บทความวิชาการ

การวิเคราะห์อาชญากรรมไซเบอร์ในประเทศไทยด้วยแนวคิดสามเหลี่ยมอาชญากรรม*

CYBERCRIME IN THAILAND: THE ANALYSIS THROUGH THE CRIME TRIANGLE FRAMEWORK

กิตติพันธ์ แท่นตั้งเจริญชัย*, ปกป้อง ศรีสนิท
Kittipan Tantangjareonchai, Pokpong Srisanit
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ กรุงเทพมหานคร ประเทศไทย
Faculty of Law, Thammasat University, Bangkok, Thailand
*Corresponding author E-mail: Kittipan.tan@dome.tu.ac.th

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์สถานการณ์และสาเหตุของปัญหาอาชญากรรมไซเบอร์ในประเทศไทย โดยประยุกต์ใช้แนวคิดสามเหลี่ยมอาชญากรรม เพื่อทำความเข้าใจองค์ประกอบสามประการ ได้แก่ เหยื่อหรือเป้าหมายที่เหมาะสม ผู้กระทำผิดที่มีแรงจูงใจ และการขาดผู้พิทักษ์ที่สามารถยับยั้งได้ อันนำไปสู่การเสนอแนะแนวทางการป้องกันอาชญากรรมเชิงรุก ผลการศึกษาพบว่า องค์ประกอบของสามเหลี่ยมอาชญากรรม 1) เหยื่อหรือเป้าหมายที่เหมาะสม มิใช่กลุ่มผู้สูงอายุหรือผู้ที่ขาดความรู้ทางเทคโนโลยี แต่กลับเป็นกลุ่มคนวัยทำงานอายุ 31 - 40 ปี ซึ่งเป็นผู้ใช้งานเทคโนโลยีจำนวนมาก แต่มีความรู้ด้านความปลอดภัยต่ำ 2) ผู้กระทำผิดที่มีแรงจูงใจ มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติที่ปฏิบัติการอย่างเป็นระบบ โดยมีผลประโยชน์ทางการเงินเป็นหลัก และ 3) การขาดผู้พิทักษ์ ช่องว่างของการบังคับใช้กฎหมายที่เน้นการตั้งรับมากกว่าเชิงรุก ซึ่งพิสูจน์ได้จากอัตราการอายัดทรัพย์สินคืนที่อยู่ในระดับต่ำมาก ดังนั้น การแก้ไขปัญหาอาชญากรรมไซเบอร์จำเป็นต้องอาศัยยุทธศาสตร์การป้องกันที่ตัดวงจรของสามเหลี่ยมอาชญากรรม ด้วยข้อเสนอแนะ 3 ประการ ได้แก่ 1) การเสริมสร้างความเข้มแข็งให้แก่เหยื่อผ่านการบูรณาการความรู้และทักษะด้านความปลอดภัยไซเบอร์เข้าสู่ระบบการศึกษา 2) การเพิ่มความเสี่ยงให้แก่ผู้กระทำผิด โดยเปลี่ยนจากการสืบสวนเชิงรับไปสู่การบังคับใช้กฎหมายเชิงรุก และ 3) การสร้างระบบให้หน่วยงานบังคับใช้กฎหมายเข้มแข็ง ผ่านการบูรณาการความร่วมมืออย่างไร้รอยต่อระหว่างภาครัฐ ภาคเอกชน เพื่อสร้างกลไกการป้องกันปราบปรามที่มีประสิทธิภาพและทันต่อสถานการณ์ ซึ่งผลจากการศึกษานี้จะทำให้ประชาชนในสังคมสามารถนำความรู้ไปใช้ในการป้องกันตนเองจากอาชญากรรมไซเบอร์ได้

คำสำคัญ: อาชญากรรมไซเบอร์ในประเทศไทย, สามเหลี่ยมอาชญากรรม, การป้องกันอาชญากรรมไซเบอร์

* Received 17 August 2025; Revised 18 September 2025; Accepted 20 September 2025

Abstract

This article analyzes the circumstances of cybercrime in Thailand by applying the Crime Triangle framework. The objective is to understand the three core elements including, the suitable target, the motivated offender, and the absence of a capable guardian to propose proactive crime prevention strategies. The study indicates that 1) The suitable target is not the elderly or technologically illiterate, but rather the working-age population (between 31-40 years old), who are heavy technology users with low cyber security awareness. 2) The motivated offender is a transnational criminal organization operating systematically, with financial gain as the primary motive. and 3) The absence of the guardian is evident in a reactive law enforcement approach rather than proactive law enforcement approach, proven by an exceedingly low asset recovery rate. Consequently, addressing cybercrime necessitates a prevention strategy focused on disrupting the crime triangle. Three recommendations have been proposed, which are 1) Empowering potential victims by integrating cybercrime knowledge and skills into the educational system. 2) Increasing the risk for offenders by shifting from a reactive investigative model to proactive law enforcement approach. 3) Strengthening the law enforcement framework through seamless collaboration between public and private sectors to establish an efficient and effective mechanism for prevention and suppression. The results of this study are intended to equip the public with the knowledge necessary to protect themselves from cybercrime.

Keywords: Cybercrime in Thailand, Crime Triangle, Cybercrime Prevention

บทนำ

ด้วยปัจจุบันเทคโนโลยีและระบบเครือข่ายอินเทอร์เน็ตพัฒนาอย่างรวดเร็วอยู่ตลอดเวลา ประกอบกับประชาชนคนไทยนั้นมีสถิติที่ใช้งานบนโลกอินเทอร์เน็ตเฉลี่ยสูงถึง 8 ชั่วโมงต่อวัน และใช้อยู่บนแพลตฟอร์มโซเชียลมีเดียและอีคอมเมิร์ซ อาทิ Youtube Facebook Line Tiktok Instragram Shopee Lazada (Datareportal, 2025) พฤติกรรมเหล่านี้สะท้อนว่าคนไทยใช้อินเทอร์เน็ตเป็นปัจจัยสำคัญของการดำรงชีวิตแบบขาดไม่ได้ ดังนั้นเมื่อมีผู้ใช้ออนไลน์อยู่ในโลกไซเบอร์จำนวนมาก ทำให้อาชญากรรมบนท้องถนน (Street Crime) หรืออาชญากรรมแบบดั้งเดิม เปลี่ยนแปลงมาเป็นอาชญากรรมไซเบอร์บนโลกออนไลน์ ซึ่งทวีความรุนแรงกลายเป็นปัญหาระดับชาติสร้างความเสียหายให้กับประชาชน สังคมและเศรษฐกิจในวงกว้าง จากข้อมูล สำนักงานตำรวจแห่งชาติ ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 30 มิถุนายน 2568 มีคดีอาชญากรรมไซเบอร์เกิดขึ้น 955,723 คดี มูลค่าความเสียหายสูงถึง 93,685 ล้านบาท (ศูนย์บริหารการรับแจ้งความออนไลน์, 2568) ดังนั้น จะเห็นได้ว่าภัยออนไลน์นั้นเป็นภัยคุกคามสวัสดิภาพของประชาชนที่จะต้องแก้ไขปัญหาอย่างเร่งด่วน ส่วนหนึ่งเป็นเพราะอาชญากรรมไซเบอร์นั้นมีลักษณะพิเศษที่สามารถปกปิดตนเองได้ ไร้ขอบเขต ไร้พรมแดน ทำให้ยากต่อการสืบสวนสอบสวนติดตามจับกุม รวมถึงการบังคับใช้กฎหมายก็ยังไม่มีประสิทธิภาพ สภาพการณ์ดังกล่าวทำให้ผู้กระทำมีเหตุผลตามหลักทฤษฎี

อาชญาวิทยาในเรื่องแรงจูงใจในการกระทำผิด ว่าได้ประเมินความเสี่ยงและผลตอบแทนแล้วว่าการก่ออาชญากรรมไซเบอร์นั้นมีความเสี่ยงต่ำแต่ได้ผลตอบแทนสูง ทำให้เกิดสภาพแวดล้อมที่เอื้อให้แก่ผู้กระทำความผิด บทความนี้จึงมีวัตถุประสงค์เพื่อศึกษาวิเคราะห์อาชญากรรมไซเบอร์ในประเทศไทยอย่างเป็นระบบ โดยประยุกต์ใช้กรอบแนวคิดสามเหลี่ยมอาชญากรรม (Crime Triangle) จากทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ซึ่งเป็นรากฐานสำคัญของแนวคิดการป้องกันอาชญากรรมโดยใช้สถานการณ์เป็นกรอบในการวิเคราะห์ ซึ่งประกอบด้วยองค์ประกอบ 3 ประการ คือ 1) เหยื่อหรือเป้าหมายที่เหมาะสม 2) ผู้กระทำผิดที่มีแรงจูงใจ 3) การขาดผู้พิทักษ์ ทั้งนี้เพื่อหาแนวทางมาตรการป้องกันอาชญากรรมไซเบอร์เชิงรุกที่มีประสิทธิภาพ และสามารถรับมือความท้าทายของอาชญากรรมไซเบอร์ในยุคปัจจุบันได้

ความหมายอาชญากรรมไซเบอร์

วิวัฒนาการของอาชญากรรมทางไซเบอร์ ได้พัฒนาเปลี่ยนแปลงมาตามลำดับ โดยมีชื่อเรียกแตกต่างหลากหลาย ตั้งแต่ อาชญากรรมคอมพิวเตอร์ และเปลี่ยนแปลงตามพัฒนาการของเทคโนโลยีตามแต่ละยุคสมัย จนถึงปัจจุบันส่วนใหญ่ใช้คำว่า อาชญากรรมไซเบอร์ (Cybercrime) (สาวตรี สุขศรี, 2563) แต่อย่างไรก็ตาม ในปัจจุบันยังไม่มีความหมายของคำว่า อาชญากรรมทางไซเบอร์ ที่เป็นสากลและยอมรับกันทั่วไป โดยจะเป็นการกำหนดนิยามแบบภาพรวม โดยจะขึ้นอยู่กับบริบทของแต่ละประเทศว่าจะแปลความหมายครอบคลุมมากน้อยเพียงใด การที่ยังไม่มีความหมายที่แน่นอนนี้ส่วนหนึ่งเป็นเพราะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว ทำให้ยังไม่สามารถให้คำจำกัดความได้ว่าการกระทำความผิดอะไรบ้างที่จะเป็นอาชญากรรมไซเบอร์ (Ajayi, E., 2016) ทั้งนี้ จากการศึกษาพบว่า ส่วนใหญ่แล้วจะให้ความหมาย อาชญากรรมไซเบอร์ คือ การกระทำใด ๆ ที่ผิดกฎหมายซึ่งเกี่ยวข้องโดยตรงกับการใช้คอมพิวเตอร์ ระบบและข้อมูลคอมพิวเตอร์ เครือข่ายดิจิทัล เทคโนโลยีสารสนเทศ ทั้งในบทบาทที่ตกเป็นเป้าหมาย (Target) และเป็นเครื่องมือ (Tool) ที่ใช้ในการกระทำความผิด โดยแบ่งออกเป็น 2 ประเภทหลัก คือ 1) อาชญากรรมไซเบอร์โดยแท้ (Cyber-dependent Crimes) คือ อาชญากรรมที่สามารถกระทำผิดได้ก็ต่อเมื่อต้องใช้คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศโดยตรง ซึ่งรูปแบบผู้กระทำความผิดในลักษณะนี้ คือ ใช้คอมพิวเตอร์เป็นเป้าหมาย (Computer as a Target) เช่น การเจาะระบบ (Hacking) การโจมตีโดยปฏิเสธการให้บริการ (Distributed Denial of Service: DDoS) รวมทั้งโปรแกรมไม่พึงประสงค์ (Malicious Software: Malware) เป็นต้น และ 2) อาชญากรรมไซเบอร์แบบผสมจากอาชญากรรมดั้งเดิมที่ใช้คอมพิวเตอร์หรือเทคโนโลยีเป็นเครื่องมือช่วยในการกระทำความผิด (Cyber-enabled Crimes) สำหรับรูปแบบของผู้กระทำความผิดในลักษณะนี้ คือ ใช้เทคโนโลยีเป็นเครื่องมือเข้ามาช่วยในการกระทำความผิด (Computer as a Tool) เช่น การฉ้อโกงออนไลน์ การเผยแพร่ภาพลามกอนาจารเด็ก การกลั่นแกล้งทางออนไลน์ (Cyberbullying) เป็นต้น (Clough, J., 2015)

ความคลุมเครือในนิยามความหมายของอาชญากรรมไซเบอร์ไม่เพียงแต่เป็นปัญหาเชิงภาษา แต่ยังเป็นปัญหาเชิงโครงสร้างที่เป็นอุปสรรคต่อการพัฒนากฎหมายให้สอดคล้องกัน รวมถึงความร่วมมือระหว่างประเทศด้วย แต่อย่างไรก็ตามได้ข้อค้น พบว่า การแก้ปัญหาเรื่องคำนิยามนั้น สามารถใช้แนวทางในการจำแนกประเภทการกระทำผิดอาชญากรรมไซเบอร์ (Typology-related Approach) ซึ่งเป็นการพิจารณาและแบ่งกลุ่มอาชญากรรมตามลักษณะการกระทำผิดต่าง ๆ (Gercke, M., 2011); (คณาธิป ทองรวีวงศ์, 2563) ซึ่งแนวทางนี้เป็นรากฐานการจัดหมวดหมู่

อาชญากรรมตามที่กำหนดไว้ในอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime) ของสภายุโรป (Council of Europe) ซึ่งถือเป็นเครื่องมือทางกฎหมายระหว่างประเทศที่มีมาตรฐานที่สุดในด้านอาชญากรรมไซเบอร์ โดยได้แบ่งอาชญากรรมไซเบอร์เป็น 4 ประเภท คือ 1) การกระทำความผิดต่อความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ (อาชญากรรมไซเบอร์โดยแท้) 2) การกระทำความผิดโดยใช้คอมพิวเตอร์เป็นเครื่องมือ (อาชญากรรมดั้งเดิมที่ใช้คอมพิวเตอร์เป็นเครื่องมือ) 3) การกระทำความผิดเกี่ยวกับเนื้อหา 4) การกระทำความผิดเกี่ยวกับลิขสิทธิ์เครื่องหมายการค้า (Council of Europe, 2001)

ลักษณะพิเศษของอาชญากรรมไซเบอร์

จากปัญหาอาชญากรรมไซเบอร์ที่มีการขยายตัวอย่างรวดเร็วและเป็นภัยคุกคามต่อประชาชนที่ยังไม่สามารถป้องกันได้อย่างมีประสิทธิภาพนั้น ปัจจัยสำคัญนั้น คือ ลักษณะพิเศษของอาชญากรรมไซเบอร์ที่ไม่เหมือนอาชญากรรมดั้งเดิม กล่าวคือ 1) อินเตอร์เน็ตเป็นปัจจัยสำคัญอย่างขาดไม่ได้ทำให้จำนวนผู้เกี่ยวข้องกับอาชญากรรมไซเบอร์มีจำนวนเพิ่มมากขึ้นเรื่อย ๆ ทั้งตัวผู้กระทำผิดและเหยื่อหรือเป้าหมาย 2) สามารถปกปิดตัวตนได้ในโลกไซเบอร์ ซึ่งเป็นลักษณะพิเศษที่สำคัญที่ทำให้ผู้กระทำผิดตัดสินใจกระทำผิดสาเหตุเพราะสามารถปกปิดตัวเองได้มีความเสี่ยงน้อยที่จะถูกจับ 3) อาชญากรรมไซเบอร์มีความไร้ขอบเขต ไร้พรมแดน ต่างกับอาชญากรรมดั้งเดิมที่ใช้หลักทางกายภาพ แต่ในพื้นที่ไซเบอร์ผู้กระทำผิดสามารถอยู่ที่ไหนก็ได้ในโลก และออนไลน์เข้ามากระทำผิดในประเทศไทย ลักษณะพิเศษนี้ทำให้อาชญากรรมไซเบอร์ส่วนใหญ่เป็นอาชญากรรมข้ามชาติ ซึ่งต้องอาศัยความร่วมมือระหว่างประเทศในการแก้ไขปัญหา จากลักษณะพิเศษของอาชญากรรมไซเบอร์เหล่านี้ทำให้เกิดความยากในการสืบสวนสอบสวน การระบุตัวผู้กระทำความผิด การรวบรวมพยานหลักฐานดิจิทัล จึงเป็นสาเหตุสำคัญของอาชญากรรมไซเบอร์ที่เพิ่มสูงขึ้น (Dodge, C. E. & Burruss, G., 2019) อย่างไรก็ตามการแก้ไขปัญหาอาชญากรรมไซเบอร์ต้องเริ่มต้นที่สาเหตุของการเกิดอาชญากรรม ซึ่งในการศึกษานี้จะได้ใช้แนวคิดสามเหลี่ยมอาชญากรรมเป็นกรอบในการวิเคราะห์ต่อไป

แนวคิดสามเหลี่ยมอาชญากรรม

สามเหลี่ยมอาชญากรรม (Crime Triangle) เป็นองค์ประกอบที่อยู่ในทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ของ Cohen และ Felson ในปี ค.ศ.1979 โดยมีหลักการว่ากิจวัตรประจำวันที่บุคคลกระทำอยู่ในทุกวันเป็นประจำสม่ำเสมอนั้น ก่อให้เกิดเงื่อนไขหรือโอกาสของผู้กระทำความผิดที่มีแรงจูงใจที่จะกระทำความผิดต่อบุคคลนั้น ๆ ตัวอย่างเช่น การไม่อยู่บ้านเป็นประจำเพราะต้องออกไปนอกบ้านหรือต้องไปทำงานบ้านไม่มีคนเฝ้าก่อให้เกิดโอกาสหรือแรงจูงใจของผู้กระทำความผิด ที่จ้องจะลักขโมยทรัพย์สินภายในบ้าน โดยได้อธิบายสาเหตุการเกิดอาชญากรรม เกิดจากการบรรจบกันขององค์ประกอบสามประการในเวลาและสถานที่เดียวกัน ได้แก่ 1) เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target) 2) ผู้กระทำความผิดที่มีแรงจูงใจ (Motivated Offender) และ 3) การขาดหายไปของผู้พิทักษ์ที่สามารถยับยั้งได้ (Absence of Capable Guardianship) ซึ่งเรียกว่าสามเหลี่ยมอาชญากรรม (Crime Triangle) หัวใจสำคัญของทฤษฎีนี้อยู่ที่แนวคิดเชิงรุก คือ แทนที่จะมุ่งเน้นการลงโทษผู้กระทำผิดภายหลังเกิดเหตุเพียงอย่างเดียว แนวทางนี้จะให้ความสำคัญกับการจัดการสถานการณ์หรือสภาพแวดล้อม เพื่อลดหรือกำจัดโอกาสในการก่ออาชญากรรมตั้งแต่แรก หรือเรียกว่าการป้องกันก่อนเกิดเหตุ (Cohen, L. E. & Felson, M., 1979)

อย่างไรก็ตามการนำแนวคิดสามเหลี่ยมอาชญากรรมมาอธิบายการเกิดของอาชญากรรมนั้น เป็นการอธิบายอาชญากรรมที่เกิดขึ้นในโลกทางกายภาพ แต่ในทางตรงกันข้าม อาชญากรรมไซเบอร์เป็นอาชญากรรมที่เกิดขึ้นในโลกดิจิทัล ดังนั้นจึงมีความท้าทายทางทฤษฎีที่ก่อเกิดข้อขัดแย้งขึ้นเป็น 2 กลุ่ม คือ กลุ่มหนึ่งเห็นว่าองค์ประกอบของสามเหลี่ยมอาชญากรรมเป็นองค์ประกอบพื้นฐานทั่วไปของการเกิดอาชญากรรมจึงสามารถนำมาวิเคราะห์อาชญากรรมไซเบอร์ได้ (Grabosky, P. N., 2001); (Choi, K. S., 2015) และอีกกลุ่มหนึ่งแย้งว่าการเกิดอาชญากรรมนั้นเวลาและสถานที่จะต้องมีความสัมพันธ์กันอาชญากรรมจึงจะเกิด แต่สำหรับในโลกไซเบอร์นั้นสภาพแวดล้อมเปลี่ยนแปลงจากเดิม เวลาและสถานที่ไม่ใช่เรื่องหลัก เพราะอาชญากรรมไซเบอร์นั้นสามารถเกิดขึ้นเมื่อใดที่ไหนก็ได้ในโลกออนไลน์ จึงนำแนวคิดสามเหลี่ยมอาชญากรรมนี้มาใช้ไม่ได้ (Yar, M., 2005)

ทั้งนี้ ความท้าทายในเรื่องของโลกไซเบอร์ซึ่งแตกต่างไปจากโลกทางกายภาพ ไม่ว่าจะเป็นความไร้ตัวตน การไร้พรมแดนสามารถทำได้ทุกที่ ทุกเวลา ต่างจากทางกายภาพที่สถานที่และเวลาต้องตรงกันจึงเกิดอาชญากรรมขึ้นได้ ดังนั้นจึงมีนักวิชาการได้พัฒนาทฤษฎีกิจวัตรประจำวัน ขยายความเป็นทฤษฎีกิจวัตรประจำวันไซเบอร์ (Cyber-Routine Activity Theory: CRAT) โดยเห็นว่าสามารถนำเอาองค์ประกอบในกรอบแนวคิดสามเหลี่ยมอาชญากรรมมาใช้ในการอธิบายอาชญากรรมไซเบอร์ได้ (Choi, K. S. et al., 2019) การนำแนวคิดสามเหลี่ยมอาชญากรรมมาปรับใช้ในอาชญากรรมไซเบอร์ จำเป็นต้องมีการตีความหมายองค์ประกอบให้เกิดความสอดคล้องกับโลกไซเบอร์ นั่นคือ สถานที่ จากโลกทางกายภาพสู่โลกไซเบอร์ เช่น แพลตฟอร์มโซเชียลมีเดีย เว็บไซต์ แอปพลิเคชัน หรือเครือข่ายคอมพิวเตอร์ โดยมีองค์ประกอบ 3 ประการ (Vakhitova, Z. I., 2025) ดังนี้

1. เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target) คือ คน สิ่งของหรือทรัพย์สิน รวมถึงสถานที่ที่ผู้กระทำผิดต้องการเลือกกระทำ ในมุมมองของผู้กระทำผิด ความเหมาะสมของเป้าหมายสามารถประเมินหรือวิเคราะห์ได้จากคุณลักษณะ 4 ประการ หรือเรียกว่าหลัก VIVA ได้แก่ 1) คุณค่าของเป้าหมาย (Value) ว่าเป้าหมายนั้นมีมูลค่าตามที่ต้องการหรือไม่ เป็นสิ่งที่อาชญากรไซเบอร์ต้องการจากเป้าหมายหรือเหยื่อ เช่น เงิน ข้อมูลส่วนบุคคล ข้อมูลความลับทางการค้าหรือบริษัท 2) ความเฉื่อย (Inertia) หมายถึง ลักษณะทางกายภาพของเป้าหมายว่ามีน้ำหนักมากน้อยเพียงใด ง่ายต่อการเคลื่อนย้ายหรือไม่อย่างไร ซึ่งปัจจัยนี้ในโลกไซเบอร์นั้นมีลักษณะเฉพาะความไม่มีตัวตน หรือสภาพไร้น้ำหนัก ซึ่งทำให้สามารถเคลื่อนย้าย คัดลอก ส่งต่อ ได้อย่างรวดเร็ว นอกจากนั้นยังมีความหมายรวมถึง ความสามารถในการตกเป็นเหยื่อ กล่าวคือ ทักษะในการป้องกันตนเอง การตระหนักรู้ถึงอาชญากรรมไซเบอร์ หากมีความตระหนักรู้มากก็ตกเป็นเหยื่อได้น้อยลง 3) การมองเห็นเป้าหมาย (Visibility) หมายถึง เป้าหมายนั้นเปิดเผย หรือง่ายต่อการโจมตีหรือไม่ ในโลกไซเบอร์เมื่อเชื่อมต่ออินเทอร์เน็ต ผู้กระทำผิดก็สามารถมองเห็นเป้าหมายหรือเหยื่อได้จากทุกมุมโลก และ 4) การเข้าถึงเป้าหมาย (Accessibility) เป้าหมายนั้นสามารถเข้าถึงง่ายหรือไม่ หรือสามารถหลบหนีได้ง่ายหรือไม่ ในโลกไซเบอร์เมื่อมีการเชื่อมต่ออินเทอร์เน็ตผู้กระทำผิดสามารถเข้าถึงเป้าหมายได้จากทั่วทุกมุมโลก ในระยะไกล

2. ผู้มีแรงจูงใจที่จะกระทำผิด (Motivated Offender) คือ ผู้กระทำความผิด หรือคนร้ายที่มีแรงจูงใจที่จะกระทำความผิด โดยอาชญากรกลุ่มนี้จะพิจารณาดูเป้าหมาย หรือเหยื่อที่เหมาะสม หรือคิดว่าอ่อนแอ รวมทั้งไม่มีการป้องกันที่ดีพอจากตัวเองและผู้ดูแลทำให้ตัดสินใจกระทำความผิด โดยจะเห็นว่า อาชญากรไซเบอร์นั้นไม่ใช่อาชญากรมือสมัครเล่น แต่เป็นอาชญากรที่มีลักษณะองค์กรอาชญากรรมข้ามชาติ มีการแบ่งหน้าที่กันทำอย่างเป็น

ระบบ เช่น นักเจาะระบบ (Hackers) นักก่อการร้ายทางไซเบอร์ (Cyberterrorists) มิจฉาชีพหลอกลวงทางไซเบอร์ ผู้สะกดรอยทางไซเบอร์ (Cyberstalkers) เป็นต้น

3. การขาดผู้พิทักษ์หรือ หน่วยงานกำกับดูแลการบังคับใช้กฎหมาย (Absence of Capable Guardianship) คือ การขาดผู้ปกป้องคุ้มครอง การไม่มีเจ้าหน้าที่ตำรวจคอยตรวจตรา หรือเพื่อนบ้านคอยเตือนภัย รวมถึงสถานที่นั้นไม่มีกล้องวงจรปิด หรือสัญญาณกันขโมย ซึ่งก็จะทำให้เกิดช่องโอกาสที่เหมาะสมกับคนร้ายในการก่ออาชญากรรมในโลกไซเบอร์ ผู้พิทักษ์เหล่านี้ แบ่งเป็น 3 มิติ คือ 1) ผู้พิทักษ์ทางเทคนิค หรือการป้องกันตนเองทางเทคนิค การใช้เครื่องมือทางเทคโนโลยีเพื่อป้องกันผู้ใช้ด้วยการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์ เช่น โปรแกรมป้องกันไวรัส Firewall รวมถึงระบบการป้องกันภัยคุกคามทางเทคนิค 2) ผู้พิทักษ์ที่เป็นมนุษย์ เช่น เพื่อน ครอบครัว สังคมออนไลน์ต่าง ๆ รวมถึงตัวผู้ใช้ในโลกออนไลน์ด้วย หรือการป้องกันตนเอง เป็นการกระทำของตัวเป้าหมายเองเพื่อลดความเปราะบาง เช่น การตั้งรหัสผ่านที่รัดกุม การมีความรู้เท่าทันและตระหนักถึงภัยคุกคามต่าง ๆ การจำกัดการเปิดเผยข้อมูลส่วนบุคคล และ 3) ผู้พิทักษ์ที่เป็นองค์กร กล่าวคือ หน่วยงานบังคับใช้กฎหมายทั้งภาครัฐและเอกชนที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ อัยการศาล สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กรมสอบสวนคดีพิเศษ รวมถึงหน่วยงานภาคเอกชนที่เกี่ยวข้อง เช่น สถาบันการเงิน หรือผู้ให้บริการทางอินเทอร์เน็ต ซึ่งองค์ประกอบในข้อนี้มีความสำคัญ หากสร้างความเข้มแข็งให้กับผู้พิทักษ์ได้มากก็จะทำให้การป้องกันอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ (สาวตรี สุขศรี, 2560)

กล่าวได้ว่า ทั้งสามองค์ประกอบนั้นมีความสัมพันธ์ซึ่งกันและกัน โดยอาชญากรรมจะเกิดขึ้นเมื่อมีครบองค์ประกอบทั้งสามประการ กล่าวคือ จะต้องมีเหยื่อหรือผู้ถูกกระทำ มีผู้กระทำความผิดที่มีแรงจูงใจ รวมทั้งการขาดการดูแลป้องกันที่ดีพอ หรือสภาพแวดล้อมหรือสถานการณ์ที่เอื้ออำนวยให้การกระทำผิดเกิดขึ้นได้ แต่อย่างไรก็ตาม หากขาดองค์ประกอบใดองค์ประกอบหนึ่งไปอาชญากรรมก็จะไม่สามารถเกิดขึ้นได้ ดังนั้น จึงนำแนวคิดการตัดองค์ประกอบต่าง ๆ เหล่านี้ออกไป เพื่อไม่ให้เกิดอาชญากรรมขึ้น จึงได้เป็นแนวทางการป้องกันอาชญากรรม โดยจะเห็นได้ว่า อาชญากรรมไซเบอร์มีลักษณะพิเศษที่ว่า ตัวเหยื่อ หรือผู้กระทำผิดนั้นสามารถอยู่กันคนละที่ ก็สามารถกระทำผิดในโลกออนไลน์ได้ การที่เหยื่อที่มีอยู่ตลอดเวลา รวมถึงผู้กระทำผิดที่สามารถเลือกเหยื่อหรือเป้าหมายที่อ่อนแอได้อยู่ตลอดเวลาเช่นเดียวกันนั้น ทำให้ปัจจัยที่ 3 คือ เป็นปัจจัยสำคัญในการตัดช่องโอกาสในการกระทำความผิดของอาชญากรไซเบอร์ ก็คือ การมีผู้พิทักษ์ที่แข็งแรง หรือมีหน่วยงานกับดูแลบังคับใช้กฎหมายที่เข้มแข็ง นั้นเป็นส่วนสำคัญอย่างมากในการป้องกันอาชญากรรมไซเบอร์

วิเคราะห์องค์ประกอบ “เหยื่อ” หรือ “เป้าหมาย”

สำหรับประเทศไทยนั้น การเข้าสู่สังคมดิจิทัลอย่างเต็มรูปแบบได้สร้างทั้งโอกาสและความเสี่ยงควบคู่กันไป โดยเฉพาะอย่างยิ่งการเปิดสภาพแวดล้อมหรือโอกาสที่จะทำให้เกิดอาชญากรรมไซเบอร์ขึ้นอย่างแพร่หลายและรุนแรง การเปลี่ยนแปลงนี้เห็นได้อย่างชัดเจนจากข้อมูลสถิติในปี พ.ศ. 2568 ที่ระบุว่าประเทศไทยมีประชากร 71.6 ล้านคน แต่กลับมีการเชื่อมต่อเครือข่ายโทรศัพท์มือถือมากถึง 99.5 ล้านเครื่อง ซึ่งสะท้อนให้เห็นว่าประชากรไทยจำนวนไม่น้อยมีอุปกรณ์สื่อสารมากกว่าหนึ่งเครื่อง นอกจากนี้คนไทยยังเป็นหนึ่งกลุ่มที่ใช้อินเทอร์เน็ตมาก โดยมีค่าเฉลี่ยการใช้งาน

สูงถึง 8 ชั่วโมงต่อวัน โดยสถิติการใช้โซเชียลมีเดียของเพศหญิงและเพศชายจะมีอัตราส่วนใกล้เคียงกัน คือ เพศหญิงร้อยละ 50.8 และเพศชายร้อยละ 49.2 (Datareportal, 2025) ทั้งนี้ ปัจจัยสำคัญที่เป็นตัวเร่งให้เกิดการเปลี่ยนแปลงนี้ คือ สถานการณ์การแพร่ระบาดของโควิด-19 ซึ่งบีบให้วิถีชีวิตของผู้คนต้องย้ายเข้าสู่แพลตฟอร์มออนไลน์อย่างรวดเร็วและเต็มรูปแบบ ไม่ว่าจะเป็นการทำงานจากที่บ้าน (Work from Home) การเรียนออนไลน์ หรือแม้กระทั่งการทำธุรกรรมทางการเงินและการซื้อขายสินค้า การเปลี่ยนแปลงอย่างกะทันหันนี้ได้สร้างช่องโอกาสให้กลุ่มมิจฉาชีพสามารถฉกฉวยและพัฒนารูปแบบการก่ออาชญากรรมไซเบอร์ได้ง่ายขึ้น (สำนักงานกิจการยุติธรรม, 2565) ปรากฏการณ์ดังกล่าวสะท้อนผ่านสถิติคดีอาชญากรรมไซเบอร์หรือคดีออนไลน์ที่ประชาชนแจ้งความผ่านศูนย์บริหารการรับแจ้งความออนไลน์ ของสำนักงานตำรวจแห่งชาติ (ศูนย์บริหารการรับแจ้งความออนไลน์, 2568) ซึ่งเผยให้เห็นรูปแบบของภัยคุกคามที่หลากหลายและซับซ้อนขึ้นอย่างต่อเนื่อง ตามภาพด้านล่างนี้

ภาพที่ 1 สถิติคดีอาชญากรรมไซเบอร์หรือคดีออนไลน์ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568

จากสถิติอาชญากรรมไซเบอร์ คดีออนไลน์ของศูนย์บริหารการรับแจ้งความออนไลน์ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568 มีจำนวนคดีทั้งหมด 955,723 คดี เฉลี่ยวันละ 785 เรื่องต่อวัน

และเมื่อวิเคราะห์ถึงตัวเหยื่อหรือเป้าหมาย แสดงให้เห็นว่ามีประชาชนจำนวนมากที่อยู่ในโลกออนไลน์และตกเป็นเหยื่อที่อ่อนไหวต่อการถูกหลอกลวง โดยกลุ่มคนที่ตกเป็นเหยื่ออาชญากรรมไซเบอร์มากที่สุด คือ กลุ่มคนวัยทำงาน คือ กลุ่มเกณฑ์อายุ 31 - 40 ปี มีสัดส่วนจำนวนร้อยละ 29.11 ตามมาด้วยกลุ่มเกณฑ์อายุ 41 - 50 ปี มีสัดส่วนจำนวนร้อยละ 20.52 และกลุ่มเกณฑ์อายุ 26 - 30 ปี มีสัดส่วนจำนวนร้อยละ 16.98

ส่วนกลุ่มคนที่ตกเป็นเหยื่ออาชญากรรมน้อยที่สุด คือ กลุ่มเกณฑ์อายุต่ำกว่า 18 ปี มีสัดส่วนจำนวนร้อยละ 0.63 ตามมาด้วยช่วงกลุ่มเกณฑ์อายุ 60 ปีขึ้นไปร้อยละ 6.76 และกลุ่มเกณฑ์อายุ 51 - 60 ปี สัดส่วนร้อยละ 10.65 และในกลุ่มคนที่ตกเป็นเหยื่อทั้งหมดนี้เป็นเพศหญิงถึงร้อยละ 64 และเพศชายร้อยละ 36 ตามตารางแสดงกลุ่มช่วงอายุที่ตกเป็นเหยื่อคดีอาชญากรรมไซเบอร์ ดังนี้

ตารางที่ 1 แสดงข้อมูลช่วงกลุ่มอายุของเหยื่ออาชญากรรมไซเบอร์ ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568

ข้อมูลเหยื่ออาชญากรรมไซเบอร์ในประเทศไทย
ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568

ลำดับ	กลุ่มอายุ	จำนวนร้อยละของเหยื่อทั้งหมด	เพศ	
			หญิง	ชาย
1	อายุต่ำกว่า 18 ปี	0.63		
2	อายุ 18 - 25	15.35		
3	อายุ 26 - 30	16.98		
4	อายุ 31 - 40	29.11	64%	36%
5	อายุ 41 - 50	20.52		
6	อายุ 51 - 60	10.65		
7	อายุ 60 ปีขึ้นไป	6.76		

หลักการวิเคราะห์เหยื่อ VIVA ได้ดังต่อไปนี้

- Value (คุณค่า) วิเคราะห์เป้าหมายได้ว่า กลุ่มวัยทำงานอายุ 31 - 40 ปี คือ กลุ่มประชากรที่อยู่ในช่วงที่มีศักยภาพในการหารายได้สูงสุด กล่าวคือ มีเงินเดือน มีบัญชีเงินฝาก มีบัตรเครดิต มีการลงทุน และมีอำนาจในการตัดสินใจทางการเงินของครอบครัว ทำให้คนกลุ่มนี้ตกเป็นเป้าหมายที่มีคุณค่าสูงสุดสำหรับอาชญากรที่มุ่งหวังผลประโยชน์ทางการเงิน

- Inertia (ความเฉื่อย แรงต้าน หรือการขาดซึ่งแรงต้าน) วิเคราะห์เป้าหมายได้ว่า แม้ว่าคนวัยทำงานกลุ่มนี้จะเป็นผู้ที่ใช้งานเทคโนโลยีดิจิทัลในชีวิตประจำวันได้อย่างคล่องแคล่ว แต่ความรู้ความสามารถจะเน้นไปที่การใช้งานมากกว่า ความปลอดภัย หรือเรียกว่ามีวัคซีนป้องกันภัยไซเบอร์น้อยส่วนหนึ่งเกิดมาจากการไม่ตระหนักรู้เท่าทันกลโกงความโลภที่อยากได้ผลตอบแทนสูงจากการลงทุน (ดูจากสถิติมูลค่าความเสียหายสูงสุดจากคดีหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ จำนวนกว่า 3 หมื่นล้านบาท) หรือความประมาทในการซื้อของออนไลน์ (ดูจากสถิติคดีซื้อของแล้วไม่ได้ของ ของไม่ตรงปก หรือหลอกลวงซื้อขายสินค้าหรือบริการมีสัดส่วนสูงสุดถึง 44.04%)

- Visibility and Accessibility (การมองเห็นและการเข้าถึง) วิเคราะห์เป้าหมายได้ว่า กิจวัตรประจำวันของคนวัยทำงานกลุ่มอายุ 31 - 40 ปี ที่ตกเป็นเหยื่อเยอะที่สุดนั้น มีพฤติกรรมการใช้โลกออนไลน์อย่างขาดไม่ได้ ไม่ว่าจะเป็นการธนาคารออนไลน์ (Mobile Banking) การใช้โซเชียลมีเดีย การซื้อขายสินค้าอีคอมเมิร์ซออนไลน์

หรือการทำงาน ทำให้เกิดร่องรอยทางดิจิทัล (Digital Footprint) จำนวนมาก สามารถถูกมองเห็นได้ง่าย รวมทั้งอาชญากรสามารถเข้าถึงได้ตลอด 24 ชั่วโมงผ่านช่องทางต่าง ๆ อาทิ อีเมล ข้อความในโซเชียลมีเดีย หรือโทรศัพท์มือถือที่ออนไลน์อยู่ตลอด

การวิเคราะห์นี้ชี้ให้เห็นว่าเป้าหมายหลักของอาชญากรไซเบอร์ในประเทศไทยไม่ใช่ผู้ที่ขาดความรู้ทางเทคโนโลยี แต่คือ กลุ่มคนทำงานที่ใช้ชีวิตในโลกดิจิทัลอย่างเต็มรูปแบบแต่ขาดความระมัดระวังด้านความปลอดภัย ส่วนข้อสันนิษฐานที่ว่าผู้สูงอายุ คือ เหยื่อที่เหมาะสมที่สุดนั้น ถูกหักล้างด้วยข้อมูลสถิติเชิงประจักษ์ เมื่อวิเคราะห์ด้วยกรอบ VIVA จะเห็นได้ว่า แม้ผู้สูงอายุจะมี Value คุณค่าในเชิงสินทรัพย์ดิจิทัล มีเงินเก็บที่สะสมมาจากช่วงวัยหนุ่มสาว หรือเงินหลังเกษียณ แต่มี Inertia ต่ำ คือ มีความรู้เทคโนโลยีน้อย ไม่ค่อยใช้โลกโซเชียล ทำให้ Visibility การมองเห็นหรือการเข้าใช้งานออนไลน์ที่ต่ำกว่า ในทางกลับกัน กลุ่มวัยทำงานอายุ 31 - 40 ปี คือ จุดที่เข้ากับหลักการ VIVA กล่าวคือ มี Value สูง Visibility สูง Access สูง แต่มี Inertia ด้านความปลอดภัยที่ต่ำทำให้ตกเป็นเป้าหมายที่ให้ผลตอบแทนคุ้มค่าที่สุดในมุมมองของอาชญากร

และกรณีที่เป็นเพศหญิงที่ตกเป็นเหยื่ออาชญากรรมไซเบอร์ จำนวนร้อยละ 64 และเพศชาย จำนวนร้อยละ 36 จะเห็นได้ว่าสัดส่วนการตกเป็นเหยื่ออาชญากรรมไซเบอร์นั้น ผู้หญิงมีอัตราส่วนมากกว่าผู้ชายถึง 2 ต่อ 1 แม้ว่าจากสถิติการใช้โซเชียลมีเดียของเพศหญิงและเพศชายจะมีอัตราส่วนใกล้เคียงกันก็ตาม ดังนั้น สถิติการตกเป็นเหยื่อแยกตามเพศชี้ให้เห็นว่า ความเปราะบางที่แตกต่างกันทางเพศนี้มีปัจจัยเชิงจิตวิทยา สังคม เข้ามาเกี่ยวข้อง กล่าวคือ เพศหญิงตกเป็นเป้าหมายของการติดตามคุกคามทางเพศได้ง่าย รวมถึงมีความเห็นอกเห็นใจผู้อื่น นอกจากนั้นประเภทอาชญากรรมไซเบอร์ก็มีส่วนในการเลือกกลโกงที่สอดคล้องกับเพศหญิง เช่น การซื้อของออนไลน์ หรือรักลวงหลอก (Romance Scam) เป็นต้น

วิเคราะห์องค์ประกอบ “ผู้กระทำความผิด”

ผู้กระทำผิดในคดีอาชญากรรมไซเบอร์มีแรงจูงใจที่ชัดเจน โดยเฉพาะอย่างยิ่ง ผลประโยชน์ทางด้านเงินเป็นเป้าหมายสูงสุด จะเห็นได้จากสถิติว่ามีมูลค่าความเสียหายจำนวนมหาศาลถึง 93,685,935,175 บาท ซึ่งเป็นเครื่องพิสูจน์ถึงแรงจูงใจอย่างมากที่ดึงดูดให้อาชญากรไซเบอร์ลงมือกระทำความผิด เนื่องจากได้ผลตอบแทนสูงในเวลาอันรวดเร็ว รวมทั้งมีความเสี่ยงต่ำที่จะถูกจับอีกด้วย เพราะอาชญากรใช้ข้อลักษณะพิเศษของอาชญากรรมไซเบอร์ได้อย่างเต็มที่ กล่าวคือ สามารถปิดบังซ่อนเร้นตัวตนที่แท้จริงได้ในโลกออนไลน์ และสามารถปฏิบัติการจากที่ใดก็ได้ในโลก ทำให้การบังคับใช้กฎหมายและการติดตามจับกุมเป็นไปได้ยากและซับซ้อน เพราะเป็นการก่ออาชญากรรมข้ามพรมแดนหรืออาชญากรรมข้ามชาติที่ไม่สามารถเข้าจับกุมได้ในทันที เมื่อเปรียบเทียบผลตอบแทนที่ได้เป็นจำนวนมากกับโอกาสที่จะถูกดำเนินคดีที่มีเพียงเล็กน้อย ทำให้อาชญากรรมไซเบอร์ทวีความรุนแรงขึ้นอย่างต่อเนื่อง รายละเอียดของคดีประเภทต่าง ๆ ที่สร้างความเสียหายปรากฏตามตารางดังต่อไปนี้

ตารางที่ 2 แสดงข้อมูลประเภทคดีอาชญากรรมไซเบอร์ที่เกิดมากที่สุด 5 ลำดับแรก ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568

ข้อมูลประเภทคดีอาชญากรรมไซเบอร์ที่เกิดมากที่สุด 5 ลำดับแรก
ระหว่างวันที่ 1 มีนาคม พ.ศ. 2565 ถึงวันที่ 30 มิถุนายน พ.ศ. 2568

ลำดับ	ประเภทคดีอาชญากรรมไซเบอร์	จำนวนคดี (เคส)	มูลค่าความเสียหาย (บาท)
1	หลอกลวงซื้อขายสินค้าหรือบริการ (ซื้อแล้วไม่ได้ ได้ไม่ตรงปก)	429,520	4,608,913,794
2	หลอกให้โอนเงินเพื่อทำงานฯ	117,491	13,636,241,708
3	หลอกให้กู้เงิน	88,048	3,687,217,219
4	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	68,391	30,750,853,633
5	ข่มขู่ทางโทรศัพท์ (Call Center)	58,687	10,745,856,973

โดยจากสถิติสถิติคดีอาชญากรรมไซเบอร์หรือคดีออนไลน์ตั้งแต่วันที่ 1 มีนาคม พ.ศ.2565 ถึงวันที่ 30 มิถุนายน พ.ศ.2568 จากศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ จะเห็นได้ว่ามูลค่าความเสียหายนั้นมีจำนวนมากถึง 91,392,313,419 บาท ทั้งนี้ จะพบว่า คดีอาชญากรรมไซเบอร์ที่เกิดขึ้นจำนวนมากและมีความเสียหายสูงที่สุด 5 ลำดับ ได้แก่

1. คดีหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ จำนวน 68,391 คดี มีมูลค่าความเสียหาย 30,750,853,633 บาท ตัวอย่างเช่น การสร้างแฟลตฟอร์มหรือแอปพลิเคชันการลงทุนปลอม โดยหลอกลวงว่าให้ผลตอบแทนสูง เช่น หลอกให้ซื้อขายหุ้น ซื้อขายทองคำ หรือคริปโทเคอร์เรนซี

2. คดีหลอกให้โอนเงินเพื่อนทำงานหรือทำภารกิจ จำนวน 117,491 คดี มีมูลค่าความเสียหาย 13,636,241,708 บาท ตัวอย่างเช่น หลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ หรือหลอกให้สมัครงานแล้วอ้างว่าเต็ม จึงให้ทำภารกิจลงทุนแทน

3. คดีข่มขู่ทางโทรศัพท์ (Call Center) จำนวน 58,687 คดี มีมูลค่าความเสียหาย 10,745,856,973 บาท ตัวอย่างเช่น การแอบอ้างหลอกลวงเป็นเจ้าหน้าที่จากหน่วยงานภาครัฐเพื่อสร้างความน่าเชื่อถือ หรือข่มขู่ให้กลัวแล้วให้โอนเงิน

4. คดีหลอกลวงซื้อขายสินค้าหรือบริการ (ไม่เป็นขบวนการ) จำนวน 429,520 คดี มีมูลค่าความเสียหาย 4,608,913,14794 บาท ตัวอย่างเช่น การหลอกว่ามีร้านขายสินค้าต่าง ๆ แต่เมื่อรับรายการออเดอร์ หรือรับเงินแล้วไม่ส่งของ หรือส่งของที่ไม่มีคุณภาพหรือไม่ตรงตามที่ตกลงกันไว้ให้

5. คดีหลอกให้กู้เงิน จำนวน 88,048 คดี มีมูลค่าความเสียหาย 3,687,217,219 บาท ตัวอย่างเช่น การหลอกว่ามีเงินกู้ดอกเบี้ยต่ำให้กู้ แต่ต้องโอนเงินมาก่อน และไม่ได้ให้เงินกู้จริง

จากสถิติคดีที่มูลค่าความเสียหายสูงที่สุด คือ การหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ หลอกให้โอนเงินเพื่อทำภารกิจ แก๊งค์คอลเซ็นเตอร์ หลอกลวงซื้อขายของออนไลน์ และหลอกให้กู้เงิน ตามลำดับ ทั้งนี้ จะเห็นได้ว่าคดีอาชญากรรมไซเบอร์ทั้งหมดนี้ไม่สามารถทำแต่เพียงลำพังคนเดียวได้ ดังนั้น ส่วนใหญ่จึงเป็นองค์กรอาชญากรรม คือ ปฏิบัติการเป็นขบวนการมีการแบ่งมอบหน้าที่กันทำเป็นเครือข่าย มีการจัดการอย่างเป็นระบบ มีการแลกเปลี่ยน

ความรู้ในการกระทำความผิด หรือมีการสอนกันเป็นหลักสูตร และที่สำคัญมีลักษณะข้ามชาติ ไม่ใช่อาชญากรมือสมัครเล่น

อย่างไรก็ตาม แรงจูงใจหลักของผู้กระทำผิดอาชญากรรมไซเบอร์ คือ ผลประโยชน์ทางการเงิน ซึ่งมีมูลค่ามหาศาล ดังนั้น ผู้กระทำผิดเหล่านี้จึงมีการพัฒนาปรับเปลี่ยนวิธีการ รูปแบบในการหลอกลวงอยู่ตลอดเวลา หากเหยื่อหรือผู้เสียหายตามไม่ทัน หรือไม่มีภูมิคุ้มกันในการป้องกันที่ดีก็จะตกเป็นเหยื่อ เช่น แก๊งคอลเซ็นเตอร์ หลอกเป็นเจ้าหน้าที่ของรัฐ หรือหน่วยงานต่าง ๆ เพื่อสร้างความน่าเชื่อถือและข่มขู่ให้เหยื่อกลัวและให้โอนเงิน หรือการหลอกให้ลงทุนว่าได้ผลตอบแทนสูง ก็มีรูปแบบการสร้างเว็บไซต์ แพลตฟอร์ม หรือแอปพลิเคชันลงทุนปลอม ให้เทรดหุ้น เทรดทองคำ เงินสกุลดิจิทัล หรือการตกเบ็ดหลอกลวง (Phishing) การส่งโปรแกรม ลิงค์ หรือไฟล์อันตราย Malware หรือ Ransomware เข้าไปยังระบบหรือเครื่องเพื่อขโมยข้อมูลต่าง ๆ รหัสผ่าน และควบคุมอุปกรณ์จากทางไกลได้ (เตือนภัยออนไลน์, 2568)

เมื่ออาชญากรไซเบอร์ต้องการเงินจากผู้ตกเป็นเหยื่อ ดังนั้น เงินที่ได้มาจากเหยื่อจะมาถึงตัวอาชญากรได้นั้น หัวใจสำคัญขององค์กรอาชญากรรมไซเบอร์ ก็คือ บัญชีม้า ซึ่งหมายถึง บัญชีธนาคารที่เจ้าของบัญชียินยอมให้ผู้อื่นใช้โดยไม่มีเจตนาใช้เพื่อตน โดยประการที่รู้หรือควรจะรู้ว่าจะนำไปใช้ในการก่ออาชญากรรมทางเทคโนโลยีหรือความผิดอาญาอื่น ๆ ซึ่งในปัจจุบันบัญชีม้านั้นได้วิวัฒนาการไปเป็นกลุ่มองค์กรที่มีการจัดการ อย่างเป็นระบบ มีกลุ่มรับจ้างเปิดบัญชีม้า และอาชญากรไซเบอร์ก็ไม่ได้ใช้บัญชีม้าเพียงบัญชีเดียว โดยมีการโอนเงินเป็นทอด ๆ ไปหลายบัญชีม้า เพื่อปกปิดอำพรางการกระทำความผิด และให้เจ้าหน้าที่ไม่สามารถติดตามเส้นทางการเงินได้โดยง่าย ทั้งนี้ประเทศไทยก็ได้ออกกฎหมายมาเพื่อควบคุมจัดการเกี่ยวกับบัญชีม้า คือ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ.2568

วิเคราะห์องค์ประกอบ “การขาดผู้พิทักษ์ หรือหน่วยงานกำกับดูแลการบังคับใช้กฎหมาย”

อาชญากรรมเกิดขึ้นได้เมื่อมีเหยื่อที่อ่อนแอ ผู้กระทำผิดที่มีแรงจูงใจ และประการที่ 3 คือ การขาดผู้พิทักษ์หรือหน่วยงานกำกับดูแลการบังคับใช้กฎหมาย ทำให้เกิดช่องโอกาสที่มีสภาพแวดล้อมหรือสถานการณ์ที่เอื้ออำนวยให้การกระทำผิดเกิดขึ้นได้ ความสะดวกในการก่อเหตุจะหมดไปได้ด้วยการมีผู้ควบคุมหรือผู้พิทักษ์ที่เข้มแข็ง หรือกล่าวได้ว่าต้องมีการควบคุมตัดช่องโอกาส หรือสภาพแวดล้อมไม่ให้เอื้ออำนวยต่อการการกระทำความผิด ดังนั้น ผู้พิทักษ์ในโลกไซเบอร์นั้นมีความสำคัญอย่างยิ่งในการป้องกันอาชญากรรมไซเบอร์ และผู้พิทักษ์นั้นไม่ได้หมายถึงเฉพาะตำรวจ แต่ยังรวมถึงตัวผู้ใช้งานเอง ระบบเว็บไซต์ ธนาคาร และแพลตฟอร์มต่าง ๆ ซึ่งจากสถิติคดีอาชญากรรมไซเบอร์ได้สะท้อนถึงช่องว่างในการป้องกัน ดังนี้

จากจำนวนคดีที่เกิดขึ้นอย่างมากเฉลี่ยจำนวน 785 คดีต่อวัน ทำให้การทำงานของเจ้าหน้าที่ตำรวจที่เป็นหน่วยงานแรกที่เข้าดำเนินการ (First Responder) อาจล่าช้าและไม่ทันการ เนื่องด้วยเจ้าหน้าที่ไม่เพียงพอต่อคดีที่เกิดขึ้น ถึงแม้จะมีการอายัดบัญชีถึง 641,181 บัญชี แต่ยอดเงินที่อายัดได้ทันมีเพียง 10,103,769,194 บาท คิดเป็น 10.78% จากมูลค่าความเสียหายทั้งหมดกว่า 93,685,935,175 บาท ซึ่งสะท้อนให้เห็นว่าเงินส่วนใหญ่ถูกยักย้ายถ่ายเทไปอย่างรวดเร็วจนตามไม่ทัน มีช่องว่างทางเทคโนโลยีและกฎหมาย อาชญากรใช้เทคโนโลยีใหม่ ๆ เพื่อหลบเลี่ยงการตรวจจับ และมักอาศัยช่องว่างทางกฎหมายระหว่างประเทศ ทำให้การติดตามดำเนินคดีเป็นไป

ได้ยาก และที่สำคัญ คือ การตระหนักรู้ของประชาชนยังไม่เพียงพอ การที่คดีหลอกลวงซื้อของออนไลน์ซึ่งเป็นกลโกงพื้นฐานยังคงมีสัดส่วนสูงที่สุด แสดงให้เห็นว่าประชาชนจำนวนมากยังขาดความระมัดระวังในการตรวจสอบผู้ขายและความน่าเชื่อถือก่อนโอนเงิน จากการศึกษาดังกล่าว พบว่า เมื่อองค์ประกอบทั้งสามประการของสามเหลี่ยมอาชญากรรม (เหยื่อ ผู้กระทำผิดและการขาดผู้พิทักษ์) ได้บรรจบกันและอาชญากรรมเกิดขึ้นสำเร็จแล้ว โอกาสในการบรรเทาความเสียหายด้านการเงินนั้นแทบจะเป็นศูนย์ หรือเรียกว่าล้มเหลวในการป้องกันและไม่มีประสิทธิภาพในการเยียวยา

ตัวอย่างการประยุกต์ใช้สามเหลี่ยมอาชญากรรมกับคดีข่มขู่ทางโทรศัพท์ กล่าวคือ เหยื่อได้รับโทรศัพท์จากบุคคลที่อ้างว่าเป็นตำรวจ แจ้งว่าบัญชีธนาคารของเหยื่อพัวพันกับคดียาเสพติด และต้องโอนเงินทั้งหมดมาให้เจ้าหน้าที่ ปปง. ตรวจสอบเพื่อแสดงความบริสุทธิ์ โดยมิจฉาชีพจะพูดจาข่มขู่และห้ามไม่ให้วางสายหรือบอกเรื่องนี้กับใคร (ศูนย์บริการข้อมูลภาครัฐเพื่อประชาชน, 2568) โดยวิเคราะห์เหยื่อแล้ว พบว่า เหยื่อนั้น คือ ประชาชนทั่วไป โดยเฉพาะผู้สูงอายุซึ่งไม่ทันเล่ห์เหลี่ยมของมิจฉาชีพ และผู้สูงอายุมีวัฒนธรรมในการเคารพต่อผู้มีอำนาจ โดยจะใช้ความกลัวและความตกใจเป็นเครื่องมือหลักในการควบคุมเหยื่อ สำหรับการวิเคราะห์ในส่วนของผู้กระทำผิดที่มีแรงจูงใจนั้น พบว่า เป็นองค์กรอาชญากรรมขนาดใหญ่ที่ตั้งฐานปฏิบัติการในประเทศเพื่อนบ้าน โดยเฉพาะตามแนวชายแดนในพื้นที่ที่กฎหมายเข้าถึงได้ยาก ผู้ที่โทรมาหลอกลวงมักเป็นเหยื่อของขบวนการค้ามนุษย์ที่ถูกบังคับหรือหลอกให้ทำงานอีกด้วย และการวิเคราะห์ในส่วนของการขาดผู้พิทักษ์ที่มีความสามารถ พบว่า มีการใช้เทคโนโลยี Voice over IP (VoIP) เพื่อปลอมแปลงหมายเลขโทรศัพท์ให้ดูเหมือนโทรมาจากหน่วยงานจริง หลีกเลี่ยงการตรวจสอบจากเจ้าหน้าที่ และมีลักษณะการก่อเหตุข้ามพรมแดนทำให้การสืบสวนและจับกุมของเจ้าหน้าที่เป็นไปได้ยาก

ดังนั้น จึงกล่าวโดยสรุปได้ว่า สถานการณ์อาชญากรรมไซเบอร์ที่รุนแรงดังที่ปรากฏในสถิติข้างต้น เกิดจากการบรรจบกันของประชาชน (เหยื่อ) ที่เข้าถึงง่ายและยังขาดความตระหนักรู้ กลุ่มมิจฉาชีพ (ผู้กระทำผิด) ที่มีแรงจูงใจทางการเงินมหาศาลและทำงานเป็นระบบ และการป้องกัน (ผู้พิทักษ์) ที่ยังมีช่องว่างทั้งในระดับตัวบุคคลและระดับโครงสร้าง ทำให้ไม่สามารถยับยั้งอาชญากรรมได้อย่างทันท่วงที เนื่องด้วยการรับมือของอาชญากรรมไซเบอร์ของประเทศไทยมีลักษณะไล่ตามปัญหาที่เกิดขึ้น กล่าวคือ รอเมื่อเหตุเกิดแล้วถึงดำเนินการ ซึ่งผิดกับหลักการป้องกันก่อนเกิดเหตุ

สรุป

สรุปได้ว่าองค์กรในกระบวนการยุติธรรมทางอาญาจะต้องมีความรู้ความเข้าใจเกี่ยวกับการสืบสวนสอบสวนและการดำเนินคดีอาชญากรรมไซเบอร์ทั้งระบบ เพื่อที่จะบริหารจัดการวางมาตรการ และกลไกต่าง ๆ เพื่อให้บังคับใช้กฎหมายได้อย่างรวดเร็วและมีประสิทธิภาพ รวมทั้งมีกระบวนการที่สามารถช่วยเหลือเหยื่ออาชญากรรมไซเบอร์นี้ด้วย ซึ่งเป็นสิ่งที่กระบวนการยุติธรรมทางอาญาของไทยจะต้องรับมือและปรับตัวให้ทันทั้งนี้จากการวิเคราะห์สาเหตุของการเกิดอาชญากรรมไซเบอร์ในประเทศไทยโดยแนวคิดสามเหลี่ยมอาชญากรรมนั้น ทำให้ได้แนวคิดว่าหากต้องการจะแก้ไขปัญหาหรือระงับยับยั้งอาชญากรรมไซเบอร์ให้มีจำนวนคดีที่เกิดขึ้นลดลงจะต้องตัดองค์ประกอบทั้ง 3 ประการของสามเหลี่ยมอาชญากรรม จึงมีข้อเสนอแนะ ดังนี้ 1) การเสริมสร้างเหยื่อให้มีความเข้มแข็ง เป็นการลดความเหมาะสมของเป้าหมายไม่ให้ตกเป็นเหยื่ออาชญากรรมไซเบอร์ กล่าวคือ นอกจากสร้างความตระหนักรู้ภัย

ไซเบอร์ทางทฤษฎีแล้วยังต้องให้ปฏิบัติจริงด้วย โดยควรบรรจุหลักการป้องกันภัยไซเบอร์อยู่ในหลักสูตรการเรียนการสอนภาคบังคับตั้งแต่เด็กและเยาวชน และควรมีรูปแบบแพลตฟอร์มหรือแอปพลิเคชันที่สามารถเผยแพร่ความรู้ พร้อมทดสอบการปฏิบัติจริง เช่น การตั้งค่าความปลอดภัยสองชั้น การตั้งค่าความเป็นส่วนตัว โดยเฉพาะกลุ่มคนวัยทำงานที่เป็นเป้าหมายหลัก เน้นทักษะการรู้เท่าทันกลโกงภัยไซเบอร์ และไม่ประมาทในการใช้งานออนไลน์ นอกจากนั้นควรต้องนำข้อมูลสถิติอาชญากรรมไซเบอร์ที่กระจัดกระจาย พัฒนาระบบฐานข้อมูลกลางเพื่อรวบรวมสถิติอาชญากรรมแบบเรียลไทม์ สำหรับให้หน่วยงานของรัฐรวมถึงนักวิจัยนำไปวิเคราะห์แนวโน้มการเกิดอาชญากรรมเพื่อวางนโยบาย มาตรการ รวมทั้งการประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบ ในการป้องกันก่อนเกิดเหตุที่มีประสิทธิภาพได้ 2) การยับยั้งไม่ให้มีผู้กระทำผิด เพิ่มความเสี่ยงให้กับผู้กระทำผิดว่าจะถูกจับและมีบทลงโทษหนัก ด้วยหลักการเปลี่ยนจากตั้งรับเป็นเชิงรุก ไม่รอให้เกิดเหตุก่อนค่อยดำเนินการแบบปัจจุบันด้วยการใช้การข่าวนำการยุทธ จัดตั้งศูนย์ข่าวกรองภัยคุกคามเกี่ยวกับอาชญากรรมไซเบอร์ ซึ่งจะสอดรับกับข้อเสนอแนะที่ 1 ในด้านของการประชาสัมพันธ์ผ่านแพลตฟอร์ม โดยเฉพาะอาชญากรรมไซเบอร์ที่เกิดมากที่สุดในประเทศไทย คือ การหลอกลวงฉ้อโกงออนไลน์ รวมทั้งการกำหนดมาตรฐานสากลว่าด้วยการจัดการพยานหลักฐานดิจิทัลทางอาชญากรรมไซเบอร์ ให้มีแนวทางเดียวกันและสามารถลงโทษผู้กระทำผิดได้อย่างรวดเร็ว 3) การเสริมสร้างผู้พิทักษ์ หรือการสร้างระบบกำกับดูแลอาชญากรรมไซเบอร์ให้มีประสิทธิภาพด้วยการบูรณาการร่วมกันของหน่วยงานบังคับใช้กฎหมายทั้งภาครัฐและภาคเอกชน โดยควรพัฒนาหลักสูตรอาชญากรรมไซเบอร์สำหรับหน่วยงานบังคับใช้กฎหมายโดยเฉพาะ ตำรวจ อัยการ ศาล เพื่อให้สามารถทำงานคดีอาชญากรรมไซเบอร์เป็นเนื้อเดียวกันได้ รวมทั้งควรจัดตั้งศูนย์บูรณาการความร่วมมือระหว่างภาครัฐและเอกชนให้สามารถทำงานได้อย่างต่อเนื่องไร้รอยต่อ โดยเฉพาะสถาบันการเงิน ธนาคาร และผู้ให้บริการอินเตอร์เน็ต ซึ่งส่วนใหญ่มีข้อมูลและพยานหลักฐานที่เกี่ยวข้องในคดีที่จะต้องใช้ในกระบวนการยุติธรรม และที่สำคัญอาชญากรรมไซเบอร์นั้นเป็นอาชญากรรมข้ามชาติ ดังนั้นควรพัฒนาความร่วมมือระหว่างประเทศทั้งในด้านการสืบสวนสอบสวนและข้อกฎหมายที่เกี่ยวข้องเพื่อเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย อย่างไรก็ตามผลของการศึกษานี้มีประเด็นข้อท้าทายในด้านปัญหาข้อมูลเชิงสถิติ อันเนื่องมาจากการขาดมาตรฐานในการจัดเก็บ และการรายงานข้อมูลที่ไม่ครบถ้วน รวมทั้งข้อมูลที่มีอยู่อย่างกระจัดกระจาย รวมทั้งความคลุมเครือแตกต่างของนิยามอาชญากรรมไซเบอร์ สร้างความท้าทายในด้านของการเปรียบเทียบผลการศึกษาและการพัฒนาแนวนโยบายที่สอดคล้องกันต่อไป

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. (2563). กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: นิติธรรม.

เตือนภัยออนไลน์. (2568). ประเภทอาชญากรรมทางเทคโนโลยี กลุ่มกลโกงที่คนร้ายมักใช้จุดอ่อนของเหยื่อเพื่อหลอกลวงออนไลน์. เรียกใช้เมื่อ 26 กรกฎาคม 2568 จาก https://pctpr.police.go.th/knowledge.php

ศูนย์บริการข้อมูลภาครัฐเพื่อประชาชน. (2568). AOC 1441 เตือนภัย “แก๊งคอลเซ็นเตอร์” อ้างเป็น “ตำรวจ” ข่มขู่ผู้เสียหายฯ พบสูญเงินกว่า 25 ล้านบาท. เรียกใช้เมื่อ 12 กันยายน 2568 จาก https://www.gcc.go.th/?p=279195

ศูนย์บริหารการรับแจ้งความออนไลน์. (2568). สถิติคดีออนไลน์ สะสมตั้งแต่วันที่ 1 มีนาคม 2565 ถึง วันที่ 30 มิถุนายน 2568. กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. กรุงเทพมหานคร: สำนักงานตำรวจแห่งชาติ.

สาวตรี สุขศรี. (2560). อาชญากรรมคอมพิวเตอร์/ไซเบอร์ กับทฤษฎีอาชญาวิทยา. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 46(2), 415-432.

_____. (2563). กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์.

สำนักงานกิจการยุติธรรม. (2565). อาชญากรรมและกระบวนการยุติธรรมไทยในวันนี้ พ.ศ. 2565 Updating Thai Criminal Justice 2022. เรียกใช้เมื่อ 20 กรกฎาคม 2568 จาก https://www.oja.go.th/wp-content/uploads/2023/09/updating-thai-criminal-justice-2022-new.pdf

Ajayi, E. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12.

Choi, K. S. (2015). Cybercriminology and Digital Investigation. Texas: LFB Scholarly Publishing.

Choi, K. S. et al. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. Computers in Human Behavior, 35(100), 1-10.

Clough, J. (2015). Principles of Cybercrime. (2nd ed.). United Kingdom: Cambridge University Press.

Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: Routine Activity Approach. American Sociological Review, 4(44), 588-608.

Council of Europe. (2001). Convention on Cybercrime (CETS No.185). Retrieved July 20, 2025, from https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Datareportal. (2025). DIGITAL 2025: THAILAND. Retrieved July 25, 2025, from https://datareportal.com/reports/digital-2025-thailand?rq=thailand

Dodge, C. E. & Burruss, G. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. New York: Routledge.

Gercke, M. (2011). Understanding Cybercrime: Phenomena, Challenges and Legal Presponse. (2nd ed.). Switzerland: International Telecommunication Development.

Grabosky, P. N. (2001). Virtual Criminality Old Wine in New Bottles? Social and Legal Studies, 10(2), 243-249.

Vakhitova, Z. I. (2025). Cyber-Routine Activity Theory. In Pontell, H. (Ed.). Oxford Research Enclcopedia of Criminology. New York: Oxford University Press.

Yar, M. (2005). The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.