียดชัง (Hate crime) ต่อประธานาธิบดี นำมาให้เกิดกระแสการละเมิดกฎหมายอาญา ประชาชนออกมาประท้วงขับไล่รัฐบาลซีเรียอย่างหนัก จนนำไปสู่การใช้กำลังทางทหารเข้าปราบปรามกลุ่มผู้ชุมนุมอย่างรุนแรง เป็นเหตุให้มีผู้เสียชีวิตจำนวนมาก แต่ท้ายที่สุดก็ไม่สามารถโค่นล้มรัฐบาลบาชาร์ อัล-อัสซาด ได้ ลุกลามกลายเป็นสงครามกลางเมือง (Civil War) ภายในประเทศ ฝ่ายต่อต้านรัฐบาลกลายเป็น กลุ่มกบฏกองกำลังปลดปล่อยซีเรีย (Free Syrian Army) ที่ได้รับการสนับสนุนโดยสหรัฐอเมริกา ซาอุดีอาระเบีย และพันธมิตรชาติอื่นๆ ประเทศอื่นๆ เริ่มเข้ามาแทรกแซง อาทิ กลุ่มไอเอส กลุ่มชาวเคิร์ด

กลุ่ม ISIS ที่ต้องการสถาปนารัฐอิสลามขึ้นในพื้นที่ของอิรักและซีเรีย แยกตัวออกมาจากกลุ่ม อัลกออิดะห์ ส่วนชาวเคิร์ด ชนกลุ่มน้อยที่มีขนาดใหญ่ที่สุดในโลก ต้องการแยกตัวออกจากซีเรียและตุรกี พร้อมปกครองตนเอง ได้รับการสนับสนุนโดยสหรัฐอเมริกา

---

[49] Erin Blakemore. What was the Arab Spring and how did it spread?. National Geographic. Cited on March 29 2019; Available from URL: https://www.nationalgeographic.com/culture/topics/reference/arab-spring-cause/

สหรัฐอเมริกา มหาอำนาจที่เข้ามาพัวพันกับสงครามซีเรีย โดยเริ่มจากการสนับสนุนรัฐบาลก่อนที่จะหันมาสนับสนุนกลุ่มกบฏ หลังเชื่อว่ารัฐบาลซีเรียอยู่เบื้องหลังการโจมตีประชาชนด้วยแก๊สพิษ รัสเซีย ที่เข้ามาในสมรภูมิซีเรียจากความพยายามปราบปรามกลุ่มก่อการร้ายและให้การสนับสนุนรัฐบาลซีเรีย

โฆษกคณะ International Committee of the Red Cross[50] (ICRC) ในซีเรียได้กล่าวว่าบรรยากาศในซีเรียนั้น ข้อมูลข่าวสารถูกทำให้ยุ่งเหยิง (information chaos) โดยมาเข้ามาร่วมของประธานาธิบดี โดนัล ทรัมป์ ด้วยกองกำลังข่าวปลอม (Fake news) เพื่อทำลายฝ่ายตรงข้ามในปี ค.ศ. 2016 ซึ่งประธานาธิบดี บาชาร์ อัล-อัสซาด (Bashar al-Assad) กล่าวว่าเราอยู่ในยุคสมัยของข่าวปลอม

รูปที่ 57 ภาพการ์ตูนล้อเลียนเหตุการณ์ Arab Spring

ที่มา https://www.slideshare.net/sauduniversity/the-arab-spring-85793494

[50] Wade, M. (2017). Cyberarmies, infowars and fake news add to Syria's suffering in The Sydney Morning Herald.Cited on March 29 2018. Available from URL: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf

ในปี ค.ศ. 2017 รายงานของ Amnesty International report[51] เรื่อง “calculated campaign of extrajudicial execution” รายงานดังกล่าวอ้างว่าตั้งแต่เหตุการณ์อาหรับสปริงปี ค.ศ. 2011 ถึง 2015 มีนักโทษที่เป็นฝ่ายตรงข้ามประธานาธิบดี บาชาร์ อัล-อัสซาดถูกแขวนคอถึง 13,000 คน

ประธานาธิบดี บาชาร์ อัล-อัสซาดกล่าวว่า รายงานการโจมตีด้วยอาวุธเคมีต่อฝ่ายตรงข้ามรัฐบาลที่มีผู้เสียชีวิต 89 คน เป็นหลักฐานที่ทำปลอมขึ้นมาทั้งหมด 100% สิ่งที่ตามมาคือสหรัฐอเมริกา มีคำสั่งปฏิบัติการทางทหารทันที ด้วยการยิงโทมาฮอว์กถล่มซีเรียถึง 59 ลูก ข่าวเกี่ยวกับการใช้อาวุธเคมีซึ่งถือว่าเป็นอาวุธทำลายล้างสูง (WMD) ของรัฐบาลซีเรีย จึงทำให้รัฐบาลสหรัฐฯ และชาติพันธมิตรอย่างอังกฤษและฝรั่งเศส ร่วมมือกันเปิดฉากโจมตีซีเรีย โดยระบุว่าเป็นเหตุจำเป็นด้านมนุษยธรรม

สงครามกลางเมืองในประเทศ ซีเรีย ถูกยกระดับกลายเป็นสงครามตัวแทน (Proxy War) ที่มีมหาอำนาจภายในภูมิภาคและมหาอำนาจโลกเข้ามาพัวพัน มีแนวโน้มที่อาจจะขยับไปเป็นความขัดแย้งระดับภูมิภาคได้ ซึ่งชนวนสำคัญนั้นเชื่อว่าเกิดจาก Fake news เป็นข้อความอันเป็นเท็จละเมิดกฎหมายอาญา ใส่ความให้ร้ายดูหมิ่นเกียดชังระหว่างกัน จนเกิดการลุกฮือมาทำลายล้างรัฐบาล

เนื้อหา (Contents) ข่าวสาร ที่วิ่งอยู่บน Facebook twitter และ YouTube ตลอดจนสื่อออนไลน์หลายอย่างที่ต้องการโค่นล้มอำนาจผู้ปกครองประเทศในขณะนั้น ส่งผลทางจิตวิทยามวลชนก่อให้เกิดการรวมตัวต่อสู้ทางการเมืองเปลี่ยนแปลงการปกครองไปยังประเทศอื่นๆ ในโลกอาหรับอีก อาทิ อิรัก อัลจีเรีย จอร์แดน คูเวต โมร็อกโก ซูดาน เลบานอน มอริเตเนีย โอมาน ซาอุดิอาระเบีย จิบูตี และเวสเทิร์นสะฮารา

[51] Amnesty International (2017). Syria: 13,000 secretly hanged in Saydnaya military prison - shocking new report. Cited on Feb 7 2017. Available from URL: https://www.amnesty.org.uk/files/human_slaughterhouse_report_0.pdf

รูปที่ 58 ผู้ชุมนุมประท้วงบางคนจากหลายประเทศ สวมหน้ากาก กาย ฟอกส์ (สัญลักษณ์ของกลุ่มแฮ็กเกอร์ The Anonymous) ในเหตุการณ์ Arab spring เข้าร่วมชุมนุม

ที่มา https://www.theatlantic.com/technology/archive/2011/12/hacks-mattered-year-hack/333755/

ในช่วงเหตุการณ์ Arab spring ได้มีการปรากฏตัวของแฮ็กเกอร์กลุ่มใหญ่ที่ใช้ชื่อว่า The Anonymous (นิรนาม) มีสัญลักษณ์คือการ สวมหน้ากาก กาย ฟอกส์ (Guy Fawkes) ซึ่งเป็นชาวคาทอลิกหัวรุนแรงในปี ค.ศ.1605 ที่พยายามลอบสังหารพระเจ้าเจมส์ที่ 1 แห่งอังกฤษ และถูกนำมาใช้เป็นสัญลักษณ์อย่างแพร่หลายในการชุมนุมประท้วงต่างๆ หลังการเผยแพร่ภาพยนตร์เรื่อง “V for Vendetta” ซึ่งมีตัวเอกเป็นนักอนาธิปไตยที่สวมหน้ากาก กาย ฟอกส์ ตลอดเวลา โดยเขาต้องการจุดชนวนการปฏิวัติด้วยการก่อการร้ายเพื่อล้มรัฐบาลเผด็จการ

กลุ่มแฮ็กเกอร์ The Anonymous สวมหน้ากาก กาย ฟอกส์ นอกจากเป็นสัญลักษณ์แล้วยังเป็นการอำพรางตัวตนปิดบังใบหน้า ในปฏิบัติการต่อต้านรัฐบาลหลายๆ ประเทศใน โดยเผยแพร่คลิปวิดีโอแถลงการณ์ว่าจะปฏิบัติการต่อต้านอย่างไร และมีอุดมการณ์อย่างไร

โดยจะปฏิบัติการต่อต้านรัฐบาลที่พยายามปิดกั้นข้อมูลข่าวสาร ภายใต้ความเชื่อว่าประชาชนทุกคนมีสิทธิเข้าถึงข้อมูลข่าวสาร และการตอบโต้รัฐบาลต่างๆ กลุ่มแฮ็กเกอร์ The Anonymous ใช้วิธีสร้าง DDoS ระดมกด F5 ซ้ำ (Refresh เว็บไซต์นั้นเพื่อสร้าง Traffic jam ไปที่ server) โดยจะประกาศวันและเวลา ให้ทุกคนที่ร่วมอุดมการณ์เข้าเว็บไซต์เป้าหมายพร้อมกัน เพื่อให้ดูเหมือนรัฐบาลถูกโจมตีทางไซเบอร์

ความสอดคล้องกับคำถามวิจัย (การไร้ตัวตน) ในกรณีศึกษาที่ 17

ในปี 2012 กลุ่มแฮ็กเกอร์ที่ใช้ชื่อว่า The Anonymous ได้รับความนิยมอย่างสูง เป็นกลุ่มกิจกรรมระหว่างประเทศมีแฮ็กเกอร์นับพันร่วมต่อต้านรัฐบาลต่างๆ ที่ปิดกั้น “เนื้อหา หรือ Content” และโจมตีระบบการสื่อสาร และเว็บไซต์ของรัฐบาล

การไร้ตัวตนจากกรณีศึกษานี้ น่าสนใจในหลายมิติทั้ง ฝ่ายรัฐบาล ฝ่ายสื่อมวลชน ฝ่ายประชาชน กลุ่มก่อการร้าย และมหาอำนาจโลกที่เข้ามาพัวพัน โดยเครื่องมือสำคัญคือ ปฏิบัติการ DDoS เว็บไซต์รัฐบาลต่างๆ และเผยแพร่ข้อมูลข่าวสารที่ถูกปิดกั้น

กลุ่มแฮ็กเกอร์ที่ใช้ชื่อว่า The Anonymous ไม่ใช่บุคคลคนเดียว หรือคนกลุ่มใดกลุ่มหนึ่ง แต่เป็นกลุ่มที่มีอุดมการณ์ตรงกันทั่วโลกในการต่อต้านรัฐบาลที่พวกเขาเห็นว่าไม่ชอบธรรม ดังนั้นจะเห็นได้ว่าในกระบวนการสืบสวนสอบสวนจึงเป็นไปได้ยาก เพราะกลุ่มแฮ็กเกอร์อยู่นอกเขตอำนาจศาลของแต่ละประเทศ (การกระทำความผิดนอกหลักดินแดน) และเป็นไปได้ยากที่จะทำการรวบรวมพยานหลักฐานดิจิทัลเพื่อออกหมายจับไปขออำนาจยังศาลต่างประเทศเพื่อขอให้รัฐบาลต่างๆ ส่งตัวผู้ร้ายข้ามแดน การตัดสินใจก่ออาชญากรรมไซเบอร์ของกลุ่มนี้เพราะมั่นใจว่าพวกเขาไร้ตัวตน จึงใช้ชื่อว่า The Anonymous

4.2 อภิปรายผลการศึกษาเชิงคุณภาพ (17 กรณีศึกษา)

จากการสังเกตปรากฏการณ์อาชญากรรมโซเบอร์ ทั้ง 17 กรณีศึกษา จนนำมาสู่การตั้งคำถามวิจัยของดุษฎีนิพนธ์นี้ ก็คือการหาความสัมพันธ์ของอาชญากรรมไซเบอร์กับการไร้ตัวตน (Anonymity) โดยวัตถุประสงค์ในดุษฎีนิพนธ์นี้ เพื่อวิเคราะห์ว่ามีความสัมพันธ์อย่างไรหากอาชญากรมีการคิดอย่างเป็นเหตุเป็นผล ไม่ใช่การหาความสัมพันธ์เชิงสาเหตุ (Causal Relationship) ในการวิจัยนี้จะใช้วิธีวิเคราะห์ โดยใช้คณิตศาสตร์ในทฤษฎีเกมมาพัฒนาแบบจำลองความคิด (Rational Choice-Decision Conceptual Model) อธิบายเป็นรูปแบบความสัมพันธ์ที่ทำให้อาชญากรตัดสินใจก่ออาชญากรรมด้วยการคิดอย่างเป็นเหตุเป็นผล อาทิ Decision tree, Payoff Matrix และ Payoff function ต่อไป

ซึ่งจากผลการศึกษาเชิงคุณภาพอาชญากรรมไซเบอร์ 17 กรณีศึกษา พบว่า อาชญากรรมไซเบอร์ เป็นอาชญากรรมที่มีความซับซ้อนทางเทคโนโลยีและอาชญากรส่วนใหญ่มีความรู้ความสามารถสูง โดยเฉพาะการรอดพ้นจากการสืบสวนจับกุมดำเนินคดี จนกลายเป็นอาชญากรสมบูรณ์แบบ (Perfect Criminals) และถึงแม้ในที่สุดแล้วถูกสืบสวนจับกุมตัวผู้ต้องสงสัยมาดำเนินคดีได้ แต่การรวบรวมพยานหลักฐานดิจิทัลเพื่อพิสูจน์ความผิดบางกรณี กลับมีช่องว่างให้หลุดคดี ไม่อาจตัดสินลงโทษอาญาได้ง่าย

จากการสังเกตอาชญากรรมไซเบอร์ 17 กรณีศึกษา ของผู้วิจัยพบว่า อาชญากรไซเบอร์ ล้วนให้ความสำคัญที่สุดกับการปิดบังอำพรางตน การปิดบังชื่อจริงใช้ชื่อปลอมหรือนิรนาม (Anonymous name) การปิดบัง IP Address การปิดบังแม้แต่ที่อยู่ เป็นต้น เมื่อเชื่อมั่นว่าเป้าหมายหรือเหยื่อมองไม่เห็นหรือไม่รู้ตัวตนที่แท้จริงจะลงมือก่ออาชญากรรมทันทีหรือถ้าหากการตัวตนหมดไป (สามารถจับกุมดำเนินคดีได้) อาชญากรรมไซเบอร์ประเภทนั้นจะหยุดหรือไม่ ได้ผลการศึกษาเชิงคุณภาพดังนี้

กรณีศึกษาที่	การไร้ตัวตน (Anonymity)	การพิสูจน์ตัวตนได้ (Identified)
1. **เควิน มิตนิค (Kevin Mitnick)** อดีตแฮ็กเกอร์มือหนึ่งของสหรัฐอเมริกา	เข้าถึงข้อมูลบัตรเครดิตมหาศาล แต่ไม่ได้นำมาใช้ ทำไปเพราะความท้าทาย มั่นใจว่ามีความสามารถเข้าสู่ระบบคอมพิวเตอร์อย่างไร้ตัวตน จึงตัดสินใจก่ออาชญากรรมไซเบอร์	ถูกจับกุมดำเนินคดีและถูกตัดสินลงโทษทำให้ตัดสินใจเลิกก่ออาชญากรรมไซเบอร์
2. มาร์คัส ฮัตชินส์ (Marcus Hutchins) ฮีโร่ สู่อาชญากรไซเบอร์	การควบคุมข้อจำกัดการใช้ระบบคอมพิวเตอร์ของโรงเรียน และผู้ปกครอง ท้าทายการพัฒนาจนมั่นใจว่ามีความสามารถเข้าสู่ระบบคอมพิวเตอร์อย่างไร้ตัวตน จึงตัดสินใจก่ออาชญากรรมไซเบอร์ และการสร้างมัลแวร์สำหรับแฮ็กเกอร์เพื่อขาย วิน	มาร์คัส ฮัตชินส์ ถูกจับกุมดำเนินคดี วินนี่ ไม่มีใครพิสูจน์ตัวตนได้ จึงรอดพ้นกระบวนการยุติธรรม

	นี่ เลือกที่จะปิดบังอำพรางอย่างไร้ตัวตน แต่มาร์ คัส เป็นคนดังมีตัวตน และเป็นที่รับรู้ว่าเขาสร้างมัลแวร์หลายตัว	
3. เอเดรียน ลาโม่ (Adrian Lamo) แฮ็กเกอร์ไร้บ้าน	มั่นใจว่ามีความสามารถเข้าสู่ระบบคอมพิวเตอร์อย่างไร้ตัวตน จึงตัดสินใจก่ออาชญากรรมไซเบอร์ และมาเปิดเผยบอกองค์ต่างๆ ภายหลังถึงช่องโหว่ เป็นเหตุให้ถูกดำเนินคดี การไร้ตัวตนจึงเป็นความสำคัญสูงสุดของเขา ตั้งแต่ไม่มีที่อยู่เป็นหลักแหล่ง ย้ายที่นอนทุกสองคืน ใช้อินเทอร์เน็ตสาธารณะ และเมื่อถูกเปิดเผยตัวตน โดย วิกิลีคส์ เขาจึงเปิดเผยตัวตน เชลซี แมนนิ่ง กลับทำให้ถูกจับกุมดำเนินคดี	หลังถูกดำเนินคดี แม้เขายุติการก่ออาชญากรรม แต่ถูกประณามจากกลุ่มแฮ็กเกอร์ และถูกคุมความต้องหลบหนีปิดบังอำพรางตังตนจนเครียด และเสพยาเสียชีวิต ทันทีที่เปิดเผยตัวตน เชลซี แมนนิ่ง เป็นแฮ็กเกอร์ ที่ขโมยข้อมูลจากกองทัพ การตัดสินใจก่ออาชญากรรมไซเบอร์ของเขาก็ยุติลง
4. โจนาธาน เจมส์ (Jonathan James) เยาวชนคนแรกที่เป็นอาชญากรไซเบอร์	การบุกรุกระบบคอมพิวเตอร์เพนตากอน และ นาซ่า จากการสืบสวนทางเอกสารไม่พบว่าเป็นส่วนสำคัญในการตัดสินใจก่ออาชญากรรมไซเบอร์ แต่ทางการคงมีหลักฐานระบุตัวตนเพียงพอ	จะถูกเปิดเผยตัวตน จึงตัดสินใจปลิดชีวิตตนเอง

	จึงสามารถดำเนินคดีจนตัดสินลงโทษได้ แต่ในกาลต่อมา เพียงทราบว่าถูกเจ้าหน้าที่ต้องสงสัยว่ามีส่วนร่วมการขโมยข้อมูลบัตรเครดิตครั้งใหญ่ ก็ด่วนตัดสินใจฆ่าตัวตายก่อนถูกจับกุม ทำให้ตั้งข้อสังเกตว่าการไร้ตัวตนมีส่วนสำคัญต่อการติดสินใจของเขา	
5. นายทวีทรัพย์ ลลิตศศิวิมล สื่อขนานนามแฮ็กเกอร์มือหนึ่งของไทย	มั่นใจว่ามีความสามารถเข้าสู่ระบบคอมพิวเตอร์อย่างไร้ตัวตน จึงตัดสินใจก่ออาชญากรรมไซเบอร์	ถูกจับกุมดำเนินคดีและถูกตัดสินลงโทษ ยุติการก่ออาชญากรรม
6. มอส นามสมมุติ แฮ็กเกอร์คุณธรรม	การควบคุมข้อจำกัดการใช้ระบบคอมพิวเตอร์ของโรงเรียน และผู้ปกครอง ท้าทายการพัฒนาจนมั่นใจว่ามีความสามารถเข้าสู่ระบบคอมพิวเตอร์อย่างไร้ตัวตน จึงตัดสินใจก่ออาชญากรรมไซเบอร์	ยุติการก่ออาชญากรรม
7. อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ แบบ แก๊งค์คอลเซ็นเตอร์	การฉ้อโกง อย่างไร้ตัวตน ทำให้กลุ่มอาชญากร ตัดสินใจก่ออาชญากรรมไซเบอร์จำนวนมาก	ยุติการก่ออาชญากรรม
8. อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ แบบ Romance scam	การฉ้อโกง อย่างไร้ตัวตน ทำให้กลุ่มอาชญากร ตัดสินใจ	ยุติการก่ออาชญากรรม แต่บาง

	ก่ออาชญากรรมไซเบอร์จำนวนมาก	กรณีที่ยังพิสูจน์ตัวตนไม่ได้อาชญากรรมประเภทนี้ยังมีอยู่
9. การจ้างสังหารออนไลน์ผ่าน TOR และจ่ายค่าจ้างด้วย Crypto currency	บริการจ้างสังหาร อย่างไร้ตัวตน ทำให้ผู้จ้างวาน และกลุ่มอาชญากร ตัดสินใจก่ออาชญากรรมไซเบอร์และกำลังเติบโตสูง	ไม่เคยจับกุมได้
10. เว็บไซต์ค้ายาเสพติดใน TOR Network และชำระเงินด้วย Crypto currency	บริการซื้อขายยาเสพติดอย่างไร้ตัวตน ทำให้กลุ่มอาชญากร ตัดสินใจก่ออาชญากรรมไซเบอร์และกำลังเติบโตสูง	ไม่เคยจับกุมได้ทางเทคโนโลยี แต่ผู้ที่เคยถูกจับเป็นเพราะสับเพร่าเอง
11. การแฮ็กเรดาร์ตรวจจับเครื่องบินรบของกองทัพซีเรียก่อนถูกถล่มอย่างไร้ตัวตน	ความสามารถยึดระบบคอมพิวเตอร์ตรวจจับเรดาร์และบินเข้ามาทิ้งระเบิดอย่างไร้ตัวตน ทำให้ผู้ก่อการร้ายตัดสินใจก่ออาชญากรรม	ไม่เคยจับกุมได้
12. โจมตีรัฐบาลด้วย DDoS ครั้งใหญ่ที่สุดในประวัติศาสตร์โลก	ความสามารถขัดขวางระบบคอมพิวเตอร์ของรัฐบาลอย่างไร้ตัวตน ทำให้ผู้ก่อการร้ายตัดสินใจก่ออาชญากรรม	ไม่เคยจับกุมได้
13. กลุ่มก่อการร้าย ISIS ระดมทุนถล่มกรุงปารีสด้วย Bitcoin	ความสามารถในการให้ทุนทางไซเบอร์อย่างไร้ตัวตน ทำให้ผู้ก่อการร้ายตัดสินใจก่ออาชญากรรม	ไม่เคยจับกุมได้
14. นายสุรภักดิ์ ภูไชยแสง (พิสูจน์ตัวตนว่าเป็นผู้กระทำความผิดไม่ได้จากการใช้ E-mail)	ความสามารถในการหมิ่นประมาทอย่างไร้ตัวตน ทำให้อาชญากรอื่นหรือทนาย	ยกฟ้อง

	จำเลยนำไปศึกษาประกอบการตัดสินใจก่ออาชญากรรม	
15. นายสงคราม ฉิมเฉิด (พิสูจน์ตัวตนว่าเป็นผู้กระทำความผิดไม่ได้จากการใช้ E-mail)	ความสามารถในการหมิ่นประมาทอย่างไร้ตัวตน ทำให้อาชญากรอื่นหรือทนายจำเลยนำไปศึกษาประกอบการตัดสินใจก่ออาชญากรรม	ยกฟ้อง
16. นางสาวนพวรรณ ตั้งอุดมสุข (พิสูจน์ตัวตนว่าเป็นผู้กระทำความผิดไม่ได้ เพราะ IP Address เป็นชื่อแม่)	ความสามารถในการหมิ่นประมาทอย่างไร้ตัวตน ทำให้อาชญากรอื่นหรือทนายจำเลยนำไปศึกษาประกอบการตัดสินใจก่ออาชญากรรม	ยกฟ้อง
17. ปรากฏการณ์ Arab Spring เปลี่ยนแปลงการปกครองในตะวันออกกลาง	ความสามารถขัดขวางระบบคอมพิวเตอร์ของรัฐบาลอย่างไร้ตัวตน ทำให้ผู้ก่อการร้ายตัดสินใจก่ออาชญากรรม และความเชื่อมั่นการไร้ตัวตนว่าจะรอดพ้นจากการสืบสวนจับกุมแสดงออกในชื่อกลุ่มแฮ็กเกอร์ The Anonymous	ไม่เคยจับกุมได้

ตารางที่ 9 ผลการศึกษาเชิงคุณภาพ กรณีศึกษากับผลของการไร้ตัวตน และการพิสูจน์ตัวตน

จากการศึกษาทั้ง 17 กรณีศึกษา จะเห็นผลการศึกษาเชิงคุณภาพว่า “การไร้ตัวตน” มีผลอย่างสูงต่อการตัดสินใจของอาชญากรต่อการก่ออาชญากรรมไซเบอร์ จึงใช้ทฤษฎีการเลือกอย่างเป็น

เหตุเป็นผล (Rational Choice Theory) ซึ่งเป็นทฤษฎีสำคัญทางอาชญาวิทยา และสังคมศาสตร์มาตั้งต้นค้นหาจุดเริ่มต้นของการตัดสินใจประกอบอาชญากรรมไซเบอร์

ซึ่งก็คือ “การเลือกอย่างเป็นเหตุเป็นผลของอาชญากร” ของอาชญากรที่ต้องการจะได้อรรถประโยชน์หรือความพึงพอใจนั้น ต้องพิจารณาความสามารถในการไร้ตัวตนก่อนลงมือก่ออาชญากรรมไซเบอร์เป็นประเด็นสำคัญที่สุด

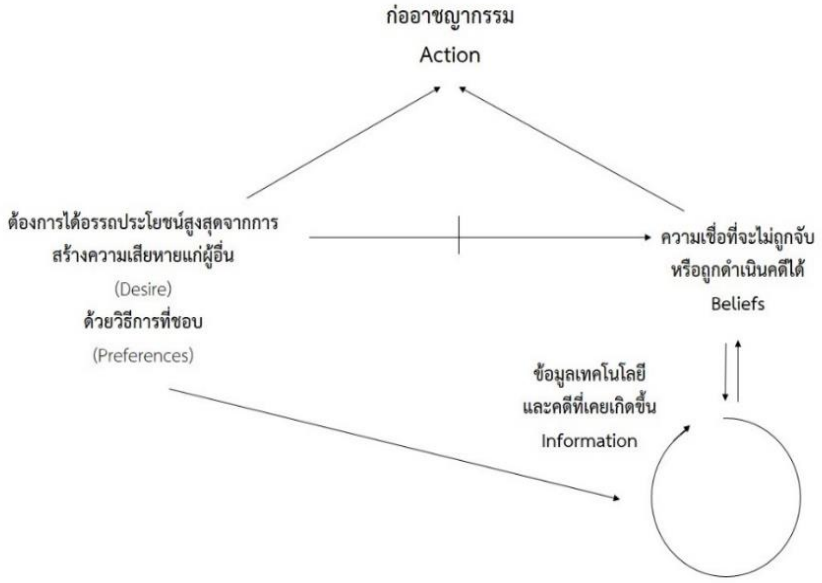
4.2.1 วิเคราะห์การเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

อาชญากรไซเบอร์ทุกประเภทที่ได้ศึกษารวบรวมจากทุกกรณีศึกษาในบทที่ 3 ของดุษฎีนิพนธ์นี้ ผู้วิจัยพบว่า “**อาชญากรไซเบอร์เป็นผู้ตัดสินใจเลือกอย่างเป็นเหตุเป็นผล**”

ความเป็นเหตุเป็นผล (Rationale) ในดุษฎีนิพนธ์นี้คือ “ความเห็นแก่ตัวที่จะเอาประโยชน์จากความเสียหายของผู้อื่นตลอดเวลาเมื่อพบโอกาส” อาชญากรจะคิดตลอดเวลาว่ามีโอกาสในการหาประโยชน์จากเหยื่อเมื่อใดจะลงมือก่ออาชญากรรมทันที แต่อาชญากรไซเบอร์จะคิดอย่างเป็นเหตุเป็นผลตลอดเวลาเมื่อพบโอกาสที่คิดว่าจะไม่มีใครจะจับได้หรือจับได้ก็เอาผิดไม่ได้ จะตัดสินใจลงมือก่ออาชญากรรมหาประโยชน์จากเหยื่อทันที

อาชญากรไซเบอร์ในดุษฎีนิพนธ์นี้ ไม่รวมถึงอาชญากรประเภทวิกลจริตและอาชญากรโดยกำเนิด ที่มีพฤติกรรมความรุนแรงขาดการใช้เหตุผล จากการศึกษาเชิงประจักษ์ผู้วิจัยไม่พบอาชญากรประเภทดังกล่าวในอาชญากรรมไซเบอร์ เพราะเนื่องด้วยอาชญากรไซเบอร์ส่วนใหญ่มีความรู้ความสามารถสูง (Perfect criminal) มีความสามารถในการใช้เทคโนโลยีให้รอดพ้นจากการถูกจับกุม โดยส่วนใหญ่จึงมีลักษณะเป็น อาชญากรตามโอกาส (Occasional criminals) และ อาชญากรติดนิสัย (Habitual criminals) อีกทั้งมีรูปแบบการคิดของอาชญากรหลักๆ 2 กรณี คือ คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation) หรือคิดได้ใจจนเกินจริง (Super-optimism) ว่าเขาสามารถที่จะหลีกพ้นโทษจากการกระทำความผิดของตนเองได้อย่างแน่นอนหรือมั่นใจว่าตนไม่มีทางถูกจับได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ

จากแบบแผนจำลองอธิบายการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ ผู้วิจัยได้วิเคราะห์เงื่อนไขที่น่าพอใจที่สุด (Optimality conditions) ทั้ง 3 ประการ มาเป็นกรอบเบื้องต้นในการทำความเข้าใจการคิดอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์ ได้ดังรูปที่ 59 นี้



รูปที่ 59 แบบแผนจำลองการเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

วิเคราะห์กระบวนการคิดตัดสินใจเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

1. ความปรารถนา (Desire)

จากการศึกษาข้อมูลจำนวนมากทั้งกรณีศึกษาและคดีต่างๆ ในบทที่ 3 พบว่า อาชญากรไซเบอร์เป็น อาชญากรตามโอกาส และ อาชญากรติดนิสัย มีความปรารถนาที่จะสร้างความเสียหายกับผู้อื่นเพื่อสร้างอรรถประโยชน์แก่ตนตลอดเวลา โดยความปรารถนาหรือความชอบนี้ปฏิบัติการในฐานะที่เป็น “ตัวขับเคลื่อนคงที่ของทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล” ให้คอยมองหาโอกาสอยู่เสมอ การตีความในข้อนี้ย่อมเป็นอื่นไม่ได้แน่นอน

2. การกระทำ ((FATF))

จากการศึกษาข้อมูลทั้งกรณีศึกษาและคดีต่างๆ ในบทที่ 3 พบว่า อาชญากรไซเบอร์จะลงมือก่ออาชญากรรมโดยเลือกหนทางที่ดีที่สุดที่จะทำให้บรรลุในสิ่งที่ปรารถนา ทั้งนี้ขึ้นอยู่กับความเชื่อ (Belief) ในข้อมูลข่าวสารที่อาชญากรนั้นมีอยู่ครบถ้วน จะลงมือก่ออาชญากรรมไซเบอร์ทันที

3. ความเชื่อ (Belief)

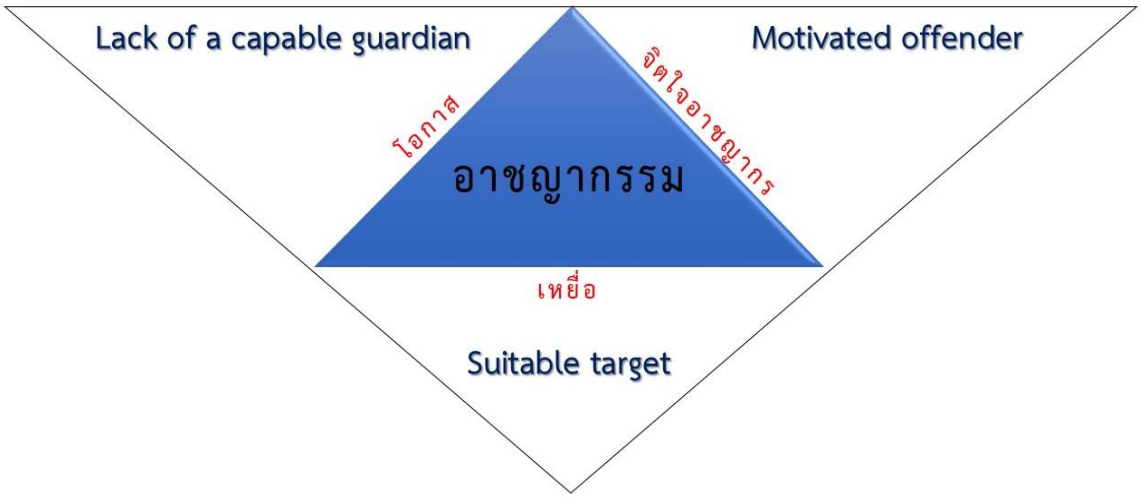
จากการศึกษาข้อมูลทั้งกรณีศึกษาและคดีต่างๆ ในบทที่ 3 พบว่า เมื่อข้อมูล (Information) ที่อาชญากรไซเบอร์ได้รับเกี่ยวกับเทคโนโลยีนั้นๆ เหมาะสมที่สุดในการก่ออาชญากรรมและพวกเขา

เชื่อว่าจะไม่ถูกจับ และไม่ถูกดำเนินคดี ซึ่งสอดคล้องกับรูปแบบการคิดของอาชญากร 2 กรณี คือ คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation) หรือคิดได้ใจจนเกินจริง (Super-optimism) ว่าเขาสามารถที่จะหลีกพ้นโทษจากการกระทำความผิดของตนเองได้อย่างแน่นอนหรือมั่นใจว่าตนไม่มีทางถูกจับได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ

วิเคราะห์การเลือกอย่างเป็นเหตุเป็นผลในอาชญากรรมไซเบอร์ด้วยทฤษฎี Routine Activities Theory

จากการทบทวนวรรณกรรมในบทที่ 2 ข้อที่ 2.4 ทฤษฎี Routine Activities Theory สามารถนำมาอภิปรายผลการเลือกอย่างเป็นเหตุเป็นผลการตัดสินใจของอาชญากรไซเบอร์

อาชญากรรมไซเบอร์เกิดขึ้นเมื่อสถานการณ์ที่หลอมรวมกันพอดีของ อาชญากร เหยื่อ พื้นที่และเวลา เมื่อเหยื่อมีพฤติกรรมที่เป็นกิจวัตรที่หละหลวมต่อการระมัดระวังป้องกัน จูงใจให้อาชญากรตัดสินใจก่ออาชญากรรมเพื่อหาประโยชน์หรือความพึงพอใจจากการสูญเสียของเหยื่อ โดยมีองค์ประกอบ 3 ประการที่เป็นเหตุทำให้เกิดอาชญากรรมสามารถอภิปรายได้ดังนี้



รูปที่ 60 วิเคราะห์อาชญากรรมไซเบอร์ด้วยทฤษฎี Routine Activities Theory

1. แรงจูงใจอาชญากร (Likely/Motivated offender)

อาชญากรมีความปรารถนาหรือความพึงพอใจที่จะหาอรรถประโยชน์จากเหยื่อตลอดเวลา อาชญากรติดตามศึกษามองหาโอกาสจากเหยื่อในการดำเนินกิจวัตร เช่น เห็นกิจวัตรประจำวันของ

เหยื่อผ่านโซเชียลมีเดีย การเดินทางไปสถานที่ใดเป็นประจำ ภาพถ่ายเหยื่อหรือสิ่งแวดล้อม เวลาที่ดำเนินเป็นกิจวัตร หรือช่องว่างของเว็บไซต์หรือระบบคอมพิวเตอร์ขององค์กร ที่อาชญากรเห็นโอกาสที่จะบุกรุกเข้าไปได้หรือลักษณะพฤติกรรมของผู้ดูแลเครือข่ายที่มีความหละหลวมในการป้องกัน ล้วนส่งผลจูงใจให้อาชญากรเลือกอย่างเป็นเหตุเป็นผลในการก่ออาชญากรรมไซเบอร์

2. มีเป้าหมายที่เหมาะ (Suitable target)

เมื่ออาชญากรไซเบอร์มีการคิดเลือกอย่างเป็นเหตุเป็นผลในการก่ออาชญากรรมไซเบอร์ อาชญากรจะมองหาเหยื่อเป้าหมายที่มีความเหมาะสมกับความสามารถของอาชญากรในการก่ออาชญากรรม เหยื่อต้องมีลักษณะไม่รู้เท่าทันภัยไซเบอร์ เหยื่ออาจจะมีบุคลิกไม่รอบคอบ สับเพร่า ไม่ระมัดระวังตัวในการป้องกันความปลอดภัย และเหยื่อมีประโยชน์ที่อาชญากรปรารถนา โดยเหยื่อเป้าหมายที่เหมาะสมนั้นยังรวมถึงการที่เหยื่อจะไม่สามารถล่วงรู้ว่าผู้ใดคืออาชญากรสร้างความเสียหายและอาชญากรล่องหนหายตัวไปอย่างไร้ตัวตนบนช่องว่างของเหยื่อ

3. ขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian)

เหยื่อมีความอ่อนแอเป็นปกติทั่วไปหรือเหยื่ออาชญากรรมไซเบอร์ ประชาชนทั่วไปเป็นผู้ใช้บริการ (User) ไม่ได้มีความรู้ระดับสูงด้านเทคโนโลยี ไม่สามารถปกป้องดูแลตนได้เอง จำเป็นต้องมีผู้พิทักษ์คอยสอดส่องดูแลความสงบเรียบร้อยและปลอดภัยในโลกออนไลน์ เช่น ผู้ให้บริการอินเทอร์เน็ตหรือผู้ดูแลความมั่นคงปลอดภัยไซเบอร์ ตำรวจ ผู้ปกครองเด็ก หน่วยงานภาครัฐ โอกาสในการเกิดอาชญากรรมจะเกิดขึ้นเมื่อขาดผู้พิทักษ์ไม่มีความสามารถเพียงพอในการป้องกันอาชญากรรมไซเบอร์ อาชญากรจะตัดสินใจเลือกอย่างเป็นเหตุเป็นผลในการก่ออาชญากรรมทันที

การตีความ (Interpretation)

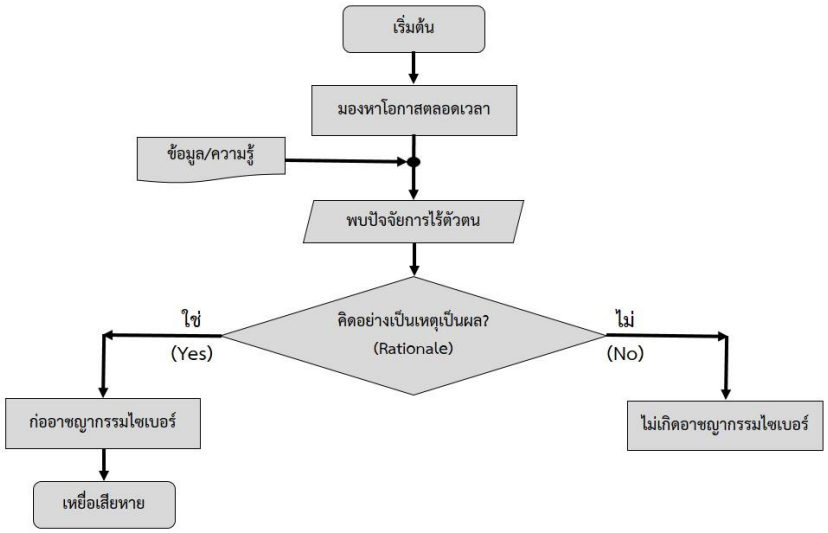
ดุษฎีนิพนธ์นี้มุ่งหาความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับการไร้ตัวตน (Anonymity) จากกระบวนความคิดอย่างเป็นเหตุและเป็นผลต่อการตัดสินใจของอาชญากรไซเบอร์ บนข้อมูลเทคโนโลยีไซเบอร์ที่อาชญากรมีเกี่ยวกับการหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล และการรวบรวมพยานหลักฐานดิจิทัลเพื่อให้รอดพ้นการถูกดำเนินคดี และเหยื่อเป็นเป้าหมายที่มีความเหมาะสมต่อความสามารถของอาชญากรที่จะก่ออาชญากรรมไซเบอร์หาประโยชน์จากเหยื่อและเชื่อมั่นว่าจะไม่ถูกจับได้ อีกทั้งยังขาดผู้พิทักษ์ที่มีความสามารถในการป้องกันอาชญากรรมไซเบอร์

ดังนั้น หัวใจสำคัญของการตัดสินใจอย่างเป็นเหตุเป็นผล (Rationale) ก่อนลงมือประกอบอาชญากรรมไซเบอร์ ก็คือ ปัจจัยการไร้ตัวตน (Anonymous factors) ที่อาชญากรเลือกใช้ตัดสินใจประกอบอาชญากรรม โดยสามารถค้นหาปัจจัยการไร้ตัวตนของเทคโนโลยีไซเบอร์ในการก่ออาชญากรรมได้ดังนี้

4.2.2 การใช้ทฤษฎีเกมวิเคราะห์ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์

สมมติฐานทางวิจัย (Research hypothesis) ในดุษฎีนิพนธ์นี้คือ

“การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน”



รูปที่ 61 กระบวนการคิดตัดสินใจเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

จากรูปที่ 61 กระบวนการคิดตัดสินใจเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์ตามสมมติฐานการวิจัย คือ อาชญากรไซเบอร์เป็นคนเห็นแก่ตัวมองหาโอกาสจากเหยื่อตลอดเวลา บนข้อมูลเทคโนโลยีเดิมที่ตนมีอยู่และค้นคว้าหาความรู้เทคโนโลยีใหม่ตลอดเวลา เมื่อพบปัจจัยการไร้ตัวตน (ตามนิยามในดุษฎีนิพนธ์นี้) และอาชญากรมีการคิดอย่างเป็นเหตุเป็นผล (Rationale) จะตัดสินใจลงมือก่ออาชญากรรมไซเบอร์ทันที

โดยที่ปัจจัยการไร้ตัวตน (Anonymous Factor) เป็นสิ่งสำคัญที่จูงใจให้อาชญากรตัดสินใจเลือกประกอบอาชญากรรมไซเบอร์เมื่อผู้พิทักษ์ก็ไม่มีความสามารถ และเหยื่อคือเป้าหมายที่เหมาะสม ดังนั้น “การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน” ตามสมมติฐานการวิจัยในดุษฎีนิพนธ์นี้ จึงใช้ทฤษฎีเกมเป็นเครื่องมือสำคัญในการวิจัยให้เห็นรูปแบบความสัมพันธ์ระหว่างการไร้ตัวตนและอาชญากรรมไซเบอร์ได้ผลดังต่อไปนี้

ทฤษฎีเกม (Prisner, 2014) มีหลักการทั่วไปดังนี้

Perfect Information: ผู้เล่นมีข้อมูลครบถ้วนสมบูรณ์ เข้าใจ กติกา รางวัล และรู้กลยุทธ์ฝั่งตรงข้าม

Rationale: ผู้เล่นทุกฝ่ายใช้ข้อมูลที่ตนมีตัดสินใจเลือกกลยุทธ์ที่ดีที่สุด อย่างเป็นเหตุและเป็นผล

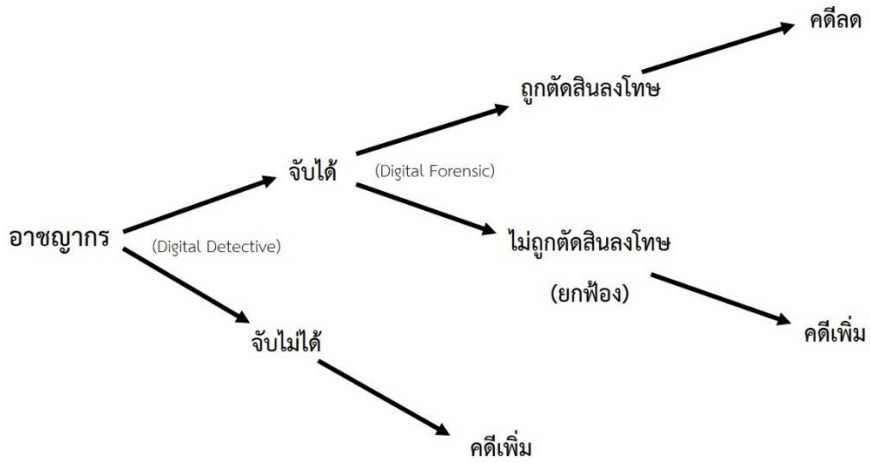
4.2.2.1 *การหา* Decision Tree

เทคนิค Decision Tree ของทฤษฎีเกมเป็นการทำความเข้าใจอย่างง่ายต่อสถานการณ์แวดล้อมที่จะเกิดอาชญากรรมไซเบอร์ขึ้นในสังคม โดยวิเคราะห์ทางเลือกของผู้เล่นเกมหรืออาชญากรในการตัดสินใจมีกี่ทางเลือกเทคโนโลยีไซเบอร์ใดในการก่ออาชญากรรม และผู้ที่ทำหน้าที่ปกป้อง (Defender) ไม่ว่าทั้งตัวเหยื่อหรือตำรวจจะดำเนินการเป็นไปในทิศทางใด ในดุษฎีนิพนธ์นี้ยกตำรวจเป็นผู้ที่ทำหน้าที่ปกป้องเพื่อความเข้าใจง่าย

จากการสังเกตปรากฏการณ์การเกิดอาชญากรรมไซเบอร์ในทุกประเภท ผู้วิจัยได้พบว่า หากอาชญากรรมไซเบอร์ประเภทใด อาชญากรรอดพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) จะทำให้อาชญากรรมไซเบอร์ประเภทนั้นเพิ่มสูงขึ้นอย่างรวดเร็ว หรือแม้สืบสวนจับกุมได้ แต่ไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีหรือการพิสูจน์ตัวตนเอาผิดทางอาญาได้ว่า ผู้ต้องสงสัยเป็นผู้ประกอบอาชญากรรม อาชญากรรมไซเบอร์ประเภทนั้นจะยังคงเพิ่มขึ้นอย่างรวดเร็ว

ในทางตรงกันข้าม หากอาชญากรรมไซเบอร์ประเภทใด สามารถสืบสวนทางดิจิทัล (Digital Detective) จนจับกุมตัวอาชญากรได้ จะทำให้อาชญากรรมไซเบอร์ประเภทนั้นลดลงอย่างรวดเร็ว และเมื่อสืบสวนจับกุมได้ แล้วสามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีหรือการพิสูจน์ตัวตนว่าผู้ต้องสงสัยเป็นผู้ประกอบอาชญากรรม จนเอาผิดทางอาญาได้

อาชญากรรมไซเบอร์ประเภทนั้นจะลดต่ำลงอย่างรวดเร็วจนหมดสิ้นไป โดยเขียน Decision Tree ของทฤษฎีเกมอาชญากรรมไซเบอร์ ดังรูปที่ 62 นี้



รูปที่ 62 Decision Tree ของทฤษฎีเกมในอาชญากรรมไซเบอร์

4.2.2.2 *การหา* Payoff Matrix

อาชญากรมีการตัดสินใจอย่างเป็นเหตุเป็นผล (Rationale) บนข้อมูลที่ตนได้รับทราบอย่างสมบูรณ์ว่า ไซเบอร์เทคโนโลยีใดจะไม่สามารถสืบสวนทางดิจิทัล (Digital Detective) จนจับกุมอาชญากรได้ อาชญากรจะลงมือก่ออาชญากรรมทันทีเพื่อให้ตนได้รับอรรถประโยชน์สูงสุด หรือแม้ถูกสืบสวนจับกุมได้ แต่ไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เอาผิดทางอาญาได้ อาชญากรก็ยังคงชั่งน้ำหนักเหตุและผลจนลงมือก่ออาชญากรรม เมื่อพบว่าอรรถประโยชน์ที่ได้รับคุ้มค่ากับความเสี่ยง

โดยให้

c คือ จำนวนคดีอาชญากรรมไซเบอร์ประเภทใด

d คือ จำนวนคดีที่สืบสวนจนจับกุมอาชญากรได้

s คือ จำนวนคดีที่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เอาผิดทางอาญาได้

สามารถหา Payoff Matrix ของทฤษฎีเกมได้ดังนี้

ตำรวจ

อาชญากร	กลยุทธ์ P1	กลยุทธ์ P2	กลยุทธ์ P3
กลยุทธ์ Q	$\frac{d}{c} = 0$	$\frac{d}{c} = 1$	$\frac{d}{c} = 1$
กลยุทธ์ 1-Q	$\frac{s}{d} = 0$	$\frac{s}{d} = 0$	$\frac{s}{d} = 1$

ตารางที่ 10 การหาค่าตาราง Payoff Matrix ของทฤษฎีเกมอาชญากรรมไซเบอร์

อธิบายเกม

ทฤษฎีเกมอาชญากรรมไซเบอร์เป็น Zero-sum game เป็นเกมที่ไม่มีจุดที่สมประโยชน์สองฝ่ายร่วมกัน แต่เป็นเกมที่อาชญากรได้ประโยชน์เท่าที่เหยื่อเสียประโยชน์ไปและการปกป้องประโยชน์ของเหยื่อเป็นหน้าที่ของตำรวจที่จะต้องหาหนทางปกป้องแก้ไขตลอดเวลา

ทฤษฎีเกมอาชญากรรมไซเบอร์เป็นกลยุทธ์ผสม (Mixed Strategies) เป็นกลยุทธ์ที่ใช้ในการเล่นเกมระหว่างสองฝ่าย โดยผู้เล่นแต่ละฝ่ายไม่ได้เล่นกลยุทธ์ใดกลยุทธ์หนึ่งเพียงวิธีเดียว แต่จะเล่นหลายวิธีผสมกัน โดยอาชญากรเป็นเจ้าของตารางจะมองหาโอกาสอยู่เสมอ และตำรวจจะคอยหากลยุทธ์ใหม่ปิดโอกาสการเกิดอาชญากรรมนั้นอยู่เสมอ

อาชญากรจะชั่งน้ำหนักความเป็นเหตุ (Cause) และความเป็นผล (Effect) อยู่ตลอดเวลาในการใช้ 2 กลยุทธ์พร้อมกัน ทั้งกลยุทธ์ Q และกลยุทธ์ 1 - Q เพื่อให้รอดพ้นการจับกุม และรอดพ้นจากการถูกดำเนินคดี ทั้ง 2 กลยุทธ์รวมกันมีค่าเท่ากับ 1 หรือ 100% (เนื่องจาก Q + (1 - Q) = 1) เป็นองค์ประกอบ ค่าของเกมอธิบายจากตาราง Payoff Matrix ได้ดังนี้

อาชญากรกับกลยุทธ์ Q

กลยุทธ์ Q คือ การไม่สามารถสืบสวนทางดิจิทัล (Digital Detective) เพื่อจับกุมอาชญากรได้ สัดส่วนของจำนวนคดีที่เกิดขึ้น (c) กับการสืบสวนจับกุมได้ (d) มีค่าเป็น 0 อาชญากรรมประเภทนั้นจะสูงขึ้นมากเมื่อ

$$\frac{d}{c} = 0$$

อาชญากรจะเลือกใช้ กลยุทธ์ Q ไปตลอด ตราบเท่าตำรวจเปลี่ยนจากกลยุทธ์ P1 เป็นกลยุทธ์ P2 หรือหาทางสืบสวนจับกุมตัวอาชญากรได้ ซึ่งหากตำรวจสามารถจับกุมตัวอาชญากรได้ทั้งหมดทุกคดีที่เกิดขึ้น สัดส่วนของจำนวนคดีที่เกิดขึ้น (c) กับการสืบสวนจับกุมได้ (d) มีค่าเป็น 1 หมายถึง คดีเกิดขึ้นเท่าใด ก็สามารถจับกุมได้เท่านั้น การไร้ตัวตนจากอาชญากรรมไซเบอร์ประเภทนั้นจะลดลงเมื่อ

$$\frac{d}{c} = 1$$

อาชญากรกับกลยุทธ์ 1 - Q

กลยุทธ์ 1 - Q คือ การไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีเอาผิดทางอาญาได้ แม้จะถูกจับกุมได้ แต่ถ้าหากอาชญากรชั่งน้ำหนักอย่างมีเหตุ และมีผล (Rationale) ว่าเทคโนโลยีไซเบอร์ประเภทใดยังคงให้อรรถประโยชน์แก่ตนมากกว่าโทษที่ได้รับ แม้จะถูกจับกุมได้ อาชญากรย่อมลงมือประกอบอาชญากรรม

สัดส่วนจำนวนคดีที่ตัดสินลงโทษได้ (s) ต่อจำนวนคดีที่จับกุมได้ (d) มีค่าเท่ากับ 0 อาชญากรจะยังคงใช้กลยุทธ์ 1-Q ไปตลอด คู่กับกลยุทธ์ Q อาชญากรรมประเภทนั้นจะยังคงเกิดขึ้น

$$\frac{s}{d} = 0$$

แต่ถ้าหากเมื่อตำรวจปรับเปลี่ยนกลยุทธ์จากกลยุทธ์ P1 เป็นกลยุทธ์ P2 จนพบกลยุทธ์ P3 เมื่อใด ทำให้สัดส่วนการตัดสินคดีลงโทษอาญาอาชญากรได้ทุกราย (s) ต่อจำนวนคดีที่จับกุมได้ (d) มีค่าเท่ากับ 1 หมายถึงทุกคดีที่จับกุมตัวอาชญากรที่เกิดขึ้นได้เท่าใด ก็สามารถรวบรวมพยานหลักฐาน

ดิจิทัลจนสามารถเอาผิดต้องคำพิพากษาตัดสินลงโทษได้ทุกราย การไร้ตัวตนจากอาชญากรรมไซเบอร์ประเภทนั้นจะหมดไปเมื่อ

$$\frac{s}{d} = 1$$

4.2.2.3 การหา Payoff Function

จาก Decision tree เห็นองค์ประกอบการตัดสินใจว่า ปัจจัยการไร้ตัวตน (Anonymous factor) ประกอบไปด้วยอะไร จนสามารถนำมาสร้าง Payoff Matrix ให้เห็นค่าของเกมได้ จึงนำมาสร้างความสัมพันธ์การตัดสินใจในการก่ออาชญากรรมของอาชญากรเขียนเป็น Payoff Function ได้ดังนี้

จำนวนคดีอาชญากรรมไซเบอร์ประเภทนั้นจะสูงมากถ้าหาก $\frac{d}{c} + \frac{s}{d} = 0$ ..... (Reeves)

จำนวนคดีอาชญากรรมไซเบอร์ประเภทนั้นจะหมดไปถ้าหาก $\frac{d}{c} + \frac{s}{d} = 2$ ..... (Reeves)

เมื่อ $\frac{d}{c} = 1$, $\frac{s}{d} = 1$

เพราะฉะนั้นจะได้ ปัจจัยการไร้ตัวตน (Anonymous factor) เท่ากับ $2 - \left[\frac{d}{c} + \frac{s}{d}\right] = 0$

ในดุษฎีนิพนธ์นี้ ให้ปัจจัยการไร้ตัวตน (Anonymous factor) เขียนแทนด้วย k จะได้ว่า

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right] \quad \text{..... (3)}$$

จะเห็นได้ว่า $0 \leq k \leq 2$

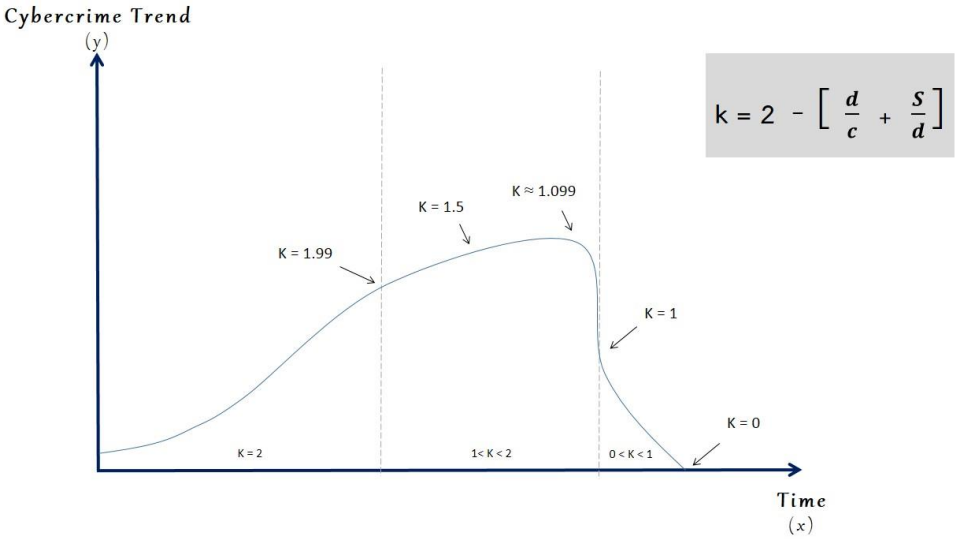
4.2.3 มโนทัศน์และข้อเสนอทฤษฎีบท

เนื่องด้วยข้อมูลทางสถิติไม่เพียงพอ ผู้วิจัยจึงพยายามหาความสัมพันธ์การไร้ตัวตนกับอาชญากรรมไซเบอร์เพิ่มเติม โดยใช้ Matrix payoff และ Payoff Function การตัดสินใจก่ออาชญากรรมไซเบอร์ของอาชญากร อันขึ้นอยู่กับปัจจัยการไร้ตัวตน (Anonymous factor) ดังที่ได้วิเคราะห์ผ่านมา โดย k มีค่าตั้งแต่ $0 \leq k \leq 2$ ซึ่งส่งผลต่อแนวโน้มการเกิดอาชญากรรมไซเบอร์ในแต่ละช่วงเวลาแตกต่างกัน และผู้วิจัยได้พิจารณาตั้งมโนทัศน์เพื่อพยายามทำความเข้าใจ และพยากรณ์การเกิดอาชญากรรมไซเบอร์ ที่ค่าปัจจัยการไร้ตัวตน (Anonymous factor) แตกต่างกัน โดยใช้วิธี Backward induction ของทฤษฎีเกมได้ดังต่อไปนี้

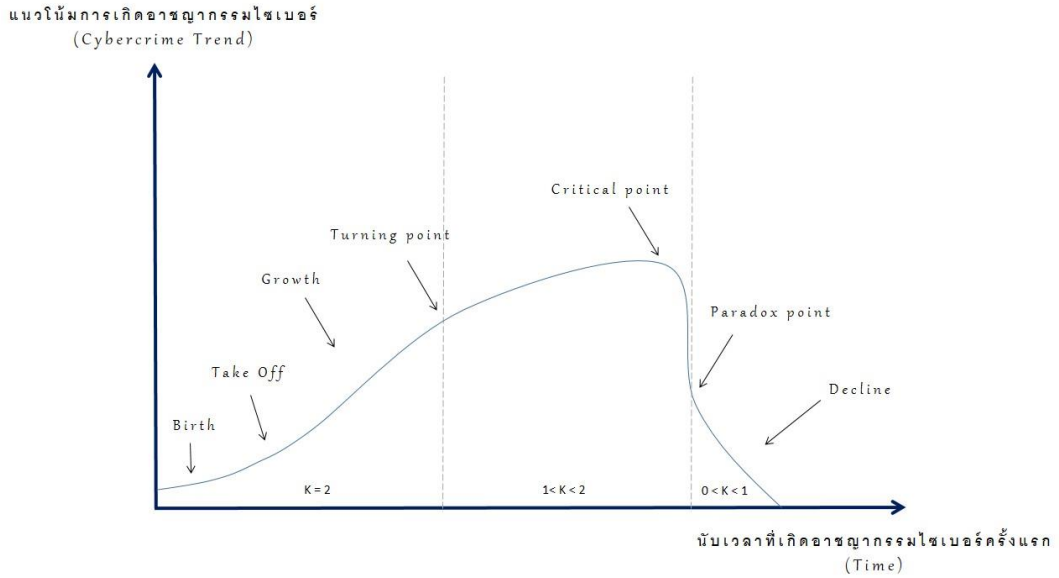
4.2.3.1 มโนทัศน์ที่ 1

“แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์เป็น **Shark fin curve”**

จาก Payoff Matrix และ Payoff Function ความสัมพันธ์การตัดสินใจในการก่ออาชญากรรมของอาชญากร ขึ้นอยู่กับค่า k หรือ ปัจจัยการไร้ตัวตน (Anonymous factor) อันมาจากสัดส่วนจำนวนคดีกับจำนวนการสืบสวนจับกุม และการรวบรวมพยานหลักฐานดิจิทัลเอาผิดอาญาดังที่ได้วิเคราะห์ไปแล้วนั้น นำมาตั้งเป็นกรอบให้เห็นภาพเพื่อทำความเข้าใจในรูปแบบกราฟ โดยใช้วิธี Backward induction ได้ดังนี้



รูปที่ 63 มโนทัศน์ความสัมพันธ์ปัจจัยการไร้ตัวตนกับการตัดสินใจในการก่ออาชญากรรมไซเบอร์



รูปที่ 64 มโนทัศน์ความสัมพันธ์แนวโน้มการเกิดอาชญากรรมไซเบอร์ (ตัวแปรตาม) กับช่วงเวลา (ตัวแปรต้น) โดยมีปัจจัยการไร้ตัวตนเป็นตัวแปรควบคุม

ผู้วิจัยได้สังเกตเห็นปรากฏการณ์อาชญากรรมไซเบอร์ในสังคมนับแต่อดีตมาจนถึงปัจจุบัน จากการศึกษาในบทที่ 3 และได้ทดลองวาดภาพที่เชื่อมโยงให้เห็นความสัมพันธ์ระหว่างการไร้ตัวตนและอาชญากรรมไซเบอร์มีความสัมพันธ์กันอย่างไร ดังรูปที่ 63-64 อธิบายเพิ่มเติมได้ดังนี้

แกน y หรือแกนตั้ง เป็น Cybercrime trend หรือ แนวโน้มการเกิดอาชญากรรมไซเบอร์

แกน x หรือแกนนอน เป็น Time หรือการนับช่วงเวลา จากปีที่เกิดอาชญากรรมไซเบอร์ เช่น ปีที่ 1 ปีที่ 2 ปีที่ 3....ปีที่ n (หรือนับเป็นเดือนหรือสัปดาห์)

สถานะที่ 1 Birth

อาชญากรกลุ่มแรกๆ ได้รับข้อมูลหรือมีการทดลอง และค้นพบว่าไซเบอร์เทคโนโลยีใหม่ที่เกิดขึ้นในสังคม สามารถประกอบอาชญากรรมได้ในคดีแรกๆ โดยไม่มีใครล่วงรู้ว่าเป็นฝีมือผู้ใด

<u>หมายเหตุ</u> k = 2

สถานะที่ 2 Take off

ข่าวสารการสร้างความเสียหายอย่างไร้ตัวตนผู้กระทำความผิด ด้วยไซเบอร์เทคโนโลยีใหม่ ทำให้รอดพ้นจากสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้แพร่กระจายสู่ อาชญากรตามโอกาสและอาชญากรติดนิสัย ต่างเริ่มเลียนแบบเทคนิควิธี และตัดสินใจประกอบอาชญากรรมด้วยไซเบอร์เทคโนโลยีนั้น

จาก Payoff Matrix ในตารางที่ 10 และ Payoff Function ในสมการที่ 3 อาชญากรตัดสินใจใช้กลยุทธ์ที่ Q และ 1- Q โดยที่ตำรวจใช้กลยุทธ์จากกลยุทธ์ P1 ทำให้แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นๆ เติบโตพุ่งสูงอย่างรวดเร็วในเวลานั้น

<u>หมายเหตุ</u> k = 2

สถานะที่ 3 Growth

ข่าวสารการสร้างความเสียหายอย่างไร้ตัวตนผู้กระทำความผิด ด้วยไซเบอร์เทคโนโลยีใหม่ ทำให้รอดพ้นจากสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้แพร่กระจายในวงกว้างสู่อาชญากรทั่วทั้งวงการอาชญากรรม ต่างก็ตัดสินใจประกอบอาชญากรรมเพื่ออรรถประโยชน์สูงสุดแก่ตน และพวกพ้อง

ทำให้แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นๆ เติบโตพุ่งสูงอย่างรวดเร็ว และสร้างความเสียหายต่อสังคมต่อเนื่อง ตามระยะเวลาที่เกิดขึ้นนับแต่ปีแรก (หรือเดือนหรือสัปดาห์แรก) หรือคดีแรกที่เกิดขึ้นไปเรื่อยๆ และยังทำการสืบสวนจับกุมไม่ได้สักคดี เมื่อพิจารณาจาก Matrix payoff ตารางที่ 10 หมายความว่าตำรวจยังมีเพียงกลยุทธ์จากกลยุทธ์ P1

<u>หมายเหตุ</u> k = 2

สถานะที่ 4 Turning point

จาก Payoff Matrix ในตารางที่ 10 และ Payoff Function ในสมการที่ 3 เมื่อตำรวจเริ่มปรับเปลี่ยนกลยุทธ์กลยุทธ์ P1 และมาค้นพบกลยุทธ์ P2 สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้ตัวอาชญากรมาดำเนินคดีครั้งแรก ปัจจัยการไร้ตัวตน (Anonymous factor) เริ่มมีค่า k น้อยกว่า 2 แต่ยังมากกว่า 1 แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นๆ จะเริ่มลดลง แบบ Diminishing (ยังคงเติบโต แต่ในอัตราการเติบโตที่ลดลง)

<u>หมายเหตุ</u> 1< k < 2

สถานะที่ 5 Critical point

จาก Payoff Matrix ในตารางที่ 13 และ Payoff Function ในสมการที่ 3 เมื่อตำรวจเริ่มเปลี่ยนมาใช้กลยุทธ์ P2 สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้ตัวอาชญากรมาดำเนินคดีได้เกือบทุกคดี จนถึงจุดวิกฤต (Critical point) ค่า k เข้าใกล้ 1 ผ่านจุดสูงสุดของฟังก์ชัน และเมื่อค่า k =1 เรียกว่าจุด Paradox point เกิดการเปลี่ยนแปลงแนวโน้มการเกิดอาชญากรรมไซเบอร์ลดลดอย่ารวดเร็วอย่างกะทันหัน แต่ยังไม่หายไปหมดเสียทีเดียว (ค่า k =1 เรียกว่าจุด Paradox point ในดุษฎีนิพนธ์นี้ควรได้รับการพัฒนาต่อ)

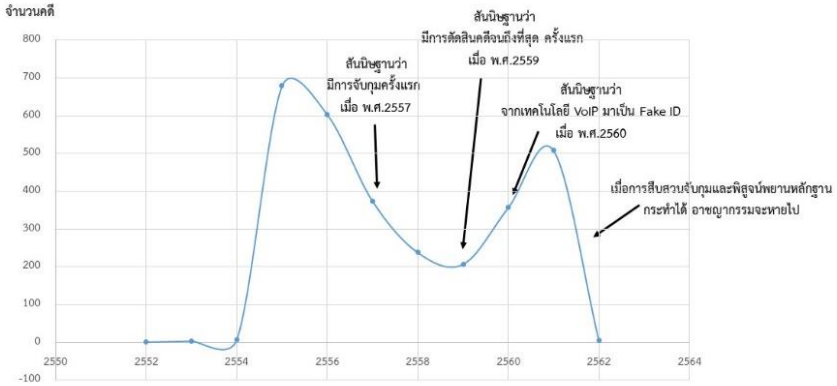
<u>หมายเหตุ</u> k = 1

สถานะที่ 6 Decline

จาก Payoff Matrix ในตารางที่ 10 และ Payoff Function ในสมการที่ 3 เมื่อตำรวจค้นพบกลยุทธ์ที่ P3 สามารถสืบสวนจับกุมอาชญากรไซเบอร์ได้ทุกคดีและสามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีหรือการพิสูจน์ตัวตนเอาผิดทางอาญาอาชญากรได้ กลายเป็นฟังก์ชันลด อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงอย่างรวดเร็วจนแนวโน้มการเกิดอาชญากรรมไซเบอร์มีค่าเขาใกล้หรือเป็น 0 หรือไม่เกิดขึ้นอีกเลย

<u>หมายเหตุ</u> 0 < k < 1

แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) จากมโนทัศน์ที่ 1 ที่อธิบายความสัมพันธ์แนวโน้มการเกิดอาชญากรรมไซเบอร์เป็นตัวแปรตาม กับช่วงเวลาเป็นตัวแปรต้น โดยมีปัจจัยการไร้ตัวตนเป็นตัวแปรควบคุม นำมาเปรียบเทียบกับกราฟคดีแก็งค์ คอลเซ็นเตอร์ ในรูปที่ 22 ที่มีสถิติคดีอาชญากรรมจำนวนมากในบทที่ 3 ซึ่งมีลักษณะกราฟใกล้เคียงกันมากดังนี้



ที่มา : ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

รูปที่ 65 ลักษณะความสัมพันธ์คดี แก๊งค์ คอลเซ็นเตอร์ กับเวลา โดยมีการสืบสวนจับกุม และการดำเนินคดีเอาผิดได้เป็นตัวแปรควบคุม

<u>การตีความ</u> คดีแก๊งคอลเซนเตอร์ ใช้เทคโนโลยี Voice over internet protocol ประกอบอาชญากรรม โดยเจ้าหน้าที่ตำรวจไม่สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) เพื่อหาตัวตนอาชญากรได้ อาชญากรรมประเภทนี้จึงเติบโตอย่างรวดเร็วในปี พ.ศ. 2554-2556 จนสามารถสืบสวนจับกุมได้เมื่อปี พ.ศ. 2557 และเมื่อมีการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีกระทำได้ถึงที่สุด อาชญากรรมประเภทนี้แทบจะหมดไป

จนกระทั่งอาชญากรเปลี่ยนกลยุทธ์จากการใช้เทคโนโลยี Voice over internet protocol มาใช้ Fake ID อาชญากรรมประเภทนี้จึงกลับมาสูงขึ้นอย่างรวดเร็วอีกครั้ง แต่ในที่สุดเจ้าหน้าที่ตำรวจสามารถสืบสวนจับกุม และดำเนินคดีจนถึงที่สุดได้ แนวโน้มอาชญากรรมประเภทนี้จึงลดลง และส่งผลให้อาชญากรรมไซเบอร์ ประเภทคดีแก๊งคอลเซ็นเตอร์หมดสิ้นไปในที่สุด

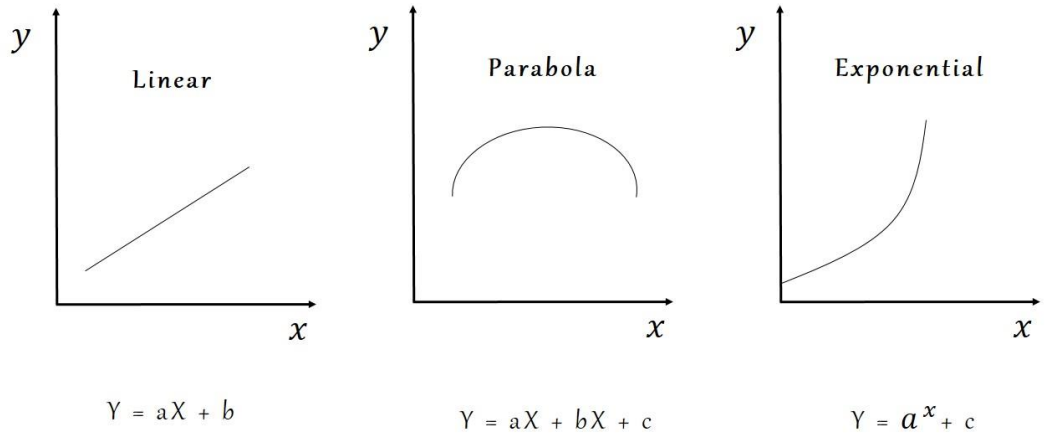
4.2.3.2 มโนทัศน์ที่ 2

“ความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน ควรมีลักษณะเป็นกราฟ และสมการ อย่างคุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล”

จากมโนทัศน์ที่ 1 แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) ที่ใช้การให้เหตุผลแบบ หลักการคิดย้อนกลับ (Backward induction) ของทฤษฎีเกม โดยชี้ให้ดูผลลัพธ์ของเหตุการณ์ว่าท้ายสุดจะเกิดอะไรขึ้น แล้วคิดถอยหลังกลับมาหาปัจจุบัน โดยใช้ผลที่ได้มาจาก Payoff Matrix ในตารางที่ 10 และ Payoff Function ในสมการที่ 3 อธิบายความสัมพันธ์

แนวโน้มการเกิดอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน จึงพยายามที่จะหาสมการทางคณิตศาสตร์ (Mathematical Model) มาอธิบายกราฟเพื่อให้นักวิจัยรุ่นต่อไปได้ใช้ประโยชน์

โดยผู้วิจัยได้เริ่มต้นพิจารณาจากรูปแบบกราฟ และสมการทางคณิตศาสตร์หลายๆ รูปแบบว่ากราฟ และสมการทางคณิตศาสตร์แบบใดจะใกล้เคียงหรือมีความเหมาะสมในการที่นำมาทดลองใช้อธิบายหรือทำนายอาชญากรรมไซเบอร์ตามวัตถุประสงค์วิทยานิพนธ์ โดยมีวิธีพิจารณาแนวทางการตั้งมโนทัศน์ ดังนี้



รูปที่ 66 ความสัมพันธ์ทั่วไปของกราฟ และฟังก์ชันแต่ละชนิด

จากแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) ในมโนทัศน์ที่ 1 ไม่ใช่ลักษณะกราฟของสมการเชิงเส้น (Linear equation) และไม่ใช่ลักษณะกราฟของสมการพาราโบลา (Parabola equation) ผู้วิจัยจึงตัดสินใจเลือกลักษณะกราฟของสมการ เอ็กซ์โปเนนเชียล (Exponential equation) มาทดลองพิสูจน์มโนทัศน์ที่ 1 ว่า พอจะมีพลังในการอธิบายได้มากน้อยเพียงใด

เหตุผลที่เลือก ฟังก์ชันเอ็กซ์โปเนนเชียล มาอธิบายความสัมพันธ์ระหว่างการไร้ตนตน และการเกิดอาชญากรรมไซเบอร์ ผู้วิจัยให้เหตุผลประกอบคุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล ดังต่อไปนี้

4.2.3.2.1 ฟังก์ชันเอ็กซ์โปเนนเชียล ไม่ติดลบและเริ่มจากค่า y= 1

คุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล เป็นกราฟ และสมการทางคณิตศาสตร์ ที่มีค่าเป็นบวกเสมอ แตกต่างจากรูปแบบสมการอื่นๆ ซึ่งหากนำมาพยายามใช้อธิบายจะค่อนข้างเห็นภาพได้ยาก และอาจไม่สามารถพิสูจน์ให้เห็นชัดได้ ซึ่ง ฟังก์ชันเอ็กซ์โปเนนเชียล มีความเหมาะสมที่สุด โดยมีรูปแบบสมการดังนี้

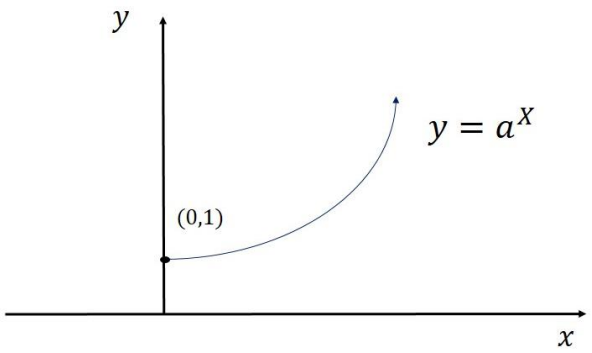
$$y = a^x + c$$

โดยที่ $0 < a$ และ $a \neq 1$ (จุดที่ a = 1 ค่า y จะเท่ากับ x)

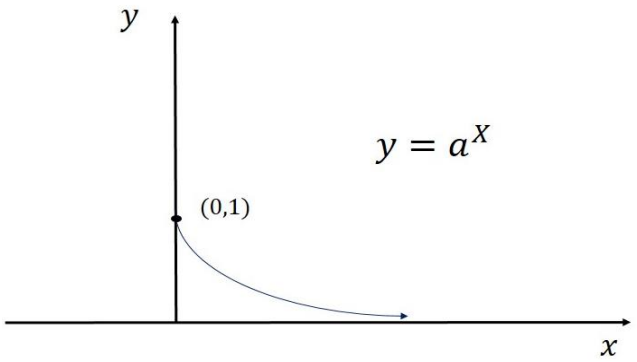
การตั้งมโนทัศน์อธิบายการเกิดอาชญากรรมไซเบอร์ในสังคม เมื่อเราพิจารณาถึงหลักความจริง การเกิดคดีขึ้นครั้งแรกนับเป็นครั้งที่ 1 ในปีแรก เป็นเลขบวก ไม่มีทางติดลบ

ฟังก์ชันเอ็กซ์โปเนนเชียล เริ่มนับที่ค่า y เท่ากับ 1 เมื่อ x เป็น 0 ($a^0 = 1$) สามารถนำมาอธิบายภาพได้ว่า เมื่ออาชญากรใช้เทคโนโลยีไซเบอร์ใดที่ตำรวจยังจับไม่ได้ อาชญากรรมประเภทนั้นจะเพิ่มสูงขึ้นเรื่อยๆ อย่างรวดเร็ว เป็นฟังก์ชันเพิ่มมีความชันกราฟมากกว่าสมการเชิงเส้น และเมื่อการใช้ไซเบอร์เทคโนโลยีใดที่ อาชญากรไม่อาจหลบพ้นตัวตนถูกจับกุมดำเนินคดี และถูกพิพากษาลงโทษ อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงเป็นฟังก์ชันลดจนมีค่าเป็น 0 ($0^x = 0$) ไม่มีทางติดลบ

หากนำมาตั้งมโนทัศน์อธิบายการเกิดอาชญากรรมไซเบอร์ในสังคม เมื่อเราพิจารณาถึงหลักความจริง การเกิดคดีขึ้นครั้งแรก นับเป็น 1 (ค่า y) ซึ่งไม่มีค่าติดลบ โดยคุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล จะเริ่มที่จุด (0,1) หรือ x (x คือ ปีที่อาชญากรรมไซเบอร์ประเภทนั้นเกิดขึ้น) มีค่าเท่ากับ 0 และ y จะมีค่าเท่ากับ 1 เสมอ ทั้งฟังก์ชันเพิ่มและ ฟังก์ชันลด



รูปที่ 67 คุณสมบัติของฟังก์ชันเพิ่ม ของฟังก์ชันเอ็กซ์โปเนนเชียล



รูปที่ 68 คุณสมบัติของฟังก์ชันลด ของฟังก์ชันเอ็กซ์โปเนนเชียล

ดังนั้นมโนทัศน์ที่ 2 “ความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน ควรมีลักษณะเป็นกราฟ และสมการ อย่างคุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล” สามารถนิยามได้ดังนี้

$$y = k^x + c \quad \text{..... (4)}$$

โดยที่

k คือ ปัจจัยการไร้ตัวตน (Anonymous factor)

y คือ Cybercrime trend หรือ แนวโน้มการเกิดอาชญากรรมไซเบอร์

x คือ Time หรือการนับช่วงเวลาจากปีที่เกิดอาชญากรรมไซเบอร์ เช่น ปีที่ 1 ปีที่ 2 ปีที่ 3....ปีที่ n (หรือนับเป็นเดือนหรือสัปดาห์)

c คือ ค่าคงที่ (ในกรณีที่มี)

โดยสามารถพิสูจน์คุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล เป็นกราฟ และสมการทางคณิตศาสตร์ ว่ามีความเป็นไปได้ที่จะสอดคล้องกับแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) กับผลที่ได้มาจาก Payoff Matrix ในตารางที่ 10 และ Payoff Function ในสมการที่ 3 อย่างไร ซึ่งสามารถพิสูจน์ได้ดังต่อไปนี้

4.2.3.2.2 เลขฐาน 0 < a และ a ≠ 1 สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor)

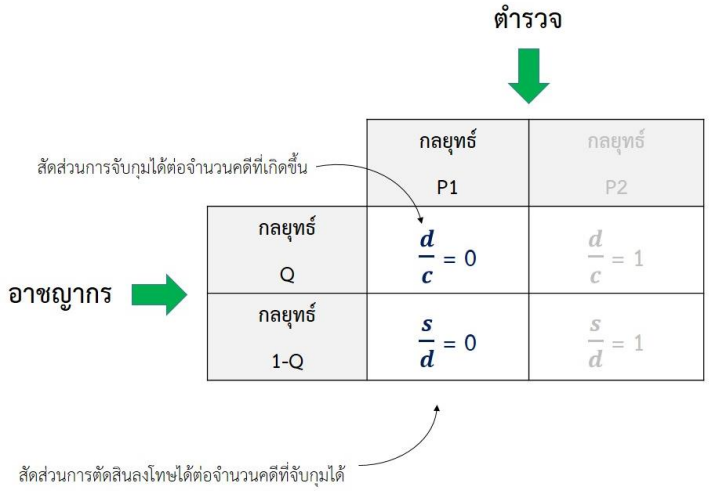
คุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล เลขฐาน a จะต้องมากกว่า 0 และไม่เท่ากับ 1 เพราะเลข 1 ยกกำลังอะไรก็เท่ากับ 1 และจุดที่ เลขฐานเริ่มมากกว่า 1 นั้นเป็นจุดเปลี่ยนเป็นฟังก์ชันลด

โดยที่

เลขฐานมากกว่า 1 เป็นฟังก์ชันเพิ่ม a > 1

เลขฐานมากกว่า 0 แต่น้อยกว่า 1 เป็นฟังก์ชันลด 0 < a <1

พิจารณาประกอบสมมติฐานทางวิจัย ค่า k หรือปัจจัยการไร้ตัวตน (Anonymous factor) ในข้อที่ 4.3.1 นำมาอธิบายรายละเอียดได้ดังนี้



ตารางที่ 11 Payoff Matrix เมื่อสถานการณ์อาชญากรรมไซเบอร์มี ค่า k = 2

สถานการณ์ที่ 1 เมื่อ k = 2

เมื่อค่า d = 0 ค่า k จะเท่ากับ 2 เสมอ นี่คือกรณี Worst case คือ มีคดีอาชญากรรมไซเบอร์ใหม่เกิดขึ้น แต่ไม่สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้เลย เจ้าหน้าที่ตำรวจรู้จักเพียงกลยุทธ์ P1 ยังไม่รู้จักกลยุทธ์ P2 ทำให้ไม่สามารถสืบสวนจับกุมได้ นับวันอาชญากรรมไซเบอร์ประเภทนั้นจะยิ่งทวีคูณเพิ่มขึ้นอย่างรวดเร็ว

ตัวอย่างสมการ

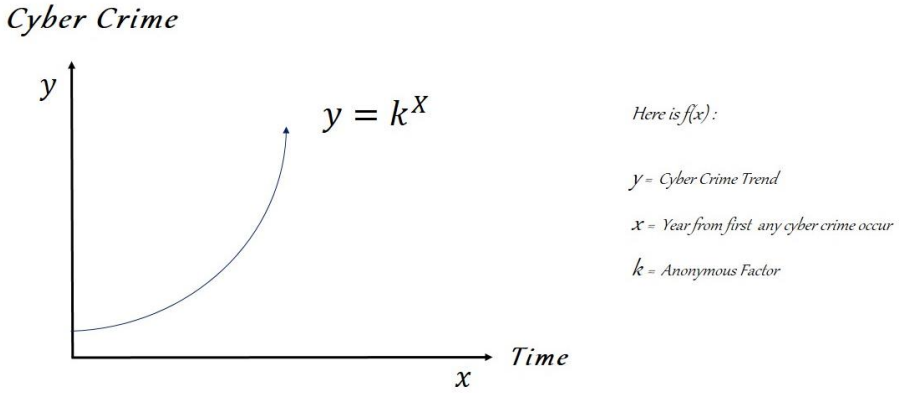
ปัจจัยการไร้ตัวตน (Anonymous factor) เมื่อ k = 2 จะได้ว่า

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{d^{0}}{c} + \frac{s}{d^{0}}\right]$$

$$k = 2$$

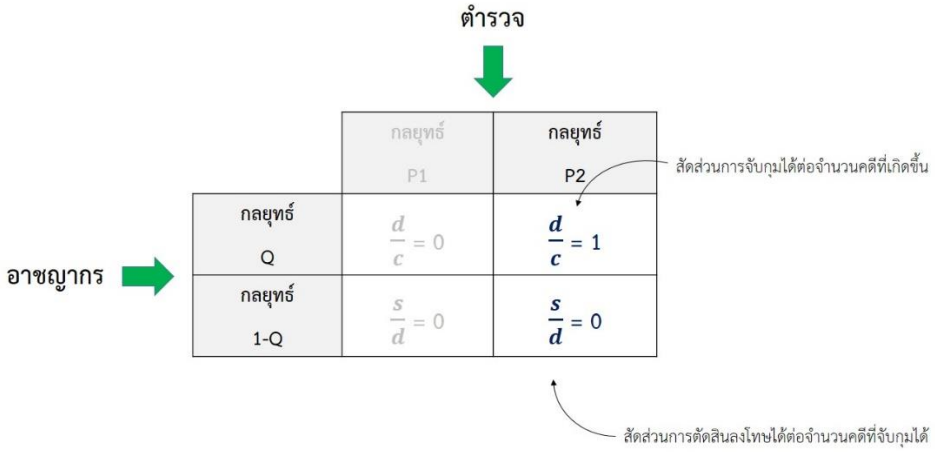
แทนค่า $f(y) = 2^{x}$



รูปที่ 69 มโนทัศน์อาชญากรรมไซเบอร์ในสังคม เป็นฟังก์ชันเพิ่ม

สถานการณ์ที่ 2 เมื่อ 1 < k < 2

เมื่อเจ้าหน้าที่ตำรวจค้นพบกลยุทธ์ P2 เริ่มสามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ ค่า d เริ่มมีค่ามากกว่า 0 ทำให้ค่า k เริ่มน้อยกว่า 2 ลงเรื่อยๆ จนเข้าใกล้ 1 ยังคงเป็นฟังก์ชันเพิ่มในอัตราที่ลดลง (Diminishing) เมื่อ 1 < k < 2



ตารางที่ 12 Payoff Matrix เมื่อสถานการณ์อาชญากรรมไซเบอร์มี เมื่อ 1 < k < 2

จะเห็นได้ว่า เมื่อค่า d เริ่มมีค่ามากกว่า 0 คือ เริ่มสามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้มี ค่า k จะเริ่มน้อยกว่า 2 แต่ยังมากกว่า 1 ดังตัวอย่างในสมการนี้

ตัวอย่างสมการ

สมมติว่า จำนวนคดีอาชญากรรมไซเบอร์ประเภทใดที่เกิดขึ้น (c) มีจำนวน 10 คดี และเริ่มจำนวนคดีที่สืบสวนจนจับกุมอาชญากรได้ (d) จำนวน 1 คดี จึงมีสัดส่วน 1 ต่อ 10 หรือมีค่าเท่ากับ 0.1 เขียนเป็นสมการได้ดังนี้

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{1}{10} + \frac{s}{d}\right] \quad (d/c \to 0.1,\ s/d \to 0)$$

$$k = 1.99$$

แทนค่า $f(y) = 1.99^{x}$

จากนั้นลองตั้งตัวอย่างสมมติเพิ่มว่า ถ้าจำนวนคดีอาชญากรรมไซเบอร์ประเภทใดที่เกิดขึ้น (c) มีจำนวนเท่ากับ 10 คดี และเริ่มจำนวนคดีที่สืบสวนจนจับกุมอาชญากรได้ (d) จำนวน 5 คดี จึงมีสัดส่วน 5 ต่อ 10 หรือมีค่าเท่ากับ 0.5 หรือ 50 % เขียนเป็นสมการได้ดังนี้

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{5}{10} + \frac{0}{d}\right]$$

$$k = 1.5$$

แทนค่า $f(y) = 1.50^{x}$

ทำให้เข้าใจได้ว่า หากเลขฐานลดจำนวนลง ความชันเส้นกราฟจะลดตาม แต่ยังเป็นกราฟฟังก์ชันเพิ่มในอัตราที่ลดลง (Diminishing) เพราะยังยกกำลัง x

สถานการณ์ที่ 3 เมื่อ k = 1

เมื่อค่า d มีค่ามากขึ้นเรื่อยๆ จนเท่ากับ 1 สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ทุกคดี กล่าวคือก่อคดีได้เท่าใด ก็สามารถสืบสวนจับกุมได้นั้น ค่า k เท่ากับ 1 เป็นจุดเปลี่ยนฟังก์ชันลดใน กราฟของสมการ เอ็กซ์โปเนนเชียล ดังตัวอย่างในสมการนี้

ตัวอย่างสมการ

สมมติว่า จำนวนคดีอาชญากรรมไซเบอร์ประเภทใดที่เกิดขึ้น (c) มีจำนวน 10 คดี และสืบสวนจนจับกุมอาชญากรได้ทุกคดี ค่า (d) มีค่าเท่าจำนวน 10 คดี จึงมีสัดส่วน 10 ต่อ 10 หรือมีค่าเท่ากับ 1 หรือหมายถึงอัตราสืบสวนจับกุมได้ 100 % เขียนเป็นสมการได้ดังนี้

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{\cancel{10}^{1}}{\cancel{10}} + \frac{\cancel{5}^{0}}{\cancel{d}} \right]$$

$$k = 1$$

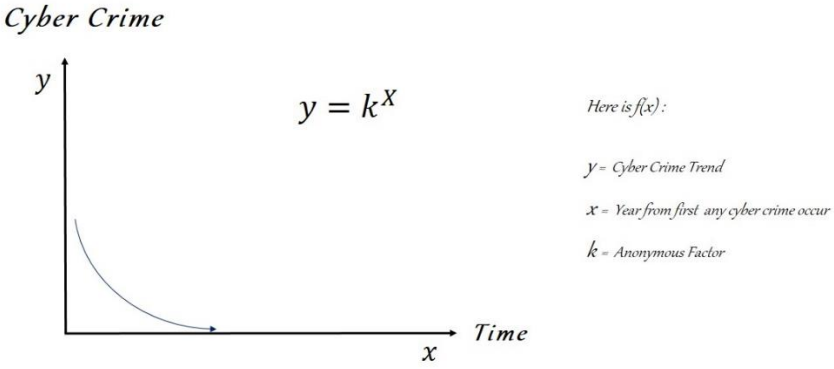
แทนค่า $f(y) = 1^{x}$

ในกรณีที่เลขฐานสมการ เอ็กซ์โปเนนเชียล มีค่าเท่ากับ 1 ค่า x ไม่ว่าค่าใดจะทำให้ค่า y เท่ากับ 1 จากแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ เมื่อค่า k เท่ากับ 1 หรือหมายถึง อัตราสืบสวนจับกุมได้ 100 % แกน y นั้นคือ แนวโน้มการเกิดอาชญากรรมไซเบอร์ ไม่ใช่จำนวนคดี ความชันของกราฟจะเกิดการตกลงมาในระดับหนึ่งซึ่งต่ำมาก หากไม่มีค่าคงที่ c ที่ได้จากการคำนวณทางมูลสถิติที่แท้จริงแล้ว ค่า yจะต้องมีค่ากับ 1 หรือมีแนวโน้มเท่าอัตราการเกิดอาชญากรรมไซเบอร์นั้นในครั้งแรก เป็นจุดเปลี่ยนเข้าสู่ฟังก์ชันลด

4.2.3.2.3 เมื่อเลขฐาน 0 < k < 1 เป็นฟังก์ชันลด สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor)

สถานการณ์ที่ 4 เมื่อ 0 < k < 1

แม้เจ้าหน้าที่ตำรวจค้นพบกลยุทธ์ P2 แล้ว อัตราสืบสวนจับกุมตำจำนวนคดีทำได้ 100 % แต่ยังไม่มีผู้ใดถูกตัดสินพิพากษารับโทษอาญาได้เลย บางคดีกลับยกฟ้องเนื่องด้วยการรวบรวมพยานหลักฐานดิจิทัลไม่ครบถ้วนสมบูรณ์ ยังมีช่องว่างทางเทคโนโลยีอยู่ แม้แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นจะลดลง แต่ยังคงเกิดในอัตราที่น้อยลง ค่า k ผ่านเลยค่าเท่ากับ 1 มาแล้วเป็นฟังก์ชันลด



รูปที่ 70 มโนทัศน์อาชญากรรมไซเบอร์ในสังคม เป็นฟังก์ชันลด

ดังตัวอย่างสมมุติในสมการนี้

ปัจจัยการไร้ตัวตน (Anonymous factor) เป็นฟังก์ชันเพิ่มเมื่อ 0 < k < 1

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{10}{10} + \frac{5}{10}\right]$$

$$k = 0.5$$

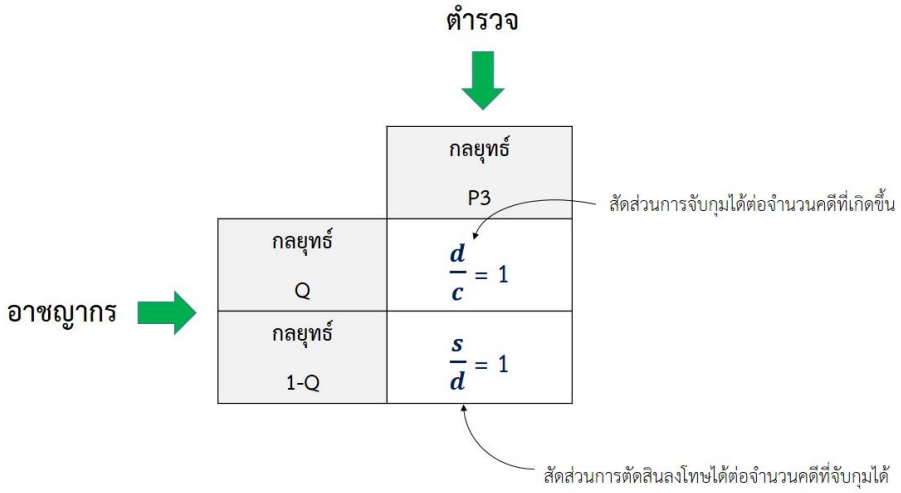
แทนค่า $f(y) = 0.5^x$

4.2.3.2.4 เมื่อเลขฐานเท่ากับ 0 สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor)

คุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล เมื่อเลขฐาน a มีค่าเท่ากับ 0 ฟังก์ชันก็มีค่า y เท่ากับ 0 สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor) เมื่อค่า k เท่ากับ 0 หมายความว่า อาชญากรรมไซเบอร์นั้นหมดไปจากสังคม

สถานการณ์ที่ 5 เมื่อ k = 0

สถานการณ์สมมติ เมื่อตำรวจสามารถค้นหากลยุทธ์ P3 ได้สำเร็จ นอกจากอาชญากรไซเบอร์ก่อคดีเท่าใดก็จับได้ทุกคดีแล้ว ยังสามารถรวบรวมพยานหลักฐานดิจิทัลได้ครบถ้วนจนสามารถลงโทษเอาผิดอาญาอาชญากรได้ทุกราย ค่า k = 0 เป็นจุดจบของอาชญากรรมไซเบอร์ประเภทนั้น เขียนได้ดังนี้



ตารางที่ 13 Payoff Matrix เมื่อสถานการณ์อาชญากรรมไซเบอร์มี ค่า k = 0

เมื่อค่า d มีค่ามากขึ้นเรื่อยๆ จนเท่ากับ 1 สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ทุกคดีแล้ว และจำนวนคดีที่สามารถรวบรวมพยานหลักฐานดิจิทัลเอาผิดทางอาญาได้ คือ s สามารถเพิ่มจำนวนการดำเนินคดีเอาผิดอาญามากขึ้นเรื่อยๆ และลดสัดส่วนการยกฟ้องลงเรื่อยๆ จนค่า k เท่ากับ 0 กราฟของสมการ เอ็กซ์โปเนนเชียล ลดลงจน y มีค่าเท่ากับ 0 ดังตัวอย่างสมมุติในสมการนี้

ปัจจัยการไร้ตัวตน (Anonymous factor) เป็นฟังก์ชันเพิ่มเมื่อ k = 2

$$k = 2 - \left[\frac{d}{c} + \frac{s}{d}\right]$$

$$k = 2 - \left[\frac{10^{1}}{10} + \frac{10^{1}}{10} \right]$$

$$k = 0$$

แทนค่า $f(y) = 0^{x}$

เป้าหมายสูงสุดของนักอาชญาวิทยาไซเบอร์ และตำรวจไซเบอร์ มีเป้าหมายร่วมกันในการป้องกัน และปราบปรามอาชญากรรมไซเบอร์ทุกประเภทนั้น คือ ค่า $k = 0$

นั่นหมายความว่า

ในเชิงป้องกัน ซึ่งเป็นหน้าที่ของนักอาชญาวิทยาไซเบอร์คือไม่ต้องการให้มีเหยื่อเกิดขึ้น หากมีไซเบอร์เทคโนโลยีใหม่เกิดขึ้นในสังคม ต้องเสนอแนะต่อรัฐให้กำหนดกฎเกณฑ์ในการกำกับดูแลให้มีปัจจัยการไร้ตัวตน (Anonymous factor) เท่ากับ 0 เพื่อป้องกันการเกิดอาชญากรรมไซเบอร์รูปแบบใหม่ในสังคม

ในเชิงปราบปราม ซึ่งเป็นหน้าที่ของตำรวจไซเบอร์ ต้องค้นคว้าหรือขอความร่วมมือจากผู้เชี่ยวชาญ ในการทำให้ ปัจจัยการไร้ตัวตน (Anonymous factor) มีค่าเท่ากับ 0 ซึ่งจะทำให้สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ และสามารถรวบรวมพยานหลักฐานดิจิทัลเอาผิดทางอาญาได้ทั้งหมด

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุปตามวัตถุประสงค์การวิจัย

จากวัตถุประสงค์ของการวิจัยที่ได้ดำเนินมาตามกรอบการวิจัยและระเบียบวิธีการวิจัย จึงขอสรุปผลการวิจัยตามวัตถุประสงค์การวิจัยดังนี้

5.1.1 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1 (การศึกษารวบรวมอาชญากรรมไซเบอร์)

วัตถุประสงค์การวิจัยในข้อที่ 1 คือ เพื่อศึกษา และรวบรวมรูปแบบการประกอบอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นจากอดีตมาจนถึงปัจจุบัน อันเป็นกรณีศึกษาเกี่ยวข้องกับการไร้ตัวตนเป็นปัจจัยสำคัญของการเกิดอาชญากรรม

กรณีศึกษาทั้งหมด 17 กรณี ที่เลือกรวบรวมยกมาเป็นการศึกษาสำคัญครอบคลุมในทุกมิติ และคดีอาชญากรรมไซเบอร์ทุกคดีมีความสอดคล้องเหมือนกันหมดในเรื่อง “การไร้ตัวตน” และต้องมี Anonymous factor อาชญากรรมไซเบอร์จึงจะเกิดขึ้น

เมื่อพิจารณาย้อนกลับในอีกมุม หากกรณีศึกษาทั้งหมด 17 กรณี ไม่มีการไร้ตัวตน หรือไม่มี Anonymous factor อาชญากรรมไซเบอร์เหล่านั้นจะไม่เกิดขึ้น

การปิดบัง อำพราง ล่องหนหายตัว เป็นหัวใจสำคัญของอาชญากรรมไซเบอร์ที่สอดคล้องกันหมดทุกกรณีที่ได้ทำการศึกษารวบรวม ผู้วิจัยจึงหยิบยกปัญหานี้ขึ้นมาให้ประจักษ์ถึงความสำคัญ

5.1.2 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 (ความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตนกับอาชญากรรมไซเบอร์)

วัตถุประสงค์การวิจัยในข้อที่ 2 คือ เพื่อศึกษาความสัมพันธ์ระหว่างปัจจัยการไร้ตัวตน (Anonymous Factor) อันเป็นเหตุให้รอดพ้นจากการสืบสวนจับกุม (Digital Detective) และการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินเอาผิดคดีอาญากับการตัดสินใจก่ออาชญากรรมไซเบอร์ของอาชญากร

จากการศึกษารวบรวมรูปแบบการประกอบอาชญากรรมไซเบอร์ตามวัตถุประสงค์การวิจัยในข้อที่ 1 พบว่า อาชญากรรมไซเบอร์ทุกประเภทมีความสอดคล้องเหมือนกันหมดคือเรื่อง การไร้ตัวตน และต้องมี Anonymous factor อาชญากรรมไซเบอร์จึงจะเกิดขึ้น และจากการศึกษาวิจัยพบว่า

การไร้ตัวตนเป็นเรื่องสำคัญของอาชญากรไซเบอร์ที่ใช้ประกอบการตัดสินใจลงมือก่ออาชญากรรม จึงมีความสัมพันธ์ต่อกัน แม้ผลการวิจัยไม่ใช่การอธิบายความสัมพันธ์เชิงสาเหตุ (Causal relationship) แต่เมื่อพิจารณาจากการอภิปรายผลในบทที่ 4 พบว่า เมื่ออาชญากรคิดอย่างเป็นเหตุเป็นผล แล้วพบว่ามีเทคโนโลยีใดมีความสามารถในการปิดบัง อำพราง อย่างไร้ตัวตน อาชญากรจะตัดสินใจก่ออาชญากรรมทันที

อาชญากรไซเบอร์ แตกต่างจากอาชญากรประเภทอื่นตรงที่ ไม่ก่ออาชญากรรม “ซึ่งหน้า” ต่อเหยื่อ ซึ่งแตกต่างจากอาชญากร Street crime อื่นๆ เช่น การวิ่งราวทรัพย์กระทำซึ่งหน้าเหยื่อ การปล้นทรัพย์ซึ่งหน้าเหยื่อ การทำร้ายร่างกาย เป็นต้น แต่อาชญากรไซเบอร์ระมัดระวังเรื่องการไม่เปิดเผยตัวตน ความลับ การปิดบัง อำพราง ตลอดจนการใช้ Bot หรือ AI คิดหาทางก่ออาชญากรรมแทนตน เป็นเรื่องสำคัญที่สุด และในทางตรงกันข้ามเมื่อ ปัจจัยการไร้ตัวตนในเทคโนโลยีใดหายไป อาชญากรรมไซเบอร์ประเภทนั้นก็จะหายไปด้วย เพราะอาชญากรไซเบอร์จะไม่ตัดสินใจเลือกใช้เทคโนโลยีนั้นประกอบอาชญากรรม

การไร้ตัวตน คือ โอกาส ตามทฤษฎีสามเหลี่ยมอาญากรรมในบทที่ 2 ซึ่งอธิบายองค์ประกอบการเกิดอาชญากรรมประกอบไปด้วยปัจจัย 3 ประการคือ เหยื่ออ่อนแอ โอกาส และจิตใจอาชญากร ซึ่งถ้าหากดึงองค์ประกอบหรือปัจจัยอันใดอันหนึ่งออก อาชญากรรมจะไม่เกิดขึ้น

จากการศึกษาวิจัยอาชญากรรมไซเบอร์ในทุกรูปแบบ ผู้วิจัยพบว่าการชั่งน้ำหนักอย่างเป็นเหตุเป็นผลของอาชญากรตลอดเวลานั่นก็คือการแสวงหา “โอกาส” โดยเฉพาะโอกาสที่จะรอดพ้นจากการสืบสวนจับกุมเป็นหัวใจสำคัญในการตัดสินใจลงมือประกอบของอาชญากรไซเบอร์

รูปที่ 71 การไร้ตัวตนเพิ่มโอกาสในการเกิดอาชญากรรม

"โอกาส" ที่อาชญากรลงมือก่ออาชญากรรมกับเหยื่อในพื้นที่และเวลาที่เหมาะสม เมื่อพิจารณาการเลือกอย่างเป็นเหตุเป็นผลในการตัดสินใจก่ออาชญากรรมไซเบอร์ด้วยทฤษฎี Routine Activities Theory จะเห็นได้ว่าองค์ประกอบสำคัญที่สุดในการที่จะเปิดโอกาสให้เกิดอาชญากรรมไซเบอร์จากการไร้ตัวตน คือ **การขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian)**

เนื่องจากอาชญากรไซเบอร์เป็นกลุ่มอาชญากรที่มีความรู้ความสามารถสูง แต่ผู้ตกเป็นเหยื่ออาชญากรรมไซเบอร์ คือ ประชาชนทั่วไปเป็นเพียงผู้ใช้บริการ (User) ไม่ได้มีความรู้ระดับสูงด้านเทคโนโลยี ไม่สามารถปกป้องดูแลตนได้เอง จำเป็นต้องมีผู้พิทักษ์คอยสอดส่องดูแลความสงบเรียบร้อยและปลอดภัยในโลกออนไลน์ เช่น ผู้ให้บริการอินเทอร์เน็ตหรือผู้ดูแลความมั่นคงปลอดภัยไซเบอร์ ตำรวจ ผู้ปกครองเด็ก หน่วยงานภาครัฐ โอกาสในการเกิดอาชญากรรมจะเกิดขึ้นเมื่อขาดผู้พิทักษ์ไม่มีความสามารถเพียงพอในการป้องกันอาชญากรรมไซเบอร์ อาชญากรจะตัดสินใจเลือกอย่างเป็นเหตุเป็นผลในการก่ออาชญากรรมทันที

การไร้ตัวตน (Anonymity) ในดุษฎีนิพนธ์นี้ คือ "โอกาส" ที่ชี้ให้เห็นความเป็นเหตุเป็นผลต่อการตัดสินใจประกอบอาชญากรรมไซเบอร์ หากเทคโนโลยีใดมีการไร้ตัวตนมาก โอกาสในการเกิดอาชญากรรมก็มากตาม แต่ถ้าหากเทคโนโลยีใดไม่มีการไร้ตัวตนและสามารถระบุตัวตน (Identify) ทุกคนได้ โอกาสในการเกิดอาชญากรรมไซเบอร์ย่อมจะน้อยลง เมื่ออาชญากรตัดสินใจเป็นไปตามทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล

5.1.3 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3 (รูปแบบความสัมพันธ์การเชื่อมโยงระหว่างการไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์)

วัตถุประสงค์การวิจัยในข้อที่ 3 คือ เพื่อสร้างรูปแบบความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์

การสร้างรูปแบบความสัมพันธ์หรือสร้าง Model ด้วยทฤษฎีเกมในดุษฎีนิพนธ์นี้ แสดงความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์ออกมาเป็น Decision Tree, Payoff Matrix และ Payoff Function อธิบายการตัดสินใจลงมือก่ออาชญากรรมไซเบอร์เมื่ออาชญากรคิดอย่างเป็นเหตุและเป็นผล

สมการ Payoff Function ได้ชี้ให้เห็นความสำคัญที่สุดที่แสดงความสัมพันธ์ออกมาด้วยปัจจัยการไร้ตัวตน (Anonymous factors) หรือ ค่า k โดยได้นำมาอธิบายรูปแบบความสัมพันธ์เพิ่มเติมเป็นแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) ที่ริเริ่มเป็นต้นแบบนำมาพัฒนาประยุกต์ใช้ได้อย่างดี

โดยการสร้างรูปแบบความสัมพันธ์หรือสร้าง Model แสดงความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์ อธิบายรายละเอียดข้อสรุปผลวิจัยเพิ่มเติมดังนี้

ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory) คือหัวใจสำคัญในการวิจัยของดุษฎีนิพนธ์นี้ โดยใช้การคิดย้อนกลับแบบ Backward induction หาผลลัพธ์ในอนาคตแล้วคิดย้อนกลับมาปัจจุบัน เป็นจุดแตกต่างจากการวิจัยทางสถิติแล้วทำนายอนาคตแล้วพรรณนาผลที่ค้นพบว่าสาเหตุอาชญากรรมไซเบอร์เกิดจากอะไร แต่การเชื่อว่าอาชญากรไซเบอร์มีการคิดตัดสินใจอย่างเป็นเหตุเป็นผลหรือมีการเลือกอย่างเป็นเหตุเป็นผล (Rationale) โดยมีองค์ประกอบดังนี้

1. อรรถประโยชน์สูงสุด (Maximizing utility)

การเลือกอย่างเป็นเหตุเป็นผล (Rationale) ที่ว่าคือ อาชญากรไซเบอร์เห็นแก่ตัวมีความปรารถนาที่จะได้อรรถประโยชน์สูงสุด (Maximizing utility) ด้วยการเอาอรรถประโยชน์นั้นจากผู้อื่นหรือเหยื่อ โดยตนอาจจะไม่เสียประโยชน์ใด

เมื่อตั้งต้นความปรารถนาของอาชญากรไซเบอร์เช่นนี้ อาชญากรจะมุ่งมั่นมองหาโอกาสตลอดเวลา และเมื่อพบโอกาสการเลือกอย่างเป็นเหตุเป็นผล จึงไม่ยากที่จะตั้งทางเลือกในการตัดสินใจของอาชญากรด้วยการคิดแบบ Backward induction ว่า อาชญากรต้องการปัจจัยใดในการตัดสินลงมือประกอบอาชญากรรม ซึ่งอยู่บนความเชื่อ และข้อมูลที่อาชญากรมีเกี่ยวกับเทคโนโลยี

นั้นๆ โดยส่วนใหญ่จึงมีลักษณะเป็น อาชญากรตามโอกาส (Occasional criminals) และ อาชญากรติดนิสัย (Habitual criminals)

2. ความเชื่อ (Belief)

ความเชื่อ (Belief) ที่รองรับการเลือกอย่างเป็นเหตุเป็นผล ต้องเป็นความเชื่อที่มีพื้นฐานที่ดีรองรับนั่นคือ “ข้อมูล” จำนวนมากที่สนับสนุนว่าจะใช้เทคโนโลยีใดในการประกอบอาชญากรรม

อาชญากรไซเบอร์มีความรู้ความสามารถสูง (Perfect criminal) มีความสามารถในการใช้เทคโนโลยีให้รอดพ้นจากการถูกจับกุม โดยสามารถจัดมีรูปแบบการคิดของอาชญากรตามทฤษฎีหลักๆ 2 กรณี คือ คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation) หรือคิดได้ใจจนเกินจริง (Super-optimism) ว่าเขาสามารถที่จะหลีกพ้นโทษจากการกระทำความผิดของตนเองได้อย่างแน่นอนหรือมั่นใจว่าตนไม่มีทางถูกจับได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ

3. ข้อมูล (Information)

ข้อมูลที่อาชญากรใช้เป็นฐานความเชื่อที่ดี และเป็นทางเลือกในการตัดสินใจของอาชญากรเมื่อคิดแบบ Backward induction แล้วพบว่า

การเลือกใช้เทคโนโลยีใดในการประกอบอาชญากรรมไซเบอร์ อาชญากรต้องมีข้อมูลเกี่ยวกับเทคโนโลยีนั้นเพียง 2 ประเด็นคือ สามารถหลบพ้นการสืบสวนจับกุมเพื่อดำเนินคดีได้หรือไม่? การรวบรวมพยานหลักฐานดิจิทัลเพื่อพิสูจน์ความผิดเป็นไปไม่ได้ ใช่หรือไม่? ไม่อาจตัดสินลงโทษอาญาได้ง่าย หากข้อมูลที่ได้รับเกี่ยวกับเทคโนโลยีนั้นๆ ครบถ้วน จะเป็นแรงดึงดูดจูงใจให้อาชญากรไซเบอร์ประกอบอาชญากรรม

ซึ่งสอดคล้องกับหลักการของ ทฤษฎีเกม ซึ่งผู้เล่นเกมต้องมี

Perfect Information: ผู้เล่นมีข้อมูลครบถ้วนสมบูรณ์ เข้าใจ กติกา รางวัล และรู้กลยุทธ์ฝั่งตรงข้าม

Rationale: ผู้เล่นทุกฝ่ายใช้ข้อมูลที่ตนมีตัดสินใจเลือกกลยุทธ์ที่ดีที่สุด และตัดสินใจเลือกอย่างเป็นเหตุเป็นผล

4. ปัจจัยการไร้ตัวตน (Anonymous factors)

จากการสังเกตปรากฏการณ์สังคมของผู้วิจัย คงไม่มีอาชญากรไซเบอร์คนใดตัดสินใจลงมือก่ออาชญากรรมทั้งๆ ที่รู้ว่า “จะถูกจับได้ทันทีแน่นอน” ไม่ใช่การตัดสินใจอย่างเป็นเหตุและเป็นผล (Rationale) อาชญากรไซเบอร์ต้องการล่องหนหายตัว ไม่ใช่การเปิดหน้าท้าทายให้ออกมาประลองกำลัง

ดังนั้น การหลบพ้นจากเจ้าหน้าที่ตำรวจไม่ให้สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) เพื่อหาตัวตนอาชญากรกระทำได้ จึงเป็นปัจจัยการไร้ตัวตนแรก ที่อาชญากรตัดสินใจเลือกอย่างเป็นเหตุ และเป็นผล

ผู้วิจัยได้สังเกตปรากฏการณ์อาชญากรรมไซเบอร์พบว่า แม้มีการสืบสวนจับกุมอาชญากรไซเบอร์ได้ แต่ยังมีคดีแบบเดียวกันเกิดขึ้นอีก อย่างเช่น คดีหมิ่นประมาทออนไลน์ ที่เห็นได้ชัดเจน จึงสันนิษฐานว่ายังมีปัจจัยการไร้ตัวตนอื่นประกอบ นั่นคือยังมีการหลุดคดีหรือถูกยกฟ้องเมื่อไม่มีการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีให้ถึงที่สุดจนถูกลงโทษอาญา อาชญากรรมประเภทนี้แทบจะหมดไป อย่างเช่น คดีแก๊งค์คอลเซ็นเตอร์ จึงยกเอาการรวบรวมพยานหลักฐานดิจิทัลมาเป็นปัจจัยการไร้ตัวตนในการตัดสินใจของอาชญากรไซเบอร์อีกปัจจัยหนึ่ง

ยกเว้น อาชญากรที่มีข้อมูลไม่เพียงพอ ไม่ทราบว่าการตัดสินใจประอบอาชญากรรมบนเทคโนโลยีนี้จะถูกจับกุมได้ และรวบรวมพยานหลักฐานเอาผิดทางอาญาได้ อาชญากรจึงไม่ Rationale

5. สมมติฐานทางวิจัย (Research hypothesis) ในดุษฎีนิพนธ์นี้คือ

“การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน”

เมื่อตั้งโจทย์ว่า อาชญากรไซเบอร์มีการตัดสินใจเลือกอย่างเป็นเหตุและเป็นผล บนความเชื่อจากข้อมูลที่ได้รับเกี่ยวกับปัจจัยการไร้ตัวตน (Anonymous Factor) โดยมีความมุ่งมั่นปรารถนาที่จะหาอรรถประโยชน์สูงสุดแก่ตนตลอดเวลา

เมื่ออาชญากรไซเบอร์พบว่าเทคโนโลยีใดมีปัจจัยการไร้ตัวตน อาชญากรจะตัดสินใจเลือกลงมือประกอบอาชญากรรมไซเบอร์ทันที

ดังนั้น “การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน” ตามสมมติฐานการวิจัย

6. ทฤษฎีเกม (Game Theory)

ทฤษฎีเกมเป็นเครื่องมือที่ใช้ในการวิจัยกระบวนการตัดสินใจของอาชญากรไซเบอร์ ในดุษฎีนิพนธ์นี้ โดยเริ่มต้นจากอาชญากรจะเลือกพิจารณากลยุทธ์ว่าเทคโนโลยีนั้นมีปัจจัยไร้ตัวตนหรือไม่ก่อนลงมือก่ออาชญากรรม

ครั้งแรกผู้วิจัยไม่ค่อยมั่นใจว่าจะได้ผลลัพธ์สอดคล้องหรือไม่ และจะวิเคราะห์ไปได้ไกลเพียงใด แต่ในที่สุดก็สามารถใช้ทฤษฎีเกมทั้ง Decision Tree, Payoff Matrix และ Payoff Function อธิบายการตัดสินใจลงมือก่ออาชญากรรมเมื่ออาชญากรคิดอย่างเป็นเหตุเป็นผล และพบว่า “การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน” สอดคล้องตามสมมติฐานการวิจัย

จากนั้นเมื่อสังเกตเห็นสมการ Payoff Function มีการเปลี่ยนแปลงตามปัจจัยการไร้ตัวตน แม้ไม่สามารถพิสูจน์จากสถิติได้เนื่องจากข้อมูลไม่เพียงพอ จึงทำได้เพียงแค่พยายามเข้าใจปรากฏการณ์ และอาจจะสามารถนำมาใช้อธิบายปรากฏการณ์ในสังคมได้ว่า อาชญากรรมไซเบอร์ประเภทนั้นๆ อยู่ในสถานะใดในขณะนั้น ควรเฝ้าระวังมากน้อยเพียงใด ปัญหาที่ยังแก้ไขไม่ได้คืออะไร หรือจะควบคุมอย่างไร

โดยตั้งเป็นมโนทัศน์ที่ช่วยพยายามอธิบายด้วยการนำรูปแบบ ฟังก์ชันเอ็กโปเนนเชียล มาใช้ประกอบการอธิบายความสัมพันธ์ของอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน เป็นรูปแบบจำลองสถานการณ์แนวโน้มการเกิดอาชญากรรมไซเบอร์ในแต่ละเทคโนโลยี ซึ่งช่วยให้พอเข้าใจสถานการณ์ได้อย่างดี และผู้วิจัยเชื่อว่าเป็นการบุกเบิกงานวิชาการที่น่าสนใจให้ผู้วิจัยรุ่นต่อไปได้ทำวิจัยเพิ่มเติม

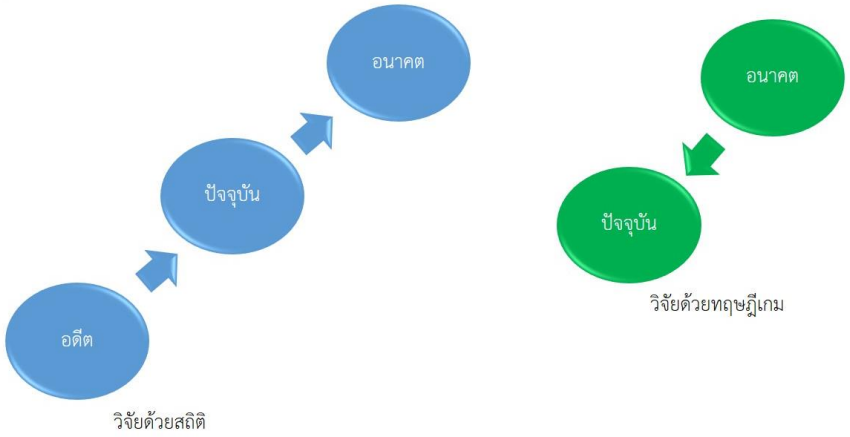
5.2 บทสรุประเบียบวิธีวิจัย

การวิจัยอาชญากรรมไซเบอร์ เป็นงานวิชาการที่มีความสลับซับซ้อนสูงมาก และเมื่อได้ลงมือปฏิบัติแล้วพบว่า ไม่สามารถใช้ระเบียบวิธีวิจัยเชิงปริมาณ และเชิงคุณภาพแบบปกติทั่วไปมาปรับใช้ได้ โดยเฉพาะการวิจัยทางสถิติ นอกจากมีข้อมูลที่เป็นข้อเท็จจริง (Facts) อาชญากรรมไซเบอร์น้อยมาก ยังขาดแคลนข้อมูลสถิติอาชญากรรมไซเบอร์ที่น่าเชื่อถือ เพราะในประเภทคดีเดียวกันแต่ละหน่วยงานอาจเก็บข้อมูลต่างกัน การเคลื่อนไหวของข้อมูลสถิติอาชญากรรมไซเบอร์ยังไม่เสถียร เช่น จับกุมแล้วปล่อยหรือฟ้องแล้วยกฟ้องหรือยกเลิกการเผยแพร่ข้อมูลสถิติ ฯลฯ ทำให้ผู้วิจัยต้องเปลี่ยนรูปแบบการวิจัยเชิงปริมาณมาให้ความสำคัญกับการวิจัยเชิงคุณภาพ แต่แล้วก็ประสบปัญหาการให้ความร่วมมือในการให้ข้อมูลหรือการให้สัมภาษณ์เพื่อการวิจัยจากอาชญากร ซึ่งให้ความสำคัญกับความลับเป็นสำคัญ

ผู้วิจัยจึงปรับตัว ด้วยการออกแบบวิธีวิจัย (Research design) ให้มีความใหม่ และยืดหยุ่นต่อสถานการณ์ โดยไม่เสียหลักการวิจัยเชิงคุณภาพ จึงใช้เวลาค้นคว้าศึกษานาน ทั้งงานวิจัยในประเทศไทยและต่างประเทศ รูปแบบการวิจัยดุษฎีนิพนธ์ต่างๆ ที่มีความเหมาะสมกับภววิสัย (Ontology) ที่ต้องการจะศึกษาวิจัย โดยเฉพาะการศึกษาวิจัยที่มีข้อมูลเชิงปริมาณน้อยมาก ผู้วิจัยจึงได้พบ “ทฤษฎีเกม” ที่ได้นำเสนอความก้าวหน้าในการวิจัยค้นหาความรู้และทดลองกระบวนทัศน์ใหม่ในการวิจัยทางด้านเศรษฐศาสตร์พฤติกรรม (รางวัลโนเบล) ซึ่งแตกต่างจากการวิจัยแบบนิรนัย (Deductive Method) ที่ใช้ข้อมูลเชิงปริมาณอย่างสถิติหรือแบบสอบถามเป็นเครื่องมือสำคัญในการค้นหาคำตอบการวิจัย แต่เมื่อสถานการณ์ไม่เหมาะสม ผู้วิจัยจึงปรับวิธีวิจัยให้เป็นแบบอุปนัย (Inductive) เพื่อให้เข้ากับบริบท ด้วยเป้าหมายที่ต้องการจะอธิบาย และทำนายปรากฏการณ์อาชญากรรมไซเบอร์ที่จะป้องกันไม่ให้มีเหยื่อรูปแบบใหม่เกิดขึ้นเลย

“ทฤษฎีเกม” ผู้วิจัยพบว่า แท้จริงแล้วเป็นเครื่องมือสำคัญที่สุดอย่างหนึ่งของนักอาชญาวิทยาที่จะนำมาใช้อธิบายความสัมพันธ์ของปรากฏการณ์ได้ดี และนำมาใช้เป็นอัลกอริธึมพยากรณ์ปรากฏการณ์อาชญากรรมในสังคมได้ จึงนำมาทดลองบุกเบิกเป็นวิธีวิจัยในดุษฎีนิพนธ์นี้ เพื่อเปิดโอกาสให้นักวิจัยทางอาชญาวิทยารุ่นใหม่ใช้เป็นกระบวนทัศน์ทางเลือก (Alternative Paradigm) ระเบียบวิธีที่ใช้ในการวิจัยเพื่อให้ได้พบความรู้ใหม่ๆ อีกมากมาย

การจะพยากรณ์หรือทำนายอนาคตอาชญากรรมใหม่ๆ ไม่อาจใช้ข้อมูลสถิติมาเป็นเครื่องมือได้เสมอไป นอกจากนั้นแล้วการจะมีสถิติเกิดขึ้นได้ ต้องมี “เหยื่อ” เกิดขึ้นก่อน ซึ่งเป้าหมายสูงสุดของนักอาชญาวิทยา คือ “ไม่ต้องการให้มีเหยื่อเกิดขึ้นเลย” ดังนั้นการจะทำนาย และพยากรณ์ปรากฏการณ์อาชญากรรมที่จะเกิดขึ้นใหม่ในสังคม โดยเฉพาะเทคโนโลยีหรือนวัตกรรมใหม่ จึงต้องเปลี่ยนกระบวนทัศน์ค้นหาวิธีวิจัยทางเลือก และทฤษฎีเกมช่วยให้นักอาชญาวิทยาจะทราบคำตอบได้ว่าอาชญากรจะตัดสินใจอย่างไร เมื่อมีปัจจัยใหม่ในการประกอบอาชญากรรมเกิดขึ้น



รูปที่ 72 การพิจารณากระบวนทัศน์ทางเลือกของผู้วิจัยระหว่างการใช้สถิติและทฤษฎีเกม

ทฤษฎีเกม เป็นกระบวนทัศน์ทางเลือกในการวิจัย โดยงานวิจัยนี้เริ่มต้นจาก จอน เอลสเตอร์ เชื่อว่าต้นตอของโครงสร้างในสังคมตามแนวคิดโครงสร้างนิยม (Structuralism) นั้น อธิบายความสัมพันธ์ทางสังคมว่ามนุษย์เป็นตามโครงสร้างสังคม แต่แท้จริงแล้วรากฐานของโครงสร้างสังคมมาจากการตัดสินใจของปัจเจกชนอันเป็นเหตุเป็นผลแล้วค่อยก่อเป็นโครงสร้างสังคม

ดุษฎีนิพนธ์นี้ จึงกลับไปที่จุดเริ่มต้นในกระบวนการตัดสินใจ (Decision making) ประกอบอาชญากรรมของอาชญากรไซเบอร์ แม้ไม่ได้เกิดจากผลการสำรวจหรือแบบสอบถาม แต่เกิดจากการสังเกตปรากฏการณ์กรณีศึกษาต่างๆ เป็นสิ่งที่ถูกสร้างขึ้นผ่านสายตาผู้วิจัย (Reality is constructed) ด้วยวิธีวิจัยเชิงปรากฏการณ์วิทยา (Phenomenological approach) และกรณีศึกษา (Case study approach) เป็นฐานข้อมูลในการตั้งคำถามวิจัย โดยศึกษากระบวนความคิดอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์ในการตัดสินใจลงมือก่ออาชญากรรม

จึงได้ออกแบบวิธีวิจัยแบบยืดหยุ่นผสมผสานด้วยแนวทางแบบอุปนัย (Inductive) ไม่ตั้งสมมติฐานการวิจัยล่วงหน้าหรือกำหนดตัวแปรเป็น Guideline ตั้งแต่ต้น แต่จะเก็บรวบรวมข้อมูล (เท่าที่หาได้ในเวลานั้น) มาวิเคราะห์ข้อมูลเชิงคุณภาพ มาตีความเบื้องต้น จากนั้นจึงค่อยตั้งสมมติฐานการวิจัย แล้วใช้ทฤษฎีเกมพัฒนาแบบจำลองความคิด (Rational Choice-Decision Conceptual Model) เป็นรูปแบบความสัมพันธ์ระหว่างทางเลือกในการตัดสินใจ ที่ทำให้อาชญากรตัดสินใจก่ออาชญากรรม อาทิเช่น Decision tree, Payoff Matrix และ Payoff function แล้วนำข้อสรุปไปสู่การอุปนัยสร้างเป็นข้อเสนอทฤษฎีบท (Proposition) ที่สามารถมีพลังในการ บรรยาย อธิบาย ทำนาย อาชญากรรมไซเบอร์ ได้ครอบคลุม และสามารถใช้เป็นแนวทางคาดคะเนอนาคตว่าเทคโนโลยีใด จะมีโอกาสเกิดอาชญากรรมไซเบอร์อย่างสูง เพื่อหาทางควบคุมปรากฏการณ์ไม่ให้เกิดอาชญากรรมไซเบอร์ดังกล่าวในสังคมได้

ดุษฎีนิพนธ์นี้ จึงใช้ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory) ซึ่งเป็นทฤษฎีสำคัญทางอาชญาวิทยา และสังคมศาสตร์ โดยเฉพาะงานของ จอน เอลสเตอร์ (ไชยยันต์ ไชยพร, 2560) เป็นฐานคิดสำคัญในการนำมาประกอบการวิจัยมาใช้เริ่มต้นค้นหากระบวนการตัดสินใจทางเลือกของอาชญากรในการตัดสินใจประกอบอาชญากรรมไซเบอร์ โดยใช้ทฤษฎีเกมเป็นเครื่องมือในการวิเคราะห์ “การตัดสินใจ” เมื่ออาชญากรไซเบอร์ มีการคิดอย่างเป็นเหตุเป็นผล

5.3 ข้อเสนอแนะการทดสอบสมมติฐานทางสถิติ (Statistical hypothesis)

ดังที่กล่าวมาว่าดุษฎีนิพนธ์นี้มีข้อมูลทางสถิติไม่เพียงพอ จึงใช้วิธีคิดย้อนกลับมา แต่ถ้าหากในอนาคตมีข้อมูลทางสถิติอาชญากรรมไซเบอร์เพียงพอ ผู้วิจัยเสนอแนะให้นักวิจัยทดสอบสมมติฐานทางสถิติ (Statistical hypothesis) ว่า “การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน” อย่างไร และทดสอบ “แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์เป็น Shark fin curve” ว่าเป็นจริงหรือไม่? และจะมีลักษณะอย่างไรโดยเปรียบเทียบกับวิธี Auto regression model ว่าจะสอดคล้องอย่างวิธี Backward induction ที่ใช้ทฤษฎีเกมดำเนินการวิจัยมาดังในดุษฎีนิพนธ์นี้หรือไม่

การตั้งสมมติฐานทางสถิติเพื่อหาความสัมพันธ์ระหว่างการเกิดอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน หากมีสถิติอาชญากรรมไซเบอร์ที่มีจำนวนมากพอ แล้วอาชญากรไซเบอร์ให้ความร่วมมือในการวิจัย อาจเริ่มต้นด้วยการหาความสัมพันธ์แบบ Correlation ระหว่างการเกิดอาชญากรรมไซเบอร์กับการไร้ตัวตน ว่ามีความสัมพันธ์ได้ ด้วยการหาสหสัมพันธ์อย่างง่าย (Simple Correlation)

สหสัมพันธ์อย่างง่าย (simple correlation) เป็นการศึกษาถึงความสัมพันธ์ระหว่างตัวแปร 2 ตัว ในลักษณะของความสัมพันธ์สมการเชิงเส้น ว่า X กับ Y มีความสัมพันธ์กันอย่างไร มากน้อยเพียงใด โดยใช้ค่าสัมประสิทธิ์สหสัมพันธ์ (coefficient of correlation) จากกลุ่มตัวอย่าง ซึ่งเป็นค่าที่ใช้วัดระดับความสัมพันธ์ระหว่างตัวแปร 2 ตัว แล้วจึงอนุมานเป็นความสัมพันธ์ของประชากร ว่ามีขนาดและทิศทางของความสัมพันธ์อย่างไร

โดยการตั้งสมมติฐานทางสถิติในดุษฎีนิพนธ์นี้คือ

“อาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตนเป็นกราฟของสมการ เอ็กซ์โปเนนเชียล”

$H0 : y = kx$

$H1 : y \neq kx$

การกำหนดตัวแปรในการวิจัย

ได้กำหนดกรอบแนวคิดการวิจัยจากการศึกษาปรากฏการณ์ต่างๆ มากำหนดตัวแปร 3 ตัว เพื่อนำมาสร้างความสัมพันธ์ ดังนี้

ตัวแปรต้น (Li) คือ นับปีที่เกิดอาชญากรรมไซเบอร์ประเภทนั้น

ตัวแปรตาม (y) คือ แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้น

ตัวแปรควบคุม (k) คือ ปัจจัยการไร้ตัวตน (Anonymous Factor)

ตัวแปรตาม เปลี่ยนแปลงตามตัวแปรต้น โดยมีตัวแปรควบคุม กำหนดอัตราการเพิ่มขึ้นหรือลดลงของตัวแปรตาม ตามสมมุติฐานทางสถิติ

โดยพิจารณาสหสัมพันธ์ด้วยการดูลักษณะความสัมพันธ์ของข้อมูลหรือตัวแปร สามารถทำได้ 2 วิธี คือ แผนภาพการกระจายข้อมูล (scatter diagram) และ การหาค่าสัมประสิทธิ์สหสัมพันธ์ (correlation coefficient) ในการวิจัยนี้ประสบปัญหาการขาดข้อมูลสถิติ จึงพิจารณาสหสัมพันธ์จากแผนภาพการกระจายข้อมูลทั้งเชิงปริมาณและคุณภาพเท่าที่ศึกษามาได้ โดยพิจารณาดังนี้

กำหนดให้ ρ คือ สัมประสิทธิ์สหสัมพันธ์อย่างง่าย เมื่อ $-1 \leq \rho \leq 1$ เนื่องจากในการวิเคราะห์สหสัมพันธ์ ไม่ได้เก็บข้อมูลจากประชากรแต่เป็นการเก็บข้อมูลจากกลุ่มตัวอย่าง ดังนั้น ค่าสัมประสิทธิ์ที่ได้ จึงเป็นค่าสัมประสิทธิ์สหสัมพันธ์อย่างง่ายของตัวอย่าง โดยใช้สัญลักษณ์ ว่า r เมื่อ $-1 \leq r \leq 1$

สูตรในการคำนวณหาค่า r คือ $\frac{\sum xy - n\bar{x}\,\bar{y}}{\sqrt{\sum(xi^2 - n\bar{x}^2)}\,\sqrt{\sum(yi^2 - n\bar{y}^2)}}$

เมื่อ n = จำนวนตัวอย่าง

$\bar{x}$ = ค่าเฉลี่ยของตัวแปร x

$\bar{y}$ = ค่าเฉลี่ยของตัวแปร y

ความหมายของค่า r

1. ค่า r เป็น + แสดงว่า x กับ y มีความสัมพันธ์ในทิศทางเดียวกัน
2. ค่า r เป็น – แสดงว่า x กับ y มีความสัมพันธ์ในทิศทางตรงกันข้าม
3. ค่า r เป็น 0 แสดงว่า x กับ y ไม่มีความสัมพันธ์กันเลย
4. ค่า | r | มีค่าเข้าใกล้ 1 แสดงว่า x กับ y มีความสัมพันธ์กันมาก
5. ค่า | r | มีค่าเข้าใกล้ 0 แสดงว่า x กับ y มีความสัมพันธ์กันน้อย

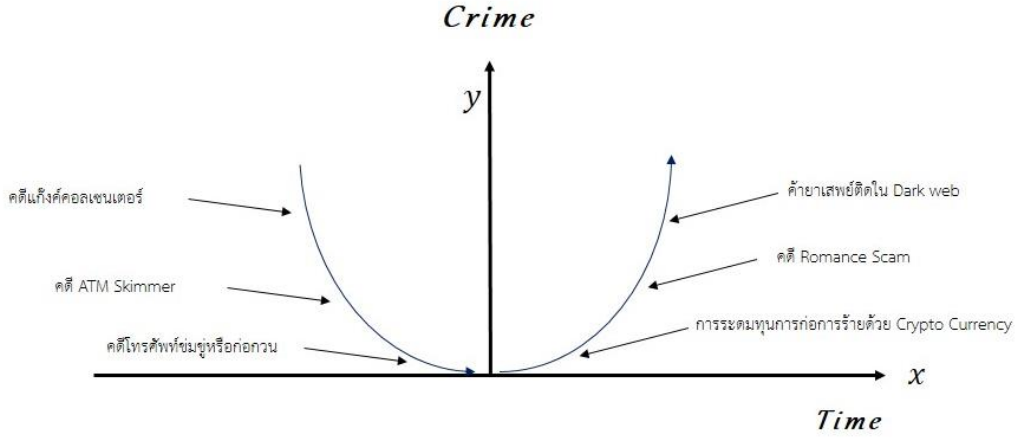
ค่าสัมประสิทธิ์การตัดสินใจ (Coefficient of Determination) เป็นค่าที่แสดงว่าตัวแปร x มีอิทธิพลต่อตัวแปร y มากน้อยเพียงใด โดยที่ค่าสัมประสิทธิ์การตัดสินใจ มีค่าเท่ากับ กำลังสองของสัมประสิทธิ์สหสัมพันธ์ หรือ r^2 โดยที่ $0 \leq r^2 \leq 1$

5.4 ข้อเสนอแนะ

อาชญากรจะค้นหาโอกาสตลอดเวลาเพื่อประกอบอาชญากรรมไซเบอร์ อาชญากรจะค้นคว้าสืบหาข้อมูลใหม่ๆ ทางไซเบอร์เทคโนโลยีอยู่เสมอ จนกระทั่งเกิดมีไซเบอร์เทคโนโลยีใหม่ขึ้นมาในสังคม และมีปัจจัยการไร้ตัวตนครบ ทั้งการซ่อนเร้นหลบพ้นจากการสืบสวนจับกุม และไม่มีโอกาสการรวบรวมพยานหลักฐานดิจิทัลเพียงพอในการดำเนินคดี อาชญากรจะลงมือประกอบอาชญากรรมทันที และจะใช้ไซเบอร์เทคโนโลยีนั้นต่อไปเรื่อยๆ จนกว่าไม่มีใครรอดพ้นจากการดำเนินคดีได้

ข้อเสนอทฤษฎีบท (Proposition or Theorem)

“เมื่อมีไซเบอร์เทคโนโลยีใหม่เกิดขึ้นในสังคม และมีปัจจัยการไร้ตัวตน อาชญากรไซเบอร์จะลงมือก่ออาชญากรรมทันที”



รูปที่ 73 ข้อเสนอทฤษฎีบท

หากเทคโนโลยีใดมีการไร้ตัวตนมาก โอกาสในการเกิดอาชญากรรมก็มากตาม หากเทคโนโลยีใดไม่มีการไร้ตัวตน สามารถระบุตัวตน (Identify) ทุกคนได้ โอกาสในการเกิดอาชญากรรมไซเบอร์ย่อมจะน้อยลง หากการตัดสินใจเป็นไปตามทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล

5.5 ข้อเสนอแนะเชิงนโยบายและกฎหมาย

รัฐไม่เคยมีการชั่งน้ำหนักหรือประเมินผลกระทบ (Cyber assessment) เมื่อมีเทคโนโลยีใหม่เกิดขึ้นในสังคมว่า ผลดีและผลเสียที่จะเกิดขึ้น มีอย่างไรบ้าง และอะไรมีมากกว่ากัน คุ้มค่าหรือไม่ที่จะปล่อยออกสู่สังคม ทำให้ส่วนใหญ่เกิดเหยื่อขึ้นแล้วจึงค่อยรับรู้ นั่นหมายความว่ามีผู้เสียหายเกิดขึ้นซ้ำแล้วซ้ำเล่าเรื่อยๆ จนข่าวสารค่อยๆ แพร่กระจายไปถึงรัฐเป็นคนสุดท้าย จึงค่อยรับทราบเหตุ และค่อยมาร่างกฎหมายหรือออกนโยบาย ซึ่งภารกิจสำคัญของนักอาชญาวิทยาคือการป้องกันไม่ให้มีเหยื่อเกิดขึ้นเลย โดยเฉพาะอาชญากรรมไซเบอร์ที่มีไซเบอร์เทคโนโลยีใหม่ๆ เกิดขึ้นทุกๆ วัน และอาชญากรรมรูปแบบใหม่ก็ไล่ตามมากขึ้นทุกวันจนนิยามประเภทอาชญากรรมแทบไม่ทัน

5.5.1 นโยบายป้องกันการไร้ตัวตน (There's No Anonymity policy)

ข้อเสนอแนะเชิงนโยบายในวิทยานิพนธ์นี้เห็นว่า รัฐควรทำ Cyber technology impact assessment ก่อนปล่อยเทคโนโลยีไซเบอร์ใหม่เข้าสู่สังคม และควรจะทำในทุกๆ เทคโนโลยี โดยเฉพาะการออกนโยบายระบุตัวตนป้องกันการไร้ตัวตน คู่ขนานไปด้วย

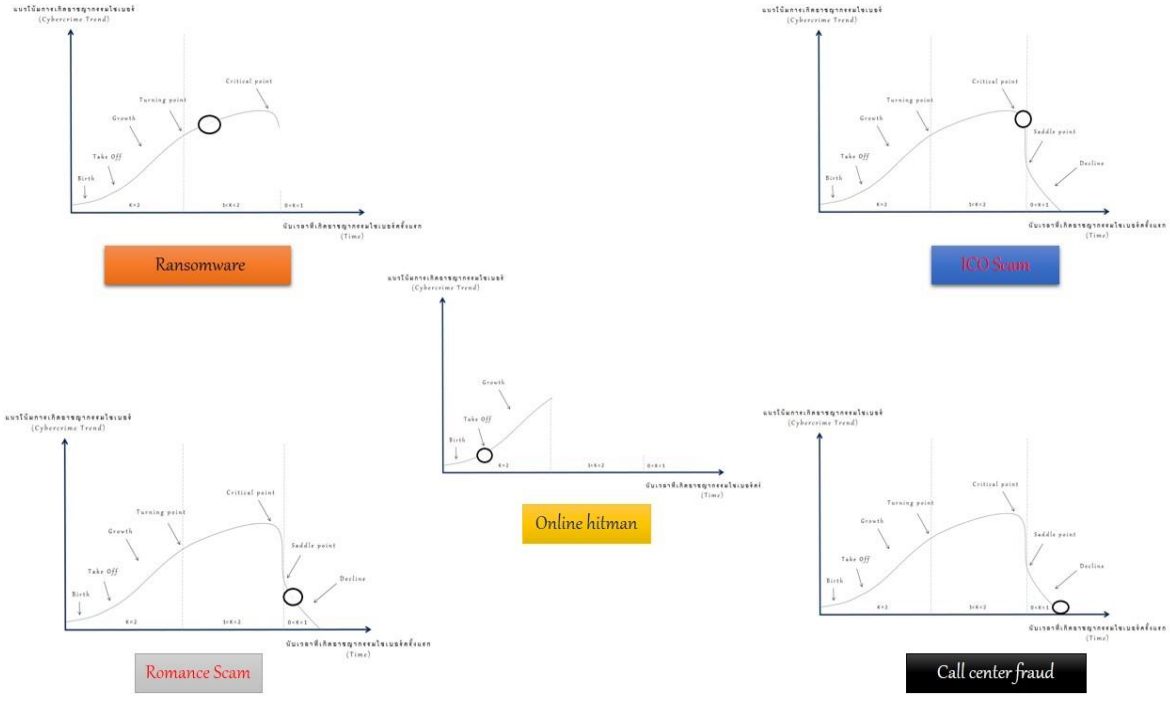
จะเห็นได้ว่า เฟซบุ๊ค (facebook) ได้ตระหนักถึงความสำคัญดังกล่าว ได้มีนโยบายปิดกั้นบัญชีผู้ใช้ที่ไม่แน่ใจว่า เป็นบุคคลจริงหรือเป็นบัญชีปลอมของอาชญากรที่ใช้สร้างความวุ่นวายและความเสียหายต่อสังคม

รถยนต์ก็ต้องมีทะเบียน ปืนก็ต้องมีทะเบียน การใช้งานเทคโนโลยีต่างๆ ก็ควรมีการระบุตัวตนลงทะเบียน โดยเฉพาะเลขหมาย IP ก็จำเป็นต้องมีทะเบียนประจำตัวบุคคล การบริหารจัดการ IP Address ก็เป็นเรื่องใหญ่ไม่แพ้กันที่รัฐควรออกมาตรการบริหารจัดการ ทั้งในแง่การจัดโซนพื้นที่เลขหมาย IP ทั้งการลงทะเบียนระบุตัวตน เลขหมาย IP และการสืบหาเลขหมาย IP ต้องทำได้ง่าย เมื่อการระบุตัวตนเกิดขึ้น การไร้ตัวตนหายไป อาชญากรรมไซเบอร์จะลดลง เพราะด้วยการชั่งน้ำหนักความเป็นเหตุเป็นผลของอาชญากรในการตัดสินใจประกอบอาชญากรรมเห็นว่า ลงมือกระทำไปก็ถูกจับกุมได้ง่าย และถูกดำเนินคดีได้ง่าย

5.5.2 Cybercrime war room

ตำรวจหรือรัฐ ควรมีระบบเทคโนโลยีสารสนเทศที่เฝ้าติดตามสถานการณ์อาชญากรรมไซเบอร์ทุกประเภทในสังคม (Monitoring system) ที่มิใช่เป็นเพียงข้อมูลคดีหรือสถิติคดีเท่านั้น แต่ต้องมีการประยุกต์ใช้นำข้อมูลคดีและสถิติมาประมวลผลใช้อย่างมีประสิทธิภาพให้สูงที่สุด อาจเปิดเผยให้ประชาชนติดตามเฝ้าระวังพร้อมไปด้วย และอาจเป็นเครื่องมือสำคัญในการชี้วัดผลการปฏิบัติงานของตำรวจ และรัฐบาล

จากแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) เป็นต้นแบบที่สามารถนำมาพัฒนาประยุกต์ใช้ได้อย่างดี และ Anonymous factors ในดุษฎีนิพนธ์นี้ ก็คือ อัลกอริธึม (Algorithm) ในระบบเทคโนโลยีปัญญาประดิษฐ์ที่จะนำมาใช้ในการประมวลผลข้อมูล โดยแสดงให้เห็นภาพได้ดังนี้



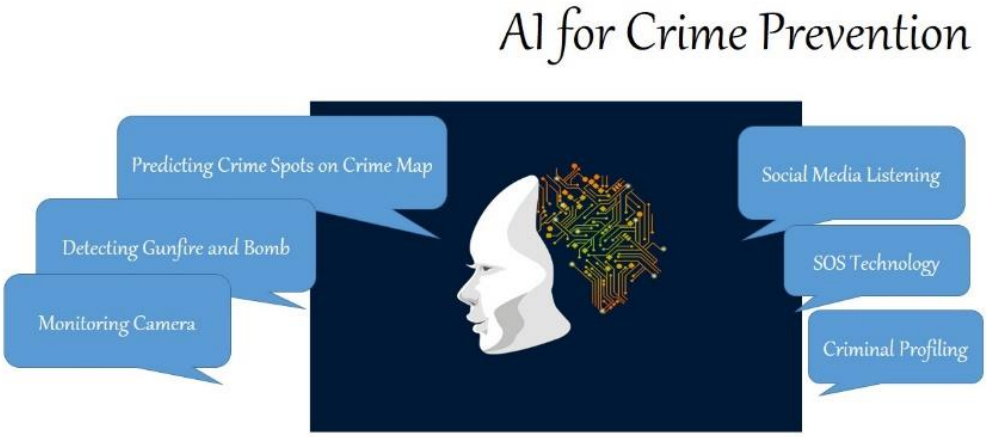
รูปที่ 74 ต้นแบบจอแสดงผลระบบเทคโนโลยีสารสนเทศที่คอยเฝ้าติดตามสถานการณ์อาชญากรรมไซเบอร์ทุกประเภทในสังคม (Monitoring system)

รูปที่ 75 War room ของ National Control Defense Center ประเทศรัสเซีย

ที่มา https://www.armyupress.army.mil/special-topics/world-hot-spots/russia/

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีหรือตำรวจไซเบอร์ ควรจะมีห้องปฏิบัติการแบบ War room คล้ายรูปที่ 75 และควรมีระบบติดตามสถานการณ์อาชญากรรมไซเบอร์ทุกประเภท ที่มีการแสดงผลคล้ายรูปที่ 74 บอกแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) แต่ละประเภทอยู่ในสถานการณ์ใด และอาชญากรรมไซเบอร์ประเภทใดควรเร่งดำเนินการ อาทิเช่น Online hitmanอยู่ในช่วง take off อาชญากรรมไซเบอร์ประเภทนี้ควรเร่งสืบสวนติดตาหามาตรการแก้ไขโดยด่วน หรือคดี ICO Scam อยู่ในสถานะแนวโน้มคดีลดลงแล้วหรือคดีแก๊งคอลเซ็นเตอร์ มีแนวโน้มจะเกิดขึ้นอีกแล้ว เป็นต้น

ส่วนในภาพรวมการแก้ไขปัญหาอาชญากรรมในสังคมรัฐหรือตำรวจต้องนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial intelligence) มาร่วมช่วยปฏิบัติงานจึงจะมีประสิทธิภาพสูงสุด เช่น AI for Crime Prevention นอกจากมีแผนที่อาชญากรรม (Crime map) ที่ระบุสถิติการเกิดอาชญากรรมแต่ละพื้นที่ในแต่ละปี ยังช่วยทำนายการเกิดอาชญากรรมในแต่ละเดือนหรือสัปดาห์ให้เจ้าหน้าที่สามารถยังมีระบบ Criminal profiling เชื่อมต่อกล้องวงจรปิดวิเคราะห์ใบหน้า พฤติกรรมผู้ต้องสงสัย ระบบตรวจจับเสียงปืนเสียงร้องขอความช่วยเหลือ ตลอดจน Social listening ที่เชื่อมต่อ Social media จะช่วยสามารถวิเคราะห์ความคิดเห็นหรือแนวโน้มผู้ที่มีแนวโน้มกำลังจะก่ออาชญากรรมมักโพสต์หรือแสดงความเห็นที่เป็นเบาะแส อาทิ กรณีจ่าคลั่งกราดยิงที่โคราช ได้โพสต์ Social media ที่แสดงแนวโน้มก่ออาชญากรรมหลายครั้ง



รูปที่ 76 เทคโนโลยีปัญญาประดิษฐ์ป้องกันอาชญากรรม

5.5.3 แก้ไขช่องโหว่กฎหมายประมวลกฎหมายวิธีพิจารณาความอาญา

ผู้วิจัยเห็นว่า กระบวนการยุติธรรมยังใช้กฎหมายเดิมที่บริบทต่างกันในอดีตและปัจจุบันมาใช้พิจารณาคดี โดยเฉพาะประมวลกฎหมายวิธีพิจารณาความอาญาที่ไม่ได้ปรับปรุงให้เข้ากับคดีเทคโนโลยีไซเบอร์สมัยใหม่ เช่น มาตรา 227 และผู้วิจัยเชื่อว่าในอนาคตนอกจากทนายความของอาชญากรจะพบช่องว่างทางกฎหมายแล้ว ปัจจัยการไร้ตัวตนจะทวีความซับซ้อนขึ้นจนไม่สามารถรวบรวมพยานหลักฐานเอาผิดอาชญากรไซเบอร์ได้เลย ดังนั้นควรบูรณการประมวลกฎหมายวิธีพิจารณาความอาญาความผิดทางเทคโนโลยีใหม่

ช่องโหว่ทางกฎหมายสามารถใช้ทฤษฎี การขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian) ช่วยในการสรุปผลได้ เพราะช่องโหว่ทางกฎหมายเป็นทั้งแรงจูงใจและเป็นโอกาสให้เกิดอาชญากรรมไซเบอร์เมื่ออาชญากรคิดคำนวณอย่างเป็นเหตุเป็นผล ซึ่งกฎหมายคือผู้พิทักษ์ในการให้ปกป้องสังคมด้วยการให้อาชญากรชั่งน้ำหนักความพึงพอใจกับความทุกข์ทรมานที่จะได้รับจากการกระทำผิดกฎหมาย ดังนั้นรัฐจึงต้องปรับปรุงกฎหมาย

5.5.4 ศาลชำนัญพิเศษการพิจารณาความอาญาความผิดทางเทคโนโลยี

ในการพัฒนากฎหมายทรัพย์สินทางปัญญา ซึ่งเป็นกฎหมายเกี่ยวข้องกับนวัตกรรม ได้มีการจัดตั้งศาลทรัพย์สินทางปัญญา ด้วยเห็นว่าลำพังผู้พิพากษาปกติที่จบทางด้านนิติศาสตร์มาโดยตรงอาจจะไม่มีความเข้าใจเทคโนโลยีเพียงพอ จึงให้มีผู้พิพากษาสมทบที่เป็นผู้เชี่ยวชาญด้านเทคโนโลยีอีก

2 ท่าน มาร่วมพิจารณาตัดสินข้อเท็จจริงในคดี และลงมติว่าถูกหรือผิด ส่วนผู้พิพากษาจะเป็นผู้กำหนดบทลงโทษ

หากพิจารณาแล้วจะเห็นว่า การกระทำความผิดอาญาความทางเทคโนโลยีใหม่ๆ หรืออาชญากรรมไซเบอร์ มีความยุ่งยากซับซ้อนกว่า การพิจารณาคดีของศาลทรัพย์สินทางปัญญามาก ดังนั้นควรมีการปรับกระบวนทัศน์การยุติธรรม แยกการพิจารณาคดีความผิดอาญาทางเทคโนโลยีใหม่ โดยจัดตั้งศาลชำนัญพิเศษการพิจารณาความอาญาความผิดทางเทคโนโลยี และให้มีผู้พิพากษาสมทบที่เป็นผู้เชี่ยวชาญด้านเทคโนโลยีมาร่วมพิจารณาตัดสินข้อเท็จจริงในคดี และลงมติว่าถูกหรือผิด ส่วนผู้พิพากษาจะเป็นผู้กำหนดบทลงโทษต่อไป

ทฤษฎีการขาดผู้พิทักษ์ที่มีความสามารถ (Lack of a capable guardian) ช่วยในการสรุปผลเป็นข้อเสนอแนะได้เช่นกัน เมื่อกระบวนการยุติธรรมก็คือผู้พิทักษ์ประชาชนในสังคมที่อ่อนแออีกประการ ซึ่งอาชญากรคิดคำนวณอย่างเป็นเหตุเป็นผลว่าความพึงพอใจกับความทุกข์ทรมานที่จะได้รับจากการกระทำผิดกฎหมายอย่างใดน้อยกว่ากัน ซึ่งถ้าหากกระบวนการพิจารณาคดีมีความรวดเร็วรุนแรง เที่ยงธรรม จะช่วยยับยั้งอาชญากรรมไซเบอร์ได้ดีขึ้น

5.5.5 การส่งเสริมให้แฮ็กเกอร์คุณธรรมเจาะระบบ

ผู้วิจัยเห็นว่า แฮ็กเกอร์คุณธรรม (White Hat Hacker) จำนวนมากคือผู้ที่จะมาช่วยปกป้องรักษาความปลอดภัยระบบคอมพิวเตอร์ให้รอดพ้นจากอาชญากร เมื่อพวกเขาพบช่องโหว่ของระบบคอมพิวเตอร์ที่สามารถบุกรุกเข้าไปได้ และเตือนให้ทราบถึงช่องว่างในการก่ออาชญากรรม นับเป็นประโยชน์ต่อการศึกษา และการทำข้อมูลอาชญากรไซเบอร์ ซึ่งพวกเขาต้องการเพียงชื่อเสียง และการยอมรับจากสังคมมากกว่าผลตอบแทน ภาครัฐ และเอกชนควรจะส่งเสริมในประเด็นนี้

ในต่างประเทศองค์กรเอกชนต่างๆ สามารถเปิดโอกาสให้ แฮ็กเกอร์คุณธรรมโจมตีระบบคอมพิวเตอร์ขององค์กรได้โดยไม่ผิดกฎหมาย และได้รับรางวัลตอบแทนอย่างสูงเรียกว่า Bug Bounty อาทิ ในสหรัฐอเมริกามีกฎหมาย The Computer Fraud and Abuse Act โดยวางหลักทั้งหมดด้วยถ้อยคำว่า “โดยไม่ได้รับอนุญาต” (Generally makes it illegal to access a computer without authorization) ดังนั้นถ้าองค์กรภาคเอกชนอนุญาตให้ก่ออาชญากรรมไซเบอร์ต่อระบบคอมพิวเตอร์ขององค์กรย่อมทำได้ไม่ผิดกฎหมาย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของไทย ก็สามารถอนุญาตให้เข้าสู่ระบบคอมพิวเตอร์ได้ แต่ไม่ได้รับการส่งเสริมเท่าที่ควร และเป็นที่เกรงกลัวโทษเพราะเป็นอาญา

แผ่นดินไม่สามารถยอมความได้มีทั้งโทษจำคุก และโทษปรับ หากองค์กรยอมให้ก่ออาชญากรรมไซเบอร์โดยยินยอมตั้งแต่แรก (มิใช่ยอมความภายหลัง) ย่อมกระทำได้ อาทิ

มาตรา 5 “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน” มาตราดังกล่าวนี้จะเห็นได้ว่าสามารถเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันและไม่ได้มีไว้สำหรับตน “โดยชอบได้” ถ้าเจ้าของระบบคอมพิวเตอร์อนุญาตให้เจาะระบบ

มาตรา 6 “ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผย**โดยมิชอบ**ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น” มาตราดังกล่าวนี้จะเห็นได้ว่าล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ผู้อื่น “โดยชอบได้” ถ้าเจ้าของระบบคอมพิวเตอร์อนุญาตให้เปิดเผยเฉพาะกรณี

มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน” มาตราดังกล่าวนี้จะเห็นได้เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันของผู้อื่น “โดยชอบได้” ถ้าเจ้าของระบบคอมพิวเตอร์อนุญาต และในอีกหลายๆ มาตราในพระราชบัญญัติฉบับนี้จะใช้ถ้อยคำว่า “โดยมิชอบ” ซึ่งถ้าหากองค์กรต่างๆ รณรงค์ส่งเสริมให้แฮ็กเกอร์คุณธรรมได้เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยชอบ แต่ปกปิดมาตรการป้องกันต่างๆ เพื่อให้แฮ็กเกอร์ได้ใช้ความสามารถถูกทาง จะเป็นประโยชน์กับทุกฝ่าย

5.5.6 เสรีภาพการไร้ตัวตนในโลกไซเบอร์

สิทธิ และเสรีภาพในโลกไซเบอร์ที่กำลังเป็นกระแสในปัจจุบัน (พ.ศ. 2564) คือ Crypto-Anarchy หรือแนวคิดอนาธิปไตยบนโลกไซเบอร์ (ไม่มีที่มานิยามทางการ เป็นความเข้าใจของผู้วิจัยที่ตีความจากเนื้อหาต่างๆ ในโลกไซเบอร์) นอกจากการปิดบังชื่อจริง ปิดบังตัวตนมิให้ใครรู้แม้กระทั่งเลขหมาย IP Address สร้างตัวตนปลอม (Avatar) ยังมีการเข้ารหัส (Encryption) ชั้นสูงในการปกปิดตัวตน เพื่อให้มีเสรีภาพในการแสดงความคิดเห็นทางการเมือง การปกครอง การวิพากษ์ และวิจารณ์อย่างที่ไม่มีใครรู้ว่าใครเป็นใครเป็นกลุ่มที่เรียกว่า Crypto-Anarchist ตลอดจนมีแนวความคิดต้องการมีธรรมนูญในโลกไซเบอร์ แยกจากโลกความจริง อย่างไรก็ตาม ผู้วิจัยมีข้อคิดเห็นดังนี้

ประการแรก รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 1 บัญญัติไว้ว่า “ประเทศไทยเป็นราชอาณาจักรอันหนึ่งอันเดียว จะแบ่งแยกมิได้” ดังนั้นภายในราชอาณาจักรไทยหากตีความบนโลกไซเบอร์จุดที่ข้อมูลคอมพิวเตอร์วิ่งผ่านเข้าออกบริเวณชายแดนราชอาณาจักรไทยก็คือ

Internet gateway ซึ่งโลกไซเบอร์ที่อยู่บนราชอาณาจักรไทยก็ไม่สามารถแบ่งแยกอำนาจอธิปไตยไปได้

ประการที่สอง การไร้ตัวตนของผู้ที่ไม่ประกอบอาชญากรรม ยังเป็นประเด็นที่น่าศึกษาข้อดีข้อเสียให้นักวิจัยรุ่นหลังได้ค้นคว้าต่อไป เพราะบางครั้งก็เป็นประโยชน์ต่อเหยื่อ หากเหยื่อไร้ตัวตนก็ช่วยให้รอดพ้นจากการคุกคาม การสะกดรอยตามออนไลน์ การตกเป็นเป้าหมายของอาชญากร และการไร้ตัวตนอย่างที่ชาว Crypto-Anarchist ปรารถนาในการใช้เสรีภาพแสดงความเห็น ผู้วิจัยเห็นด้วยว่าเป็นเรื่องดี อาจจะทำให้คนทั่วไปกล้าแสดงความคิดเห็นมากขึ้น และปลอดภัยมากขึ้น

ปัจจุบันมีผู้เข้าใจคลาดเคลื่อนเรื่องเสรีภาพแสดงความคิดเห็น (Freedom of expression) ไปมาก ทำให้เกิดคดีหมิ่นประมาทออนไลน์ (Online Defamation) และดูหมิ่นเกลียดชัง (Insult) พุ่งสูงไปทั่วโลก ซึ่งการวิพากษ์ (Criticize) และวิจารณ์ (Comment) กระทำได้ แต่มิใช่การหมิ่นประมาทหรือแสดงความดูหมิ่นเกลียดชังหรืออาฆาตมาดร้ายผู้ใด และเนื่องจากเป็นคดีอาญาที่มีโทษรุนแรง ส่งผลให้เด็กและเยาวชน ตลอดจนผู้ไม่เข้าใจขอบเขตของเสรีภาพการแสดงความคิดเห็นต้องตกเป็นจำเลย กระทบต่อการเรียน การทำงาน เมื่อต้องโทษอาญา และเป็นภาระต่องานยุติธรรมอย่าสูง

ผู้วิจัยเห็นว่าเสรีภาพของมนุษย์ในการไร้ตัวตนบนโลกไซเบอร์มีได้เมื่อเป็นไปด้วยความสุจริตตราบเท่าที่ไม่ไปละเมิดสิทธิผู้ใดและเมื่อการไร้ตัวตนไปละเมิดสิทธิผู้ใด อีกทั้งมีโทษอาญากำกับไว้ ผู้นั้นก็กลายเป็นอาชญากรไซเบอร์ตามนิยามในดุษฎีนิพนธ์นี้เช่นกัน

บรรณานุกรม

2000., Robert A. Reeves. (). Arlington National Cemetery. October 16. (2000). Colonel William F. Friedman (The godfather of Cryptology) "Knowledge is Power". (SANS Institute).

Guidance for a RISK-BASED approach, VIRTUAL CURRENCIES,, (2015).

Cohen, Lawrence E., & Felson. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*.

Development, ITU. (2012). *Understanding cybercrime: phenomena, challenges and legal response*: The ITU publication,.

Fairclough, N. . (1995). *Critical discourse analysis: the critical study of language. London: Longman*: New York: Longman.

Gottschalk, Petter. (2010). *Policing Cyber Crime*: Ventus Publishing ApS.

Handbook, MMC Cyber. (2018). *Perspectives on the next wave of cyber*: Marsh & McLennan Companies.

Kabay, M. E. (2008). *A Brief History of Computer Crime: An Introduction for Students. School of Graduate Studies*: Norwich University.

Li, Johannes Xingan. (2017). Cyber Crime and Legal Countermeasures:

A Historical Analysis. *International Journal of Criminal Justice Sciences (IJCJS) – Official Journal of the South Asian*

Society of Criminology and Victimology (SASCV), Vol. 12 (2): 196–207. doi:10.5281/zenodo.1034658

Lindeman, Tracey (Producer). (2014). A look back at Montreal's race-related 1969 Computer Riot. Retrieved from https://www.cbc.ca/news/canada/montreal/a-look-back-at-montreal-s-race-related-1969-computer-riot-1.2538765

Prisner, Erich. (2014). Game Theory through Examples. *The Mathematical Association of America*(2014 Washington, DC.).

Reeves, Robert A. (2000). Colonel William F. Friedman (The godfather of Cryptology) "Knowledge is Power". *Arlington National Cemetery*(SANS Institute).

Whiteside, Thomas. (1978). *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud* Ty Crowell Co.

ภาคผนวก

สถิติคดีอาชญากรรมไซเบอร์ในประเทศไทย

ข้อมูลสถิติจาก ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) เป็นหน่วยงานสังกัด สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (สพธอ.) มาศึกษา โดยตั้งข้อสังเกตว่าอาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) เนื่องจากมีจำนวนสถิติสูงที่สุด จึงเลือกเป็นกลุ่มตัวอย่างมาพิจารณาเป็นต้นแบบเพื่อตั้งสมมุติฐาน ดังนี้

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2554

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content							12	8	6	7	39	5	**77**
Availability							1	2	2	0	1	0	**6**
Fraud							44	38	56	69	66	36	**309**
Information gathering							28	13	18	14	12	8	**93**
Information security							0	0	0	0	0	0	**0**
Intrusion Attempts							9	20	19	19	16	11	**94**
Intrusion							0	0	0	0	0	0	**0**
Malicious code							6	10	14	7	18	8	**63**
Other							0	0	0	1	0	3	**4**
รวม							**100**	**91**	**115**	**117**	**152**	**71**	**646**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2555

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	1	0	0	0	1	0	0	0	0	**3**
Availability	0	1	0	0	0	0	0	0	1	0	0	0	**2**
Fraud	16	37	32	42	32	32	51	54	74	49	48	67	**534**
Information gathering	4	5	10	8	8	5	5	10	5	0	1	1	**62**
Information security	0	1	0	0	0	0	0	0	0	0	1	0	**2**
Intrusion Attempts	3	3	13	8	8	6	7	10	8	2	2	5	**75**
Intrusion	1	1	1	1	0	3	1	0	0	0	1	4	**13**
Malicious code	3	6	9	12	7	4	7	3	8	8	10	5	**82**
Other	4	5	3	2	1	2	2	0	0	0	0	0	**19**
รวม	**31**	**59**	**69**	**74**	**56**	**52**	**73**	**78**	**96**	**59**	**63**	**82**	**792**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2556

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	2	3	1	1	2	0	0	0	1	2	0	**13**
Availability	1	0	0	0	0	0	0	8	0	1	0	0	**10**
Fraud	36	48	49	56	78	56	110	53	53	54	59	42	**694**
Information gathering	3	0	0	0	0	2	0	0	0	3	0	0	**8**
Information security	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Intrusion Attempts	56	23	17	23	16	11	24	16	24	46	24	36	**316**
Intrusion	6	3	50	61	115	94	67	63	89	46	27	10	**631**
Malicious code	1	4	6	4	3	11	9	7	5	6	5	12	**73**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**104**	**80**	**125**	**145**	**213**	**176**	**210**	**147**	**171**	**157**	**117**	**100**	**1745**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2557

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	**8**
Availability	0	0	2	2	0	0	1	3	0	0	0	0	**8**
Fraud	59	68	69	72	145	85	94	66	98	88	101	62	**1007**
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	**29**
Information security	0	1	0	0	0	2	0	0	1	0	0	0	**4**
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	75	**504**
Intrusion	9	150	77	33	55	50	69	47	86	32	35	66	**709**
Malicious code	3	7	129	125	102	226	304	161	263	98	132	188	**1738**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**112**	**257**	**315**	**291**	**352**	**393**	**514**	**319**	**482**	**265**	**316**	**391**	**4007**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2558

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	2	0	0	0	0	2	0	0	0	2	1	1	**8**
Availability	0	0	0	0	0	0	0	0	0	0	1	5	**6**
Fraud	75	83	100	90	155	134	113	99	70	67	80	75	**1141**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	0	0	1	0	0	0	0	0	0	0	0	0	**1**
Intrusion Attempts	83	89	65	27	60	44	63	51	52	59	43	28	**664**
Intrusions	69	76	88	12	78	187	159	83	51	105	42	55	**1005**
Malicious code	104	83	174	143	140	209	192	97	143	119	92	50	**1546**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**333**	**331**	**428**	**272**	**433**	**576**	**527**	**330**	**316**	**352**	**259**	**214**	**4371**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2559

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Availability	0	0	0	0	0	0	0	0	0	0	0	29	**29**
Fraud	98	95	66	73	164	125	104	52	57	55	43	70	**1002**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	0	0	0	0	0	0	0	0	0	0	2	18	**20**
Intrusion Attempts	35	39	36	62	69	70	59	82	42	35	66	111	**706**
Intrusions	175	51	122	96	53	44	158	60	95	37	40	89	**1020**
Malicious code	97	123	80	104	168	167	49	14	78	30	89	21	**1020**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**405**	**308**	**304**	**335**	**454**	**406**	**370**	**208**	**272**	**157**	**240**	**338**	**3797**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2560

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Availability	100	218	212	0	0	9	1	0	0	0	0	0	**540**
Fraud	60	60	71	55	60	70	103	81	80	50	63	88	**841**
Information gathering	1	4	3	0	0	0	0	0	0	0	0	0	**8**
Information security	0	1	19	0	0	0	0	14	15	7	4	8	**68**
Intrusion Attempts	85	65	89	106	84	88	74	62	52	78	79	77	**939**
Intrusions	157	35	84	47	18	42	40	29	19	23	51	25	**570**
Malicious code	25	31	29	26	32	29	14	19	6	20	7	33	**271**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**428**	**414**	**507**	**234**	**194**	**238**	**232**	**205**	**172**	**178**	**204**	**231**	**3,237**

▾ สถิติภัยคุกคาม ประจำปี พ.ศ. 2561

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	1	0	0	0	0	0	0	0	0	**1**
Availability	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Fraud	78	73	84	60	82	84	86	87	61	94	66	74	**929**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	0	2	1	2	1	0	0	5	0	2	2	3	**18**
Intrusion Attempts	74	100	59	57	64	103	111	114	100	76	126	118	**1102**
Intrusions	56	43	33	48	25	19	30	16	32	15	15	3	**335**
Malicious code	13	8	12	3	19	10	14	7	11	4	15	11	**127**
Other	0	0	0	0	0	1	0	6	0	1	0	0	**8**
รวม	**221**	**226**	**189**	**171**	**191**	**217**	**241**	**235**	**204**	**192**	**224**	**209**	**2520**

▼ สถิติภัยคุกคาม ประจำปี พ.ศ. 2562

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	0	0	0	0	0	0	0	0	0	**1**
Availability	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Fraud	87	46	59	0	0	0	0	0	0	0	0	0	**192**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	39	0	0	0	0	0	0	0	0	0	0	0	**39**
Intrusion Attempts	78	90	62	0	0	0	0	0	0	0	0	0	**230**
Intrusions	12	10	24	0	0	0	0	0	0	0	0	0	**46**
Malicious code	20	8	13	0	0	0	0	0	0	0	0	0	**41**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**236**	**154**	**159**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**549**

ตารางที่ 1 ก ข้อมูลสถิติอาชญากรรมไซเบอร์ในประเทศไทยจาก พ.ศ.2554-2562

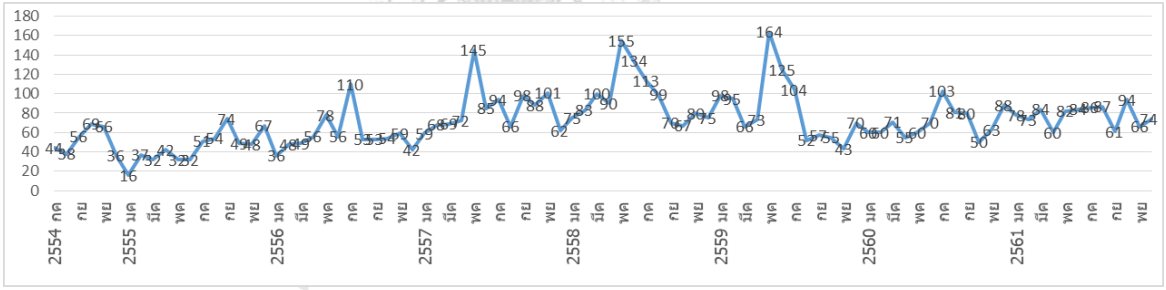
ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert)

ประชากร

กลุ่มประชากรที่เลือกมาเป็นต้นแบบการสังเกต คือ ข้อมูลสถิติอาชญากรรมไซเบอร์ประเภท **ฉ้อโกงออนไลน์ (Fraud)** ในประเทศไทยจากปี พ.ศ.2554-2561 ดังนี้

อาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) รวม	6,457 ครั้ง
ค่าเฉลี่ยอาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud)	71.74 ครั้งต่อเดือน
ส่วนเบี่ยงเบนมาตรฐานมีค่าเท่ากับ (Standard Deviation)	6,4153.124

ตารางที่ 3 ก ข้อมูลเชิงสถิติอาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) ในประเทศไทยจาก พ.ศ.2554-2561



รูปที่ 1 ก กราฟเชิงเส้นอาชญากรรมไซเบอร์ประเภท ฉ้อโกงออนไลน์ (Fraud) ในประเทศไทย จากข้อมูลสถิติรายเดือนตั้งแต่ปี พ.ศ.2554-2561

บทสัมภาษณ์เชิงลึก ระหว่างผู้วิจัย แฮ็กเกอร์คุณธรรม มอส นามสมมุติ (มีบันทึกเสียงเป็นหลักฐาน)

“น้องมอส” นามสมมุติ ผู้อ้างตนเป็นแฮ็กเกอร์คุณธรรม (White hacker) ที่ยินยอมให้สัมภาษณ์ทางโทรศัพท์ โดยไม่ให้พบตัวจริง จึงได้ทำการสัมภาษณ์แบบเชิงลึก โดยใช้บทสนทนาเป็นเครื่องมือ

แฮ็กเกอร์ หรืออาชญากรไซเบอร์ ส่วนใหญ่เป็นอาชญากรสมบูรณ์แบบ (Perfect criminal) ก่ออาชญากรรมแล้วไม่เคยถูกจับได้ และเบาะแสเพียงน้อยนิด ไม่ว่าจะ เพศ นามแฝง อายุ วิธีการ ฯลฯ อาจจะเป็นหนทางไปสู่การสืบสวนจับกุมได้ทั้งนั้น จึงเป็นเรื่องที่พวกเขาต้องอำพรางตัวตน

ผู้วิจัยได้สัมภาษณ์เชิงลึก แฮกเกอร์คุณธรรม (White hat) โดยไม่เคยพบตัวจริงมาก่อน ได้รับการติดต่อผ่านจากผู้ช่วยอาจารย์วิศวกรคอมพิวเตอร์ท่านหนึ่งแนะนำให้ และผู้วิจัยได้โทรศัพท์ไปบอกกล่าวขอบเขตการสัมภาษณ์ให้ทราบก่อน แล้วโทรกลับไปสัมภาษณ์จริงอีกครั้ง ในระหว่างสัมภาษณ์ทางโทรศัพท์ได้ขออนุญาตเปิดลำโพง และบันทึกเสียงไว้เป็นหลักฐานทางวิชาการ

มอส (นามสมมุติ) อายุ 28 ปี จบการศึกษาระดับปริญญาโทวิศวกรรมคอมพิวเตอร์มหาวิทยาลัยชั้นนำของไทย มีความสนใจคอมพิวเตอร์ตั้งแต่อายุ 4-5 ขวบ แต่เพื่อเล่นเกมส์คอมพิวเตอร์ ยังไม่ได้สนใจเรื่อง Cyber security จนกระทั่งอยู่ชั้นมัธยมปีที่ 1-2 ผู้วิจัยได้ถอดบทสัมภาษณ์ออกมาเป็นข้อความดังนี้

ผู้วิจัย: “งั้นช่วยเล่าประสบการณ์ในการ Hack หรือว่าเรื่อง Cyber security ตั้งแต่ ม.1 ม.2 ให้ฟังหน่อยครับว่าอะไร? เอ่อ...สนุกๆ หรือว่าอะไรน่าสนใจครับ เชิญเลยครับ”

มอส: “ตอนนั้นนะครับ ตอนนั้นยังเด็กอยู่ ตอนนั้นก็ยังเป็นเด็กแบบว่าเกรียนๆ หน่อยนึง ก็อยากรู้อยากลองประมาณนั้น ก็คือ ทำโปรแกรม พวกไวรัส บ้างประมาณนี้น่ะครับ แล้วก็ไปทำพวก Key logger พวกขโมยรหัสผ่านประมาณนี้อะครับ

ผู้วิจัย: “โอ้โห!!”

มอส: “เพราะว่าในตอนนั้น โรงเรียนผมอะครับ เขาจะ...อาจารย์เนี่ย จะตั้งรหัสผ่านให้กับนักเรียนเนี่ยใช้ นักเรียนจะใช้ WiFi จะเข้าได้แค่...จะเข้าเว็บได้ไม่ครบอะครับ ทีนี้ผมก็อยากว่า...ก็อยากเข้าเว็บที่ได้มากกว่าที่อาจารย์กำหนด ผมก็เลยทำ Key logger ไปฝังไว้ในเครื่องอาจารย์ แล้วเวลาอาจารย์พิมพ์ ก็จะส่งทั้ง Username และ Password กลับมาหาผม”

ผู้วิจัย: “ตั้งแต่ ม.1 ม.2 เลยนี่นะฮะ?!!”

มอส: “ใช่ครับ เพราะตั้งการได้รหัสผ่านของอาจารย์มา”

ผู้วิจัย: “แล้วรู้วิธีเขียนโปรแกรมทำ Key logger ได้ยังไง ตั้งแต่ยังเด็กขนาดนั้นครับ?

มอส: “อันนี้น่ะครับ มันจะมี...แต่ก่อนน่ะครับมันจะมีหนังสืออยู่เล่มนึง...มันก็นานแล้ว ผมก็จำหนังสือนั้นไม่ได้ละ มันเขียนด้วยภาษา ซี ครับ...ก็คือมันจะฝังไว้เฉยๆ....ผมก็ได้รหัสผ่านของอาจารย์มาเพื่อที่จะเข้าเว็บ อ่า...ที่มันนอกเหนือจากที่กำหนด ที่ลิมิตไว้ได้อะครับ”

ผู้วิจัย: “อ๋อครับๆ แล้วพอตอนที่เราทำได้นี่ครับ ดีใจไหมครับ? ตื่นเต้นยังไงไหมครับ”

มอส: “อ๋ออันนั้น...ดีใจตื่นเต้นมาก เพราะเราทำครั้งแรกเลย” น้ำเสียงหัวเราะกลั้วเบาๆ ฟังแล้วรู้สึกว่าดีใจ

ผู้วิจัย: “แล้วอาจารย์รู้ไหมครับ?”

มอส: “....มารู้ทีหลังครับว่าผมเป็นคนใช้...แต่อาจารย์เขาไม่ว่าอะไร...อาจารย์เขาเลยรู้เราอะ มีความสามารถทางด้านนั้นอะ อาจารย์ก็เลยส่งพวกไปแข่ง...ทักษะวิชาการประมาณนี้ครับ”

ผู้วิจัย: “โอ้! เยี่ยมเลยครับ โอเคครับ นั่นคือจุดเริ่มต้น...งั้นก็ขอทราบประสบการณ์ต่อๆ มาที่สำคัญๆ ที่สนุกๆ อีกครับ...ในการ Hack ในการเจาะระบบทำนองนี้ครับ” ผู้วิจัย

มอส: “....อ่า....ส่วนมากก็ประมาณก็ ส่วนมากจะเป็นพวกเปลี่ยนหน้าเว็บ ของ...โรงเรียน เว็บ อ่า....หน่วยงานต่างๆ เฉยๆ ครับ ก็เลยไม่ได้ทำอะไรที่มันสร้างความเสียหายมากอะครับ ตอนนั้นก็ยังเป็นเด็กอยู่ก็เลย...ความสามารถก็ยังไม่มากพอ ก็เลยเปลี่ยนหน้าเว็บเป็นรูปอื่นอะไรประมาณนี้อะครับ”

ผู้วิจัย: “อืม ครับๆ แต่ว่าหลักการก็รู้แล้วล่ะว่า เข้าไป Server ได้ก็เปลี่ยนได้ แต่ถ้าเข้าไประบบธนาคง ธนาคาร...” มอสพูดแทรกขึ้นมา

มอส: “ใช่ๆ ครับๆ ธนาคาร....มันเกิดจากการตั้ง Password ของผู้ดูแลระบบเอง เขาตั้ง Password ที่ไม่แข็งแรงประมาณนี้อะครับ ตั้ง Password ว่า Password ประมาณนี้อะครับ ก็เลยสุ่มๆ ไปก็เลยเข้าได้ มันก็ไม่ได้ใช้ความรู้อะไรมาก มันอยู่ที่ว่า...ผู้ดูแลระบบเขาตั้ง Password เขาตั้งระบบป้องกัน นี่ครับมันอ่อนแอไป”

ผู้วิจัย: “เขาเรียกอะไรนะ... Brute force attack ใช่ไหมครับ?”

มอส: “ใช่ๆ ครับ เขาเรียก Brute force Password ไงครับ”

ผู้วิจัย: “อ๋อครับ...แล้วมีประสบการณ์ที่แบบ คราวนี้มีแบบเราเจาะเองจริงๆ เลยไหม? แบบใช้ความสามารถจริงๆ เลย”

มอส: “...อ่า...อันนั้นถ้าบอกว่าเจาะเองจริงๆ เลยอันนี้....ยังไม่ขนาดนั้นครับ ก็คือว่า...” ตอบช้าลงมาก เหมือนใช้เวลาไตร่ตรอง การเรียบเรียงคำในประโยคสะดุดไปมา “หลังจากนั้นน่ะ ก็คือว่า...พออาจารย์ส่งพวก ส่งแข่งทักษะวิชาการบ่อยๆ ใช่ไหมครับ ความคิดก็เลย ความคิดก็เลยเปลี่ยนจากด้านแบบว่า...เกรียนๆ มาฝั่งด้านดีมากกว่า ว่าเราอยากใช้เพื่อ เพื่อเราจะป้องกันว่าเราจะ...เรา Hack ได้แบบนี้ คนอื่นก็น่าจะ Hack ได้ แต่เราก็อยากจะป้องกันไม่ให้โดน Hack มากกว่าครับ เราอยากจะช่วยคนอื่นมากกว่า...”

ผู้วิจัย: “ก็คือเราเป็น White hacker ว่างั้นเถอะ?”

มอส: “ใช่ๆ ครับ ไปทางนั้นมากกว่าครับ”

ผู้วิจัย: “อะไรเป็นเหตุผลที่เราตัดสินใจลงมือเปลี่ยนเว็บ...อย่างที่เล่าให้ฟัง?”

มอส: “อ๋ออันนั้นนะครับ....เว็บโรงเรียนเนี่ย แบบว่า โรงเรียนนั้นเราไม่ชอบโรงเรียนนี้เนี่ย เพื่อความสะใจอะไรประมาณนั้นอะครับ ตอนนั้นเป็นเด็กอยู่ เราไม่ชอบโรงเรียนนี้ เราไม่ชอบองค์กรนี้...เราก็อยากทำ แก้ไขหน้าเว็บเปลี่ยนแปลงอะไรของเขาไปเรื่อยอะครับ”

ผู้วิจัย: หัวเราะ “ฮ่าๆ...แต่โตมานี่ยังไม่ทำอะไรที่มากกว่านั้นใช่ไหมฮะ?”

มอส: “ใช่ๆ โตมาไปอยู่ฝั่ง White hat มากกว่า”

ผู้วิจัย: “ตอนเราเป็นเด็กนี่ เรามั่นใจได้แค่ไหนว่า...เขาสืบหาเราไม่ได้หรือจับเราไม่ได้ มั่นใจขนาดไหนครับ?”

มอส: “อ่า...ตอนเด็กเนี่ย ไปอ่าน อ่าไปอ่านในเว็บมาก่อนว่า ให้เราใช้...ตอนนั้นเป็นเด็กอยู่ก็เลยไม่มีโปรแกรมเป็นของตัวเอง ก็เลยไปอ่านในพวก ในเว็บบอร์ดอะไรบ้าง ประมาณว่า ให้ใช้ จะมี Browser อยู่ตัวนึง ที่ชื่อว่า Tor ถ้าใช้ Browser ตัวนี้เขาจะ Track กลับมาไม่ได้ว่าเราเนคนเข้าไปในระบบของเขา มันจะเปลี่ยน IP ไปเรื่อยๆ อะครับ เป็น IP ประเทศอื่น ไม่ใช่ประเทศไทยอะครับ”

ผู้วิจัย: “อ๋อ...Hack ผ่าน Tor Browser ก็มั่นใจแน่นอนว่าสืบเราไม่ได้?”

มอส: “ใช่ๆ ครับ”

ผู้วิจัย: “แล้วก็มั่นใจว่า...”

มอส: “ใช่ครับ...แล้วข้างบ้านมี WiFi เราก็ทำการ Brute Force เอาตัว Password WiFi ข้างบ้านมาใช้ WiFi ตัวนั้นมันก็ไม่ใช่ของเราละ”

ผู้วิจัย: “ก็สบาย...ถึงจับได้ก็มั่นใจว่า ไม่มีหลักฐานดำเนินคดีกับเราได้อยู่ดี?”

มอส: “ใช่ครับ เพราะว่า... IP ที่กลับมา ที่ ที่...IP Address ที่เขาได้ไปมันไม่ใช่ของบ้านเรา เป็น IP Address ของบ้านอื่นเขา”

ผู้วิจัย: “โอเค ก็สรุปได้ว่า...มั่นใจว่าหาเราไม่ได้ สองก็คือถึงจับได้ก็ไม่มีหลักฐานว่าเป็นตัวเราแน่นอนนะครับ?”

มอส: “ใช่ๆ ครับ”

ผู้วิจัย: “คำถามสุดท้ายละกันนะครับ...ก็...เราเป็นคนหาโอกาสตลอดเวลา หาช่องว่างตลอดเวลาหรือเห็นช่องว่างแล้วค่อยลงมือ?”

มอส: ตอบสวนทันทีไม่คิดนาน “อันนี้ผมจะมองหาตลอดเวลาครับว่า...เนี่ยมันมีระบบใหม่ๆ ขึ้นมา ระบบใหม่ๆ มันมีช่องโหว่อยู่รึป่าว ซึ่ง สมมุติว่าเรา Hack ระบบนี้ที่ไม่เคยมีใคร Hack ได้เนี่ย อันนี้ภูมิใจมากครับ จะทำให้เราภูมิใจ ซึ่งในวงการแฮ็กเกอร์เนี่ย ถ้าคนไหนเจาะระบบไหนได้ แล้วมันไม่เคยมีช่องโหว่มาก่อนไม่เคยมีใครเจาะได้ แล้วคนนั้นจะได้หมายเลข CVE ครับ เรียกว่า CVE หมายเลขช่องโหว่แต่ละคน ก็จะมีชื่อของแต่ละคน แฮ็กเกอร์คนนี้ได้ CVE ตัวไหนไปบ้างเกี่ยวกับเทคโนโลยีใหม่ๆ

ผู้วิจัย: “แล้วมี CVE มอส ไหมครับ?”

มอส: “อ่า...ของผมยังไม่มีครับ ผมทำ Pen test (Penetration test) เจาะระบบไปตรงๆ ครับ ยังไม่ได้หาช่องโหว่อะไรขนาดนั้น”

ผู้วิจัย: “โอเค ครับๆ ได้ความรู้มาก มีเรื่องอะไรเสริมอีกมั๊ยครับ? ที่อยากจะเล่า....แล้วในกลุ่มแฮ็กเกอร์มีการแลกเปลี่ยนข้อมูลอะไรกันมั๊ยครับ?”

มอส: “ส่วนมากจะอยู่ใน Dark web ครับ”

ผู้วิจัย: “เข้าผ่าน TOR ใช่ไหมครับ?”

มอส: “ใช่ครับ เข้าผ่าน TOR แต่พวก Dark web ก็อันตรายนิดนึงครับ เวลาคุยกันอยู่ใน dash board อะไรพวกเนี่ย คุยกันเนี่ย ส่ง link ส่งอะไรกันมา กดมั่วไม่ได้เลยครับ เพราะเราไว้ใจใครไม่ได้เหมือนกันครับวงการนี้”

จากนั้นผู้วิจัย และมอส ได้สนทนากันในประเด็นความสนใจส่วนตัว และลากัน

ผู้วิจัย: “โอเค ครับงั้นขอบคุณมากครับ?”

มอส: “ครับสวัสดีครับ”

ประวัติผู้เขียน

ชื่อ-สกุล	ปรเมศวร์ กุมารบุญ
วัน เดือน ปี เกิด	29/03/2515
สถานที่เกิด	ประเทศไทย
วุฒิการศึกษา	วท.ม.มหาวิทยาลัยธรรมศาสตร์ น.บ.จุฬาลงกรณ์มหาวิทยาลัย
ที่อยู่ปัจจุบัน	99/38 ม.1 ต.บางรักน้อย อ.เมือง จ.นนทบุรี 11000
ผลงานตีพิมพ์	1. บทความวิจัยเรื่อง “อาชญากรรมไซเบอร์สายพันธ์ใหม่ใช้ Fintech เพื่อสนับสนุนเส้นทางการเงินผู้ก่อการร้ายและองค์กรอาชญากรรมข้ามชาติ” งานประชุมวิชาการระดับชาติ เพื่อเสนอผลงานวิจัยและวิทยานิพนธ์ สาขานิติวิทยาศาสตร์และการบริหารงานยุติธรรม ครั้งที่ 2 ประจำปี 2560 2. บทความวิจัยเรื่อง “ทฤษฎีนวัตกรรมนำาพาอาชญากรรม (A Theory of Innovation Conducts Crime)” วารสารวิชาการ อาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ปี 2561 เล่มที่ 1 (Peer reviews) 3. บทความวิจัยเรื่อง "เทคนิคการสืบสวนหาความจริงจากเรื่องการไร้ตัวตนคนจ้างสังหารออนไลน์ในองค์กรอาชญากรรม Besa mafia ด้วยวิธีวิจัยแบบวิเคราะห์วาทกรรมเชิงวิพากษ์" (Peer reviews) งานประชุมวิชาการระดับชาติ เพื่อเสนอผลงานวิจัยและวิทยานิพนธ์ สาขานิติวิทยาศาสตร์และการบริหารงานยุติธรรม ประจำปี 2563 4. บทความเรื่อง "การจ้างสังหารออนไลน์อย่างไร้ตัวตน" (Peer reviews) วารสารโรงเรียนนายร้อยตำรวจ ปีที่ 1 ฉบับที่ 1 ปี 2563