

ความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน
ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
Collaborative Governance Among Public, Private, Civil Society
and People Sectors for Prevention and Suppression
of Technology-Related Crimes

พัฒน์พันธ์ บูระพันธ์^{1*} / สุวรรณณี แสงมหาชัย²

Pattanapant Boorapant / Suwannee Sangmahachai

¹สาขารัฐประศาสนศาสตร์ มหาวิทยาลัยรามคำแหง

Public Administration, Ramkhamhaeng University

อีเมล : pattanapant@gmail.com

²สาขารัฐประศาสนศาสตร์ มหาวิทยาลัยรามคำแหง

Public Administration, Ramkhamhaeng University

อีเมล : suwanneeru@yahoo.com

DOI: <https://doi.org/10.14456/jhusoc.2026.15>

Received: 26 June 2026 ; Revised: 21 July 2026 ; Accepted: 27 July 2026

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาบริบท เงื่อนไขตั้งต้น และสภาพปัญหาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย 2) วิเคราะห์รูปแบบ กระบวนการ และปัจจัยเชิงยุทธศาสตร์ที่มีผลต่อประสิทธิภาพของความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน 3) เสนอรูปแบบการกำกับดูแลแบบร่วมมือที่เหมาะสม ใช้วิธีวิจัยเชิงคุณภาพ โดยสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ 24 คน จาก 4 ภาคส่วน การสังเกตแบบมีส่วนร่วม และการวิเคราะห์คำพิพากษาคดีหลอกลวงออนไลน์แบบผสมผสาน วิเคราะห์เนื้อหาเชิงตีความร่วมกับการตรวจสอบสามเส้า

ผลการวิจัยพบว่า 1) อาชญากรรมทางเทคโนโลยีของไทยเป็นปัญหาสาธารณะที่ซับซ้อนสูง ขยับเคลื่อนโดยเครือข่ายอาชญากรรมข้ามชาติเชิงอุตสาหกรรม มีความไม่สมดุลของอำนาจ-ทรัพยากร และปัญหาเชิงโครงสร้าง 5 ประเด็น ได้แก่ คอขวดกระบวนการยุติธรรม ช่องโหว่การตีความกฎหมาย ข้อจำกัดการกำกับดูแลคดีล้นมือ และข้อจำกัดข้ามชาติ 2) ความร่วมมือเป็น “กลไกคู่ตั้งรับ-เชิงรุก แบบหลายระดับ” ขยับเคลื่อนด้วยความไว้วางใจ พันธสัญญาร่วม และปัจจัยเชิงยุทธศาสตร์ 3 ประการ 3) รูปแบบที่เหมาะสมคือ โมเดลการกำกับดูแลแบบบูรณาการ 4 เสาหลักกับ 5 ชั้นกลไก ส่งผลให้จำนวนคดีและมูลค่าความเสียหายลดลง ข้อเสนอแนะเชิงนโยบาย ได้แก่ ปรับปรุงกฎหมายและกระบวนการยุติธรรมให้รับมือกับความซับซ้อนของคดีไซเบอร์ ขยายปากเกร็ดโมเดล และกำหนด KPI ระดับชาติ

คำสำคัญ : ความร่วมมือ, การกำกับดูแลแบบร่วมมือ, ปัญหาสาธารณะที่ซับซ้อนสูง, อาชญากรรมทางเทคโนโลยี

¹ Corresponding author's E-mail: pattanapant@gmail.com

Abstract

This research aimed to: 1) examine the context, starting conditions, and problems of technology-related crime prevention and suppression in Thailand; 2) analyze the patterns, processes, and strategic factors affecting the effectiveness of collaboration among the public, private, civil society, and people sectors; and 3) propose an appropriate collaborative governance model. This qualitative study employed in-depth interviews with 24 key informants from the four sectors, participant observation, and documentary analysis of court judgments on hybrid online scam cases, using interpretive content analysis alongside triangulation.

The findings revealed that: 1) technology-related crime in Thailand is a highly complex public problem driven by industrialized transnational crime networks, marked by a power-resource imbalance and five structural problems: justice-process bottlenecks, legal-interpretation loopholes, regulatory limitations, case overload, and cross-border constraints; 2) collaboration operates as a “Reactive-Proactive Dual Mechanism in Multi-Level Governance,” driven by trust, joint commitments, and three strategic factors; and 3) the appropriate model is an integrated collaborative governance model combining four pillars with five mechanism layers, resulting in reductions in both the number of cases and financial damages. Policy recommendations include improving laws and the justice process to cope with the complexity of cyber cases, expanding the Pakkret grassroots model, and setting national KPIs.

Keywords: Collaboration, Collaborative Governance, Wicked Problem, Technology-Related Crimes

บทนำ

ในช่วงทศวรรษที่ผ่านมา การหลอกลวงและฉ้อโกงออนไลน์ ได้พัฒนาจากอาชญากรรมทั่วไปไปสู่ “อุตสาหกรรมอาชญากรรม” ที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ เครื่องมือดิจิทัลต้นทุนต่ำ และเครือข่ายอาชญากรรมข้ามชาติ ซึ่งดำเนินงานในรูปแบบศูนย์หลอกลวงกระจายอยู่ในประเทศเพื่อนบ้าน ได้แก่ เมียนมา กัมพูชา ลาว และฟิลิปปินส์ (United Nations Office on Drugs and Crime [UNODC], 2024) องค์การพันธมิตรต่อต้านการหลอกลวง (Global Anti-Scam Alliance [GASA]) ประเมินการมูลค่าความเสียหายระดับโลกในปี ค.ศ. 2024 สูงถึงกว่า 1 ล้านล้านดอลลาร์สหรัฐ (GASA, 2024) ขณะที่ INTERPOL (2026) รายงานว่าจำนวนหมายประกาศสะกดกัน (Notices) และคำขอความร่วมมือระหว่างประเทศ (Diffusions) ที่เกี่ยวข้องกับการฉ้อโกงเพิ่มขึ้นร้อยละ 54 ตั้งแต่ปี ค.ศ. 2024 สะท้อนว่าโลกกำลังเผชิญกับ “การปฏิวัติอุตสาหกรรมอาชญากรรม” ที่ขับเคลื่อนด้วยเทคโนโลยี

สำหรับประเทศไทย สถานการณ์อาชญากรรมออนไลน์ได้ทวีความรุนแรงจนกลายเป็นวิกฤตระดับชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (2567) รายงานว่าตั้งแต่เดือนมีนาคม พ.ศ. 2565 ถึงเดือนพฤศจิกายน พ.ศ. 2567 มีเรื่องร้องเรียนผ่านระบบรับแจ้งความออนไลน์ (thaipoliceonline.com) สะสมรวม 739,494 คดี มูลค่าความเสียหายรวม 77,360 ล้านบาท เฉลี่ยวันละ 77 ล้านบาท เฉพาะปี พ.ศ. 2567 ปีเดียวมีคดี

มากกว่า 400,000 คดี มูลค่าความเสียหายกว่า 60,000 ล้านบาท ปรากฏการณ์ดังกล่าวมีลักษณะเป็น “ปัญหาสาธารณะที่ซับซ้อนสูง” ตามแนวคิดของ Rittel and Webber (1973) ที่มีมิติเชื่อมโยงกันอย่างซับซ้อนทั้งด้านเทคโนโลยี กฎหมาย เศรษฐกิจ สังคม และพฤติกรรมมนุษย์ ส่งผลให้หน่วยงานภาครัฐเพียงลำพังไม่สามารถจัดการได้อย่างมีประสิทธิภาพ ทั้งนี้ สำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งสหประชาชาติ (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2026) ได้เผยแพร่รายงานในชื่อ “A Wicked Problem” ระบุว่าอุตสาหกรรมหลอกลวงออนไลน์ในเอเชียตะวันออกเฉียงใต้มีมูลค่าประมาณ 43,800 ล้านดอลลาร์สหรัฐฯ ต่อปีเฉพาะในภูมิภาคกลุ่มน้ำโขง โดยมีผู้ถูกบังคับเป็นแรงงานในศูนย์หลอกลวงไม่น้อยกว่า 300,000 คนจาก 66 ประเทศ

รัฐบาลไทยได้พัฒนากลไกความร่วมมือผ่านการประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และฉบับที่ 2 พ.ศ. 2568 ตลอดจนการจัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center: AOC 1441) เมื่อวันที่ 1 พฤศจิกายน พ.ศ. 2566 ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่เป็นกลไกตั้งรับ (reactive mechanism) ในการรับแจ้งเหตุและไต่สวนคดี คู่ขนานกับศูนย์ต่อต้านการฉ้อโกงออนไลน์ (Anti-Cyber Scam Center: ACSC) ภายใต้สำนักงานตำรวจแห่งชาติ ทำหน้าที่เป็นกลไกเชิงรุก (proactive mechanism) ในการสืบสวนและรื้อถอนเครือข่ายอาชญากรรมข้ามชาติ

จากบริบทดังกล่าวข้างต้น เมื่อพิจารณาการทบทวนวรรณกรรมอย่างเป็นระบบ พบว่างานวิจัยด้านการกำกับดูแลแบบร่วมมือ (collaborative governance) ส่วนใหญ่ยังมุ่งเน้นปัญหาสาธารณะแบบดั้งเดิม เช่น การจัดการทรัพยากรธรรมชาติ สาธารณสุข และการศึกษา ขณะที่งานวิจัยที่นำกรอบทฤษฎีดังกล่าวมาประยุกต์ใช้กับปัญหาอาชญากรรมทางเทคโนโลยีอย่างเป็นระบบยังมีจำนวนน้อยมาก โดยเฉพาะในบริบทประเทศกำลังพัฒนา เช่น ประเทศไทย (Ansell & Gash, 2008; Emerson et al., 2012) การศึกษานี้มุ่งตอบช่องว่างงานวิจัย 3 ประการ ประการแรก ยังไม่มีการศึกษาอย่างเป็นระบบว่าเงื่อนไขตั้งต้น (starting conditions) และบริบทเชิงโครงสร้าง (structural context)ใด ที่ส่งผลต่อการเกิดขึ้นและการคงอยู่ของความร่วมมือพหุภาคีในการจัดการอาชญากรรมทางเทคโนโลยีของประเทศไทย ประการที่สอง ผลงานวิชาการที่พบและวรรณกรรมกระแสหลักตั้งอยู่บนสมมติฐานที่ว่าความร่วมมือเกิดขึ้นโดยความสมัครใจ แต่กรณีของประเทศไทยใช้กฎหมาย กำหนด “ความรับผิดชอบ” บังคับให้ธนาคารพาณิชย์ ผู้ให้บริการโทรคมนาคม และแพลตฟอร์มดิจิทัลต้องเข้าร่วมเป็นส่วนหนึ่งของเครือข่ายการป้องกันและปราบปราม จึงยังไม่มีคำตอบเชิงประจักษ์ว่าการบังคับเชิงกฎหมายเช่นนี้ส่งผลต่อคุณภาพของความร่วมมืออย่างไร ทั้งในมิติความไว้วางใจ ความสมัครใจ และความต่อเนื่องของความร่วมมือ และประการที่สาม “โมเดลสองศูนย์” (Dual-Center Model) ของไทยที่ศูนย์ AOC ทำหน้าที่กลไกตั้งรับ คู่ขนานกับศูนย์ ACSC ที่ทำหน้าที่กลไกเชิงรุก เป็นนวัตกรรมเชิงโครงสร้างที่แตกต่างจากโมเดลศูนย์เดียวของประเทศอื่นในภูมิภาค เช่น Anti-Scam Command ของสิงคโปร์ (Singapore Police Force, 2022) ซึ่งยังไม่เคยได้รับการวิเคราะห์ผ่านกรอบทฤษฎีการกำกับดูแลแบบร่วมมือในวรรณกรรมระดับสากลมาก่อน

ดังนั้น การศึกษาความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชนในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จึงมีความสำคัญอย่างยิ่งต่อการพัฒนาแนวทางการกำกับดูแลที่สอดคล้องกับบริบทประเทศและสามารถสร้างความปลอดภัยทางไซเบอร์ที่ยั่งยืน

วัตถุประสงค์ของงานวิจัย

1. เพื่อศึกษาบริบท เงื่อนไขตั้งต้น และสภาพปัญหาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย
2. เพื่อศึกษาวิเคราะห์รูปแบบ กระบวนการ และปัจจัยเชิงยุทธศาสตร์ที่มีผลต่อประสิทธิภาพของความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
3. เพื่อเสนอรูปแบบการพัฒนาเครือข่ายการกำกับดูแลแบบร่วมมือ ที่เหมาะสมกับบริบทของประเทศไทย

การทบทวนวรรณกรรม

1. แนวคิดปัญหาสาธารณะที่ซับซ้อนสูงและการกำกับดูแลสาธารณะแนวใหม่

แนวคิด “wicked problem” ของ Rittel and Webber (1973) อธิบายว่า Wicked Problem มีลักษณะเฉพาะคือ ขอบเขตของปัญหาเปลี่ยนแปลงตามมุมมองของผู้มีส่วนได้เสีย ไม่มีเกณฑ์วัดความสำเร็จที่ตายตัว และเชื่อมโยงกับหลายมิติทั้งโครงสร้างสังคม กฎหมาย เทคโนโลยี เศรษฐกิจ และพฤติกรรมมนุษย์ Roberts (2000) ได้พัฒนาต่อยอดโดยเสนอกลยุทธ์การรับมือ 3 รูปแบบ คือ กลยุทธ์เชิงอำนาจ กลยุทธ์เชิงแข่งขัน และกลยุทธ์เชิงร่วมมือ (collaborative strategy) โดยชี้ว่าในสถานะที่ปัญหาซับซ้อนสูง กลยุทธ์เชิงร่วมมือเป็นแนวทางที่เหมาะสมที่สุด สอดคล้องกับ Grint (2005) ที่เสนอว่า wicked problem ต้องการ “ภาวะผู้นำ” แบบมีส่วนร่วม ไม่ใช่เพียง “การจัดการ” หรือ “การบัญชาการ” ในบริบทของอาชญากรรมทางเทคโนโลยี ลักษณะ wicked problem ปรากฏชัดเจนในหลายมิติ กล่าวคือ ปัญหาที่มีลักษณะข้ามพรมแดน (transboundary) ที่ผู้กระทำผิด เหยื่อ และกระแสมุ่งอยู่คนละเขตอำนาจศาล ทำให้ไม่มีหน่วยงานใดมีอำนาจและทรัพยากรเพียงพอรับมือได้เพียงลำพัง อีกทั้งรูปแบบอาชญากรรมเปลี่ยนแปลงอย่างรวดเร็วตามพัฒนาการของเทคโนโลยี ซึ่งสะท้อนลักษณะสำคัญที่ Rittel and Webber (1973) ระบุไว้ว่าทุกความพยายามแก้ไขปัญหาย่อมเปลี่ยนธรรมชาติของปัญหานั้นเอง ดังนั้น กลยุทธ์เชิงร่วมมือของ Roberts (2000) ที่เปิดพื้นที่ให้ผู้มีส่วนได้เสียจากทุกภาคส่วนร่วมนิยามและแก้ไขปัญหาอย่างต่อเนื่อง จึงเป็นแนวทางที่สอดคล้องกับธรรมชาติของปัญหานี้มากที่สุด

Osborne (2006, 2010) เสนอกระบวนทัศน์ “การกำกับดูแลสาธารณะแนวใหม่” (New Public Governance: NPG) ที่ชี้ว่าการแก้ไขปัญหาสารณะที่ซับซ้อนต้องอาศัยกระบวนการที่เปิดให้ภาคส่วนต่างๆ เข้ามามีส่วนร่วมในการกำหนดนโยบาย ตัดสินใจ และดำเนินการร่วมกัน บนพื้นฐานของเครือข่ายความร่วมมือ (network governance) มากกว่าการพึ่งพาระบบราชการแบบลำดับชั้น (Hierarchical Bureaucracy) หรือกลไกตลาด (Market Mechanism) เพียงอย่างเดียว ซึ่งสอดคล้องกับลักษณะของอาชญากรรมทางเทคโนโลยีที่มีพลวัตเปลี่ยนแปลงรวดเร็วและข้ามพรมแดน กรอบ NPG วางอยู่บนหลักการสำคัญ คือ การยอมรับสภาพ “รัฐพหุนิยม” (plural state) ที่ตระหนักว่าหน่วยงานหลากหลายทั้งภาครัฐและนอกภาครัฐมีส่วนในการส่งมอบบริการสาธารณะ และ “สังคมพหุนิยม” (pluralist state) ที่ยอมรับว่ามีหลายค่านิยมและเป้าหมายที่อาจขัดแย้งกัน สอดคล้องกับ Rhodes (1997) ที่เสนอว่าการกำกับดูแลสมัยใหม่ดำเนินผ่าน “เครือข่ายที่จัดตัวเอง” (self-organizing networks) ซึ่งมีลักษณะพึ่งพาอาศัยกันระหว่างองค์การ มีการแลกเปลี่ยนทรัพยากร และมีกฎกติกาที่เกิดจากการเจรจาระหว่างสมาชิกเครือข่าย ขณะที่ Klijn and Koppenjan (2016) เสริมว่าเครือข่ายการกำกับดูแลที่มีประสิทธิภาพต้องอาศัยการจัดการความซับซ้อนและความไม่แน่นอนผ่านกลไกการ

สร้างความไว้วางใจเป็นแกนกลาง โดย Osborne เน้นว่ากลไกความไว้วางใจ และสัญญาเชิงสัมพันธ์ (relational contracts) มีความสำคัญในการประสานงานระหว่างภาคส่วนมากกว่าสัญญาเชิงบังคับ (formal contracts) หรือกลไกตลาดเพียงอย่างเดียว โดยข้อเสนอของนักวิชาการเหล่านี้สะท้อนให้เห็นในบริบทของความร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ต้องอาศัยเครือข่ายความร่วมมือหลายภาคส่วนในการจัดการปัญหาที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว

2. แนวคิดการกำกับดูแลแบบร่วมมือและระบอบการกำกับดูแลแบบร่วมมือ

Ansell and Gash (2008) ได้พัฒนากรอบทฤษฎี “collaborative governance” จากการวิเคราะห์กรณีศึกษา 137 กรณีจากหลากหลายภาคนโยบาย โดยระบุว่าความสำเร็จของความร่วมมือขึ้นอยู่กับตัวแปรสำคัญ ได้แก่ (1) เงื่อนไขตั้งต้น ซึ่งรวมถึงประวัติความร่วมมือหรือความขัดแย้งในอดีต ความสมดุลของอำนาจ และทรัพยากร แรงจูงใจในการเข้าร่วม (2) การออกแบบเชิงสถาบัน (institutional design) (3) ภาวะผู้นำเชิงอำนวยความสะดวก (facilitative leadership) และ (4) กระบวนการความร่วมมือ (collaborative process) ที่ประกอบด้วยการสร้างความไว้วางใจ การสร้างพันธมิตรสัญญา ร่วม และการสร้างความเข้าใจร่วมกัน

ต่อมา Emerson et al. (2012) ได้ขยายกรอบดังกล่าวเป็น “collaborative governance regime” (CGR) ที่ครอบคลุมมิติของบริบทระบบ (system context) ปัจจัยขับเคลื่อน พลวัตของความร่วมมือ (collaborative dynamics) และผลลัพธ์-การปรับตัว (outcomes-adaptation) ที่กว้างขวางยิ่งขึ้น โดยเฉพาะการระบุปัจจัยขับเคลื่อน 4 ประการ คือ ภาวะผู้นำ ผลประโยชน์ที่จะตามมา (consequential incentives) การพึ่งพาอาศัยกัน (interdependence) และความไม่แน่นอน กรอบ CGR มีลักษณะเป็นมิติซ้อน (nested dimensions) โดยบริบทระบบ ซึ่งครอบคลุมสภาพแวดล้อมทางกฎหมาย เศรษฐกิจ สังคม และการเมือง เป็นตัวกำหนดเงื่อนไขที่หล่อหลอมรูปแบบของระบอบการกำกับดูแลแบบร่วมมือ ภายในระบอบดังกล่าว พลวัตของความร่วมมือประกอบด้วย 3 องค์ประกอบที่ทำงานเป็นวงจรเสริมพลัง ได้แก่ การมีส่วนร่วมอย่างมีหลักการ (principled engagement) แรงจูงใจร่วม (shared motivation) และสมรรถนะในการดำเนินการร่วม (capacity for joint action) โดยผลลัพธ์ของความร่วมมือจะย้อนกลับไปปรับเปลี่ยนบริบทระบบและปัจจัยขับเคลื่อน สร้างวงจรการเรียนรู้และปรับตัวอย่างต่อเนื่อง (adaptation cycle) ทำให้กรอบ CGR ครอบคลุมกว้างกว่ากรอบของ Ansell and Gash (2008) ซึ่งเน้นกระบวนการภายในวงจรความร่วมมือเป็นหลัก

3. แนวคิดการกำกับดูแลแบบร่วมมือหลายภาคส่วน (PPPPs) และทฤษฎีความสัมพันธ์ระหว่างองค์การ

ทฤษฎีความสัมพันธ์ระหว่างองค์การ (Inter-Organizational Relationship: IOR) ของ Oliver (1990) และ Pfeffer and Salancik (2003) อธิบายเหตุผลที่องค์การจากต่างภาคส่วนเลือกสร้างความร่วมมือเมื่อทรัพยากรของตนไม่เพียงพอต่อการรับมือปัญหาเพียงลำพัง สอดคล้องกับมุมมองของ Provan and Kenis (2008) ที่ระบุว่าในเครือข่ายที่ความไว้วางใจยังไม่สูงพอ สัญญาข้อตกลง และ กลไกและข้อบังคับทางกฎหมาย (legal mandate) เป็นกลไกการบริหารเครือข่ายที่ใช้ทดแทนได้ ทั้งนี้ Oliver (1990) ได้จำแนกแรงจูงใจในการสร้างความสัมพันธ์ระหว่างองค์การไว้หลายประการ อาทิ ความจำเป็น (necessity) ที่ไม่อาจดำเนินการได้เพียงลำพัง ความไม่สมมาตรของอำนาจและทรัพยากร (asymmetry) และการต่างตอบแทน (reciprocity) ขณะที่ Pfeffer and Salancik (2003) อธิบายผ่านทฤษฎีการพึ่งพาทรัพยากร (resource dependence theory) ว่าองค์การจะแสวงหาความร่วมมือกับองค์การอื่นเมื่อทรัพยากรที่จำเป็นอยู่นอกขอบเขตของตน ส่วน Provan and Kenis (2008) เสนอเพิ่มเติมว่ารูปแบบการบริหารเครือข่ายที่เหมาะสมขึ้นอยู่กับปัจจัยสำคัญ ได้แก่ ระดับความไว้วางใจ จำนวนสมาชิกเครือข่าย ฉันทามติด้านเป้าหมาย และความจำเป็นในสมรรถนะ

ระดับเครือข่าย โดยเฉพาะในเครือข่ายที่ยังอยู่ในระยะเริ่มต้น กลไกสัญญาข้อตกลงและข้อบังคับทางกฎหมาย จึงทำหน้าที่สร้างกรอบความร่วมมือที่ชัดเจนและบังคับใช้ได้ก่อนที่ความไว้วางใจจะพัฒนาขึ้น

สรุป จากการทบทวนแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง พบว่า อาชญากรรมทางเทคโนโลยีเป็น wicked problem ที่ไม่อาจแก้ไขได้โดยภาคส่วนใดเพียงลำพัง จำเป็นต้องอาศัยกระบวนการทัศน์การกำกับดูแลสาธารณะแนวใหม่ที่เปิดพื้นที่ให้หลายภาคส่วนเข้ามาเป็นหุ้นส่วนในการแก้ไขปัญหา โดยการศึกษาเรียนรู้การกรอบของ Ansell and Gash (2008), Emerson et al. (2012) และ Osborne (2010) เพื่อใช้วิเคราะห์ปรากฏการณ์ความร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย ครอบคลุมตั้งแต่เงื่อนไขเบื้องต้น กระบวนการความร่วมมือ ปัจจัยเชิงยุทธศาสตร์ ไปจนถึงผลลัพธ์และความยั่งยืน

วิธีดำเนินการวิจัย

การศึกษาความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เป็นการวิจัยเชิงคุณภาพตามแนวทางปรากฏการณ์วิทยา (phenomenology) ซึ่งมุ่งค้นหา “แก่นสาระของประสบการณ์” ตามที่บุคคลผู้อยู่ในปรากฏการณ์รับรู้และให้ความหมายจริง โดยผู้วิจัยระบอบคติและกรอบความเชื่อเดิมของตนเพื่อให้ความหมายปรากฏจากมุมมองของผู้ให้ข้อมูลเอง (Schutz, 1967; Moustakas, 1994) เหตุผลที่เลือกใช้แนวทางนี้เนื่องจากความร่วมมือระหว่างภาคส่วนเกิดขึ้นจริงผ่านการปฏิสัมพันธ์และการสร้างความไว้วางใจระหว่างผู้ปฏิบัติงาน ซึ่งล้วนเป็นมิติเชิงอัตวิสัยที่ไม่อาจเข้าใจได้ครบถ้วนจากโครงสร้างองค์การหรือตัวบทกฎหมายเพียงลำพัง หากต้องเข้าถึงผ่าน “ประสบการณ์ที่ถูกใช้จริง” (lived experience) ของผู้ปฏิบัติงานโดยตรง (Creswell & Poth, 2018) ผู้วิจัยเก็บรวบรวมข้อมูลด้วยการสัมภาษณ์เชิงลึกเป็นหลัก ผสานกับการวิเคราะห์เอกสาร (documentary analysis) ได้แก่ กฎหมาย คำพิพากษาคดีหลอกลวงฉ้อโกงออนไลน์แบบผสมผสาน (hybrid scam) รายงานผลการปฏิบัติการของศูนย์ AOC 1441 และศูนย์ ACSC ตลอดจนสถิติการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ เพื่อให้การวิเคราะห์มีความน่าเชื่อถือ ครอบคลุม และสอดคล้องกับวัตถุประสงค์ของการวิจัย

ผู้ให้ข้อมูลสำคัญ

การวิจัยนี้กำหนดผู้ให้ข้อมูลสำคัญ (key informants) ตามแนวคิดของ Marshall (1996) ที่เน้นการคัดเลือกบุคคลผู้มีความรู้ลึกและประสบการณ์ตรงในปรากฏการณ์ที่ศึกษา จำนวน 24 คน แบ่งเป็น 4 กลุ่ม ได้แก่ (1) ภาครัฐ 11 ราย จากศูนย์ AOC 1441 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ศูนย์ ACSC สำนักงานตำรวจแห่งชาติ บช.สอท. บช.ก. กสทช. ธปท. พนักงานสอบสวน และเทศบาลนครปากเกร็ด (2) ภาคเอกชน 5 ราย จากธนาคารพาณิชย์ ผู้ให้บริการเครือข่ายโทรคมนาคม และผู้พัฒนาแอปพลิเคชัน (3) ภาคประชาสังคม 4 ราย จากสภาองค์กรของผู้บริโภค มูลนิธิอินเทอร์เน็ตรวมพัฒนาไทย และเครือข่ายผู้บริโภค และ (4) ภาคประชาชน 4 ราย ทุกรายเป็นผู้มีประสบการณ์ตรงและมีบทบาทในกระบวนการนโยบายหรือการปฏิบัติการด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

การได้มาซึ่งผู้ให้ข้อมูลสำคัญใช้การคัดเลือกแบบเจาะจง (purposive sampling) ตามแนวทางของ Patton (2015) โดยกำหนดเกณฑ์การคัดเลือก (inclusion criteria) แยกตามภาคส่วน ได้แก่ (1) ภาครัฐ เป็นผู้บริหารหรือผู้ปฏิบัติงานที่มีอำนาจหน้าที่โดยตรงด้านการกำกับดูแลหรือการบังคับใช้กฎหมาย และมีประสบการณ์ในกลไกความร่วมมือไม่น้อยกว่า 1 ปี (2) ภาคเอกชน เป็นผู้แทนองค์กรในห่วงโซ่ปฏิบัติการที่ดูแลโครงสร้างพื้นฐานหรือข้อมูลดิจิทัล และมีบทบาทเชื่อมประสานกับภาครัฐโดยตรง (3) ภาคประชาสังคม

เป็นผู้แทนองค์การที่เฝ้าระวัง คัดกรอง หรือช่วยเหลือผู้เสียหายอย่างต่อเนื่อง และ (4) ภาคประชาชน เป็นผู้ที่มีประสบการณ์ตรงในกลไกป้องกันระดับชุมชนหรือผู้ได้รับผลกระทบ ทั้งนี้ ทุกรายเข้าร่วมโดยสมัครใจและให้ความยินยอมก่อนการสัมภาษณ์ เกณฑ์ดังกล่าวทำให้ได้ข้อมูลเชิงลึกที่สะท้อนกลไกความร่วมมือ ปัญหาอุปสรรค และผลลัพธ์จากมุมมองของแต่ละภาคส่วนอย่างแท้จริง

การกำหนดจำนวนผู้ให้ข้อมูลใช้เกณฑ์การอิ่มตัวของข้อมูล (data saturation) ตามแนวทางของ Guest et al. (2006) โดยเก็บและวิเคราะห์ข้อมูลควบคู่กันเป็นระยะ และถือว่าข้อมูลอิ่มตัวเมื่อการสัมภาษณ์รายใหม่ไม่ปรากฏแก่นสาระใหม่ ซึ่งพบว่าประเด็นเริ่มซ้ำตั้งแต่ประมาณรายที่ 20 ผู้วิจัยจึงสัมภาษณ์จนครบ 24 ราย เพื่อยืนยันความอึดตัวครบทุกภาคส่วน การสัมภาษณ์ใช้เวลาครั้งละประมาณ 1–2 ชั่วโมง ณ สถานที่ที่ผู้ให้ข้อมูลสะดวก ทั้งแบบเผชิญหน้า และแบบออนไลน์ผ่านโปรแกรมสนทนาแบบเห็นหน้า โดยขออนุญาตบันทึกเสียงและจดบันทึกภาคสนามทุกครั้ง

การสร้างเครื่องมือและตรวจสอบคุณภาพเครื่องมือ

เครื่องมือหลักในงานวิจัยคือ แบบสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (semi-structured in-depth interview) ออกแบบคำถามปลายเปิดให้สอดคล้องกับวัตถุประสงค์การวิจัยและกรอบแนวคิดของ Ansell and Gash (2008) และ Emerson et al. (2012) ครอบคลุม 4 มิติหลัก ได้แก่ บริบทและเงื่อนไขตั้งต้น กระบวนการร่วมมือ ปัจจัยเชิงยุทธศาสตร์ และผลลัพธ์-ความยั่งยืน แบบสัมภาษณ์ผ่านการตรวจสอบข้อคำถามโดยอาจารย์ที่ปรึกษาผู้เชี่ยวชาญ และผ่านการทดลองสัมภาษณ์ก่อนเก็บข้อมูลภาคสนาม โดยผู้วิจัยทำหน้าที่เป็นเครื่องมือหลัก ร่วมกับเครื่องบันทึกเสียงและการจดบันทึกภาคสนาม

การตรวจสอบคุณภาพของข้อมูลใช้ 3 วิธีประกอบกันตามแนวทางของ Lincoln and Guba (1985) ได้แก่ (1) การตรวจสอบสามเส้า (triangulation) ด้านข้อมูล (ผู้ให้ข้อมูล 4 ภาคส่วนและเอกสารทุติยภูมิ) ด้านวิธีการ (สัมภาษณ์ สังเกตการณ์ วิเคราะห์เอกสาร) และด้านผู้วิจัย (ตรวจสอบการตีความร่วมกับอาจารย์ที่ปรึกษา) (2) การตรวจสอบโดยผู้ให้ข้อมูล (member checking) โดยส่งบทสรุปสาระสำคัญพร้อมการตีความกลับไปให้ผู้ให้ข้อมูลยืนยันความถูกต้องและความตรงตามเจตนา หากพบความคลาดเคลื่อนจะแก้ไขก่อนการวิเคราะห์ขั้นสุดท้าย และ (3) การตรวจสอบโดยผู้ทรงคุณวุฒิ (peer debriefing) โดยนำแนวคำถาม ระบบรหัส และข้อค้นพบเบื้องต้นหารือกับอาจารย์ที่ปรึกษาและผู้เชี่ยวชาญด้านรัฐประศาสนศาสตร์และอาชญากรรมทางเทคโนโลยีเป็นระยะ เพื่อทดสอบความสมเหตุสมผลของการตีความ อันเป็นการเพิ่มความน่าเชื่อถือ (credibility) และการยืนยันได้ (confirmability) ของผลการวิจัย

การเก็บรวบรวมข้อมูลและการวิเคราะห์ข้อมูล

ผู้วิจัยเก็บข้อมูลระหว่างเดือนธันวาคม พ.ศ. 2568 ถึงเดือนเมษายน พ.ศ. 2569 จาก 3 แหล่งหลัก ได้แก่ (1) การสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ 24 ราย ระยะเวลา 1–2 ชั่วโมง (2) การสังเกตการณ์อย่างมีส่วนร่วม ทั้งการติดตามปรากฏการณ์อาชญากรรมทางเทคโนโลยีผ่านสื่อ และการเข้าร่วมเวทีสัมมนาความร่วมมือหลายภาคส่วนระดับชาติและระดับท้องถิ่น โดยกำหนดประเด็นสังเกตไว้ล่วงหน้า ได้แก่ รูปแบบการปฏิสัมพันธ์ระหว่างผู้แทนภาคส่วนต่าง ๆ การแสดงบทบาทและภาวะผู้นำในเวทีร่วม ท่าทีต่อข้อเสนอของภาคส่วนอื่น และบรรยากาศความไว้วางใจที่สะท้อนความเป็น “ชุมชนผู้ปฏิบัติงาน” พร้อมจดบันทึกภาคสนามอย่างเป็นระบบ และ (3) การวิเคราะห์เอกสารที่เกี่ยวข้อง ได้แก่ กฎหมาย คำพิพากษาคดีหลอกหลวงออนไลน์ แบบผสมผสาน รายงานผลการปฏิบัติการของศูนย์ AOC 1441 และศูนย์ ACSC และสถิติการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ

การวิเคราะห์ข้อมูลใช้แนวทางปรากฏการณ์วิทยาเชิงตีความ 4 ขั้นตอน โดยผู้วิจัยเข้ารหัสข้อมูลด้วยมือ (manual coding) ทั้งหมด เพื่อให้ใกล้ชิดกับข้อมูลมากที่สุดและตรวจสอบย้อนกลับได้ทุกขั้นตอน ได้แก่ (1) การทำความเข้าใจข้อมูลในระดับลึก (data immersion) ถอดบทสัมภาษณ์แบบคำต่อคำ อ่านบทพรรณซ้ำ ควบคู่กับการฟังเสียงบันทึก และแขวนอคติชั่วคราว (bracketing) (2) การสกัดประโยคสำคัญและการให้รหัส ชีตเน้นถ้อยคำที่สะท้อนประสบการณ์ตรง กำหนดรหัสเชิงพรรณนา และจัดทำสมุดรหัสนี้กนิยามพร้อมตัวอย่างข้อความ เพื่อความคงเส้นคงวาและร่องรอยการตรวจสอบ (audit trail) (3) การสังเคราะห์แก่นสาระร่วม (emergent themes) จัดกลุ่มรหัสเป็นหน่วยความหมาย (meaning units) และเปรียบเทียบความสอดคล้อง-แตกต่างของมุมมองระหว่าง 4 ภาคส่วน และ (4) การบูรณาการข้อค้นพบกับการอภิปรายกับดูแลแบบร่วมมือเพื่อสรุปผลตามวัตถุประสงค์ ทั้งนี้ ทุกขั้นตอนใช้การตรวจสอบสามเส้า ด้านข้อมูล วิธีการ และผู้วิจัย ร่วมกับการตรวจสอบโดยผู้ให้ข้อมูล และผู้ทรงคุณวุฒิ เพื่อความโปร่งใสและความน่าเชื่อถือของกระบวนการวิเคราะห์ข้อมูล

ผลการวิจัย

1. ผลการศึกษาบริบท เจอนไขตั้งต้น และสภาพปัญหาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย พบว่า อาชญากรรมทางเทคโนโลยีของไทยเป็น “ปัญหาสาธารณะที่ซับซ้อนสูง” ที่ขับเคลื่อนโดยเครือข่ายอาชญากรรมข้ามชาติซึ่งมีโครงสร้างเชิงอุตสาหกรรม แบ่งหน้าที่เป็น 8 กลุ่มปฏิบัติการที่ทำงานสอดประสานกันอย่างเป็นระบบ เมื่อวิเคราะห์ตามตัวแปรเจอนไขตั้งต้น ของ Ansell and Gash (2008) พบความสัมพันธ์ที่ชัดเจนระหว่างเจอนไขตั้งต้นทั้ง 3 มิติกับการก่อรูปของความร่วมมือ กล่าวคือ (1) ความไม่สมดุลของอำนาจและทรัพยากร ที่ภาคเอกชนได้เปรียบเชิงเทคโนโลยีและข้อมูล ขณะที่ภาครัฐมีอำนาจตามกฎหมายแต่ขาดแคลนกำลังคนและการเข้าถึงพยานหลักฐาน เป็นแรงกดดันเชิงโครงสร้างที่ทำให้ “ไม่มีฝ่ายใดสามารถดำเนินการได้เพียงลำพัง” และผลักดันให้ทุกภาคส่วนต้องพึ่งพากัน (2) แรงจูงใจในการเข้าร่วม 3 รูปแบบ ได้แก่ เชิงกฎหมาย (legal compulsion) เชิงผลประโยชน์ (self-interest) และเชิงคุณค่า (value-driven motivation) ซึ่งเป็นตัวแปรที่กำหนดระดับความผูกพันของแต่ละภาคส่วนต่อเครือข่าย และ (3) ประวัติความร่วมมือที่พัฒนาจากภาวะ “ต่างคนต่างทำ” ไปสู่ “ชุมชนผู้ปฏิบัติงาน” (community of practice)

ขณะเดียวกัน สภาพปัญหาเชิงโครงสร้าง 5 ประเด็น ได้แก่ คอขวดกระบวนการยุติธรรมจากการไม่ยอมรับพยานหลักฐานอิเล็กทรอนิกส์เต็มรูปแบบ ช่องโหว่ของคำว่า “เท่าที่จำเป็น” ใน พ.ร.ก. มาตรา 4 และ 5 การครอบงำหน่วยงานกำกับดูแลในภาคโทรคมนาคม ภาวะคดียึดมือของพนักงานสอบสวน และข้อจำกัดการบังคับใช้กฎหมายข้ามชาติ เป็นตัวแปรเจอนไขที่จำกัดประสิทธิผลของความร่วมมือโดยตรง โดยเฉพาะภาวะ “คดียึดมือ” ซึ่งสะท้อนความไม่สมดุลเชิงทรัพยากรอย่างเป็นรูปธรรมที่สุด ดังที่พนักงานสอบสวนระดับพื้นที่สะท้อนว่า “พนักงานสอบสวน 1 คน รับคดีใหม่เข้ามาทุกวัน เฉลี่ยตำรวจ 1 คน รับ 1 คดีต่อวัน ทำให้ไม่มีเวลาไปทำคดีเก่า คดีออนไลน์ส่วนใหญ่มีการโอนเงินเป็นทอด ๆ 15-20 ทอด ก่อนแปลงเป็นสกุลเงินดิจิทัล ‘cryptocurrency’” (ผู้ให้ข้อมูลภาครัฐ R05, 11 มีนาคม 2569) สอดคล้องกับผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ยืนยันว่าสภาพปัญหาดังกล่าวคือแรงขับเคลื่อนสำคัญของความร่วมมือ ดังคำกล่าวที่ว่า “ทุกภาคส่วนต่างตระหนักว่า ไม่สามารถทำงานแบบต่างคนต่างทำได้อีกต่อไป เพราะประชาชนจะเดือดร้อน” (ผู้ให้ข้อมูลภาครัฐ R01, 27 มีนาคม 2569) ข้อค้นพบส่วนนี้ชี้ว่า เจอนไขตั้งต้นเชิงลบ (ความไม่สมดุลและสภาพ

ปัญหา) กลับทำหน้าที่เป็น “ปัจจัยเร่ง” ให้เกิดความร่วมมือ เมื่อมีกลไกกฎหมายเข้ามาเปลี่ยนแรงกดดันให้เป็นพันธมิตร

2. ผลการศึกษาวิเคราะห์รูปแบบ กระบวนการ และปัจจัยเชิงยุทธศาสตร์ที่มีผลต่อประสิทธิภาพของความร่วมมือ พบว่า รูปแบบความร่วมมือของประเทศไทยมีลักษณะเป็น “กลไกคู่ตั้งรับ-เชิงรุก แบบหลายระดับ” (reactive-proactive dual mechanism in multi-level governance) โดยศูนย์ AOC 1441 ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่กลไกตั้งรับแบบจุดเดียวเบ็ดเสร็จ (one-stop service) คู่ขนานกับศูนย์ ACSC ภายใต้สำนักงานตำรวจแห่งชาติที่ทำหน้าที่กลไกเชิงรุก การทำงานคู่ขนานของสองกลไกนี้เปลี่ยนตัวชี้วัดความสำเร็จจาก “จำนวนคดี” ไปสู่ “ความเร็วในการตอบสนอง” ซึ่งเป็นตัวแปรผลลัพธ์ที่ผู้ปฏิบัติงานทุกภาคส่วนให้น้ำหนักตรงกัน ดังที่ผู้ปฏิบัติงานศูนย์ ACSC ประเมินว่า “ต้องยอมรับตามตรงว่าจำนวนคดีไม่ได้ลดลงมากนัก ยิ่งทรง ๆ อยู่ แต่สิ่งที่เปลี่ยนไปอย่างชัดเจน คือ ความเร็วในการตอบสนอง การอายัดบัญชีที่ได้ภายใน 1-3 ชั่วโมง การแชร์ข้อมูลข้ามองค์กรที่ราบรื่นขึ้น และความสามารถในการสกัดกั้นความเสียหายระหว่างทาง” (ผู้ให้ข้อมูลภาครัฐ R04, 26 มีนาคม 2569) สอดคล้องกับผู้แทนธนาคารพาณิชย์ที่ระบุถึง “การลดระยะเวลาการรับแจ้งและอายัดบัญชีจากที่เคยใช้เวลาเป็นวัน ลงมาเหลือเพียง 1-3 ชั่วโมง” (ผู้ให้ข้อมูลภาคเอกชน E02, 22 มีนาคม 2569)

กระบวนการความร่วมมือขับเคลื่อนด้วย 3 องค์ประกอบที่สัมพันธ์กันเป็นวงจรเสริมพลัง ได้แก่ (1) การสร้างความไว้วางใจ ผ่านการปฏิสัมพันธ์ซ้ำในเวทีร่วมและการปลดล็อกข้อจำกัดเชิงกฎหมายผ่าน “PDPA waiver” (2) การกำหนดพันธสัญญาร่วม 5 ประเภท (เชิงกฎหมาย เชิงสถาบัน เชิงปฏิบัติการ เชิงสมัครใจ และเชิงคุณค่า) โดยพันธสัญญาเชิงกฎหมายเป็นจุดเปลี่ยนสำคัญที่เปลี่ยนพฤติกรรมของภาคเอกชนมากที่สุด ดังที่ผู้แทน กสทช. อธิบายว่า “การกำหนดความรับผิดชอบร่วมกัน หากเกิดความเสียหาย ศาลจะพิจารณาว่า ธนาคารพาณิชย์หรือผู้ให้บริการโทรคมนาคมปฏิบัติตามกฎเกณฑ์ที่ผู้กำกับดูแลกำหนดหรือไม่ ซึ่งเป็นการบังคับให้เกิดความรับผิดชอบร่วมกันในระบบนิเวศนี้” (ผู้ให้ข้อมูลภาครัฐ R06, 23 มีนาคม 2569) และ (3) การสร้างความเข้าใจร่วมกัน โดยเฉพาะการยอมรับร่วมกันว่าจุดอ่อนเชิงจิตวิทยาและพฤติกรรมของบุคคลหรือ “กิเลส” เป็นช่องโหว่ที่ควบคุมยากที่สุด เพราะไม่อาจแก้ไขได้ด้วยมาตรการทางเทคนิคหรือกฎหมายเพียงอย่างเดียว ดังคำสัมภาษณ์ที่ว่า “อาชญากรรมเหล่านี้มักเล่นกับความโลภและความอยากได้เงิน เมื่อก่อนคนเต็มใจเล่นหวย แต่เดี๋ยวนี้เปลี่ยนเป็นการลงทุนที่ให้ผลตอบแทนสูง ซึ่งเล่นกับ ‘กิเลส’ โดยตรง” (ผู้ให้ข้อมูลภาครัฐ R01, 27 มีนาคม 2569) และข้อมูลเชิงประจักษ์ที่ว่า “เหยื่อกว่าร้อยละ 70 มีความรู้เกี่ยวกับกลโกงอยู่แล้ว แต่เมื่อเผชิญเหตุการณ์จริง สภาวะทางอารมณ์ส่งผลให้ขาดสติ” (ผู้ให้ข้อมูลภาครัฐ R05, 11 มีนาคม 2569) ซึ่งนำไปสู่ความเข้าใจร่วมว่าทิศทางการแก้ปัญหาต้องเปลี่ยนจาก “ปลายน้ำ” สู่ “ต้นน้ำ”

ส่วนปัจจัยเชิงยุทธศาสตร์ที่มีผลต่อประสิทธิภาพของความร่วมมือมี 3 ประการ ได้แก่ (1) ภาวะผู้นำเชิงอำนาจความสะดวก 3 ระดับ (ระดับนโยบาย ระดับผู้บริหารหน่วยงาน และระดับปฏิบัติการ) โดยในระดับปฏิบัติการปรากฏภาวะผู้นำแบบกระจายอำนาจ จากล่างขึ้นบน ดังที่ผู้ปฏิบัติงานศูนย์ ACSC ระบุว่า “ผมไม่อยากจะใช้คำว่า ‘leadership’ แบบผูกขาด แต่เราใช้หลักการทำงานแบบ ‘agile’ คือ เราให้อำนาจและส่งเสริมให้คนทำงานในหน่วยย่อยลุกขึ้นมาเป็นผู้นำ โอเคเดี่ยวนั้นส่วนใหญ่มันมาจากคนทำงานหน้างาน (bottom-up) ไม่ใช่มาจากการนั่งนึกของผู้บังคับบัญชา” (ผู้ให้ข้อมูลภาครัฐ R08, 26 มีนาคม 2569) (2) ความเป็นสถาบันของโครงสร้าง “กลไกคู่ตั้งรับ-เชิงรุก แบบหลายระดับ” ที่เสริมด้วยกลไกการประชุมกลุ่มย่อยไม่เป็นทางการรายเดือนระหว่างผู้ปฏิบัติงาน (informal fine-tune mechanism) ซึ่งช่วยลดการกล่าวโทษกันในเวทีทางการ ดังที่ผู้แทนภาครัฐ อธิบายว่า “การประชุมในรูปแบบคณะกรรมการชุดใหญ่แบบเป็นทางการ มักทำให้เกิดการกล่าวโทษกัน (blame game) เราจึงเสนอให้ใช้การประชุมกลุ่มย่อยแบบไม่เป็นทางการระหว่าง

ผู้ปฏิบัติงาน...อย่างน้อยเดือนละ 1 ครั้ง เพื่อทำความเข้าใจ อัปเดตปัญหา และตกลงโปรโตคอลร่วมกันก่อน เมื่อไปถึงการประชุมระดับนโยบาย งานจะสามารถขับเคลื่อนได้อย่างราบรื่น” (ผู้ให้ข้อมูลภาครัฐ R06, 23 มีนาคม 2569) และ (3) นวัตกรรมและเทคโนโลยีสนับสนุนและขับเคลื่อนการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้แก่ ระบบจัดการข้อมูลและแลกเปลี่ยนข้อมูลทุจริต (CFR), ระบบแลกเปลี่ยนข้อมูลการให้บริการโทรคมนาคมเพื่อการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (TDEX), ระบบการรับแจ้งความออนไลน์ (TPO), แอปพลิเคชันที่พัฒนามาเพื่อการแจ้งเตือนและป้องกันภัยออนไลน์ อาทิเช่น Cyber Check, Whoscall, DE-fence, True Cyber Safe และโครงการบูรณาการเพื่อการปราบปรามฉ้อโกงออนไลน์ (Project Delta)

3. ผลการศึกษาเพื่อเสนอรูปแบบการพัฒนาเครือข่ายการกำกับดูแลแบบร่วมมือที่เหมาะสมกับบริบทของประเทศไทย ผู้วิจัยได้สังเคราะห์โมเดลการกำกับดูแลอาชญากรรมทางเทคโนโลยีแบบผสมผสานหลายภาคส่วน “Thai 4P-Hybrid Cyber Governance Model” ที่บูรณาการ 4 เสาหลัก (public-private-civil society-people) เข้ากับ 5 ชั้นกลไก โดยแต่ละชั้นกลไกสัมพันธ์โดยตรงกับข้อค้นพบเชิงประจักษ์ กล่าวคือ ชั้นกฎหมาย (legal) ตอบปัญหาการไม่เข้าร่วมของภาคเอกชนด้วยความรับผิดชอบร่วม ชั้นสถาบัน (institutional) ตอบความซับซ้อนเชิงบทบาทด้วยโมเดลศูนย์คู่ ชั้นปฏิบัติการ (operational) ตอบข้อจำกัดด้านความเร็วด้วยระบบการติดตามสถานการณ์และเฝ้าระวังแบบทันเหตุการณ์ และระบบเทคโนโลยีที่เป็นเครื่องมือ อาทิเช่น CFR, TDEX, TPO และ SLA 1-3 ชั่วโมง ชั้นรากหญ้า (grassroots) ตอบการเข้าถึงกลุ่มเปราะบางด้วยปากเกร็ดโมเดล และชั้นพฤติกรรม (behavioral) ตอบปัจจัย “กิเลส” ด้วยมาตรการสะกดเชิงพฤติกรรม ทั้งนี้ บทบาทของชั้นรากหญ้าสะท้อนการแบ่งงานที่เสริมกันระหว่างท้องถิ่นกับหน่วยบังคับใช้กฎหมาย ดังที่ผู้แทนเทศบาลนครปากเกร็ดระบุว่า “หน้าที่หลักของเทศบาล คือ การป้องกันและการสร้างภูมิคุ้มกันเพื่อไม่ให้ประชาชนตกเป็นเหยื่อ ส่วนหน้าที่การปราบปรามก็เป็นอำนาจของเจ้าหน้าที่ตำรวจโดยตรง” (ผู้ให้ข้อมูลภาครัฐ R07, 10 มีนาคม 2569)

จากโมเดลดังกล่าว ผลการวิจัยนำเสนอข้อค้นพบใหม่ 5 ประการ ได้แก่ (1) โมเดลศูนย์คู่แบบพึ่งพิงร่วม (Dual-Center Symbiosis Model) (2) ความร่วมมือที่ขับเคลื่อนด้วยกฎหมาย (legal-driven collaboration) ซึ่งขัดกับสมมติฐานความสมัครใจของ Ansell and Gash (2008) (3) กลไกปรับเปลี่ยนแบบไม่เป็นทางการ (4) โมเดลรากหญ้าที่บูรณาการเมืองอัจฉริยะเข้ากับการป้องกันไซเบอร์ (Pakkret Grassroots Model) และ (5) ปัจจัย “กิเลส” ในฐานะช่องโหว่ทางพฤติกรรมที่ควบคุมยากที่สุด นำไปสู่การเสนอชั้นพฤติกรรม (behavioral layer) เป็นชั้นที่ 5 ต่อยอดกรอบ CGR ของ Emerson et al. (2012) ผลลัพธ์เชิงประจักษ์ของเครือข่ายความร่วมมือ ได้แก่ การอายัดบัญชีม้า 1.18 ล้านบัญชี ป้องกันความเสียหาย 21,980 ล้านบาท ลดคดีร้อยละ 44 และลดคดีแอปดูดเงินจาก 3,000 คดี เหลือ 0 คดี โดยศูนย์ AOC 1441 ได้รับรางวัล WSIS Prizes 2025 ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union, 2025) ซึ่งมีใช้ความสำเร็จขององค์การเดียว หากแต่เป็นผลลัพธ์ร่วมของทุกภาคส่วนที่บูรณาการการทำงานจนเกิดประสิทธิผลเชิงประจักษ์

อภิปรายผล

การวิจัยเชิงคุณภาพครั้งนี้มิได้กำหนดสมมติฐานเชิงสถิติ แต่มีข้อสันนิษฐานเชิงทฤษฎีตามวัตถุประสงค์ทั้ง 3 ข้อ เมื่อเปรียบเทียบผลการวิจัยกับข้อสันนิษฐานและวัตถุประสงค์ที่ตั้งไว้ พบว่า ผลการวิจัยสอดคล้องกับข้อสันนิษฐานใน 2 ประเด็นหลัก ได้แก่ (1) เงื่อนไขความไม่สมดุลของอำนาจและทรัพยากรใน

ระดับ “ไม่มีฝ่ายใดครอบงำ” เป็นเงื่อนไขตั้งต้นของการเกิดความร่วมมือ ตามกรอบของ Ansell and Gash (2008) และ (2) ความไว้วางใจ พันธสัญญาร่วม และภาวะผู้นำเชิงอำนาจความสะดวก เป็นตัวแปรกระบวนการที่กำหนดประสิทธิภาพของความร่วมมือ ขณะเดียวกัน ผลการวิจัยแตกต่างจากข้อสันนิษฐานเดิมอย่างมีนัยสำคัญ 2 ประเด็น ได้แก่ (1) ความร่วมมือของไทยมิได้เกิดจากความสมัครใจตามสมมติฐานหลักของทฤษฎีดั้งเดิม หากแต่ถูกขับเคลื่อนด้วยการบังคับเชิงกฎหมาย และ (2) การค้นพบตัวแปรเชิงพฤติกรรม “กิเลส” และกลไกไม่เป็นทางการ ซึ่งเป็นองค์ประกอบที่กรอบทฤษฎีเดิมยังไม่ครอบคลุม รายละเอียดการอภิปรายจำแนกตามวัตถุประสงค์ ดังนี้

1. บริบท เงื่อนไขตั้งต้น และสภาพปัญหาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ผลการศึกษาด้านบริบทและเงื่อนไขตั้งต้น พบว่าประเทศไทยมีความไม่สมดุลของอำนาจและทรัพยากรในระดับ “ไม่มีฝ่ายใดครอบงำ” (non-dominance) ซึ่งเป็นเงื่อนไขเริ่มต้นที่จำเป็นสำหรับการเกิดการทำกับดักแบบร่วมมือ สอดคล้องกับข้อเสนอของ Ansell and Gash (2008) อย่างไรก็ตาม กรณีของประเทศไทยมีลักษณะเฉพาะคือ ความไม่สมดุลดังกล่าวไม่ได้นำไปสู่ความร่วมมือโดยอัตโนมัติ แต่ต้องอาศัย “เครื่องมือบังคับเชิงกฎหมาย” ผ่านพระราชกำหนดเป็นจุดเปลี่ยนสำคัญ ขัดกับสมมติฐานหลักของกรอบทฤษฎีดั้งเดิมที่เน้นความร่วมมือแบบสมัครใจและสอดคล้องกับงานของ Provan and Kenis (2008) ที่ระบุว่าในเครือข่ายที่ความไว้วางใจยังไม่สูงพอ อำนาจบังคับทางกฎหมายสามารถใช้ทดแทนได้ ขณะที่ลักษณะของปัญหาที่เป็นปัญหาสาธารณะที่ซับซ้อนสูง ตามแนวคิดของ Rittel and Webber (1973) ทำให้การจัดการแบบลำดับขั้นไม่สามารถตอบสนองได้ สอดคล้องกับข้อเสนอของ Peters (2017) และ OHCHR (2026) ที่ระบุว่าอุตสาหกรรมหลอกลวงในเอเชียตะวันออกเฉียงใต้เป็นปัญหาสาธารณะที่ซับซ้อนสูงที่ต้องการแนวทางการมีส่วนร่วมของทั้งสังคม

2. รูปแบบ กระบวนการ และปัจจัยเชิงยุทธศาสตร์ที่มีผลต่อประสิทธิภาพของความร่วมมือ

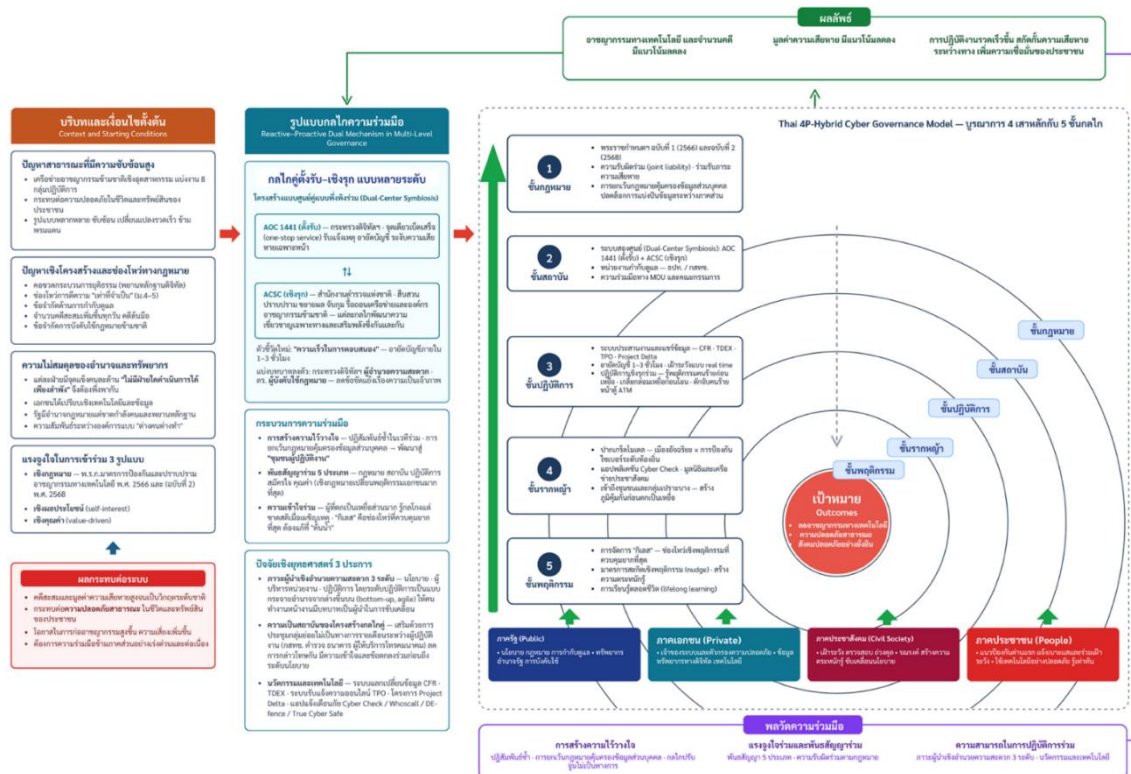
ผลการศึกษาด้านรูปแบบ “กลไกคู่ตั้งรับ-เชิงรุก แบบหลายระดับ” สะท้อนแนวคิด “division of labor” ของ Durkheim (1893/1984) ที่ประยุกต์ในระดับองค์การ กล่าวคือ การแบ่งหน้าที่ระหว่างศูนย์ AOC 1441 ซึ่งรับแจ้งเหตุ อายัดบัญชี และระงับความเสียหายเฉพาะหน้า กับศูนย์ ACSC ซึ่งสืบสวนและรื้อถอนเครือข่ายอาชญากรรม ทำให้แต่ละกลไกพัฒนาความเชี่ยวชาญเฉพาะทางและเสริมพลังซึ่งกันและกัน นับเป็นนวัตกรรมเชิงโครงสร้างที่สอดคล้องกับขนาดของปัญหาและความซับซ้อนของระบบราชการไทย และแตกต่างจากประเทศในภูมิภาค เช่น สิงคโปร์ที่รวมภารกิจไว้ที่ “Anti-Scam Command” ภายใต้สำนักงานตำรวจสิงคโปร์เพียงศูนย์เดียว (Singapore Police Force, 2022) กระบวนการความร่วมมือที่พัฒนาไปสู่ “ชุมชนผู้ปฏิบัติงาน” สอดคล้องกับแนวคิด communities of practice ของ Wenger (1998) ส่วนการประชุมรายเดือนแบบไม่เป็นทางการของหน่วยงานที่ร่วมมือกัน อาทิ กสทช. ตำรวจ ธนาคาร และผู้ให้บริการเครือข่ายโทรคมนาคม ทำหน้าที่เป็น “micro-trust builder” ที่ลดการ “กล่าวโทษกัน” ในระดับนโยบายเป็นข้อค้นพบใหม่ที่ขยายขอบเขตของกรอบ CGR ของ Emerson et al. (2012) สอดคล้องกับแนวคิด “weak tie” ของ Granovetter (1973) ที่ทำให้ข้อมูลและความเข้าใจไหลผ่านได้รวดเร็ว ปัจจัยเชิงยุทธศาสตร์ “ภาวะผู้นำเชิงอำนาจความสะดวก” 3 ระดับ สอดคล้องกับแนวคิด multi-level leadership ของ Crosby and Bryson (2010) โดยกรณีของไทยมีลักษณะเด่นในการแบ่งบทบาทระหว่างกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) ในฐานะผู้อำนวยความสะดวก กับสำนักงานตำรวจแห่งชาติในฐานะผู้บังคับใช้กฎหมาย ที่ลงตัวกันและลดความขัดแย้งเรื่องความเป็นเจ้าภาพของประเด็นปัญหา (issue ownership) การจัดวางบทบาทเช่นนี้ทำให้ความร่วมมือของไทยขับเคลื่อนได้ต่อเนื่องโดยไม่ต้องพึ่งพาการรวมศูนย์อำนาจไว้ที่หน่วยงานใดหน่วยงานหนึ่ง

3. รูปแบบการพัฒนาเครือข่ายการกำกับดูแลแบบร่วมมือที่เหมาะสมกับบริบทของประเทศไทย

โมเดลการกำกับดูแลอาชญากรรมทางเทคโนโลยีแบบผสมผสานหลายภาคส่วน “Thai 4P-Hybrid Cyber Governance Model” ที่ผู้วิจัยพัฒนาขึ้น (ดังแสดงในภาพ 1) มีโครงสร้างเป็นวงกลมซ้อน 5 ชั้น ตามแนวคิดการสะสมชั้นของสถาบัน (institutional layering) ของ Thelen (2003) โดยแต่ละชั้นตอบสนองข้อค้นพบจากการวิจัยด้วยกลไกที่เป็นรูปธรรม กล่าวคือ (1) ชั้นกฎหมาย - พระราชกำหนดทั้ง 2 ฉบับ ความรับผิดชอบร่วม (joint liability) และการยกเว้น PDPA ปลดล็อกการแบ่งปันข้อมูลระหว่างภาคส่วน (2) ชั้นสถาบัน - ศูนย์ข้อมูล AOC 1441 (ตั้งรับ) และ ACSC (เชิงรุก) ทำงานเสริมกันภายใต้หน่วยงานกำกับดูแล ธปท. และ กสทช. (3) ชั้นปฏิบัติการ - กลไกความร่วมมือและระบบ CFR, TDEX, TPO แปลงความร่วมมือให้เป็นระบบงานที่วัดผลได้ (4) ชั้นรากหญ้า - ปากเกร็ดโมเดลและแอปพลิเคชัน Cyber Check นำการป้องกันลงถึงชุมชนและกลุ่มเปราะบาง และ (5) ชั้นพฤติกรรม - การจัดการ “กิลด์” ด้วยมาตรการระงับคดีเชิงพฤติกรรม ทั้ง 5 ชั้นขับเคลื่อนโดย 4 เสาหลัก คือ ภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ที่ทำงานคู่ขนานเสริมกันโดยไม่ทดแทนกัน จุดเด่นเชิงแนวคิดของโมเดลคือการบรรจุชั้นพฤติกรรมเป็นชั้นอิสระ และการแยกบทบาทภาคประชาสังคมออกจากภาคประชาชนอย่างชัดเจน ซึ่งขยายขอบเขตของกรอบพหุภาคี PPP (Public-Private Partnership) แบบดั้งเดิม

ภาพ 1

โมเดลการกำกับดูแลอาชญากรรมทางเทคโนโลยีแบบผสมผสานหลายภาคส่วน บูรณาการ 4 เสาหลักกับ 5 ชั้นกลไก (Thai 4P-Hybrid Cyber Governance Model)



ที่มา: สังเคราะห์จากผลการวิจัยของ พัฒน์พันธ์ บูรณพันธ์ และสุวรรณี แสงมหาชัย (2569) - Thai 4P-Hybrid Cyber Governance Model บูรณาการ 4 เสาหลักกับ 5 ชั้นกลไก ตามกรอบ Ansell & Gash (2008) และ Emerson et al. (2012)

องค์ความรู้ใหม่

งานวิจัยนี้พบองค์ความรู้ใหม่ว่า ความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มิได้เป็นความสัมพันธ์เชิงเส้นตรงหรือโครงสร้างที่ตายตัว หากแต่เป็น “ระบบนิเวศเชิงบูรณาการ” ซึ่งองค์ประกอบ 4 ส่วนทำงานเชื่อมโยงกันเป็นวงจร กล่าวคือ ปัจจัยแวดล้อม (ความซับซ้อนของอาชญากรรมข้ามชาติ ความไม่สมดุลของอำนาจ-ทรัพยากร กฎหมาย พระราชกำหนดทั้งสองฉบับ และพลวัตของเทคโนโลยี) เป็นเงื่อนไขก่อรูปของกลไกความร่วมมือ 5 ชั้น ที่ขับเคลื่อนโดย 4 เสาหลัก ก่อให้เกิดความร่วมมือเชิงพลวัตผ่านความไว้วางใจ พันธสัญญาร่วม และภาวะผู้นำเชิงอำนาจความสะดวก และส่งมอบผลลัพธ์เชิงประจักษ์ที่ย้อนกลับไปเสริมความชอบธรรมและความยั่งยืนของระบบ

องค์ความรู้ใหม่นี้ตกผลึกเป็นข้อค้นพบเชิงแนวคิด 5 ประการที่สอดคล้องกับผลการวิจัยโดยตรง ได้แก่ (1) โมเดลศูนย์คู่แบบพึ่งพิงร่วม (2) ความร่วมมือที่ขับเคลื่อนด้วยกฎหมาย (3) กลไกปรับจูนแบบไม่เป็นทางการ (4) ปากเกร็ดโมเดลที่บูรณาการเมืองอัจฉริยะกับการป้องกันไซเบอร์ระดับท้องถิ่น และ (5) ปัจจัย “กิเลส” ที่นำไปสู่การเสนอขึ้นพหุติกรรม ต่อยอดกรอบ CGR ของ Emerson et al. (2012) อย่างไรก็ตาม ความยั่งยืนของระบบนิเวศนี้ยังขึ้นอยู่กับการแก้ไขจุดเปราะบาง 5 ประเด็น (การครอบงำหน่วยงานกำกับดูแล คอขวดพยานหลักฐานดิจิทัล คดีล้นมือ ช่องโหว่ “เท่าที่จำเป็น” และข้อจำกัดข้ามชาติ) ให้พัฒนาเป็นกลไกเชิงสถาบันที่มั่นคง ข้อเสนอสำคัญคือ ความสำเร็จของความร่วมมือไม่ได้ขึ้นอยู่กับองค์ประกอบใดเพียงลำพัง หากแต่ขึ้นอยู่กับ “การบูรณาการอย่างสมดุล” ของทุกองค์ประกอบในระบบนิเวศไซเบอร์ ซึ่งสามารถประยุกต์ใช้เป็นต้นแบบระดับภูมิภาคสำหรับประเทศกำลังพัฒนาอื่นได้

การวิจัยครั้งนี้สรุปได้ว่า ความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาสังคม และภาคประชาชน ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของประเทศไทย ขับเคลื่อนผ่าน “กลไกคู่ตั้งรับ-เชิงรุก แบบหลายระดับ” ที่บูรณาการ AOC 1441 (เชิงรับ) และ ACSC (เชิงรุก) เข้าด้วยกัน ภายใต้กรอบพระราชกำหนดสองฉบับและเครือข่ายความร่วมมือทุกภาคส่วน โดยมีเป้าหมายร่วมคือการลดอาชญากรรมทางเทคโนโลยีและสร้างความปลอดภัยสาธารณะ ซึ่งส่งผลเชิงประจักษ์อย่างมีนัยสำคัญต่อการลดความเสียหายและจำนวนคดี ผลการวิจัยตกผลึกเป็นโมเดลการกำกับดูแลแบบผสมผสานหลายภาคส่วน 4 เสาหลักกับ 5 ชั้นกลไก พร้อมข้อค้นพบเชิงแนวคิด 5 ประการ ที่ช่วยขยายขอบเขตองค์ความรู้ด้านการกำกับดูแลแบบร่วมมือ

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย (1) เร่งผลักดัน “Project Delta” และร่าง “ป.วิ.ไซเบอร์” เพื่อให้พยานหลักฐานดิจิทัลได้รับการยอมรับในชั้นอัยการและศาล (2) บังคับใช้มาตรการป้องกันและปราบปรามอย่างเป็นรูปธรรมภายในกรอบเวลาที่ชัดเจน และ (3) จัดตั้งกลไกประสานงานอย่างเป็นทางการกับแพลตฟอร์มต่างชาติ พร้อมจัดทำรายงานผลการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีประจำปี

2. ข้อเสนอแนะเชิงปฏิบัติการ (1) ขยายผลการบูรณาการความร่วมมือในระดับท้องถิ่น จากกรณีตัวอย่าง “ปากเกร็ดโมเดล” สู่องค์กรปกครองส่วนท้องถิ่นทั่วประเทศ (2) ยกระดับการคัดกรองภัยไซเบอร์ระดับเครือข่ายให้เป็น “บริการมาตรฐาน” ของผู้ให้บริการทุกราย พร้อมระบบคัดกรองกลุ่มเสี่ยง (blacklist pre-screening) ก่อนเปิดชมและบัญชี และ (3) กำหนดให้การประชุมปรับจูนแบบไม่เป็นทางการรายเดือนเป็นมาตรฐานระหว่างผู้ปฏิบัติงานทุกภาคส่วน เพื่อยกระดับความร่วมมือสู่กลไกเชิงสถาบันที่ยั่งยืน

3. ข้อเสนอแนะสำหรับการวิจัยในอนาคต (1) การวิจัยเชิงปริมาณเพื่อทดสอบความเที่ยงตรงของโมเดล (2) การวิจัยเปรียบเทียบโมเดลการกำกับดูแลในภูมิภาคอาเซียน (3) การวิจัยเชิงปฏิบัติการเพื่อขยายปากเกร็ดโมเดล และ (4) การวิจัยพฤติกรรมศาสตร์เชิงลึกเกี่ยวกับ “ปัจจัยกิลเลส” เพื่อออกแบบมาตรการสะกิดเชิงพฤติกรรมที่มีประสิทธิผลยิ่งขึ้น

เอกสารอ้างอิง

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2567). รายงานสถานการณ์อาชญากรรมทางเทคโนโลยีและผลการดำเนินงานของศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ AOC 1441.
<https://www.mdes.go.th/mission/153>
- พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. (2566, 16 มีนาคม). *ราชกิจจานุเบกษา*, 140(17 ก), 1-11.
- พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568. (2568, 12 เมษายน). *ราชกิจจานุเบกษา*, 142(27 ก), 5-13.
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543-571.
<https://doi.org/10.1093/jopart/mum032>
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.
- Crosby, B. C., & Bryson, J. M. (2010). Integrative leadership and the creation and maintenance of cross-sector collaborations. *The Leadership Quarterly*, 21(2), 211-230.
- Durkheim, E. (1984). *The division of labor in society* (W. D. Halls, Trans.). Free Press. (Original work published 1893)
- Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory*, 22(1), 1-29.
<https://doi.org/10.1093/jopart/mur011>
- Global Anti-Scam Alliance. (2024). *The Global State of Scams Report 2024*.
<https://www.gasa.org>
- Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, 78(6), 1360-1380.
- Grint, K. (2005). Problems, problems, problems: The social construction of leadership. *Human Relations*, 58(11), 1467-1494.
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1), 59-82.
- International Telecommunication Union. (2025). *WSIS Prizes 2025 winner: AOC 1441, Thailand*.
<https://www.itu.int>
- INTERPOL. (2026). *INTERPOL Global Financial Fraud Threat Assessment*. INTERPOL.
- Klijn, E. H., & Koppenjan, J. (2016). *Governance networks in the public sector*. Routledge.

- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.
- Marshall, M. N. (1996). The key informant technique. *Family Practice*, 13(1), 92-97.
- Moustakas, C. (1994). *Phenomenological research methods*. Sage.
- Office of the United Nations High Commissioner for Human Rights. (2026). "A wicked problem": Seeking human rights-based solutions to trafficking into cyber scam operations in South-East Asia. <https://www.ohchr.org/sites/default/files/documents/issues/trafficking/report-a-wicked-problem.pdf>
- Oliver, C. (1990). Determinants of interorganizational relationships: Integration and future directions. *Academy of Management Review*, 15(2), 241-265.
- Osborne, S. P. (2006). The new public governance? *Public Management Review*, 8(3), 377-387.
- Osborne, S. P. (Ed.). (2010). *The new public governance? Emerging perspectives on the theory and practice of public governance*. Routledge.
- Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). Sage.
- Peters, B. G. (2017). What is so wicked about wicked problems? A conceptual analysis and a research program. *Policy and Society*, 36(3), 385-396.
- Pfeffer, J., & Salancik, G. R. (2003). *The external control of organizations: A resource dependence perspective*. Stanford University Press.
- Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, 18(2), 229-252.
- Rhodes, R. A. W. (1997). *Understanding governance: Policy networks, governance, reflexivity and accountability*. Open University Press.
- Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, 4(2), 155-169.
- Roberts, N. (2000). Wicked problems and network approaches to resolution. *International Public Management Review*, 1(1), 1-19.
- Schutz, A. (1967). *The phenomenology of the social world* (G. Walsh & F. Lehnert, Trans.). Northwestern University Press.
- Singapore Police Force. (2022). *Opening of Anti-Scam Command office* [Press release]. <https://www.police.gov.sg>
- Thelen, K. (2003). How institutions evolve: Insights from comparative-historical analysis. In J. Mahoney & D. Rueschemeyer (Eds.), *Comparative historical analysis in the social sciences* (pp. 208-240). Cambridge University Press.
- United Nations Office on Drugs and Crime. (2024). *Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat*. https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
- Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge University Press.