วารสารวิชาการโรงเรียนนายร้อยพระจุลจอมเกล้า
CRMA Journal

อัลกอริทึมแห่งความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์
The Algorithm of Relationship between Anonymity and Cybercrime

ดร. ปรเมศวร์ กุมารบุญ
Dr. Poramez Kumarnboon

วิศวกรรมและเทคโนโลยีการป้องกันประเทศ
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เขตปทุมวัน กรุงเทพมหานคร 10330 ประเทศไทย
Defense Engineering and Technology, Faculty of Engineering, Chulalongkorn University, Pathumwan, Bangkok 10330, Thailand.
Corresponding Author. E-mail : poramez@live.com
(Received: September 10, 2022, Revised: March 6, 2023, Accepted: March 9, 2023)

บทคัดย่อ : บทความวิจัยนี้มุ่งหมายเพื่อสร้างอัลกอริทึมให้คอมพิวเตอร์ประมวลผลเพื่อพยากรณ์การเกิดอาชญากรรมไซเบอร์ และโอกาสก่อการร้าย จากความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ที่วิเคราะห์ด้วยทฤษฎีเกม เป็นวิธีวิจัยแบบผสมผสานเพื่อเข้าใจกระบวนการตัดสินใจของอาชญากรไซเบอร์โดยทฤษฎีการคิดอย่างเป็นเหตุเป็นผล และใช้ทฤษฎีเกมเป็นเครื่องมือในการอธิบายความสัมพันธ์ด้วย ต้นไม้การตัดสินใจ ตารางผลตอบแทน และสมการผลตอบแทน ผลการวิจัยได้พิสูจน์ว่าการไร้ตัวตนและการเกิดอาชญากรรมไซเบอร์มีความสัมพันธ์ระหว่างกัน

คำสำคัญ : อาชญากรรมไซเบอร์ การก่อการร้ายไซเบอร์ การไร้ตัวตน

Abstract : The aim of using Game theory in this research paper for computer processing algorithm to predicts cybercrime and terrorist probability, that there is the relationship between anonymity and cybercrime in almost in every domain. Consequently, this research is mixed method, and purpose to understand cyber criminal's decision-making by rational choice theory that has been used Game theory as an explanation via Decision Tree, Payoff Matrix and Payoff Function. The result of this research proved that cybercrimes and anonymity are related.

Keyword: Cybercrime, Cyber terrorism, Anonymity

1. บทนำ

แนวโน้มการก่อการร้ายพันทาง (Hybrid terrorist) เปลี่ยนรูปแบบยุทธวิธีไปสู่มิติไซเบอร์มากขึ้น (Cyber-space domain) เรียกว่าเป็น Non-Kinetic Acts (NKA) ไม่ใช้การปะทะโดยตรง ไม่จับตัวประกัน ไม่วางระเบิด พลีชีพ ไม่จี้เครื่องบิน ไม่กราดยิง แต่เปลี่ยนมาก่อการร้ายด้วยการก่อวินาศกรรมโครงสร้างพื้นฐานสาธารณะสำคัญ ด้วยการใช้มัลแวร์หรือแรนซัมแวร์ยึดระบบคอมพิวเตอร์ที่ใช้ควบคุม ท่อส่งน้ำมัน ท่อส่งก๊าซ ระบบไฟฟ้า ระบบรถไฟ ระบบประปา เป็นต้น อีกทั้งปฏิบัติการสงครามจิตวิทยาผ่านไซเบอร์เทคโนโลยีปลุกระดม (Radicalized) ให้ลุกขึ้นมาก่อการร้ายหรือเกลียดชังกันเองระหว่างคนในชาติ และเกิดเส้นทางการเงินการก่อการร้ายใหม่ผ่านระบบสินทรัพย์ดิจิทัล

การก่อการร้ายไซเบอร์ (Cyber terrorism) เป็นรูปแบบใหม่ที่ปฏิวัติวิธีการก่อการร้ายดั้งเดิม (Disrupted traditional terrorism) ด้วยหลายเหตุผลที่สนับสนุน อาทิ เช่น ค่าใช้จ่ายถูกกว่า สร้างความเสียหายได้มากกว่า ทำให้คนตายในวงกว้างได้มากกว่า ระดมทุนหรือโอนเงินข้ามพรมแดนได้ง่ายกว่า และสามารถก่อการร้ายระยะไกลได้โดยไม่ต้องไปยังพื้นที่ (Remotely) ทำให้ไม่มีโอกาสจับกุมตัว

ควบคู่ไปกับการก่อการร้ายไซเบอร์ก็คืออาชญากรรมไซเบอร์และกลุ่มองค์กรอาชญากรรมข้ามชาติที่ทวีความรุนแรงสร้างความเสียหายต่อชีวิตและทรัพย์สินของประชาชนในสังคม อย่างที่รัฐทั่วโลกแทบไม่มีโอกาสปกป้องประชาชนได้ทันล่วงหน้า ผลงานของทุกรัฐทั่วโลกออกมาในรูปแบบการแถลงข่าวการจับกุม จับได้มากมีผลงานมาก แต่ในความจริงแล้วการเกิดคดีขึ้นหมายถึงมีเหยื่อเกิดขึ้นแล้วสักคน อาจเสียทรัพย์หรือเสียชีวิตไปแล้ว โดยไม่อาจมีใครปกป้องประชาชนได้ทัน

ดังนั้นความสามารถในการพยากรณ์ว่าอาชญากรรมไซเบอร์หรือการก่อการร้ายด้วยเทคโนโลยีใดจะมีโอกาสเกิดขึ้นในสังคม รัฐจึงจะสามารถป้องกันล่วงหน้าได้ก่อนและจะไม่มีประชาชนตกเป็นเหยื่อสักคนเมื่อมีเทคโนโลยีใหม่เกิดขึ้นในสังคม และปิดโอกาสการก่อการร้าย งานวิจัยชิ้นนี้จึงค้นหาจุดร่วมของการเกิดอาชญากรรมไซเบอร์และการก่อการร้ายทางไซเบอร์โดยใช้ทั้ง ทฤษฎีเกม และทฤษฎีอาชญาวิทยา มาสร้างอัลกอริทึมเป็นสมการคณิตศาสตร์ให้ระบบคอมพิวเตอร์ประมวลผลเพื่อพยากรณ์แนวโน้มของไซเบอร์เทคโนโลยีใดจะเกิดอาชญากรรมไซเบอร์หรือการก่อการร้าย มากขึ้นหรือลดลง เพื่อแสดงผลในห้องบัญชาการ (War room) ในการเฝ้าติดตามสถานการณ์อาชญากรรมไซเบอร์หรือแนวโน้มการก่อการร้ายในอนาคต

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union) หรือ ITU เป็นองค์กรชำนัญพิเศษแห่งสหประชาชาติซึ่งมีหน้าที่ในการให้คำแนะนำรัฐต่างๆ ในการกำกับดูแลกิจการสื่อสาร ได้ตีพิมพ์เอกสารทางวิชาการเรื่อง Understanding Cybercrime: Phenomena, Challenge and Legal Response [7] ประเด็นที่น่าสนใจกล่าวว่า “Cybercrime และ Cyber Security เป็นเรื่องที่แยกจากกันคนละประเด็น”

ITU Development [7] ได้นิยามไว้ว่า Cyber Security เป็นเรื่องสำคัญของการพัฒนาเทคโนโลยีข้อมูลข่าวสาร (Information Technology) ที่เกี่ยวข้องกับบริการอินเทอร์เน็ต ที่จะต้องปกป้องข้อมูลข่าวสารไม่ให้ถูกทำลาย โดยเฉพาะเครือข่ายและข้อมูลข่าวสารของโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญหรือ Critical Information Infrastructures (CII) อาทิ เครือข่ายการสื่อสารของระบบการไฟฟ้า เครือข่ายการสื่อสารของระบบส่งก๊าซธรรมชาติ เครือข่ายโทรคมนาคม เป็นต้น ล้วนส่งผลกระทบต่อเศรษฐกิจ และความมั่นคงของชาติ หากการรักษาความปลอดภัยบกพร่อง

แต่ Cybercrime เป็นอาชญากรรมทุกรูปแบบที่เกิดจากการใช้ประโยชน์เครือข่ายโทรคมนาคมและเทคโนโลยีสารสนเทศ (ICT Network) ซึ่งเป็นเรื่องวิกฤติสำหรับ

หน่วยงานสืบสวนสอบสวนและเป็นประเด็นท้าทายในการบังคับใช้กฎหมายในปัจจุบัน

ปัจจุบันอาชญากรรมไซเบอร์เติบโตกว้างขวางไปมาก ในกระบวนการยุติธรรมอาญามีประโยคภาษาละตินว่า Nullum crimen sine lege แปลว่า no crime without law หมายถึง จะไม่มีอาชญากรรมถ้าไม่มีกฎหมายบัญญัติว่าเป็นโทษอาญา ดังนั้นการก่ออาชญากรรมทุกประเภทที่ย้ายจากโลก Offline ขึ้นไปสู่โลก Online เป็นอาชญากรรมไซเบอร์ทั้งหมด กล่าวคือถ้าไม่มีไซเบอร์เทคโนโลยีมาเกี่ยวข้องอาชญากรรมประเภทนั้นจะเกิดขึ้นไม่ได้ [2]

เนื่องจากศัพท์บางคำยังใหม่และยังไม่มีคำนิยามอย่างเป็นทางการ ณ ปัจจุบัน (พ.ศ. 2565) ในการวิจัยนี้จึงขอนิยามศัพท์เป็นการเฉพาะเพื่อให้เป็นการเข้าใจตรงกันและเป็นไปในทิศทางเดียวกัน

“การไร้ตัวตน” (Anonymity) ในบทความวิจัยนี้ หมายถึงองค์ประกอบ 2 ปัจจัยหลัก (Anonymous Factors) ที่ช่วยให้อาชญากรรอดพ้นโทษอาญาได้ คือ

(ก.) การหลบพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective)

(ข.) การรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีทำไม่ได้

การวิจัยนี้ ผู้วิจัยได้ตั้งข้อสันนิษฐานจากการสังเกตปรากฏการณ์ในสังคมโลกพบว่า

เหตุผลหนึ่ง การตัดสินใจลงมือก่ออาชญากรรมไซเบอร์หรือการก่อการร้ายทางไซเบอร์อาจเป็นเพราะอาชญากรหรือผู้ก่อการร้ายเชื่อมั่นว่า “จะไม่มีวันถูกจับ สามารถหลบพ้นจากการสืบสวนจับกุมทางดิจิทัลได้” จึงกล้าลงมือประกอบอาชญากรรมหรือก่อการร้าย แต่หากเจ้าหน้าที่สามารถสืบสวนจับกุมได้โดยง่ายหรือหาตัวผู้ก่อการร้ายหรืออาชญากรได้รวดเร็ว อาชญากรหรือผู้ก่อการร้ายจะชั่งน้ำหนักเหตุผลไม่ลงมือก่ออาชญากรรมหรือก่อการร้าย เช่น หากอาชญากรต้องการลักทรัพย์ย่อมเลือกลักทรัพย์บ้านหลังที่ไม่มีกล้องวงจรปิดหรือหาวิธีทำลายกล้องวงจรปิดเสียก่อน

เหตุผลอีกประการ กล่าวคือ อาชญากรยังเชื่อมั่นว่า แม้ถูกจับกุมตัวได้ในที่สุด แต่เจ้าหน้าที่จะไม่สามารถรวบรวมพยานหลักฐานดิจิทัลเพื่อดำเนินคดีเอาผิดได้ จึงยังกล้าตัดสินใจประกอบอาชญากรรม

ต่อไปบทความนี้ขอใช้คำว่า “อาชญากร” หมายถึงอาชญากรไซเบอร์และผู้ก่อการร้ายทางไซเบอร์ และการก่ออาชญากรรมไซเบอร์หมายรวมถึงการก่อการร้ายทางไซเบอร์ เพื่อประหยัดถ้อยคำ

รูปแบบการก่ออาชญากรรมไซเบอร์แต่ละประเภทขึ้นอยู่กับเทคโนโลยีการไร้ตัวตนในแต่ละชนิดแต่ละยุคสมัย กล่าวคือ ในยุคหนึ่งหรือในอดีต เทคโนโลยีประเภทหนึ่งสามารถช่วยอาชญากรปิดบังตัวตนล่องหนหายตัวได้ แต่พอเวลาผ่านไปเทคโนโลยีการสืบสวนจับกุมพัฒนาก้าวหน้าขึ้นสามารถสืบสวนจับกุมอาชญากรได้ เช่น ในอดีตแก๊งค์คอลเซ็นเตอร์ใช้เทคโนโลยีโทรศัพท์เสียงผ่านอินเทอร์เน็ต (VOIP) ปิดบังอำพรางตัวตนในการก่ออาชญากรรมมาหลายปี และเมื่อเทคโนโลยีการสืบสวนจับกุมก้าวหน้าแก๊งค์คอลเซ็นเตอร์หมดไปในช่วงหนึ่งและเปลี่ยนรูปแบบวิธีการใหม่ๆ ในการปิดบังอำพรางจนเกิดคดีมากขึ้นในปัจจุบัน

หากอาชญากรรมไซเบอร์ประเภทใดทำการ สืบสวนจับกุมไม่ได้หรือรวบรวมพยานหลักฐานเพื่อดำเนินคดีไม่ได้ อาชญากรรมไซเบอร์ประเภทนั้นจะเติบโตอย่างรวดเร็ว แต่ถ้าหากเมื่อใดเจ้าหน้าที่ตำรวจสามารถสืบสวนจับกุมอาชญากรรมไซเบอร์ประเภทนั้นได้ และสามารถรวบรวมพยานหลักฐานเพื่อดำเนินคดีได้ครบถ้วน อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงจนหมดสิ้นไป

2. คำถามวิจัย

“การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตนอย่างไร?”

3. วัตถุประสงค์ของการวิจัย

3.1 เพื่อศึกษา และรวบรวมรูปแบบการประกอบอาชญากรรมไซเบอร์ในสังคมที่เคยเกิดขึ้นจากอดีตมาจนถึงปัจจุบัน อันเป็นกรณีศึกษาเกี่ยวข้องกับการไร้ตัวตนมีความสัมพันธ์กับการเกิดอาชญากรรม

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

3.3 เพื่อสร้างรูปแบบความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์ ด้วยทฤษฎีเกม เพื่อเป็นอัลกอริทึมอย่างสมการคณิตศาสตร์ให้ระบบคอมพิวเตอร์ประมวลผลพยากรณ์

4. ระเบียบวิธีวิจัย

การวิจัย ใช้วิธีการวิจัยแบบผสมผสาน (Mixed research method) ทั้งการวิจัยเชิงปริมาณ (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 และวิเคราะห์ถึงความเป็นเหตุเป็นผลในการตัดสินใจกระทำความผิดจากการสัมภาษณ์เชิงลึก (In-depth Interview) เป็นการสัมภาษณ์จากผู้ให้ข้อมูลสำคัญ 3 ท่าน โดยไม่เคยพบตัวจริงและไม่ทราบชื่อจริง ทำการสัมภาษณ์ทางโทรศัพท์ เป็นอดีตแฮ็กเกอร์และปัจจุบันเป็นวิศวกรด้านความมั่นคงปลอดภัยไซเบอร์ 1 ท่าน และอีก 2 ท่านเป็นอดีตแฮ็กเกอร์ทำงานอยู่ในแวดวงไอทีไทย

5. การดำเนินการศึกษาวิจัย

อาชญากรไซเบอร์ทุกประเภทที่ผู้วิจัยได้ศึกษาในทุกกรณี และทุกคดีพบว่า “**อาชญากรไซเบอร์เป็นผู้เห็นแก่ตัวและตัดสินใจเลือกอย่างเป็นเหตุเป็นผล**” **(Rationale)**

อาชญากรไซเบอร์ในการวิจัยนี้ ไม่รวมถึงอาชญากรประเภทวิกลจริต และอาชญากรโดยกำเนิดที่มีพฤติกรรมความรุนแรงขาดการใช้เหตุผล จากการศึกษาเชิงประจักษ์ผู้วิจัยไม่พบอาชญากร 2 ประเภทดังกล่าวในอาชญากรรมไซเบอร์ [2] เพราะเนื่องด้วยอาชญากรไซเบอร์ส่วนใหญ่มีความรู้ความสามารถสูง มีความสามารถในการใช้เทคโนโลยีให้รอดพ้นจากการถูกจับกุม (Perfect criminal) โดยส่วนใหญ่จึงมีลักษณะเป็น อาชญากรตามโอกาส (Occasional criminals) และอาชญากรติดนิสัย (Habitual criminals) โดยมีรูปแบบการคิดของอาชญากรหลักๆ 2 กรณี คือ คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation) หรือคิดได้ใจจนเกินจริง (Super-optimism) ว่าสามารถที่จะหลีกพ้นโทษจากการกระทำความผิดของตนเองได้อย่างแน่นอนหรือมั่นใจว่าตนไม่มีทางถูกจับได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ [3]

ลักษณะอาชญากร และรูปแบบการคิดของอาชญากรในลักษณะต่างๆ จากที่ได้ศึกษามาเชื่อว่า การกระทำพฤติกรรม อาศัยกระบวนการทางปัญญาเป็นสำคัญในการชั่งน้ำหนักตัดสินใจ สอดคล้องกับทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ ที่ให้แผนภาพลึกซึ้งมายิ่งขึ้น

ไชยันต์ ไชยพร [1] การเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ อธิบายสิ่งที่จูงใจให้เกิดการกระทำมีอยู่ 2 ประการนั่นคือ

ก. ความปรารถนา (Desire)

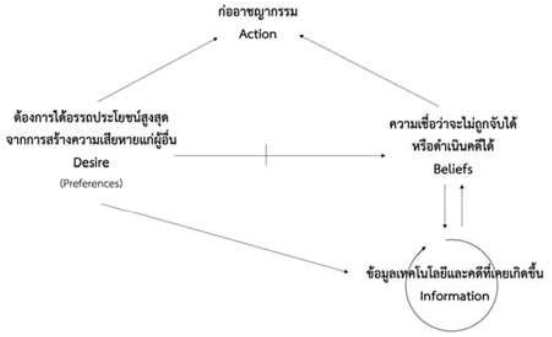
ข. ความเชื่อ (Belief)

ทั้งสองสิ่งนี้เป็นเหตุผลที่เพียงพอในการหาวิธีการใดที่จะทำเพื่อให้บรรลุผลเป้าหมาย เอลสเตอร์ อธิบายเพิ่มว่า ความปรารถนา มีความพอใจเลือก (Preferences) ที่ประกอบไปด้วย พอใจเลือกที่มีเนื้อหา และพอใจเลือกแค่รูปแบบ

ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผลนี้สามารถแสดงมาในรูปแบบกราฟที่แสดงฟังก์ชันอรรถประโยชน์ที่จุดต่างๆ กันได้ โดยแต่ละจุดมีค่าที่แสดงไว้ ทำให้บอกได้ว่าผู้ที่เลือกอย่างเป็นเหตุเป็นผลจะเลือกการกระทำใดที่จะให้ผลลัพธ์สูงสุด (Maximizing utility) ต่ออรรถประโยชน์ของตน แต่ความปรารถนานี้คือความปรารถนาที่เห็นแก่ตัวหรือตนพึงพอใจหรือชั่วร้าย ด้วยเอาประโยชน์จากผู้อื่น

ในส่วนความเชื่อ (Belief) ที่รองรับการเลือกอย่างเป็นเหตุเป็นผล ต้องเป็นความเชื่อที่มีพื้นฐานที่ดีรองรับ นั่นคือ “ข้อมูล” จำนวนมากที่สนับสนุน

แบบแผนจำลองอธิบายการเลือกอย่างเป็นเหตุเป็นผลของ เอลสเตอร์ [1] ตั้งบนสมมติฐานว่า การกระทำหนึ่งๆ ที่เกิดขึ้น ถือว่าเป็นการกระทำที่เกิดจากการตัดสินใจเลือกอย่างเป็นเหตุเป็นผลได้ โดยผู้วิจัยได้วิเคราะห์เงื่อนไขที่น่าพอใจที่สุด (Optimality conditions) ทั้ง 3 ประการ มาเป็นกรอบเบื้องต้นในการทำความเข้าใจการคิดอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์ ได้ดังภาพที่ 1 นี้



ภาพที่ 1 แบบแผนจำลองการเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

5.1 การวิเคราะห์

5.1.1 ความปรารถนา (Desire)

จากการศึกษาข้อมูลจำนวนมากทั้งกรณีศึกษาและคดีต่างๆ [2] พบว่า อาชญากรไซเบอร์เป็น อาชญากรตามโอกาส และ อาชญากรติดนิสัย มีความปรารถนาที่จะสร้างความเสียหายกับผู้อื่นเพื่อสร้างอรรถประโยชน์แก่ตนตลอดเวลา โดยความปรารถนาหรือความชอบนี้ปฏิบัติการในฐานะที่เป็น “ตัวขับเคลื่อนคงที่ของทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล” ให้คอยมองหาโอกาสอยู่เสมอ การตีความในข้อนี้ย่อมเป็นอื่นไม่ได้แน่นอน

5.1.2 การกระทำ (Action)

จากการศึกษาข้อมูลทั้งกรณีศึกษาและคดีต่าง ๆ ผู้วิจัยพบว่า อาชญากรไซเบอร์จะลงมือก่ออาชญากรรมโดยเลือกหนทางที่ดีที่สุดที่จะทำให้บรรลุในสิ่งที่ปรารถนา ทั้งนี้ขึ้นอยู่กับความเชื่อ (Belief) และข้อมูลข่าวสารที่อาชญากรนั้นมีอยู่ครบถ้วน จะลงมือก่ออาชญากรรมไซเบอร์ทันที

5.1.3 ความเชื่อ (Belief)

จากการศึกษาข้อมูลทั้งกรณีศึกษาและคดีต่างๆ ผู้วิจัยพบว่า เมื่อข้อมูล (Information) ที่อาชญากรไซเบอร์ได้รับเกี่ยวกับเทคโนโลยีนั้นๆ เหมาะสมที่สุดในการก่ออาชญากรรม ซึ่งเชื่อว่า พวกเขาจะไม่ถูกจับ และไม่ถูกดำเนินคดี ซึ่งสอดคล้องกับรูปแบบการคิดของอาชญากร 2 กรณี คือ คิดว่าตนเองมีอำนาจเหนือผู้อื่น (Power orientation) หรือคิดได้ใจจนเกินจริง (Super-optimism) ว่าเขาสามารถที่จะหลีกพ้นโทษจาก การกระทำความผิดของตนเองได้อย่างแน่นอนหรือมั่นใจว่าตนไม่มีทางถูกจับได้ โดยเฉพาะมีประสบการณ์กระทำความผิด และสามารถเอาตัวรอดได้บ่อยๆ

5.2 การตีความ (Interpretation)

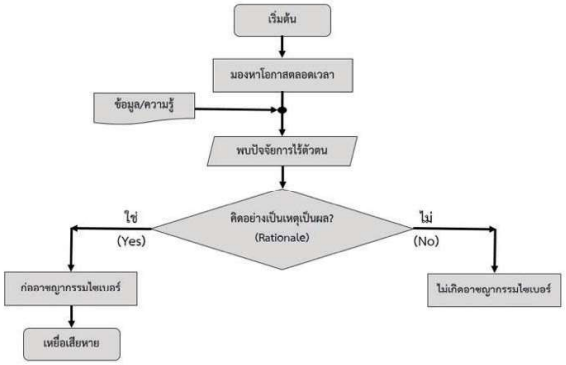
การวิจัยนี้มุ่งหาความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับการไร้ตัวตน (Anonymity) จากกระบวนความคิดอย่างเป็นเหตุและเป็นผลต่อการตัดสินใจของอาชญากรไซเบอร์บนข้อมูลเทคโนโลยีที่อาชญากรมีเกี่ยวกับการ

หลบพ้นจากการสืบสวนจับกุมทางดิจิทัล และการรวบรวมพยานหลักฐานดิจิทัลเพื่อให้รอดพ้นการถูกดำเนินคดี

ดังนั้น หัวใจสำคัญของการตัดสินใจอย่างเป็นเหตุเป็นผล (Rationale) ก่อนลงมือประกอบอาชญากรรมไซเบอร์ คือ ปัจจัยการไร้ตัวตน (Anonymous factors) ที่อาชญากรเลือกตัดสินใจประกอบอาชญากรรม โดยสามารถค้นหาปัจจัยการไร้ตัวตนของเทคโนโลยีไซเบอร์ในการก่ออาชญากรรมได้ดังนี้

5.3 การใช้ทฤษฎีเกมวิเคราะห์ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์

สมมติฐานทางวิจัย (Research hypothesis) คือ“การตัดสินใจประกอบอาชญากรรมไซเบอร์มีความสัมพันธ์กับการไร้ตัวตน”



ภาพที่ 2 กระบวนการคิดตัดสินใจเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์

จากภาพที่ 2 กระบวนการคิดตัดสินใจเลือกอย่างเป็นเหตุเป็นผลของอาชญากรไซเบอร์ตามสมมติฐานการวิจัย คือ อาชญากรไซเบอร์เห็นแก่ตัวมองหาโอกาสจากเหยื่อตลอดเวลา บนข้อมูลเทคโนโลยีเดิมที่ตนมีอยู่และค้นคว้าหาความรู้เทคโนโลยีใหม่ตลอดเวลา [2] เมื่อพบปัจจัยการไร้ตัวตน (ตามนิยามในการวิจัยนี้) และอาชญากรมีการคิดอย่างเป็นเหตุเป็นผล (Rationale) จะตัดสินใจลงมือก่ออาชญากรรมไซเบอร์ทันที จึงใช้ทฤษฎีเกมเป็นเครื่องมือสำคัญในการวิจัยให้เห็นรูปแบบความสัมพันธ์ระหว่างการไร้ตัวตนและอาชญากรรมไซเบอร์ได้ผลดังต่อไปนี้

5.4 การใช้ทฤษฎีเกมวิเคราะห์หาปัจจัยการไร้ตัวตนเพื่อตั้งสมมุติฐานการวิจัย

ทฤษฎีเกม มีหลักการทั่วไปดังนี้ [4]

Perfect Information: ผู้เล่นมีข้อมูลครบถ้วนสมบูรณ์เข้าใจ กติกา รางวัล และรู้กลยุทธ์ฝั่งตรงข้าม

Rationale: ผู้เล่นทุกฝ่ายใช้ข้อมูลที่ตนมีตัดสินใจเลือกกลยุทธ์ที่ดีที่สุด อย่างเป็นเหตุและเป็นผล

5.4.1 การหา Decision Tree

เทคนิค Decision Tree ของทฤษฎีเกมเป็นการทำความเข้าใจอย่างง่ายต่อสถานการณ์แวดล้อมที่จะเกิดอาชญากรรมไซเบอร์ขึ้น โดยวิเคราะห์ทางเลือกของผู้เล่นเกมหรืออาชญากรในการตัดสินใจมีกี่ทางเลือกในการก่ออาชญากรรม และผู้ที่ทำหน้าที่ปกป้อง (Defender) ไม่ว่าทั้งตัวเหยื่อหรือตำรวจจะดำเนินการเป็นไปในทิศทางใดในการวิจัยนี้ยกตำรวจเป็นผู้ที่ทำหน้าที่ปกป้องเพื่อความเข้าใจง่าย

จากการสังเกตปรากฏการณ์การเกิดอาชญากรรมไซเบอร์ในทุกประเภท ผู้วิจัยได้พบว่า หากอาชญากรรมไซเบอร์ประเภทใด อาชญากรรอดพ้นจากการสืบสวนจับกุมทางดิจิทัล (Digital Detective) จะทำให้อาชญากรรมไซเบอร์ประเภทนั้นเพิ่มสูงขึ้นอย่างรวดเร็ว หรือแม้จะสืบสวนจับกุมได้ แต่ไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีเอาผิดทางอาญาผู้ต้องสงสัยได้ อาชญากรรมไซเบอร์ประเภทนั้นจะยังคงเพิ่มขึ้นอย่างรวดเร็วต่อไป

ในทางตรงกันข้าม หากอาชญากรรมไซเบอร์ประเภทใด สามารถสืบสวนทางดิจิทัล (Digital Detective) จนจับกุมตัวอาชญากรได้ จะทำให้อาชญากรรมไซเบอร์ประเภทนั้นลดลงอย่างรวดเร็ว แต่เมื่อสืบสวนจับกุมได้ และสามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีจนเอาผิดทางอาญาได้ อาชญากรรมไซเบอร์ประเภทนั้นจะลดต่ำลงอย่างรวดเร็ว

จนหมดไป โดยเขียน Decision Tree ของทฤษฎีเกมอาชญากรรมไซเบอร์ [2] ดังภาพที่ 3 นี้

ภาพที่ 3 Decision Tree ของทฤษฎีเกม

5.4.2 การหา Payoff Matrix

อาชญากรมีการตัดสินใจอย่างเป็นเหตุเป็นผล (Rationale) บนข้อมูลที่ตนได้รับทราบอย่างสมบูรณ์ว่า ไซเบอร์เทคโนโลยีใดจะไม่สามารถสืบสวนทางดิจิทัล (Digital Detective) ได้ อาชญากรจะลงมือก่ออาชญากรรมทันทีเพื่อให้ตนได้รับอรรถประโยชน์สูงสุด หรือแม้ถูกสืบสวนจับกุมได้ แต่ไม่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เอาผิดทางอาญาได้ [5] อาชญากรก็ยังคงชั่งน้ำหนักเหตุและผลจนลงมือก่ออาชญากรรม เมื่อพบว่าอรรถประโยชน์ที่ได้รับคุ้มค่ากับความเสี่ยง

ตารางที่ 1 การหาค่าตาราง Payoff Matrix ของทฤษฎีเกมอาชญากรรมไซเบอร์

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

โดยให้

c คือ จำนวนคดีอาชญากรรมไซเบอร์ประเภทใด

d คือ จำนวนคดีที่สืบสวนจนจับกุมอาชญากรได้

s คือ จำนวนคดีที่สามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เอาผิดทางอาญาได้

สามารถหา Payoff Matrix ของทฤษฎีเกมได้ดังนี้

อธิบายเกม

ทฤษฎีเกมอาชญากรรมไซเบอร์เป็น Zero-sum game เป็นเกมที่ไม่มีจุดที่สมประโยชน์สองฝ่ายร่วมกัน แต่เป็นเกมที่อาชญากรได้ประโยชน์เท่าที่เหยื่อเสียประโยชน์ไป และการปกป้องประโยชน์ของเหยื่อเป็นหน้าที่ของตำรวจที่จะต้องหาหนทางปกป้องตลอดเวลา

ทฤษฎีเกมอาชญากรรมไซเบอร์เป็นกลยุทธ์ผสม (Mixed Strategies) เป็นกลยุทธ์ที่ใช้ในการเล่นเกมระหว่างสองฝ่าย โดยผู้เล่นแต่ละฝ่ายไม่ได้เล่นกลยุทธ์ใดกลยุทธ์หนึ่งเพียงวิธีเดียว แต่จะเล่นหลายวิธีผสมกัน โดยอาชญากรเป็นเจ้าของตารางจะมองหาโอกาสอยู่เสมอ และตำรวจจะคอยหากลยุทธ์ใหม่ปิดโอกาสการเกิดอาชญากรรมนั้นอยู่เสมอ [4]

อาชญากรชั่งน้ำหนักความเป็นเหตุ (Cause) และความเป็นผล (Effect) ตลอดเวลาในการใช้ 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 แต่ถ้าหากอาชญากรชั่งน้ำหนักอย่างเป็นเหตุเป็นผล (Rationale) ว่าเทคโนโลยีไซเบอร์ประเภทใดยังคงให้อรรถประโยชน์แก่ตนมากกว่าโทษที่ได้รับ แม้จะถูกจับกุมได้ อาชญากรย่อมลงมือประกอบอาชญากรรมต่อไป

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

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

หากตำรวจปรับเปลี่ยนกลยุทธ์จากกลยุทธ์ P1 เป็นกลยุทธ์ P2 จนพบกลยุทธ์ P3 เมื่อใด จะทำให้สัดส่วนการตัดสินคดีลงโทษอาญาอาชญากรได้ทุกราย (s) ต่อจำนวนคดีที่จับกุมได้ (d) มีค่าเท่ากับ 1 หมายถึงทุกคดีที่จับกุมตัวอาชญากรได้เท่าใด สามารถรวบรวมพยานหลักฐานดิจิทัลจนเอาผิดต้องคำพิพากษาตัดสินลงโทษได้ทุกราย การไร้ตัวตนจากอาชญากรรมไซเบอร์ประเภทนั้นจะหมดไปเมื่อ

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

5.4.3 การหา Payoff Function

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

จำนวนคดีอาชญากรรมไซเบอร์ประเภทนั้นจะสูงมากถ้าหาก

$$\frac{d}{c} + \frac{s}{d} = 0 \qquad (1)$$

จำนวนคดีอาชญากรรมไซเบอร์ประเภทนั้นจะหมดไปถ้าหาก

$$\frac{d}{c} + \frac{s}{d} = 2 \qquad (2)$$

เมื่อ

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

เพราะฉะนั้นจะได้ ปัจจัยการไร้ตัวตน (Anonymous factor) เท่ากับ

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

ดังนั้น ในการวิจัยนี้ให้ปัจจัยการไร้ตัวตน (Anonymous factor) เขียนแทนด้วย k จะได้

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

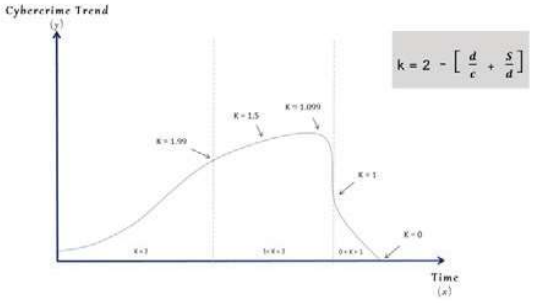
จะได้ $0 \le k \le 2$

6. ผลการวิจัย

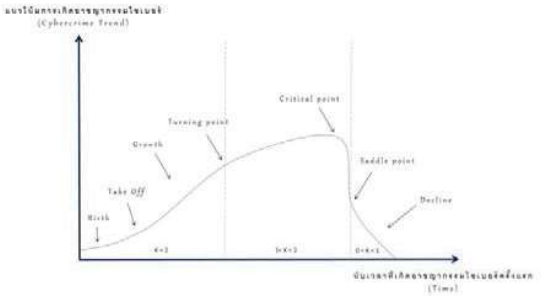
ผู้วิจัยใช้ Matrix payoff และ Payoff Function การตัดสินใจก่ออาชญากรรมไซเบอร์ของอาชญากร อันขึ้นอยู่กับปัจจัยการไร้ตัวตน (Anonymous factor) ดังที่ได้วิเคราะห์ผ่านมา โดย k มีค่าตั้งแต่ 0 ≤ k ≤ 2 ซึ่งส่งผลต่อแนวโน้มการเกิดอาชญากรรมไซเบอร์ในแต่ละช่วงเวลาแตกต่างกัน และผู้วิจัยได้ตั้งมโนทัศน์เพื่อพยายามทำความเข้าใจการเกิดอาชญากรรมไซเบอร์ ที่ค่าปัจจัยการไร้ตัวตน (Anonymous factor) แตกต่างกัน โดยใช้วิธี Backward induction ของทฤษฎีเกมได้ดังต่อไปนี้

6.1 มโนทัศน์ที่ 1: "แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์เป็น Cybercrime trend curve"

จาก Payoff Matrix และ Payoff Function ความสัมพันธ์การตัดสินใจในการก่ออาชญากรรมของอาชญากรขึ้นอยู่กับค่า k หรือ ปัจจัยการไร้ตัวตน (Anonymous factor) อันมาจากสัดส่วนจำนวนคดีกับจำนวนการสืบสวนจับกุม และการรวบรวมพยานหลักฐานดิจิทัลเอาผิดอาญา ดังที่ได้วิเคราะห์ไปแล้วนั้น นำมาตั้งเป็นกรอบให้เห็นภาพเพื่อทำความเข้าใจในรูปแบบกราฟ โดยใช้วิธี Backward induction ได้ดังนี้



ภาพที่ 4 มโนทัศน์ความสัมพันธ์ปัจจัยการไร้ตัวตนกับการตัดสินใจในการก่ออาชญากรรมไซเบอร์



ภาพที่ 5 มโนทัศน์ความสัมพันธ์แนวโน้มการเกิดอาชญากรรมไซเบอร์ (ตัวแปรตาม) กับช่วงเวลา (ตัวแปรต้น) โดยมีปัจจัยการไร้ตัวตนเป็นตัวแปรควบคุม

ผู้วิจัยได้สังเกตเห็นปรากฏการณ์อาชญากรรมไซเบอร์ในสังคมนับแต่อดีตมาจนถึงปัจจุบัน และได้ทดลองวาดภาพที่เชื่อมโยงให้เห็นความสัมพันธ์ระหว่างการไร้ตัวตนและอาชญากรรมไซเบอร์มีความสัมพันธ์กันอย่างไร ดังภาพที่ 4-5 อธิบายเพิ่มเติมได้ดังนี้

แกน y หรือแกนตั้ง เป็น Cybercrime trend หรือแนวโน้มการเกิดอาชญากรรมไซเบอร์

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

สถานะที่ 1 Birth

อาชญากรกลุ่มแรกๆ ได้รับข้อมูลหรือมีการทดลองและค้นพบว่าไซเบอร์เทคโนโลยีใหม่ที่เกิดขึ้นในสังคมสามารถประกอบอาชญากรรมได้ในคดีแรกๆ โดยไม่มีใครล่วงรู้ว่าเป็นฝีมือผู้ใด

<u>หมายเหตุ</u> k = 2

สถานะที่ 2 Take off

ข่าวสารการสร้างความเสียหายอย่างไร้ตัวตนผู้กระทำความผิด ด้วยไซเบอร์เทคโนโลยีใหม่ทำให้รอดพ้นจากสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้แพร่กระจายสู่ อาชญากรตามโอกาส และอาชญากรติดนิสัย ต่างเริ่มเลียนแบบเทคนิควิธี และตัดสินใจประกอบ

อาชญากรรมด้วยไซเบอร์เทคโนโลยีนั้น

จาก Payoff Matrix ในตารางที่ 1 และ Payoff Function ในสมการที่ (3) อาชญากรตัดสินใจเลือกใช้กลยุทธ์ที่ Q และ 1- Q โดยที่ตำรวจใช้กลยุทธ์ P1 ทำให้แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นๆ เติบโตพุ่งสูงอย่างรวดเร็วในเวลานั้น

หมายเหตุ k = 2

สถานะที่ 3 Growth

ข่าวสารการสร้างความเสียหายอย่างไร้ตัวตนผู้กระทำความผิด ด้วยไซเบอร์เทคโนโลยีใหม่ทำให้รอดพ้นจากสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้แพร่กระจายในวงกว้างสู่อาชญากรทั่วทั้งวงการอาชญากรรมต่างก็ตัดสินใจประกอบอาชญากรรมเพื่ออรรถประโยชน์สูงสุดแก่ตน และพวกพ้อง

ทำให้แนวโน้มการเกิดอาชญากรรมไซเบอร์ประเภทนั้นๆ เติบโตพุ่งสูงอย่างรวดเร็ว และสร้างความเสียหายต่อสังคมต่อเนื่อง ตามระยะเวลาที่เกิดขึ้นนับแต่ปีแรก (หรือเดือนแรกหรือสัปดาห์แรก) หรือคดีแรกที่เกิดขึ้นไปเรื่อยๆ และยังทำการสืบสวนจับกุมไม่ได้สักคดี เมื่อพิจารณาจาก Matrix payoff ตารางที่ 1 หมายความว่าตำรวจยังมีเพียงกลยุทธ์จากกลยุทธ์ P1 เท่านั้น

หมายเหตุ k = 2

สถานะที่ 4 Turning point

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

หมายเหตุ 1< k < 2

สถานะที่ 5 Critical point

จาก Payoff Matrix ในตารางที่ 1 และ Payoff Function ในสมการที่ (3) เมื่อตำรวจเปลี่ยนมาใช้กลยุทธ์ P2 สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) ได้ตัวอาชญากรมาดำเนินคดีเรื่อยๆ จนได้เกือบทุกคดี จนถึงจุดวิกฤต (Critical point) ค่า k เข้าใกล้ 1 และเมื่อค่า k =1 แนวโน้มการเกิดอาชญากรรมไซเบอร์จะลดลงรวดเร็วอย่างกะทันหัน แต่ยังไม่หายไปหมดเสียทีเดียว

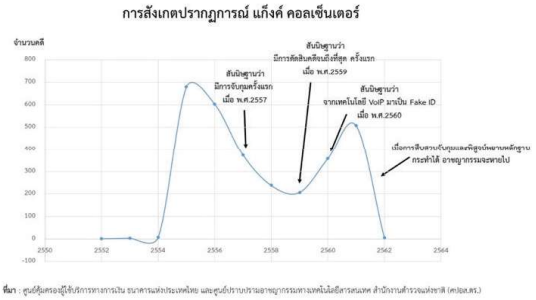
หมายเหตุ k = 1

สถานะที่ 6 Decline

จาก Payoff Matrix ในตารางที่ 1 และ Payoff Function ในสมการที่ (3) ในที่สุดเมื่อตำรวจค้นพบกลยุทธ์ P3 สามารถสืบสวนจับกุมอาชญากรไซเบอร์ได้ทุกคดี และสามารถรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) พิสูจน์ตัวตนดำเนินคดีเอาผิดทางอาญาอาชญากรได้ทุกคดี อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงอย่างรวดเร็วจนแนวโน้มการเกิดอาชญากรรมไซเบอร์มีค่าเป็น 0 หรืออาจจะไม่กลับมาเกิดขึ้นอีกเลย

หมายเหตุ 0 < k < 1

เมื่อลองเปรียบเทียบกับข้อเท็จจริงในสังคมกับแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Cybercrime trend curve) คล้ายครีบปลาฉลามหรืออาจจะเรียกว่า Shark fin curve จากมโนทัศน์ที่ 1 ที่อธิบายความสัมพันธ์แนวโน้มการเกิดอาชญากรรมไซเบอร์เป็นตัวแปรตามกับช่วงเวลาเป็นตัวแปรต้น โดยมีปัจจัยการไร้ตัวตนเป็นตัวแปรควบคุม นำมาเปรียบเทียบกับกราฟคดีแก็งค์คอลเซ็นเตอร์ ในภาพที่ 6 ซึ่งมีลักษณะกราฟใกล้เคียงกันมากดังนี้



ภาพที่ 6 ลักษณะความสัมพันธ์คดี แก๊งค์คอลเซ็นเตอร์ กับเวลา โดยมีการสืบสวนจับกุม และการดำเนินคดีเอาผิดได้เป็นตัวแปรควบคุม

การตีความ

เดิมแก๊งค์คอลเซนเตอร์ [2] ใช้เทคโนโลยี Voice over internet protocol ประกอบอาชญากรรม โดยเจ้าหน้าที่ตำรวจไม่สามารถสืบสวนจับกุมทางดิจิทัล (Digital Detective) เพื่อหาตัวตนอาชญากรกระทำได้ อาชญากรรมประเภทนี้จึงเติบโตอย่างรวดเร็วในปี พ.ศ. 2554-2556 จนสามารถสืบสวนจับกุมคดีแรกได้เมื่อปี พ.ศ. 2557 อาชญากรรมจึงลดอย่างรวดเร็วและเมื่อมีการรวบรวมพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อดำเนินคดีกระทำได้ถึงที่สุด อาชญากรรมประเภทนี้แทบจะหมดไป

จนกระทั่งอาชญากรเปลี่ยนกลยุทธ์จากการใช้เทคโนโลยี VoIP มาใช้ Fake ID อาชญากรรมประเภทนี้จึงกลับมาสูงขึ้นอย่างรวดเร็วอีกครั้ง แต่ในที่สุดเจ้าหน้าที่ตำรวจสามารถสืบสวนจับกุม และดำเนินคดีจนถึงที่สุดได้ แนวโน้มอาชญากรรมประเภทนี้จึงลดลง และส่งผลให้อาชญากรรมไซเบอร์เปลี่ยนไปใช้เทคนิคอื่นไปเรื่อยๆ

6.2 มโนทัศน์ที่ 2: “ความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน ควรมีลักษณะเป็นกราฟ และสมการ อย่างคุณสมบัติของฟังก์ชันเอ็กซ์โปเนนเชียล”

จากมโนทัศน์ที่ 1 แบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Cybercrime trend curve) ที่ใช้การให้เหตุผลแบบ หลักการคิดย้อนกลับ (Backward induction) ของทฤษฎีเกม [1] โดยชี้ให้ดูผลลัพธ์ของเหตุการณ์ว่าท้ายสุดจะเกิดอะไรขึ้น แล้วคิดถอยหลังกลับมาหาปัจจุบัน โดยใช้ผลที่ได้มาจาก Payoff Matrix ในตารางที่ 1 และ Payoff Function ในสมการที่ (3) อธิบายความสัมพันธ์แนวโน้มการเกิดอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน จึงพยายามที่จะหาสมการทางคณิตศาสตร์ (Mathematical Model) มาอธิบายใช้ประโยชน์

โดยผู้วิจัยได้เริ่มต้นพิจารณาจากรูปแบบกราฟและสมการทางคณิตศาสตร์หลายรูปแบบเพื่อพิจารณาว่าแบบใดจะใกล้เคียงหรือมีความเหมาะสมในการที่นำมาทดลองใช้อธิบายหรือทำนายอาชญากรรมไซเบอร์ตามวัตถุประสงค์ โดยมีวิธีพิจารณาแนวทางการตั้งมโนทัศน์ดังนี้

จากแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Cybercrime trend curve) ในมโนทัศน์ที่ 1 ไม่ใช่ลักษณะกราฟของสมการเชิงเส้น (Linear equation) และไม่ใช่ลักษณะกราฟของสมการ พาราโบลา (Parabola equation) ผู้วิจัยจึงตัดสินใจเลือกลักษณะกราฟของสมการ เอ็กซ์โพเนนเชียล (Exponential equation) มาทดลองพิสูจน์มโนทัศน์ที่ 1 ว่า พอจะมีพลังในการอธิบายได้มากน้อยเพียงใด

เหตุผลที่เลือก ฟังก์ชันเอ็กซ์โพเนนเชียล มาอธิบายความสัมพันธ์ระหว่างการไร้ตนตน และการเกิดอาชญากรรมไซเบอร์ ผู้วิจัยให้เหตุผลประกอบคุณสมบัติของ ฟังก์ชันเอ็กซ์โพเนนเชียล ดังต่อไปนี้

(ก) ฟังก์ชันเอ็กซ์โพเนนเชียล ไม่ติดลบ และเริ่มจากค่า y= 1

คุณสมบัติของ ฟังก์ชันเอ็กซ์โพเนนเชียล เป็นกราฟและสมการทางคณิตศาสตร์ ที่มีค่าเป็นบวกเสมอ แตกต่างจากรูปแบบสมการอื่นๆ ซึ่งหากนำมาพยายามใช้อธิบายจะค่อนข้างเห็นภาพได้ยาก และอาจไม่สามารถพิสูจน์ให้

เห็นชัดได้ ซึ่ง ฟังก์ชันเอ็กซ์โพเนนเชียล มีความเหมาะสมที่สุด โดยมีรูปแบบสมการดังนี้

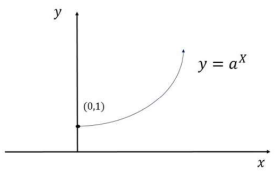
$$y = a^x + c$$

โดยที่ 0 < a และ a ≠ 1 (จุดที่ a = 1 ค่า y จะเท่ากับ x)

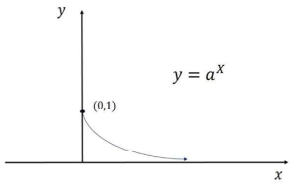
การตั้งมโนทัศน์อธิบายการเกิดอาชญากรรมไซเบอร์ในสังคม เมื่อพิจารณาถึงหลักความจริง การเกิดคดีขึ้นครั้งแรกนับเป็นครั้งที่ 1 ในปีแรก เป็นเลขบวก ไม่มีทางติดลบ

ฟังก์ชันเอ็กซ์โพเนนเชียล เริ่มนับที่ค่า y เท่ากับ 1 เมื่อ x เป็น 0 ($x^0 = 1$) สามารถนำมาอธิบายภาพได้จากนั้นเมื่ออาชญากรใช้เทคโนโลยีไซเบอร์ใดที่ตำรวจยังจับไม่ได้ อาชญากรรมประเภทนั้นจะเพิ่มสูงขึ้นเรื่อยๆ อย่างรวดเร็ว เป็นฟังก์ชันเพิ่มมีความชันกราฟมากกว่าสมการเชิงเส้น และเมื่อการใช้ไซเบอร์เทคโนโลยีใดที่อาชญากรไม่อาจหลบพ้นตัวตนจนถูกจับกุมดำเนินคดี และถูกพิพากษาลงโทษ อาชญากรรมไซเบอร์ประเภทนั้นจะลดลงอย่างรวดเร็วเป็นฟังก์ชันลดจนมีค่าเป็น 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



ภาพที่ 7 คุณสมบัติของฟังก์ชันเพิ่มของฟังก์ชันเอ็กซ์โพเนนเชียล



ภาพที่ 8 คุณสมบัติของฟังก์ชันลด ของฟังก์ชันเอ็กซ์โพเนนเชียล

ดังนั้นมโนทัศน์ที่ 2 “ความสัมพันธ์ระหว่างอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน ควรมีลักษณะเป็นกราฟ และสมการ อย่างคุณสมบัติของ ฟังก์ชันเอ็กซ์โปเนนเชียล” สามารถนิยามได้ดังนี้

$$y = k^x + c \qquad (4)$$

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 ฟังก์ชันเอ็กซ์โพเนนเชียล เป็นกราฟ และสมการทางคณิตศาสตร์ ว่ามีความเป็นไปได้ที่จะสอดคล้องกับแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Cybercrime trend curve) กับผลที่ได้มาจาก Payoff Matrix ในตารางที่ 1 และ Payoff Function ในสมการที่ 3 อย่างไร ซึ่งสามารถพิสูจน์ได้ดังต่อไปนี้

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

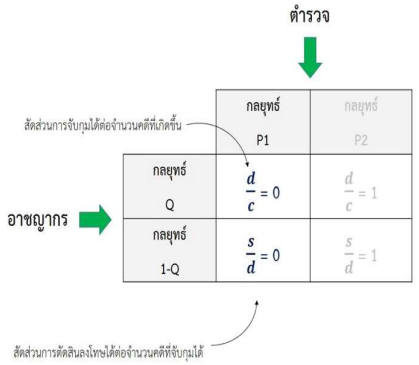
คุณสมบัติของ ฟังก์ชันเอ็กซ์โพเนนเชียล เลขฐาน a จะต้องมากกว่า 0 และไม่เท่ากับ 1 เพราะเลข 1 ยกกำลังอะไรก็เท่ากับ 1 และจุดที่ เลขฐานเริ่มมากกว่า 1 นั้นเป็นจุดเปลี่ยนเป็นฟังก์ชันลด
โดยที่

เลขฐานมากกว่า 1 เป็นฟังก์ชันเพิ่ม a > 1

เลขฐานมากกว่า 0 แต่น้อยกว่า 1 เป็นฟังก์ชันลด 0 < a <1

พิจารณาประกอบสมมติฐานทางวิจัย ค่า k หรือ ปัจจัยการไร้ตัวตน (Anonymous factor) นำมาอธิบายรายละเอียดได้ดังนี้

ตารางที่ 2 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

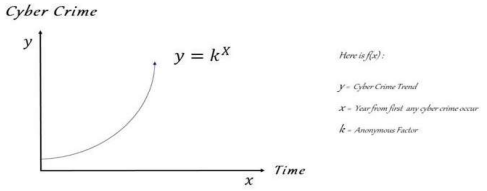
ปัจจัยการไร้ตัวตน (Anonymous factor) เมื่อ k = 2 จะได้ว่า

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

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

$$k = 2$$

แทนค่า $f(y) = 2^x$

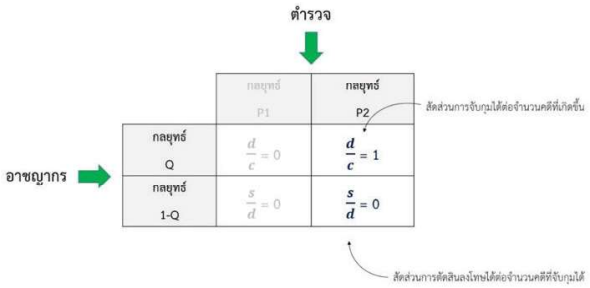


ภาพที่ 9 มโนทัศน์อาชญากรรมไซเบอร์ในสังคมเป็นฟังก์ชันเพิ่ม

สถานการณ์ที่ 2 เมื่อ 1 < k < 2

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

ตารางที่ 3 Payoff Matrix เมื่อสถานการณ์อาชญากรรมไซเบอร์มี เมื่อ 1 < k < 2



จะเห็นได้ว่า เมื่อค่า d เริ่มมีค่ามากกว่า 0 คือ เริ่มสามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้มีค่า 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

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

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

$$k = 1.99$$

แทนค่า $f(y) = 1.99^{x}$

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

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

$$k = 2 - \left[\frac{5}{10} + \frac{s}{d}\right] \quad (d/c = 0.5,\ s/d = 0)$$

$$k = 1.5$$

แทนค่า $f(y) = 1.50^{x}$

ทำให้เข้าใจว่า หากเลขฐานลดจำนวนลง ความชันเส้นกราฟจะลดตาม แต่ยังเป็นกราฟฟังก์ชันเพิ่มในอัตราที่ลดลง (Diminishing) เพราะยังยกกำลัง x

สถานการณ์ที่ 3 เมื่อ k = 1

เมื่อค่า d มีค่ามากขึ้นเรื่อยจนเท่ากับ 1 สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ทุกคดี ค่า k เท่ากับ 1 เป็นจุดเปลี่ยนฟังก์ชันลดใน กราฟของสมการเอ็กซ์โพเนนเชียล ดังตัวอย่างในสมการนี้

ตัวอย่างสมการ

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

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

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

$$k = 1$$

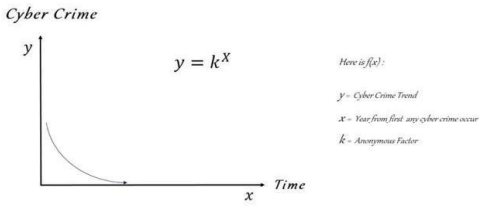
แทนค่า $f(y) = 1^{x}$

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

(ค) 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



ภาพที่ 10 มโนทัศน์อาชญากรรมไซเบอร์ในสังคมเป็นฟังก์ชันลด

ดังตัวอย่างสมมุติในสมการนี้ เมื่อปัจจัยการไร้ตัวตน (Anonymous factor) เป็นฟังก์ชันเพิ่มเมื่อ 0 < k < 1

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

$$k = 2 - \left[\frac{\cancel{10}^{1}}{\cancel{10}} + \frac{\cancel{5}^{0.5}}{\cancel{10}}\right]$$

$$k = 0.5$$

แทนค่า $f(y) = 0.5^x$

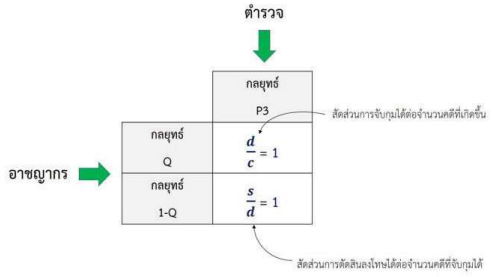
(ง) เมื่อเลขฐานเท่ากับ 0 สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor)

คุณสมบัติของ ฟังก์ชันเอ็กซ์โพเนนเชียล เมื่อเลขฐาน a มีค่าเท่ากับ 0 ฟังก์ชันก็มีค่า y เท่ากับ 0 สอดคล้องกับปัจจัยการไร้ตัวตน (Anonymous factor) เมื่อค่า k เท่ากับ 0 หมายความว่าอาชญากรรมไซเบอร์นั้นหมดไปจากสังคม

สถานการณ์ที่ 5 เมื่อ k = 0

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

ตารางที่ 4 Payoff Matrix เมื่อสถานการณ์อาชญากรรมไซเบอร์มี ค่า k = 0



เมื่อค่า d มีค่ามากขึ้นเรื่อยๆ จนเท่ากับ 1 สามารถสืบสวนจับกุมนำตัวอาชญากรมาดำเนินคดีได้ทุกคดีแล้ว และจำนวนคดีที่สามารถรวบรวมพยานหลักฐานดิจิทัลเอาผิดทางอาญาได้ คือ s สามารถเพิ่มจำนวนการดำเนินคดีเอาผิดอาญามากขึ้นเรื่อยๆ และลดสัดส่วนการยกฟ้องลงเรื่อยๆ จน ค่า k เท่ากับ 0 กราฟของสมการ เอ็กซ์โพเนนเชียล ลดลงจน y มีค่าเท่ากับ 0 ดังตัวอย่างสมมุติในสมการนี้

ปัจจัยการไร้ตัวตน (Anonymous factor) เป็นฟังก์ชันเพิ่มเมื่อ k = 2

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

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

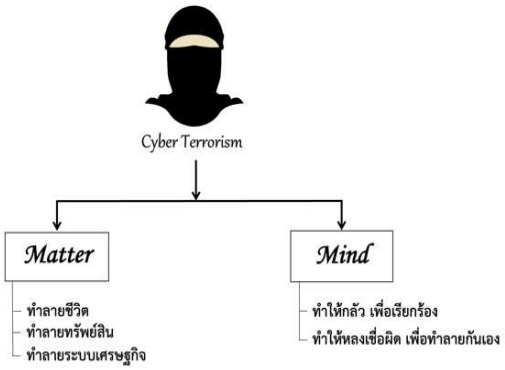
$$k = 0$$

แทนค่า $f(y) = 0^x$

7. สรุปผลและข้อเสนอแนะ

อาชญากรไซเบอร์ แตกต่างจากอาชญากรประเภทอื่นตรงที่ ไม่ก่ออาชญากรรม “ซึ่งหน้า” ต่อเหยื่อ [2] ซึ่งแตกต่างจากอาชญากร Street crime อื่นๆ เช่น การวิ่งราวทรัพย์กระทำซึ่งหน้าเหยื่อ การปล้นทรัพย์ซึ่งหน้าเหยื่อ การทำร้ายร่างกาย เป็นต้น แต่อาชญากรไซเบอร์ระมัดระวังเรื่องการไม่เปิดเผยตัวตน ความลับ การปิดบังอำพราง ตลอดจนการใช้ Bot หรือ AI คิดหาทางก่ออาชญากรรมแทนตน เป็นเรื่องสำคัญที่สุด และในทางตรงกันข้ามเมื่อ ปัจจัยการไร้ตัวตนในเทคโนโลยีใดหายไป อาชญากรรมไซเบอร์ประเภทนั้นก็จะหายไปด้วย เพราะอาชญากรไซเบอร์จะไม่ตัดสินใจเลือกใช้เทคโนโลยีนั้นประกอบอาชญากรรม

แนวโน้มการก่อการร้ายก็เช่นกัน การไร้ตัวตนบนโลกไซเบอร์ยังเป็นประโยชน์ต่อการก่อการร้ายสมัยใหม่และสร้างความเสียหายได้มากกว่าการก่อการร้ายแบบเดิม



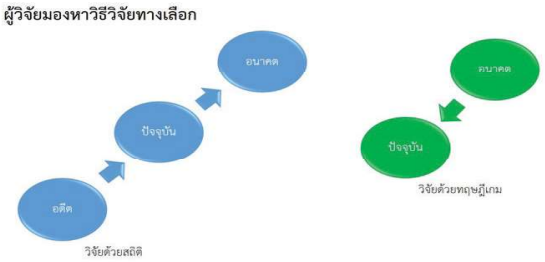
ภาพที่ 11 การไร้ตัวตนกับการก่อการร้ายไซเบอร์

กลุ่มก่อการร้ายก็คิดอย่างเป็นเหตุเป็นผลเช่นเดียวกับอาชญากรไซเบอร์ “การไร้ตัวตน คือ โอกาส” ในการตัดสินใจลงมือก่อการร้าย

ดังนั้นวิธีป้องกันการก่อการร้ายทางไซเบอร์ต้องมุ่งไปที่การเปิดเผยตัวตนเปิดเผยที่มาของอุปกรณ์ปลายทาง (Terminals) และปิดกั้นการสื่อสารอุปกรณ์ปลายทางที่

ไม่สามารถระบุตัวตนผู้ใช้ได้ และเฝ้าระวังเทคโนโลยีใหม่ๆ จากโลกไซเบอร์ว่ามีโอกาสใช้ในการก่อการร้ายมากน้อยเพียงใด [6]

วิธีวิจัยโดยใช้การคิดย้อนกลับแบบ Backward induction [1] หาผลลัพธ์ในอนาคตแล้วคิดย้อนกลับมาปัจจุบัน เป็นจุดแตกต่างจากการวิจัยทางสถิติในอดีตเพื่อทำนายอนาคต ซึ่งเป็นประโยชน์ต่อวิธีวิจัยทางเลือกที่มีข้อมูลสถิติน้อย



ภาพที่ 12 การพิจารณากระบวนทัศน์ทางเลือกของผู้วิจัยระหว่างการใช้สถิติและทฤษฎีเกม

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

สมการ Payoff Function ได้ชี้ให้เห็นความสำคัญที่สุดที่แสดงความสัมพันธ์ออกมาด้วย ปัจจัยการไร้ตัวตน (Anonymous factors) หรือ ค่า k โดยได้นำมาอธิบายรูปแบบความสัมพันธ์เพิ่มเติมเป็นแบบจำลองแนวโน้มการเกิดอาชญากรรมไซเบอร์ (Shark fin curve) ที่ริเริ่มเป็นต้นแบบนำมาพัฒนาประยุกต์ใช้ได้อย่างดี โดยการสร้างรูปแบบความสัมพันธ์หรือสร้าง Model แสดงความสัมพันธ์การเชื่อมโยงระหว่าง การไร้ตัวตน (Anonymity) กับอาชญากรรมไซเบอร์ และนำมาตั้งเป็นมโนทัศน์เป็นฟังก์ชันเอ็กโพเนนเชียล มาใช้อธิบายความสัมพันธ์ของอาชญากรรมไซเบอร์กับปัจจัยการไร้ตัวตน และยังเป็นจุดร่วมของการก่อการร้ายทางไซเบอร์

สมการคณิตศาสตร์ (3)-(4) ที่ได้จากงานวิจัยนี้จะเป็นอัลกอริทึมให้ระบบคอมพิวเตอร์ประมวลผลเพื่อพยากรณ์แนวโน้มการเกิดอาชญากรรมไซเบอร์หรือการก่อการร้าย แสดงผลในห้องบัญชาการ (War room) ในการเฝ้าติดตามสถานการณ์เพื่อกำหนดมาตรการป้องกันและปราบปราม และผู้วิจัยเชื่อว่าเป็นการบุกเบิกงานวิชาการที่น่าสนใจให้ผู้วิจัยรุ่นต่อไปได้ทำวิจัยเพิ่มเติมต่อไป

8. บรรณานุกรม

(1) ไชยันต์ ไชยพร, "Jon elster & Rational choice theory", *สำนักพิมพ์ way of book*, มีนาคม (2560).

(2) ปรเมศวร์ กุมารบุญ, "ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์", *ดุษฎีนิพนธ์, จุฬาลงกรณ์มหาวิทยาลัย*, (2563).

(3) L.E. Cohen, M. Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review*, pp. 44, (1979).

(4) E. Prisner, "Game Theory through Examples", *Published and Distributed by The Mathematical Association of America*, Washington, DC, (2014).

(5) L.E. Daniel, L.E. Daniel, ผู้แปล สุนีย์ สกาวรัตน์, "การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย", *บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)*, (2559).

(6) M. E. Kabay, "A Brief History of Computer Crime: An Introduction for Students", *School of Graduate Studies*, Norwich University, (2008).

(7) ITU Development, "Understanding cybercrime: phenomena, challenges and legal response", *The ITU publication*, September (2012).