วารสารวิชาการรัตนบุศย์
RATANABUTH JOURNAL
ISSN: 2697-6641 (Print), ISSN: 2822-0080 (Online)

วารสารวิชาการรัตนบุศย์ ปีที่ 7 ฉบับที่ 2 : พฤษภาคม – สิงหาคม 2568

นโยบายป้องกันอาชญากรรมไซเบอร์ในประเทศไทย: การวิเคราะห์เชิงเปรียบเทียบกับต่างประเทศ
Cybercrime Prevention Policy in Thailand: A Comparative Analysis with International Standards

ปฏิภาณ ใจซื่อ
ภักดี โพธิ์สิงห์
นักศึกษาปริญญาเอก รป.ด. (รัฐประศาสนศาสตร์) มหาวิทยาลัยราชภัฏมหาสารคาม
อาจารย์ประจำคณะรัฐศาสตร์และรัฐประศาสนศาสตร์ มหาวิทยาลัยราชภัฏมหาสารคาม
Patiphan Jaisue
Phekdee Phosing
D.P.A. Student (Public Administration), Rajabhat Mahasarakham University
Lecturer of Political Science and Public Administration, Rajabhat Mahasarakham University
Corresponding E-mail : patipan_259888@hotmail.com

วันที่รับบทความ: 13 กรกฎาคม 2568; วันแก้ไขบทความ 21 สิงหาคม 2568; วันที่ตอบรับบทความ: 22 สิงหาคม 2568
Received: July 13, 2025; Revised: August 21, 2025; Accepted: August 22, 2025

บทคัดย่อ

การศึกษานี้มุ่งวิเคราะห์เปรียบเทียบนโยบายป้องกันอาชญากรรมไซเบอร์ระหว่างประเทศไทยกับ 3 ประเทศพัฒนาแล้ว ได้แก่ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย โดยใช้วิธีการวิเคราะห์เอกสารและการศึกษาเปรียบเทียบ ภายใต้กรอบการวิเคราะห์ 5 มิติ คือ กฎหมาย โครงสร้างหน่วยงาน การมีส่วนร่วมภาคเอกชน ความร่วมมือระหว่างประเทศ และการพัฒนาทรัพยากรมนุษย์ ผลการศึกษาพบว่า ประเทศที่ประสบความสำเร็จมีลักษณะร่วม 3 ประการ คือ การบูรณาการความร่วมมือแบบพหุภาคี การมีหน่วยงานกลางที่เข้มแข็ง และกลไกแลกเปลี่ยนข้อมูลแบบเรียลไทม์ ขณะที่ประเทศไทยยังประสบข้อจำกัด 4 ด้าน ได้แก่ การขาดกลไกความร่วมมือถาวร ระบบประเมินผลที่ไม่มีประสิทธิภาพ บทบาทจำกัดในระดับนานาชาติ และความตระหนักรู้ของประชาชนที่ต่ำ การศึกษาเสนอแนะ 4 มาตรการ คือ การจัดตั้งแพลตฟอร์มแลกเปลี่ยนข้อมูลภัยคุกคาม การพัฒนาระบบติดตามประเมินผล การขยายบทบาทในเวทีนานาชาติ และการส่งเสริมวัฒนธรรมความมั่นคงไซเบอร์

คำสำคัญ: นโยบายไซเบอร์; ความมั่นคงไซเบอร์; การศึกษาเปรียบเทียบ; อาชญากรรมไซเบอร์

Abstract

This study aims to comparatively analyze cybercrime prevention policies between Thailand and three developed countries—namely, the United States, Singapore, and Estonia—through document analysis and comparative study. The analysis is framed across five dimensions: legislation, institutional structure, private sector participation, international cooperation, and human resource development. The findings reveal that successful countries share three common characteristics: multilateral cooperation integration, the presence of a strong central agency, and real-time information-sharing mechanisms. In contrast, Thailand

continues to face four key limitations: the absence of permanent cooperation mechanisms, ineffective evaluation systems, limited engagement at the international level, and low public awareness. The study proposes four policy recommendations: establishing a threat intelligence-sharing platform, developing monitoring and evaluation systems, expanding Thailand's role in international forums, and fostering a culture of cybersecurity.

Keywords: Cyber policy; Cybersecurity; Comparative study; Cybercrime

บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เข้ามามีบทบาทในทุกมิติของชีวิตมนุษย์ ตั้งแต่การทำธุรกรรมทางการเงิน การติดต่อสื่อสาร การศึกษา ไปจนถึงการดำเนินธุรกิจระหว่างประเทศ ทำให้สังคมโลกเชื่อมโยงกันอย่างไร้พรมแดน อย่างไรก็ตาม การพัฒนาทางเทคโนโลยีที่รวดเร็วดังกล่าวได้ก่อให้เกิดช่องโหว่ที่อาชญากรไซเบอร์สามารถแสวงประโยชน์ได้อย่างง่ายดาย (Wall, 2007) อาชญากรรมทางไซเบอร์ (Cybercrime) จึงกลายเป็นภัยคุกคามรูปแบบใหม่ที่มีลักษณะซับซ้อน ไม่จำกัดขอบเขตทางภูมิศาสตร์ และก่อให้เกิดผลกระทบทั้งในระดับบุคคล องค์กร และประเทศ ภัยคุกคามไซเบอร์ในปัจจุบันมีความหลากหลาย ตั้งแต่การโจรกรรมข้อมูลส่วนบุคคล การหลอกลวงทางออนไลน์ การเจาะระบบขององค์กร ไปจนถึงการก่อการร้ายไซเบอร์ (cyberterrorism) ซึ่งมีเป้าหมายเพื่อทำลายโครงสร้างพื้นฐานที่สำคัญของรัฐ เช่น ระบบธนาคาร การสื่อสาร และพลังงาน (Goodman, 2016) ผลกระทบของอาชญากรรมไซเบอร์จึงไม่เพียงจำกัดอยู่ในด้านการสูญเสียทางเศรษฐกิจเท่านั้น แต่ยังส่งผลต่อความมั่นคงของชาติและสิทธิความเป็นส่วนตัวของประชาชนอีกด้วย

จากสถานการณ์ภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากขึ้นทั่วโลก ทำให้รัฐบาลของประเทศต่าง ๆ ต้องตื่นตัวและให้ความสำคัญกับการพัฒนานโยบายและมาตรการในการป้องกันอาชญากรรมไซเบอร์อย่างจริงจัง ไม่เพียงเพื่อรักษาความมั่นคงของโครงสร้างพื้นฐานที่สำคัญของประเทศ เช่น ระบบการเงิน พลังงาน การขนส่ง และสาธารณูปโภคเท่านั้น แต่ยังรวมถึงการปกป้องสิทธิของประชาชนในด้านความเป็นส่วนตัว ความมั่นคงของข้อมูล และเสรีภาพในการใช้อินเทอร์เน็ต โดยเฉพาะประเทศที่มีความก้าวหน้าทางเทคโนโลยีและเศรษฐกิจดิจิทัลอย่างเข้มแข็ง เช่น สหรัฐอเมริกา ได้จัดตั้งหน่วยงานเฉพาะทางอย่าง CISA (Cybersecurity and Infrastructure Security Agency) ภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) เพื่อรับผิดชอบด้านการเฝ้าระวังและตอบสนองต่อภัยคุกคามไซเบอร์ในระดับชาติ รวมถึงส่งเสริมความร่วมมือกับภาคเอกชนในการแลกเปลี่ยนข้อมูลด้านความปลอดภัยไซเบอร์ (Carr, 2016)

นอกจากนี้ สหรัฐฯ ยังมีกรอบกฎหมายสำคัญ เช่น Computer Fraud and Abuse Act (CFAA) และ Cybersecurity Information Sharing Act (CISA Act) ที่เปิดโอกาสให้หน่วยงานภาครัฐและเอกชนสามารถแลกเปลี่ยนข้อมูลภัยคุกคามได้อย่างถูกต้องตามกฎหมาย (Goodman, 2016) เอสโตเนีย เป็นอีกตัวอย่างของประเทศที่ประสบความสำเร็จในการวางระบบความมั่นคงทางไซเบอร์อย่างมีแบบแผน ภายหลังจากประสบเหตุโจมตีทางไซเบอร์ครั้งใหญ่ในปี 2007 เอสโตเนียได้พัฒนา Cybersecurity Strategy อย่างต่อเนื่อง พร้อมจัดตั้ง Estonian Information System Authority (RIA) เพื่อทำหน้าที่บริหารจัดการความปลอดภัยไซเบอร์ของหน่วยงานภาครัฐทั้งหมด อีกทั้งยังเป็นประเทศแรกที่ให้บริการ e-Residency ซึ่งเป็นระบบที่ต้องมี

มาตรฐานความปลอดภัยทางไซเบอร์สูงมาก (OECD, 2021) สำหรับ สิงคโปร์ รัฐบาลได้ประกาศใช้ Cybersecurity Act (2018) เพื่อมอบอำนาจให้หน่วยงาน Cyber Security Agency of Singapore (CSA) มีบทบาทในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของระบบโครงสร้างพื้นฐานสำคัญ โดยเน้นการวางระบบเฝ้าระวังภัยไซเบอร์ การทดสอบเจาะระบบ (penetration testing) และการสร้างขีดความสามารถของบุคลากรด้านไซเบอร์อย่างต่อเนื่อง นอกจากนี้ สิงคโปร์ยังได้พัฒนา Cybersecurity Masterplan 2020 ซึ่งกำหนดทิศทางของประเทศในการรับมือภัยคุกคามในอนาคต ด้วยการส่งเสริมความร่วมมือระหว่างรัฐ เอกชน และสถาบันการศึกษา (Cyber Security Agency of Singapore, 2020) จะเห็นได้ว่า ประเทศเหล่านี้ต่างมีจุดร่วมที่สำคัญคือ การวางนโยบายอย่างเป็นระบบ, การจัดตั้งหน่วยงานเฉพาะทาง, และ การสนับสนุนด้านกฎหมายที่ทันสมัยและยืดหยุ่น เพื่อตอบสนองต่อภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ทั้งนี้ แนวทางของประเทศเหล่านี้สามารถใช้เป็นแบบอย่างหรือจุดอ้างอิงในการพัฒนานโยบายของประเทศไทยให้มีประสิทธิภาพมากยิ่งขึ้นในบริบทของความมั่นคงทางไซเบอร์ที่ซับซ้อนในปัจจุบัน

ในบริบทของประเทศไทย รัฐบาลได้ตระหนักถึงความสำคัญของภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยเฉพาะในช่วงทศวรรษที่ผ่านมา ซึ่งเป็นช่วงที่อาชญากรรมไซเบอร์มีความรุนแรงและซับซ้อนมากขึ้น โดยอาศัยช่องว่างของกฎหมายและการขาดความพร้อมของระบบดิจิทัลภาครัฐและเอกชน เพื่อเป็นการรับมือกับปัญหาดังกล่าว รัฐบาลไทยจึงได้ดำเนินการจัดทำนโยบายและออกกฎหมายเพื่อสร้างกรอบการควบคุมและดำเนินคดีกับผู้กระทำความผิดในโลกออนไลน์อย่างจริงจัง กฎหมายหลักที่ใช้เป็นเครื่องมือในการควบคุมพฤติกรรมบนโลกไซเบอร์คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งต่อมาได้มีการแก้ไขเพิ่มเติมในปี พ.ศ. 2560 เพื่อให้สอดคล้องกับสภาพแวดล้อมทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว กฎหมายฉบับนี้ครอบคลุมทั้งการกระทำความผิดที่เกี่ยวกับการเจาะระบบ การแพร่กระจายมัลแวร์ การปลอมแปลงข้อมูล และการเผยแพร่ข้อมูลอันเป็นเท็จ โดยกำหนดบทลงโทษที่ชัดเจน และเปิดช่องให้มีการร้องทุกข์ผ่านช่องทางออนไลน์ได้ (สำนักงานคณะกรรมการกฤษฎีกา, 2560) นอกจากนี้ ยังมีการกำหนดอำนาจหน้าที่ให้แก่เจ้าหน้าที่ผู้รับผิดชอบในการตรวจสอบและยึดอุปกรณ์ดิจิทัลได้ตามกฎหมาย ซึ่งถือเป็นพัฒนาการที่สำคัญในการเพิ่มประสิทธิภาพด้านการบังคับใช้กฎหมายไซเบอร์ในไทย อย่างไรก็ตาม การมีกฎหมายเพียงอย่างเดียวไม่เพียงพอที่จะรับมือกับภัยไซเบอร์ที่มีความซับซ้อนและขยายตัวอย่างรวดเร็ว รัฐบาลจึงได้จัดตั้ง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งเป็นองค์กรหลักในการกำหนดนโยบาย วางแผนยุทธศาสตร์ และดำเนินมาตรการด้านความมั่นคงทางไซเบอร์ในระดับชาติ โดยสำนักงานแห่งนี้มีหน้าที่ในการกำกับดูแลการดำเนินงานของหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure – CII) เช่น ระบบการเงิน การสื่อสาร พลังงาน และการขนส่ง (สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, 2565)

นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติยังมีบทบาทในการจัดทำ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565–2570 ซึ่งกำหนดทิศทางการดำเนินงานด้านความมั่นคงไซเบอร์ของประเทศอย่างชัดเจนใน 5 ด้านหลัก ได้แก่ 1) การพัฒนาและเสริมสร้างศักยภาพด้านไซเบอร์ของประเทศ 2) การป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ 3) การตอบสนองและฟื้นฟูระบบจากเหตุการณ์ไซเบอร์ 4) การบังคับใช้กฎหมายและการยกระดับกฎหมายที่เกี่ยวข้อง และ 5) การส่งเสริมความร่วมมือระหว่างประเทศ (สำนักงานคณะกรรมการการรักษาความมั่นคง

ปลอดภัยไซเบอร์แห่งชาติ, 2565) แม้ประเทศไทยจะมีความคืบหน้าในการกำหนดนโยบายและกลไกด้านความมั่นคงไซเบอร์อย่างเป็นรูปธรรม แต่ยังคงเผชิญกับความท้าทายสำคัญในด้านการบังคับใช้กฎหมาย การขาดแคลนบุคลากรที่มีความเชี่ยวชาญ การขาดการบูรณาการข้อมูลระหว่างหน่วยงาน และการมีส่วนร่วมของภาคเอกชนและประชาชนในวงกว้าง ซึ่งเป็นปัจจัยที่ควรได้รับการพัฒนาเพื่อเพิ่มศักยภาพของประเทศในการป้องกันและรับมือกับอาชญากรรมไซเบอร์ได้อย่างยั่งยืน

จากบริบทของภัยคุกคามทางไซเบอร์ที่ขยายตัวอย่างรวดเร็วและส่งผลกระทบในหลากหลายมิติ ทั้งด้านเศรษฐกิจ ความมั่นคงของรัฐ และสิทธิของพลเมือง ทำให้การกำหนดนโยบายด้านความมั่นคงไซเบอร์กลายเป็นภารกิจที่ท้าทายและจำเป็นอย่างยิ่งสำหรับรัฐบาลของทุกประเทศ ประเทศไทยเองก็ไม่อาจหลีกเลี่ยงการเผชิญหน้ากับความท้าทายดังกล่าว ซึ่งไม่เพียงต้องอาศัยความพร้อมในด้านกฎหมายและกลไกการบังคับใช้เท่านั้น แต่ยังต้องอาศัยวิสัยทัศน์เชิงนโยบายที่สามารถรับมือกับการเปลี่ยนแปลงของเทคโนโลยีและรูปแบบของภัยคุกคามใหม่ ๆ ได้อย่างมีประสิทธิภาพและยืดหยุ่นในระยะยาว บทความวิชาการฉบับนี้จึงมุ่งเน้นการศึกษานโยบายด้านการป้องกันและรับมือกับอาชญากรรมทางไซเบอร์ของประเทศไทยอย่างเป็นระบบ โดยเฉพาะการวิเคราะห์เชิงเปรียบเทียบกับแนวทางของประเทศที่ได้รับการยอมรับในระดับนานาชาติว่าเป็นผู้นำด้านความมั่นคงไซเบอร์ ได้แก่ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย ซึ่งแต่ละประเทศล้วนมีบริบทการพัฒนานโยบายที่แตกต่างกัน ทั้งในเชิงโครงสร้างการบริหาร กฎหมาย เทคโนโลยี และการมีส่วนร่วมของภาคส่วนต่าง ๆ ที่สามารถส่งเสริมให้เกิดการจัดการภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ การวิเคราะห์เชิงเปรียบเทียบในบทความนี้จะใช้เกณฑ์พิจารณาหลักหลายด้าน เช่น กรอบกฎหมาย หน่วยงานที่รับผิดชอบเชิงนโยบาย กลไกการมีส่วนร่วมของภาคเอกชน การบริหารจัดการเหตุการณ์ไซเบอร์ (incident response) และการส่งเสริมการพัฒนาทรัพยากรมนุษย์ด้านความมั่นคงไซเบอร์

แม้ว่าจะมีงานวิจัยด้านความมั่นคงไซเบอร์อยู่ไม่น้อย แต่ส่วนใหญ่ยังมุ่งเน้นไปที่การศึกษาเชิงเทคนิคด้านการป้องกันระบบสารสนเทศ หรือกรณีศึกษาเฉพาะเหตุการณ์ (incident-based) มากกว่าการวิเคราะห์เชิงนโยบายในภาพรวม โดยเฉพาะงานที่เปรียบเทียบเชิงโครงสร้างระหว่างประเทศไทยกับประเทศที่ถือเป็นผู้นำด้านนโยบายความมั่นคงไซเบอร์ยังคงมีอยู่อย่างจำกัด อีกทั้ง งานศึกษาที่มีอยู่จำนวนมากไม่ได้ให้ความสำคัญกับบทบาทของภาคเอกชน การบูรณาการเชิงสถาบัน และการสร้างวัฒนธรรมความมั่นคงไซเบอร์ในสังคมโดยรวม ดังนั้น ช่องว่างขององค์ความรู้ที่สำคัญคือ การขาดการศึกษาเชิงเปรียบเทียบด้านนโยบายความมั่นคงไซเบอร์ในมิติที่หลากหลาย (กฎหมาย สถาบัน ภาคเอกชน ความร่วมมือระหว่างประเทศ และการพัฒนาทรัพยากรมนุษย์) ซึ่งมีความจำเป็นอย่างยิ่งต่อการออกแบบข้อเสนอเชิงนโยบายที่สอดคล้องกับบริบทของประเทศไทย ผลการวิเคราะห์จะถูกนำไปสังเคราะห์เพื่อจัดทำข้อเสนอเชิงนโยบายที่เหมาะสมกับ บริบททางสังคม เศรษฐกิจ และระบบราชการของประเทศไทยอันจะช่วยเสริมสร้างศักยภาพในการป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และยกระดับการบริหารจัดการด้านความมั่นคงไซเบอร์ของประเทศให้มีมาตรฐานทัดเทียมนานาชาติในระยะยาว

วัตถุประสงค์การวิจัย

1. เพื่อวิเคราะห์นโยบายป้องกันอาชญากรรมไซเบอร์ของประเทศไทย
2. เพื่อเปรียบเทียบนโยบายไซเบอร์ระหว่างไทยกับประเทศพัฒนาแล้ว

กรอบนโยบายป้องกันอาชญากรรมไซเบอร์ในประเทศไทย

ประเทศไทยในฐานะประเทศกำลังพัฒนาที่มีการขยายตัวของการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารอย่างรวดเร็ว ได้เผชิญกับความท้าทายจากภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง ส่งผลให้ภาครัฐต้องเร่งกำหนดกรอบแนวคิดเชิงนโยบายและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อปกป้องผลประโยชน์ของรัฐ ภาคธุรกิจ และประชาชน โดยมีการจัดทำและบังคับใช้กลไกหลักสำคัญใน 3 ด้าน ได้แก่ กฎหมายเฉพาะทางระดับชาติ นโยบายแผนยุทธศาสตร์ระดับชาติ และโครงสร้างหน่วยงานหลักด้านความมั่นคงไซเบอร์ซึ่งสามารถอธิบายได้ดังนี้

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม พ.ศ. 2560

กฎหมายฉบับนี้ถือเป็นรากฐานทางกฎหมายในการควบคุมและดำเนินคดีกับผู้กระทำความผิดในโลกไซเบอร์ โดยเฉพาะในกรณีที่ไม่สามารถใช้กฎหมายอาญาทั่วไปได้อย่างครอบคลุม พระราชบัญญัตินี้มีบทบัญญัติที่ครอบคลุมพฤติกรรมที่เป็นอาชญากรรมทางไซเบอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การลักลอบนำข้อมูลออก การทำลายหรือขัดขวางระบบคอมพิวเตอร์ การแพร่กระจายไวรัสหรือมัลแวร์ การปลอมแปลงข้อมูล รวมถึงการเผยแพร่ข้อมูลเท็จที่ก่อให้เกิดความเสียหายต่อบุคคลหรือลักษณะโดยรวมของสาธารณะ (สำนักงานคณะกรรมการกฤษฎีกา, 2560) ฉบับแก้ไขเพิ่มเติมในปี พ.ศ. 2560 ได้ปรับปรุงให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง โดยเพิ่มอำนาจของเจ้าหน้าที่รัฐในการสืบสวนและตรวจสอบคดีไซเบอร์ พร้อมทั้งเพิ่มบทลงโทษในกรณีที่การกระทำความผิดส่งผลกระทบต่อระบบสาธารณูปโภค หรือโครงสร้างพื้นฐานสำคัญของรัฐ นอกจากนี้ ยังกำหนดมาตรการการควบคุมเนื้อหาที่เผยแพร่บนอินเทอร์เน็ต ซึ่งสร้างการถกเถียงในประเด็นเสรีภาพและสิทธิมนุษยชนในสังคมไทยอยู่พอสมควร

2. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565–2570

เพื่อให้การดำเนินงานด้านความมั่นคงไซเบอร์มีทิศทางและแผนการพัฒนาอย่างต่อเนื่อง รัฐบาลจึงได้กำหนดนโยบายและแผนระดับชาติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ซึ่งจัดทำโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และมีผลบังคับใช้ในช่วงปี พ.ศ. 2565–2570 แผนฉบับนี้มีเป้าหมายหลักเพื่อเสริมสร้าง ระบบความมั่นคงปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure – CII) ซึ่งครอบคลุมด้านการเงิน การสื่อสาร พลังงาน ขนส่ง และบริการสาธารณสุข ตลอดจนสร้างระบบตอบสนองต่อเหตุการณ์ภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ยังมุ่งเน้นการ เสริมสร้างความตระหนักรู้และวัฒนธรรมความปลอดภัยไซเบอร์ในหมู่ประชาชน โดยเฉพาะในกลุ่มเยาวชนและผู้สูงอายุ ซึ่งมักตกเป็นเหยื่อของอาชญากรไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2565) เนื้อหาในแผนแบ่งออกเป็น 5 เป้าหมายหลัก ได้แก่

2.1 การปกป้องระบบสารสนเทศของประเทศ

2.2 การพัฒนาบุคลากรด้านไซเบอร์

2.3 การสร้างขีดความสามารถในการตอบโต้ภัยไซเบอร์

2.4 การเสริมสร้างความร่วมมือในระดับนานาชาติ และการวางระบบติดตามประเมินผลและทบทวนแผนงาน

3. การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานใหม่ที่จัดตั้งขึ้นตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีสถานะเป็นหน่วยงานของรัฐที่ไม่อยู่ภายใต้การควบคุมของกระทรวงใดโดยตรง ทำหน้าที่เป็นหน่วยงานหลักในการกำหนดนโยบาย วางแผนยุทธศาสตร์ และประสานการดำเนินการกับหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน เพื่อป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ในระดับประเทศ บทบาทสำคัญของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้แก่

3.1 การจัดตั้ง ศูนย์ประสานงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC)

3.2 การสนับสนุนการวางมาตรฐานการรักษาความปลอดภัยของระบบข้อมูลในองค์กรภาครัฐ

3.3 การประสานงานด้านนโยบายกับองค์กรระหว่างประเทศ เช่น ASEAN, UN และ ITU

3.4 การรวบรวม วิเคราะห์ และเผยแพร่ข้อมูลภัยคุกคามไซเบอร์ในประเทศ

3.5 การส่งเสริมการฝึกอบรม และการสร้างเครือข่ายผู้เชี่ยวชาญด้านไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ยังมีภารกิจในการผลักดันให้เกิดการบูรณาการความร่วมมือแบบบูรณาการระหว่างภาครัฐ เอกชน และภาคประชาสังคม เพื่อเสริมสร้างความตระหนักรู้และสร้างระบบนิเวศความมั่นคงทางไซเบอร์ของประเทศอย่างยั่งยืน (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2565)

สรุปได้ว่า ประเทศไทยมีความพยายามในการกำหนดนโยบายและสร้างกลไกด้านความมั่นคงทางไซเบอร์อย่างครอบคลุม แต่ก็ยังคงเผชิญกับข้อจำกัดในด้านการบังคับใช้กฎหมาย การพัฒนากำลังคนเฉพาะทาง และความไม่ทั่วถึงของความรู้ความเข้าใจในระดับประชาชนทั่วไป ดังนั้น การประเมินผลเชิงเปรียบเทียบกับประเทศที่มีความก้าวหน้าในด้านนี้จึงมีความสำคัญต่อการกำหนดแนวทางพัฒนานโยบายให้มีความทันสมัย สอดคล้องกับบริบทโลก และสามารถตอบสนองต่อภัยคุกคามไซเบอร์ที่เปลี่ยนแปลงอยู่ตลอดเวลา

นโยบายป้องกันอาชญากรรมไซเบอร์ในต่างประเทศ

จากการศึกษานโยบายความมั่นคงทางไซเบอร์ของประเทศพัฒนาแล้ว อาทิ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย พบว่า หัวใจสำคัญของการบริหารจัดการความมั่นคงไซเบอร์ในประเทศเหล่านี้คือ การบูรณาการ นโยบายและการดำเนินงานระหว่างภาครัฐ ภาคเอกชน และภาคประชาชนอย่างเป็นระบบและต่อเนื่อง โดยมีการจัดตั้งกลไกถาวรที่เอื้อต่อการแลกเปลี่ยนข้อมูลข่าวสาร การวางแผนร่วมกัน และการตอบสนองต่อภัยคุกคามอย่างทันท่วงที ตัวอย่างเช่น สหรัฐอเมริกามีการจัดตั้ง Information Sharing and Analysis Centers (ISACs) ซึ่งเป็นเวทีความร่วมมือระหว่างอุตสาหกรรมเอกชนในสาขาต่าง ๆ กับรัฐบาลกลางในการแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ในลักษณะ real-time (Carr, 2016)

1. สหรัฐอเมริกา สหรัฐอเมริกาถือเป็นต้นแบบของประเทศที่มีระบบการรักษาความมั่นคงทางไซเบอร์ที่ครอบคลุมและเชื่อมโยงภาคส่วนต่าง ๆ อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งการเน้นความร่วมมือกับภาคเอกชน ซึ่งถือเป็นผู้ถือครองโครงสร้างพื้นฐานสำคัญ (critical infrastructure) ถึงกว่า 80% ของประเทศ กลไกหลักคือการจัดตั้ง Information Sharing and Analysis Centers (ISACs) ซึ่งเปิดโอกาสให้หน่วยงานเอกชนในภาคส่วนต่าง ๆ เช่น พลังงาน การเงิน การขนส่ง และสาธารณสุข ร่วมมือกับรัฐบาลในการแลกเปลี่ยนข้อมูลภัยคุกคามแบบ real-time เพื่อยกระดับการตอบสนองเชิงรุก (Carr, 2016) การมีหน่วยงาน

อย่าง Cybersecurity and Infrastructure Security Agency (CISA) ภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) ช่วยส่งเสริมบทบาทของรัฐบาลกลางในการเป็นผู้อำนวยความสะดวก (facilitator) และผู้นำในยามเกิดวิกฤตทางไซเบอร์ นอกจากนี้ การมีกรอบยุทธศาสตร์ความมั่นคงไซเบอร์ระดับชาติ (National Cyber Strategy) ที่ได้รับการปรับปรุงอย่างต่อเนื่องยังสะท้อนถึงระบบนโยบายที่เน้น adaptive governance และตอบสนองต่อบริบทภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว (White House, 2023)

2. สิงคโปร์ สิงคโปร์มีลักษณะของรัฐที่มีประสิทธิภาพในการบริหารจัดการสูง และนำแนวคิดเรื่อง whole-of-government approach มาใช้ในการกำหนดนโยบายไซเบอร์ โดยมีการจัดตั้ง Cyber Security Agency of Singapore (CSA) เป็นหน่วยงานหลักในการกำกับดูแลและดำเนินงานด้านความมั่นคงไซเบอร์ระดับชาติ ภายใต้สำนักนายกรัฐมนตรี แนวทางของสิงคโปร์เน้นการบูรณาการระหว่างยุทธศาสตร์ความมั่นคงไซเบอร์กับยุทธศาสตร์ดิจิทัลระดับชาติ เช่น Smart Nation Initiative โดยมีการลงทุนอย่างต่อเนื่องในโครงสร้างพื้นฐานดิจิทัล ความมั่นคงทางข้อมูล และการพัฒนา “Digital Trust” ผ่านกฎหมายและมาตรฐาน เช่น Cybersecurity Act 2018 ซึ่งกำหนดให้ผู้ประกอบการโครงสร้างพื้นฐานสำคัญต้องปฏิบัติตามมาตรฐานความมั่นคงที่กำหนด และรายงานเหตุการณ์ต่อ CSA อย่างเป็นระบบ (Choo, 2019) นอกจากนี้ สิงคโปร์ยังให้ความสำคัญกับการสร้างขีดความสามารถของบุคลากรในระยะยาวผ่าน Cybersecurity Talent Development Fund และการร่วมมือกับมหาวิทยาลัยในการผลิตแรงงานทักษะสูง ซึ่งถือเป็นการวางรากฐานเชิงระบบที่แข็งแกร่ง

3. เอสโตเนีย เอสโตเนียได้รับการยอมรับว่าเป็นผู้นำระดับโลกด้านรัฐบาลดิจิทัล โดยเริ่มพัฒนา e-Government อย่างเป็นรูปธรรมตั้งแต่ต้นทศวรรษ 2000 ภายหลังการโจมตีทางไซเบอร์ครั้งใหญ่ในปี 2007 เอสโตเนียได้เร่งพัฒนากลไกการป้องกันประเทศในมิติไซเบอร์อย่างจริงจัง หนึ่งในแนวทางสำคัญคือการจัดตั้ง Cyber Defence Unit (CDU) ภายใต้การกำกับของกองทัพ แต่เปิดรับอาสาสมัครที่เป็นผู้เชี่ยวชาญจากภาคประชาชนและภาคเอกชนให้เข้ามาร่วมปฏิบัติงานร่วมกับรัฐ (Tikk et al., 2010) เอสโตเนียใช้แนวทาง resilience-based security ซึ่งไม่ได้มองเพียงด้านการป้องกันภัย แต่รวมถึงการเตรียมพร้อม การรับมือ และการฟื้นฟูระบบหลังการโจมตี ระบบ X-Road ของเอสโตเนียเป็นโครงสร้างพื้นฐานข้อมูลที่เชื่อมโยงหน่วยงานภาครัฐทั้งหมดเข้าด้วยกันอย่างปลอดภัย โดยใช้การเข้ารหัสแบบ public key infrastructure (PKI) และบันทึกธุรกรรมแบบโปร่งใส (transparent logging) ซึ่งทำให้ประชาชนสามารถเข้าถึงบริการออนไลน์อย่างมั่นใจ (Kaska et al., 2019) โมเดลของเอสโตเนียชี้ให้เห็นว่าการพัฒนาความมั่นคงทางไซเบอร์ที่ยั่งยืนจำเป็นต้องอาศัยความร่วมมือแบบ “bottom-up” โดยสร้างจิตสำนึก ความไว้วางใจ และทักษะไซเบอร์ของประชาชนควบคู่กับนโยบายของรัฐ

4. ประเทศไทย ประเทศไทยแม้จะมีนโยบายและโครงสร้างพื้นฐานด้านความมั่นคงไซเบอร์ในระดับหนึ่งแล้ว เช่น การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และการออกแผนยุทธศาสตร์ระดับชาติ แต่ยังประสบปัญหาหลายประการที่ส่งผลต่อประสิทธิภาพการดำเนินงาน โดยเฉพาะในประเด็นของ กลไกการประเมินผล และ การมีส่วนร่วมของภาคเอกชน ซึ่งยังคงดำเนินไปในลักษณะต่างฝ่ายต่างทำ ขาดเวทีความร่วมมือเชิงยุทธศาสตร์ที่เป็นระบบและต่อเนื่อง อีกทั้งยังไม่มีกลไกกลางที่มีอำนาจเพียงพอในการบูรณาการข้อมูลภัยคุกคามจากทุกภาคส่วนให้เป็นฐานข้อมูลระดับชาติ นอกจากนี้ความร่วมมือระหว่างประเทศของไทยในด้านความมั่นคงไซเบอร์ยังค่อนข้างจำกัด ทั้งในเชิงกลไกทางนโยบายและความสามารถทางเทคนิค เมื่อเปรียบเทียบกับประเทศสมาชิก NATO หรือแม้แต่สิงคโปร์ ซึ่งมีบทบาทนำ

ในเวทีอาเซียนและระดับสากล โดยเฉพาะในการเป็นเจ้าภาพจัดตั้ง ASEAN Cybersecurity Centre of Excellence (ACCE) ที่มุ่งพัฒนาเครือข่ายความร่วมมือและมาตรฐานกลางระดับภูมิภาค ในขณะที่ไทยแม้จะเข้าร่วมความร่วมมือบางกลุ่ม เช่น FIRST, ASEAN-Japan Cybersecurity Capacity Building แต่ยังขาดความต่อเนื่องและการลงทุนด้านทรัพยากรอย่างจริงจัง (OECD, 2021) อีกประเด็นหนึ่งที่สะท้อนถึงข้อจำกัดของไทยคือ การขาด ระบบประเมินผลและติดตามความก้าวหน้าของนโยบายและยุทธศาสตร์ไซเบอร์ ซึ่งส่งผลให้การดำเนินงานจำนวนมากอยู่ในลักษณะของหลักการ มากกว่าการนำไปปฏิบัติจริง และขาดหลักฐานเชิงประจักษ์ในการปรับปรุงนโยบายให้ตอบสนองต่อบริบทภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว

ตารางที่ 1 การวิเคราะห์เปรียบเทียบความมั่นคงทางไซเบอร์แต่ละประเทศ

ประเด็น	ประเทศไทย	สหรัฐอเมริกา	สิงคโปร์	เอสโตเนีย
กฎหมายเฉพาะทาง	พ.ร.บ.คอมพิวเตอร์ (2560)	Computer Fraud and Abuse Act (CFAA)	Cybersecurity Act (2018)	Cybersecurity Act (2018)
หน่วยงานหลัก	สกมช.	CISA (Cybersecurity and Infrastructure Security Agency)	CSA (Cyber Security Agency of Singapore)	Estonian Information System Authority (RIA)
ระดับการมีส่วนร่วมภาคเอกชน	ยังจำกัด	สูง	สูง	สูง
การให้ความรู้ประชาชน	มีแต่ยังไม่ทั่วถึง	มีระบบการศึกษาไซเบอร์	มี Cybersecurity Masterplan	มีหลักสูตรไซเบอร์ในระดับชาติ
ความร่วมมือระหว่างประเทศ	กำลังพัฒนา	สมาชิก NATO และกลุ่ม Five Eyes	ASEAN Cybersecurity Centre	NATO และ EU Cyber Defense Cooperation

5. วิเคราะห์กรณีความมั่นคงทางไซเบอร์ของประเทศไทย เทียบกับสหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย

5.1 ความแตกต่างเชิงระบบ โครงสร้าง การบูรณาการ และการมีส่วนร่วม จากการเปรียบเทียบพบว่า ประเทศพัฒนาแล้วอย่าง สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย มีระบบการบริหารจัดการด้านความมั่นคงทางไซเบอร์ที่มี โครงสร้างเชิงระบบที่ชัดเจนและมีกลไกบูรณาการแบบถาวร ซึ่งเอื้อให้เกิดการแลกเปลี่ยนข้อมูลและตอบสนองภัยคุกคามได้อย่างทันท่วงที

5.1.1 สหรัฐอเมริกา ใช้แนวทางแบบ multi-stakeholder governance โดยมี ISACs เป็นแพลตฟอร์มสำหรับภาคเอกชนและรัฐบาลในการแลกเปลี่ยนข้อมูลเชิงลึกแบบ real-time ซึ่งช่วยเพิ่มศักยภาพ

ในการตอบสนองต่อภัยคุกคามระดับประเทศได้อย่างมีประสิทธิภาพ (Carr, 2016) การมีหน่วยงานกลางอย่าง CISA ช่วยลดความซ้ำซ้อน และขับเคลื่อนนโยบายอย่างมีพลังผ่านการเชื่อมโยงกับผู้มีส่วนได้ส่วนเสียต่าง ๆ

5.1.2 สิงคโปร์ มีการจัดตั้ง CSA ที่อยู่ภายใต้การกำกับของสำนักนายกรัฐมนตรี ซึ่งทำให้การกำหนดยุทธศาสตร์และการบังคับใช้กฎหมายเกิดขึ้นอย่างรวมศูนย์และมีอำนาจ การออกกฎหมายเฉพาะด้าน เช่น Cybersecurity Act 2018 ยังเป็นเครื่องมือทางนโยบายที่ใช้ควบคุมและกำกับโครงสร้างพื้นฐานสำคัญ (Choo, 2019)

5.1.3 เอสโตเนีย โดดเด่นด้วยโมเดล bottom-up cyber resilience ที่เปิดโอกาสให้ภาคประชาชนและเอกชนมีส่วนร่วมอย่างแท้จริง ผ่านหน่วย Cyber Defence Unit (CDU) ที่อาสาสมัครผู้เชี่ยวชาญสามารถมีบทบาทในการป้องกันประเทศด้านไซเบอร์ (Tikk et al., 2010) โครงสร้างอย่าง X-Road ก็ช่วยให้รัฐมีข้อมูลแบบรวมศูนย์ที่ปลอดภัย

5.1.4 ประเทศไทย ยังขาดกลไกบูรณาการที่มีประสิทธิภาพในเชิงระบบ แม้จะมีการจัดตั้ง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และการออก พระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ. 2562 แต่การทำงานระหว่างหน่วยงานรัฐกับเอกชนยังดำเนินไปแบบแยกส่วน ขาดความต่อเนื่อง และเวทีถาวรในการสื่อสารข้อมูลภัยคุกคาม เช่นเดียวกับที่ ISACs ทำหน้าที่ในสหรัฐฯ (OECD, 2021)

5.2 บริบทการเมือง การบริหาร และความพร้อมของประเทศ บริบททางการเมืองและการบริหารมีผลอย่างมากต่อการออกแบบและดำเนินนโยบายไซเบอร์ในแต่ละประเทศ

5.2.1 สหรัฐอเมริกา มีการเมืองแบบเสรีนิยมที่เปิดโอกาสให้ภาคเอกชนมีบทบาทสำคัญในโครงสร้างความมั่นคง การออกนโยบายจึงต้องอาศัยฉันทามติในวงกว้างและความร่วมมือระหว่างหน่วยงานต่างระดับ

5.2.2 สิงคโปร์ ซึ่งเป็นรัฐรวมศูนย์ที่มีการวางแผนเชิงกลยุทธ์สูง มีความสามารถในการควบคุมนโยบายได้ทั้งแนวดิ่งและแนวนอน ทำให้สามารถดำเนินการตามยุทธศาสตร์ Smart Nation ได้อย่างมีประสิทธิภาพ

5.2.3 เอสโตเนีย แสดงให้เห็นถึงการสร้างนโยบายที่สะท้อนความเป็นประชาธิปไตยแบบมีส่วนร่วม ประชาชนมีบทบาทสำคัญในการร่วมดูแลความมั่นคงไซเบอร์ของรัฐ และความเชื่อมั่นในรัฐบาลดิจิทัลสูง (Kaska et al., 2019)

ในขณะที่ ประเทศไทย แม้จะมีการออกนโยบายในระดับยุทธศาสตร์ แต่ยังขาดกลไกการติดตามประเมินผล และปรับตัวต่อการเปลี่ยนแปลงที่รวดเร็วของภัยคุกคาม ทำให้นโยบายหลายฉบับยังคงอยู่ในลักษณะของ แผนกระดาษ มากกว่าการนำไปปฏิบัติจริง และยังขาดความเชื่อมั่นที่ผู้คนมีต่อความปลอดภัย ความเป็นส่วนตัว และความน่าเชื่อถือของระบบดิจิทัล จากภาคประชาชนและธุรกิจ (OECD, 2021)

ข้อเสนอแนะการวิเคราะห์เชิงเปรียบเทียบ

1. การวิเคราะห์ข้อดี ข้อจำกัดของประเทศพัฒนาแล้ว

สหรัฐอเมริกา มีความโดดเด่นด้านกลไกความร่วมมือระหว่างรัฐและเอกชน เช่น ISACs และหน่วยงานกลางอย่าง CISA ที่มีอำนาจสูง แต่ข้อจำกัดคือโครงสร้างแบบ multi-stakeholder governance อาจซับซ้อน ทำให้การประสานงานล่าช้าในบางกรณี

สิงคโปร์ มีข้อดีคือ ความสามารถในการบูรณาการเชิงนโยบายอย่างมีเอกภาพ และการใช้กฎหมายควบคุมโครงสร้างพื้นฐานสำคัญ แต่ข้อจำกัดคือการรวมศูนย์อำนาจมากเกินไปอาจลดความยืดหยุ่นและการมีส่วนร่วมจากภาคประชาชน

เอสโตเนีย โดดเด่นด้วยการมีส่วนร่วมของประชาชนและความเชื่อมั่นในรัฐบาลดิจิทัล แต่ข้อจำกัดคือประเทศมีขนาดเล็กและมีบริบทเฉพาะ ทำให้ไม่สามารถถ่ายโอนโมเดลได้ทั้งหมดไปใช้ในประเทศขนาดใหญ่กว่า

2. การวิเคราะห์ข้อดี ข้อจำกัดของประเทศไทย

ข้อดี คือมีการจัดตั้ง สกมช. และมีพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ. 2562 ซึ่งถือเป็นก้าวแรกที่สำคัญในการสร้างกรอบกฎหมายและสถาบันกลาง

ข้อจำกัด ได้แก่ การทำงานแบบแยกส่วนระหว่างหน่วยงานรัฐและเอกชน ขาดกลไกการติดตามและประเมินผลที่มีประสิทธิภาพ และยังมีบทบาทจำกัดในความร่วมมือระหว่างประเทศ

3. การเปรียบเทียบระหว่างไทยกับต่างประเทศ

ข้อเหมือน คือ ทุกประเทศต่างตระหนักถึงความสำคัญของภัยคุกคามไซเบอร์ และมีการจัดตั้งหน่วยงานกลางที่ทำหน้าที่กำกับ

ข้อแตกต่าง อยู่ที่ความเข้มแข็งของกลไกความร่วมมือและระดับการมีส่วนร่วมของเอกชนโดยสหรัฐอเมริกาและสิงคโปร์เปิดพื้นที่ให้เอกชนเข้ามามีบทบาทสูง ขณะที่ไทยยังคงจำกัดและขาดเวทีถาวรในการแลกเปลี่ยนข้อมูลในด้าน การสร้างวัฒนธรรมความมั่นคงไซเบอร์ เอสโตเนียและสิงคโปร์ให้ความสำคัญอย่างต่อเนื่อง แต่ประเทศไทยยังไม่สามารถสร้างความตระหนักรู้ในวงกว้างได้

4. ข้อเสนอแนะสำหรับการประยุกต์ใช้ที่ดีในประเทศไทย

นำแนวคิด ISACs ของสหรัฐฯ มาปรับใช้ในลักษณะ Cybersecurity Exchange Platform ที่เปิดโอกาสให้ภาครัฐ เอกชน และภาควิชาการแลกเปลี่ยนข้อมูลภัยคุกคามแบบเรียลไทม์

นำโมเดล whole-of-government ของสิงคโปร์ มาใช้ โดยบูรณาการยุทธศาสตร์ความมั่นคงไซเบอร์กับยุทธศาสตร์ดิจิทัลของประเทศ เช่น Thailand 4.0

ประยุกต์แนวทาง bottom-up resilience ของเอสโตเนีย โดยส่งเสริมให้ประชาชน องค์กรภาคประชาสังคม และภาคธุรกิจเข้ามามีบทบาทในการปกป้องและสร้างความไว้วางใจในระบบดิจิทัล

5. ข้อเสนอแนะเพื่อการพัฒนาและปรับปรุงของประเทศไทย

ด้านโครงสร้าง: จัดตั้งหน่วยงานกลางที่มีอำนาจจริงในการบูรณาการข้อมูลภัยคุกคามไซเบอร์

ด้านนโยบายและกฎหมาย: พัฒนากลไกติดตามและประเมินผลที่มีหลักฐานเชิงประจักษ์

ด้านความร่วมมือระหว่างประเทศ: เพิ่มบทบาทในเวทีระดับภูมิภาคและนานาชาติ เช่น ASEAN และ OECD เพื่อยกระดับมาตรฐานความร่วมมือ

ด้านวัฒนธรรมและสังคม: ส่งเสริมการเรียนรู้และความตระหนักด้านความมั่นคงไซเบอร์ในทุกระดับตั้งแต่โรงเรียน มหาวิทยาลัย ไปจนถึงสถานประกอบการ

ข้อเสนอแนะเชิงนโยบาย

จากการเปรียบเทียบนโยบายด้านความมั่นคงทางไซเบอร์ระหว่างประเทศไทยกับประเทศพัฒนาแล้วอาทิ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย พบว่าประเทศไทยยังขาดความพร้อมในหลายมิติ ทั้งในเชิงระบบการบริหารจัดการ ความร่วมมือข้ามภาคส่วน และกลไกการติดตามประเมินผลอย่างต่อเนื่อง เพื่อเสริมสร้างขีด

ความสามารถในการรับมือกับภัยคุกคามไซเบอร์อย่างยั่งยืน จึงสามารถเสนอแนวทางเชิงนโยบายที่เหมาะสมได้ดังนี้

1. จัดตั้งกลไกความร่วมมือถาวรระหว่างภาครัฐและเอกชน ประเทศไทยควรจัดตั้ง แพลตฟอร์มกลางระดับชาติ เช่น National Cyber Threat Intelligence Exchange Platform ที่เปิดโอกาสให้หน่วยงานรัฐและเอกชนสามารถ แลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์แบบ real-time และประสานการตอบสนองร่วมกันได้อย่างมีประสิทธิภาพ ทั้งนี้สามารถใช้โมเดลของ ISACs ในสหรัฐอเมริกาเป็นต้นแบบ ซึ่งพิสูจน์แล้วว่าเป็นกลไกสำคัญในการเชื่อมโยงภาคส่วนต่าง ๆ และช่วยลดความเสียหายจากภัยคุกคามได้อย่างเป็นรูปธรรม (Carr, 2016; White House, 2023) การมีศูนย์กลางข้อมูลภัยคุกคามจะช่วยให้รัฐบาลสามารถสร้างฐานข้อมูลระดับชาติ เพื่อใช้วิเคราะห์แนวโน้มและวางมาตรการเชิงรุกได้ดียิ่งขึ้น

2. กำหนดกรอบการประเมินผลนโยบายไซเบอร์อย่างเป็นระบบ ข้อจำกัดสำคัญของไทยในปัจจุบันคือการขาด ระบบติดตามและประเมินผล ที่มีประสิทธิภาพ ซึ่งทำให้นโยบายจำนวนมากไม่สามารถแปลงเป็นการปฏิบัติจริงได้ ดังนั้น รัฐควรกำหนด ตัวชี้วัดผลสำเร็จหลัก (KPIs) ของยุทธศาสตร์ไซเบอร์อย่างชัดเจน เช่น จำนวนการตอบสนองภัยคุกคามภายในเวลาที่กำหนด อัตราการรายงานเหตุการณ์ไซเบอร์จากภาคเอกชน หรือระดับการเข้าร่วมขององค์กรต่าง ๆ ในระบบแลกเปลี่ยนข้อมูล ซึ่งต้องสามารถตรวจสอบได้และมีความเชื่อถือได้ (OECD, 2021) นอกจากนี้ ระบบประเมินผลควรออกแบบให้มีการรายงานต่อสาธารณะ เพื่อสร้างแรงกดดันเชิงนโยบาย และเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียสามารถสะท้อนความคิดเห็นในการปรับปรุงนโยบาย

3. ขยายบทบาทของไทยในเวทีความร่วมมือระดับภูมิภาค ประเทศไทยควรมีบทบาทเชิงรุกมากขึ้นในระดับภูมิภาค โดยเฉพาะใน เวทีอาเซียน เช่น ASEAN Ministerial Conference on Cybersecurity และ ASEAN Cybersecurity Cooperation Strategy เพื่อเสริมสร้างความน่าเชื่อถือของประเทศในฐานะพันธมิตรด้านไซเบอร์ รวมถึงเปิดโอกาสในการเข้าถึงองค์ความรู้ เทคโนโลยี และการฝึกอบรมจากนานาชาติ การเข้าร่วมในเวทีอย่าง ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) และ ASEAN-Japan Cybersecurity Capacity Building Centre ควรดำเนินไปอย่างต่อเนื่อง พร้อมการลงทุนทรัพยากรที่เพียงพอเพื่อยกระดับขีดความสามารถบุคลากรและระบบตอบสนองของประเทศ (OECD, 2021)

4. พัฒนาแนวทางการมีส่วนร่วมของภาคประชาชน ความมั่นคงทางไซเบอร์ไม่สามารถเกิดขึ้นได้จากภาครัฐหรือองค์กรขนาดใหญ่เพียงฝ่ายเดียว หากแต่ต้องอาศัยความตระหนักรู้และการมีส่วนร่วมจากประชาชน รัฐบาลจึงควรจัดตั้งโครงการ สร้างวัฒนธรรมความมั่นคงไซเบอร์ (Cybersecurity Awareness Culture) ผ่านการให้ความรู้และฝึกอบรมในระดับชุมชน โรงเรียน และภาคแรงงาน เช่น การพัฒนาหลักสูตรสำหรับครู การจัดค่ายฝึกอบรมสำหรับนักเรียน และการฝึกอบรมสำหรับ SMEs ประเทศเอสโตเนียเป็นตัวอย่างที่ดีในการสร้างพลเมืองดิจิทัลที่มีภูมิคุ้มกัน ผ่านความร่วมมือระหว่างรัฐ โรงเรียน และประชาชนในการส่งเสริมทักษะด้านไซเบอร์ (Kaska et al., 2019)

องค์ความรู้ใหม่

จากการศึกษานโยบายความมั่นคงทางไซเบอร์ของประเทศต่าง ๆ ได้แก่ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย เทียบกับประเทศไทย ทำให้เห็นภาพรวมขององค์ประกอบเชิงระบบและบริบทที่มีผลต่อความสำเร็จ

ในการดำเนินนโยบายความมั่นคงทางไซเบอร์อย่างยั่งยืน องค์ความรู้สำคัญที่ได้จากการวิเคราะห์เปรียบเทียบสามารถสรุปได้ดังนี้

1. ความมั่นคงไซเบอร์เป็นภารกิจแบบพหุภาคี

ประเทศที่ประสบความสำเร็จในการจัดการภัยคุกคามทางไซเบอร์มักมีลักษณะร่วมที่สำคัญคือการสร้างระบบความมั่นคงทางไซเบอร์ในลักษณะพหุภาคี (multi-stakeholder model) ซึ่งหมายถึงการเปิดพื้นที่ความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชนอย่างจริงจังและต่อเนื่อง สหรัฐอเมริกาเป็นตัวอย่างที่โดดเด่น โดยมีการจัดตั้ง ISACs หรือศูนย์แลกเปลี่ยนข้อมูลระหว่างภาคเอกชนและรัฐบาลในแต่ละอุตสาหกรรมสำคัญ (Carr, 2016) ซึ่งช่วยให้การตอบสนองต่อภัยคุกคามไซเบอร์สามารถดำเนินไปแบบเรียลไทม์และลดผลกระทบในวงกว้าง ในทำนองเดียวกัน เอสโตเนียเปิดรับอาสาสมัครจากภาคประชาชนที่มีทักษะเข้ามาร่วมกับหน่วยงานด้านความมั่นคงไซเบอร์ของรัฐ ผ่านการจัดตั้ง Cyber Defence Unit (Tikk et al., 2010) สะท้อนให้เห็นว่าความมั่นคงไซเบอร์ไม่อาจพึ่งพารัฐฝ่ายเดียว แต่ต้องอาศัยการระดมทรัพยากรและความสามารถจากทุกภาคส่วน

2. การมีหน่วยงานกลางที่มีอำนาจและระบบเชื่อมโยงข้อมูล

การมีหน่วยงานกลางที่มีอำนาจและสามารถเชื่อมโยงข้อมูลจากหลายหน่วยงานเป็นอีกหนึ่งปัจจัยสำคัญ ตัวอย่างเช่น สหรัฐอเมริกามี CISA ที่มีบทบาทกำกับยุทธศาสตร์และการดำเนินงานเชิงบูรณาการของทั้งรัฐและเอกชน (White House, 2023) ขณะที่สิงคโปร์มี CSA ซึ่งอยู่ภายใต้สำนักนายกรัฐมนตรี ทำให้การกำหนดยุทธศาสตร์ไซเบอร์สามารถขับเคลื่อนได้อย่างมีเอกภาพ (Choo, 2019) ในกรณีของเอสโตเนีย ระบบ X-Road ซึ่งเป็นโครงสร้างพื้นฐานกลางในการเชื่อมโยงข้อมูลของทุกหน่วยงานภาครัฐ เป็นหลักฐานสำคัญที่ชี้ว่าข้อมูลคือรากฐานของระบบไซเบอร์ที่แข็งแกร่ง (Kaska et al., 2019) แตกต่างจากประเทศไทยที่แม้จะมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แต่ยังขาดกลไกที่สามารถรวบรวมข้อมูลภัยคุกคามจากทุกภาคส่วนได้อย่างมีประสิทธิภาพ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2566)

3. การบูรณาการนโยบายไซเบอร์กับยุทธศาสตร์ดิจิทัลระดับชาติ

ประเทศที่มีนโยบายไซเบอร์ที่ยั่งยืนมักไม่มองไซเบอร์เป็นแค่เรื่องเทคนิค แต่เป็นส่วนหนึ่งของระบบเศรษฐกิจและความมั่นคงโดยรวม สิงคโปร์คือแบบอย่างสำคัญในการบูรณาการไซเบอร์เข้ากับ Smart Nation Strategy (Choo, 2019) ในขณะที่เอสโตเนียถือว่าการพัฒนารัฐบาลดิจิทัลและความมั่นคงไซเบอร์เป็นรากฐานเดียวกัน (Kaska et al., 2019) ตรงข้ามกับประเทศไทยที่ยังดำเนินการแบบแยกส่วนระหว่างหน่วยงาน (OECD, 2021)

4. ความร่วมมือระหว่างประเทศช่วยเสริมขีดความสามารถภายในประเทศ

สหรัฐอเมริกาและเอสโตเนียมีบทบาทเชิงรุกในเวทีระดับนานาชาติ เช่น NATO, EU หรือ Five Eyes ขณะที่สิงคโปร์เป็นเจ้าภาพ ASEAN Cybersecurity Centre of Excellence (Kaska et al., 2019) ซึ่งช่วยสร้างมาตรฐานกลางในภูมิภาคอาเซียน ส่วนประเทศไทยแม้จะเข้าร่วมความร่วมมือบางเวที เช่น FIRST และ ASEAN-Japan Cybersecurity Centre แต่ยังขาดบทบาทเชิงนำและความต่อเนื่องในการลงทุน (OECD, 2021; ThaiCERT, 2023)

5. การส่งเสริมทักษะไซเบอร์ของประชาชน

เอสโตเนียให้ความสำคัญอย่างยิ่งกับการสร้างพลเมืองดิจิทัลที่มีภูมิคุ้มกันภัยไซเบอร์ตั้งแต่ระดับการศึกษาไปจนถึงการฝึกอบรมในชุมชน (Tikk et al., 2010; Kaska et al., 2019) ในขณะที่ประเทศไทยยังไม่มีแนวทางที่ชัดเจน แม้จะมีความพยายามผ่านแคมเปญต่าง ๆ แต่ยังไม่เป็นระบบ (ThaiCERT, 2023)

สรุป

การศึกษาเชิงเปรียบเทียบนโยบายการป้องกันอาชญากรรมทางไซเบอร์ระหว่างประเทศไทยกับประเทศพัฒนาแล้ว ได้แก่ สหรัฐอเมริกา สิงคโปร์ และเอสโตเนีย พบว่า ประเทศที่มีระบบความมั่นคงไซเบอร์ที่เข้มแข็งมักมีลักษณะร่วมสำคัญ คือ การบูรณาการความร่วมมือจากภาครัฐ ภาคเอกชน และภาคประชาชนอย่างเป็นระบบ พร้อมทั้งมีหน่วยงานกลางที่มีอำนาจกำกับและกลไกเชิงยุทธศาสตร์ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลภัยคุกคามอย่างทันท่วงที นอกจากนี้ ยังให้ความสำคัญต่อการพัฒนาทรัพยากรมนุษย์ การส่งเสริมการมีส่วนร่วมของสังคม และการขับเคลื่อนความร่วมมือระหว่างประเทศอย่างต่อเนื่อง สำหรับประเทศไทย แม้จะมีความพยายามในการขับเคลื่อนนโยบายด้านความมั่นคงไซเบอร์ ผ่านการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และการกำหนดยุทธศาสตร์ในระดับชาติ หากแต่ยังคงเผชิญข้อจำกัดหลายประการ ได้แก่ การขาดกลไกความร่วมมือถาวรระหว่างรัฐและเอกชน ระบบการประเมินผลที่ไม่ชัดเจน การบูรณาการข้อมูลภัยคุกคามที่ยังไม่เป็นระบบ ตลอดจนบทบาทที่จำกัดในเวทีความร่วมมือระดับภูมิภาคและนานาชาติ อีกทั้ง ความตระหนักรู้และทักษะด้านไซเบอร์ของประชาชนไทยยังอยู่ในระดับที่จำเป็นต้องได้รับการพัฒนาอย่างจริงจัง ดังนั้น จึงควรดำเนินการตามข้อเสนอเชิงนโยบาย ได้แก่ 1) จัดตั้งกลไกกลางเพื่อการแลกเปลี่ยนข้อมูลภัยคุกคามแบบเรียลไทม์ระหว่างภาครัฐและเอกชน 2) พัฒนาระบบติดตามและประเมินผลนโยบายที่มีตัวชี้วัดที่ชัดเจนและตรวจสอบได้ 3) ขยายบทบาทของประเทศไทยในเวทีความร่วมมือระดับภูมิภาคและนานาชาติ 4) ส่งเสริมการมีส่วนร่วมของประชาชนผ่านการปลูกฝังวัฒนธรรมความมั่นคงทางไซเบอร์ตั้งแต่ระดับการศึกษาไปจนถึงระดับแรงงาน บทเรียนจากประเทศพัฒนาแล้วสะท้อนให้เห็นว่า ความมั่นคงทางไซเบอร์ไม่ใช่เพียงประเด็นด้านโครงสร้างพื้นฐานหรือกฎหมาย หากแต่ต้องอาศัยระบบนิเวศแห่งความร่วมมือที่ประกอบด้วยข้อมูล ความเชื่อมั่น และการมีส่วนร่วมของทุกภาคส่วน อันจะเป็นรากฐานสำคัญต่อการป้องกันอาชญากรรมทางไซเบอร์และการยกระดับความมั่นคงของประเทศในระยะยาว

เอกสารอ้างอิง

สำนักงานคณะกรรมการกฤษฎีกา. (2560). **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560**. กรุงเทพฯ: สำนักงานคณะกรรมการกฤษฎีกา.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2565). **นโยบายและแผนระดับชาติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565–2570**. กรุงเทพฯ: สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). **รายงานประจำปี 2566**. กรุงเทพฯ: สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2565). **แนวนโยบายและแผนแม่บทดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศไทย ระยะที่ 2**. กรุงเทพฯ: สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ.

Carr, M. (2016). Public–private partnerships in national cyber security strategies. **International Affairs**, 92(1), 43–62.

Choo, K.-K. R. (2019). Cybersecurity in Singapore: Governance, policy and strategy. **Journal of Cyber Policy**, 4(3), 1–19.

Cyber Security Agency of Singapore. (2020). **Singapore cybersecurity strategy**. Retrieved from https://www.csa.gov.sg.

Goodman, M. (2016). **Future crimes: Inside the digital underground and the battle for our connected world**. Anchor Books.

Kaska, K., Beckvard, H., & Minárik, T. (2019). **Cybersecurity strategy documents: A comparative study. NATO Cooperative Cyber Defence Centre of Excellence**. https://ccdcoe.org/library/publications/.

Kaska, K., Berzins̄, J., & Nissen, T. E. (2019). **Cybersecurity in the EU and beyond: Cyber defence and the future of conflict**. NATO Strategic Communications Centre of Excellence.

OECD. (2021). Cybersecurity policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the internet economy. **OECD Digital Economy Papers**, No. 329.

OECD. (2021). **Digital security policy for a trusted and inclusive digital transformation in Thailand**. https://www.oecd.org/publications.

ThaiCERT. (2023). **รายงานสถานการณ์ภัยคุกคามไซเบอร์ประเทศไทย 2566–2567. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์**. สืบค้นจาก https://www.thaicert.or.th.

Tikk, E., Kaska, K., & Vihul, L. (2010). **International cyber incidents: Legal considerations**. NATO Cooperative Cyber Defence Centre of Excellence.

White House. (2023). **National Cybersecurity Strategy**. The White House.