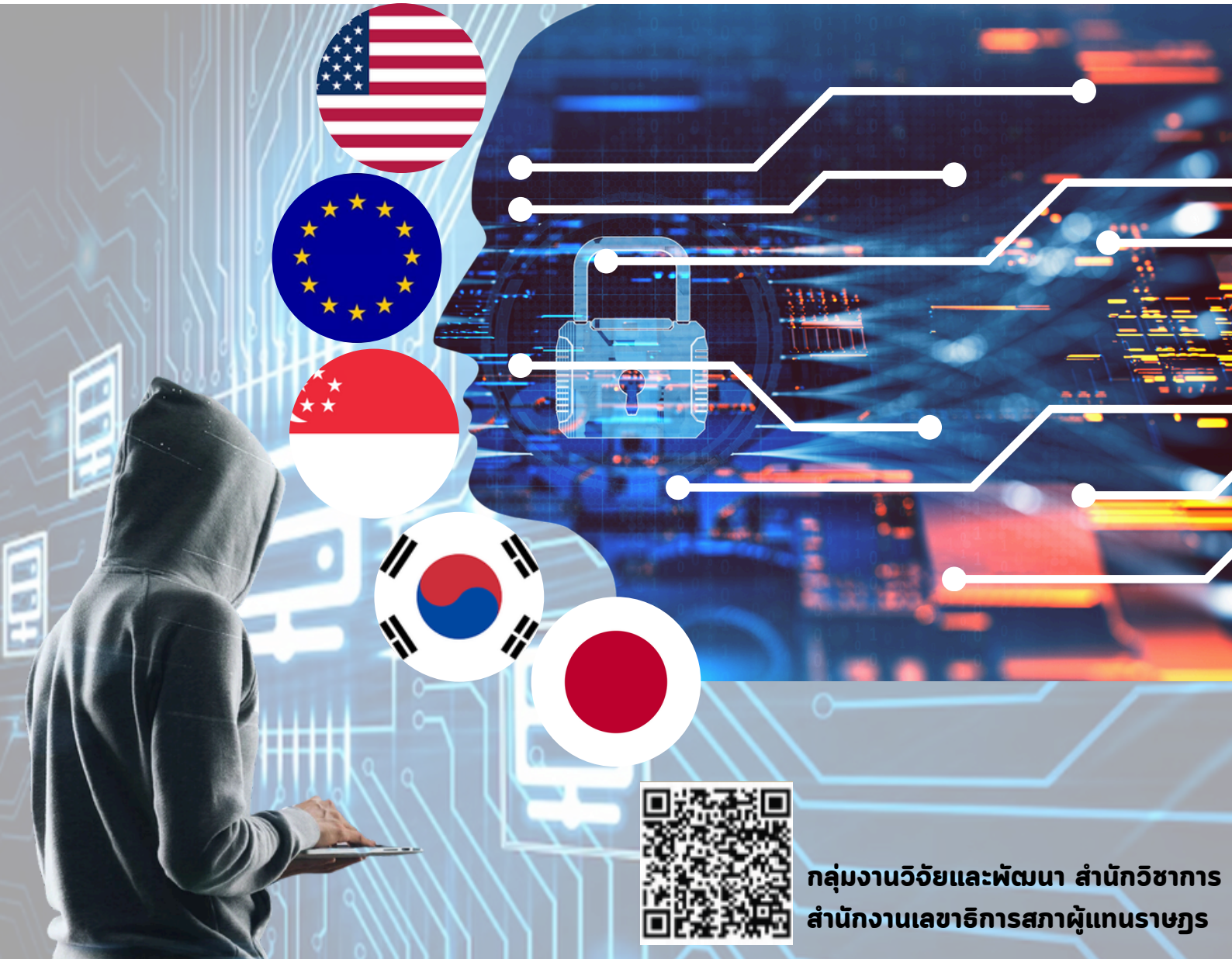
วิจัยปริทัศน์
(Research Review Article)
ฉบับที่ 60 เดือนกรกฎาคม 2568

นโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ



กลุ่มงานวิจัยและพัฒนา สำนักวิชาการ
สำนักงานเลขาธิการสภาผู้แทนราษฎร

นโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ

บูชิตา ไวทยานนท์*

บทคัดย่อ

ในยุคดิจิทัลที่เทคโนโลยีมีบทบาทสำคัญ อาชญากรรมทางเทคโนโลยี (Cybercrime) ได้กลายเป็นภัยคุกคามที่มีความรุนแรงและซับซ้อนมากขึ้น โดยมีรูปแบบต่าง ๆ เช่น การแฮ็กข้อมูล การโจมตีทางไซเบอร์ การขโมยข้อมูลส่วนบุคคล การฉ้อโกงออนไลน์ ซึ่งมีผลกระทบต่อบุคคล องค์กร และรัฐ การจัดการกับอาชญากรรมเหล่านี้จำเป็นต้องใช้มาตรการที่มีประสิทธิภาพจากทั้งภาครัฐและเอกชน ประเทศที่มีความก้าวหน้าในด้านการรับมือกับอาชญากรรมไซเบอร์ เช่น สหรัฐอเมริกา สหภาพยุโรป สิงคโปร์ เกาหลีใต้ และญี่ปุ่น ได้มีการพัฒนานโยบายที่ครอบคลุม โดยใช้กลไกทางกฎหมาย การบังคับใช้เทคโนโลยี และการสร้างการรับรู้แก่ประชาชน

ผลการศึกษาพบว่า ประเทศสหรัฐอเมริกามีแนวทางด้านความมั่นคงทางไซเบอร์ที่เป็นระบบ โดยกำหนดนโยบายระดับชาติและจัดตั้งหน่วยงานเฉพาะเพื่อป้องกันและสืบสวนอาชญากรรมทางเทคโนโลยี รวมถึงส่งเสริมความร่วมมือกับภาคเอกชนและสนับสนุนการพัฒนาเทคโนโลยีเพื่อรับมือกับภัยคุกคามอย่างมีประสิทธิภาพ ขณะที่สหภาพยุโรปให้ความสำคัญกับการรักษาสมดุลระหว่างความปลอดภัยของระบบสารสนเทศและการคุ้มครองสิทธิส่วนบุคคล โดยออกร่างกฎหมายระดับภูมิภาคและจัดตั้งกลไกสนับสนุนการพัฒนามาตรฐานและแนวปฏิบัติร่วมระหว่างประเทศสมาชิก ประเทศสิงคโปร์มีแผนแม่บทด้านความมั่นคงไซเบอร์ที่ชัดเจน โดยมุ่งเน้นการพัฒนาโครงสร้างพื้นฐาน การเสริมสร้างทักษะบุคลากร และการสร้างความร่วมมือกับนานาประเทศเพื่อเพิ่มขีดความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิผล ประเทศเกาหลีใต้ให้ความสำคัญกับการรับมือภัยคุกคามจากภายนอก โดยจัดตั้งหน่วยงานเฉพาะเพื่อดูแลความมั่นคงทางอินเทอร์เน็ต ทั้งด้านการวิเคราะห์ การเตรียมความพร้อม และการฝึกซ้อมสถานการณ์อย่างสม่ำเสมอ และประเทศญี่ปุ่นดำเนินนโยบายแบบองค์รวม โดยเน้นการประสานงานระดับชาติ การส่งเสริมวัฒนธรรมความปลอดภัยในสังคม และความร่วมมือระหว่างประเทศ เพื่อสร้างความมั่นคงทางไซเบอร์อย่างยั่งยืนและทันต่อการเปลี่ยนแปลงของภัยคุกคามในอนาคต

ทั้งนี้ การพัฒนานโยบายการป้องกันและปราบปรามอาชญากรรมไซเบอร์จำเป็นต้องมีการบูรณาการความร่วมมือระหว่างประเทศ เนื่องจากภัยคุกคามทางไซเบอร์มักเกิดขึ้นข้ามพรมแดน การศึกษานโยบายจากต่างประเทศและเปรียบเทียบประสิทธิภาพในการจัดการช่วยให้สามารถเสนอนโยบายที่เหมาะสมสำหรับประเทศไทย เช่น การปรับปรุงกฎหมายให้ทันสมัย การตั้งหน่วยงานกลางที่ดูแลด้านความมั่นคงไซเบอร์ การพัฒนาทรัพยากรมนุษย์ด้านเทคโนโลยี และการส่งเสริมการศึกษาความปลอดภัยไซเบอร์ให้กับประชาชน การศึกษาและนำแนวทางดังกล่าวมาปรับใช้จะช่วยเสริมสร้างความมั่นคงทางไซเบอร์และลดผลกระทบจากอาชญากรรมทางเทคโนโลยีในประเทศไทยได้อย่างมีประสิทธิภาพ

---

*วิทยากรชำนาญการพิเศษ กลุ่มงานวิจัยและพัฒนา สำนักวิชาการ

บทนำ

ในยุคปัจจุบัน พบว่าเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทอย่างมากต่อวิถีชีวิตของมนุษย์ในทุกมิติ ตั้งแต่ระดับบุคคลไปจนถึงระดับองค์กรและระดับชาติ การเชื่อมโยงข้อมูลผ่านระบบดิจิทัล การทำธุรกรรมทางอิเล็กทรอนิกส์ การบริหารจัดการภาครัฐแบบอิเล็กทรอนิกส์ (E-Government) ตลอดจนการเกิดขึ้นของเศรษฐกิจดิจิทัล (Digital Economy) ได้สะท้อนให้เห็นถึงความสำคัญของเทคโนโลยีที่แทรกซึมเข้าสู่โครงสร้างพื้นฐานของสังคมอย่างหลีกเลี่ยงไม่ได้ ในขณะเดียวกัน การแพร่หลายของเทคโนโลยีก็ได้ก่อให้เกิดรูปแบบใหม่ของภัยคุกคาม โดยเฉพาะในรูปของอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ (Cybercrime) ซึ่งมีลักษณะเฉพาะที่แตกต่างจากอาชญากรรมทั่วไปอย่างมีนัยสำคัญ ทั้งในด้านวิธีการ ความเร็วในการก่อเหตุ ขอบเขตผลกระทบ ตลอดจนความยากลำบากในการติดตามและบังคับใช้กฎหมาย (นวลน้อย ตรีรัตน์, 2567) องค์การตำรวจสากล (Interpol) ได้ให้คำนิยามอาชญากรรมไซเบอร์ว่าเป็นอาชญากรรมที่กระทำผ่านเครือข่ายคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต โดยมีจุดประสงค์เพื่อเจาะระบบ ขโมยข้อมูล สร้างความเสียหาย หรือแสวงหาผลประโยชน์ในทางที่ผิด ความซับซ้อนของอาชญากรรมไซเบอร์นั้นอยู่ที่การข้ามพรมแดนโดยไม่ต้องเดินทางจริง การใช้เทคนิคซ่อนร่องรอย การประยุกต์ใช้เทคโนโลยีขั้นสูง เช่น AI และ Deepfake ตลอดจนการรวมตัวกันของอาชญากรไซเบอร์ในลักษณะของเครือข่ายข้ามชาติ ทั้งหมดนี้ล้วนท้าทายต่อระบบกฎหมายและการบังคับใช้ในรูปแบบดั้งเดิม ปัจจุบันหลายประเทศทั่วโลกต่างเผชิญกับปัญหาอาชญากรรมทางเทคโนโลยีในระดับที่แตกต่างกันไป ทั้งนี้ขึ้นอยู่กับระดับการพัฒนาเทคโนโลยี โครงสร้างพื้นฐานด้านดิจิทัล ระบบการศึกษา และความเข้มแข็งของกลไกบังคับใช้กฎหมาย อย่างไรก็ตาม ประเทศที่สามารถรับมือกับภัยคุกคามนี้ได้อย่างมีประสิทธิภาพมักจะมีลักษณะร่วมกัน คือ การมีนโยบายที่ชัดเจน ระบบกฎหมายที่ทันสมัย กลไกการบูรณาการระหว่างภาคส่วนต่าง ๆ และการให้ความสำคัญกับการสร้างวัฒนธรรมความมั่นคงทางไซเบอร์ในหมู่ประชาชน

วิจัยปริทัศน์ฉบับนี้จึงขอนำเสนอเนื้อหาในหัวข้อเรื่อง **“นโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ”** ประกอบด้วย 1) ความหมายและประเภทของอาชญากรรมทางเทคโนโลยี 2) แนวโน้มของอาชญากรรมทางเทคโนโลยีในระดับโลก 3) ปัจจัยที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยี 4) ผลกระทบของอาชญากรรมทางเทคโนโลยี 5) กรณีศึกษานโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ ได้แก่ สหรัฐอเมริกา สหภาพยุโรป สิงคโปร์ 6) แนวปฏิบัติที่ดีจากประเทศเกาหลีใต้และญี่ปุ่น 7) การวิเคราะห์เปรียบเทียบเชิงระบบเกี่ยวกับนโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี และ 8) ข้อเสนอแนะเชิงนโยบายสำหรับประเทศไทย

ความหมายและประเภทของอาชญากรรมทางเทคโนโลยี

อาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ หมายถึง การกระทำความผิดทางอาญาที่มีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการกระทำผิดหรือเป็นเป้าหมายของการกระทำความผิด ซึ่งครอบคลุมถึงการเจาะระบบเครือข่าย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การแพร่กระจายไวรัสคอมพิวเตอร์ การหลอกลวงผ่านระบบออนไลน์ ตลอดจนการเผยแพร่ข้อมูลอันเป็นเท็จผ่านโซเชียลมีเดีย (รณกร วาพันสุ และจิรวุฒิ ลิปิพันธ์, 2566) ลักษณะเด่นของอาชญากรรมประเภทนี้ คือ ความไร้พรมแดนการกระทำสามารถเกิดขึ้นได้โดยไม่ต้องอยู่สถานที่เดียวกันกับผู้เสียหาย และสามารถสร้างความเสียหายได้ในวงกว้างภายในระยะเวลาอันสั้น

อาชญากรรมทางเทคโนโลยีสามารถแบ่งออกได้หลากหลายตามลักษณะของการกระทำความผิด เช่น 1) การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การแฮกระบบ การดักข้อมูลจากการสื่อสารออนไลน์ 2) การปลอมแปลงหรือดัดแปลงข้อมูล เช่น การเปลี่ยนแปลงเนื้อหาข้อมูลในระบบฐานข้อมูลขององค์กรรัฐหรือเอกชน 3) การฉ้อโกงผ่านระบบเทคโนโลยี เช่น การหลอกโอนเงินผ่านแอปพลิเคชัน หรือเว็บไซต์ปลอม (Phishing) 4) อาชญากรรมเกี่ยวกับเนื้อหาหรือข้อมูล เช่น การเผยแพร่ภาพลามกอนาจารเด็ก การข่มขู่ผ่านสื่อออนไลน์ และ 5) การใช้เทคโนโลยีเพื่อจารกรรมข้อมูล เช่น การฝังมัลแวร์เพื่อขโมยข้อมูลสำคัญ (ศ.ชัชนันท์ ลีระเติมพงษ์, 2564) ด้วยความซับซ้อนและลักษณะเฉพาะของอาชญากรรมทางเทคโนโลยี หน่วยงานรัฐจึงจำเป็นต้องปรับปรุงกฎหมายและแนวนโยบายในการป้องกันและปราบปรามให้สอดคล้องกับสถานการณ์ โดยเฉพาะอย่างยิ่งการประสานงานระหว่างประเทศ การพัฒนาบุคลากรเฉพาะทาง และการส่งเสริมความตระหนักรู้ของประชาชนเกี่ยวกับภัยไซเบอร์ ถือเป็นปัจจัยสำคัญที่จะช่วยลดปัญหาในระยะยาว (สัจจะ โชคบุญส่งสวัสดิ์, 2566) ทั้งนี้ การยกระดับการบังคับใช้กฎหมายควรอยู่ภายใต้หลักสิทธิมนุษยชนและการคุ้มครองข้อมูลส่วนบุคคล เพื่อไม่ให้เกิดการละเมิดสิทธิของประชาชนโดยไม่ชอบด้วยกฎหมาย

แนวโน้มของอาชญากรรมทางเทคโนโลยีในระดับโลก

แนวโน้มของอาชญากรรมทางเทคโนโลยีในระดับโลกมีการเปลี่ยนแปลงอย่างรวดเร็วและซับซ้อนมากขึ้น โดยเฉพาะในยุคที่เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เข้ามามีบทบาทสำคัญในชีวิตประจำวันของคนทั่วโลก การแพร่ระบาดของโรคโควิด-19 ได้เร่งให้เกิดการเปลี่ยนแปลงทางดิจิทัลอย่างรวดเร็ว ซึ่งส่งผลให้การใช้อินเทอร์เน็ตและเทคโนโลยีดิจิทัลเพิ่มขึ้นอย่างมาก ในขณะเดียวกัน อาชญากรไซเบอร์ได้ปรับตัวและพัฒนาวิธีการโจมตีที่ซับซ้อนมากขึ้น เพื่อแสวงหาผลประโยชน์จากช่องโหว่ที่เกิดขึ้นในระบบดิจิทัล จากการศึกษาของนวลน้อย ตรีรัตน์ (2567) พบว่าภัยคุกคามทางไซเบอร์ได้กลายเป็นหนึ่งในความเสี่ยงระดับโลกที่สำคัญ โดยเฉพาะในด้านเศรษฐกิจและความมั่นคง รายงานของ World Economic Forum (WEF) ใน ค.ศ. 2023 และ 2024 ได้จัดอันดับอาชญากรรมทางเทคโนโลยีให้อยู่ 1 ใน 10 ขอความเสี่ยงระดับโลกทั้งในระยะสั้นและระยะยาว เนื่องจากการพัฒนาและการใช้งานเทคโนโลยีใหม่ ๆ มักจะมาพร้อมกับการควบคุมดูแลที่ยังไม่เพียงพอ ทำให้อาชญากรสามารถใช้ประโยชน์ได้ นอกจากนี้ การศึกษาของอรรคภพ รอดจินดา (2566) ชี้ให้เห็นว่า การพัฒนาด้านเทคโนโลยีดิจิทัลที่ก้าวกระโดดส่งผลให้เกิดการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ที่มีรูปแบบการกระทำผิดที่หลากหลาย ทั้งการเจาะระบบเพื่อทดสอบความสามารถของตนเอง การเจาะระบบเพื่อประโยชน์ในทางการเมือง หรือการทำลายระบบสาธารณูปโภคที่สำคัญ การกระทำเหล่านี้ถือเป็นภัยคุกคามที่ไร้พรมแดน และมีผลกระทบในทุกมิติไม่ว่าจะเป็นเศรษฐกิจ สังคม และความมั่นคงของประเทศ สำหรับประเทศไทยอาชญากรรมทางเทคโนโลยีได้กลายเป็นปัญหาระดับชาติที่ต้องการการแก้ไขจากทุกภาคส่วน โดยเฉพาะอย่างยิ่งในยุค New Normal ที่การใช้งานเทคโนโลยีเพิ่มขึ้นอย่างมาก ส่งผลให้เกิดอาชญากรรมไซเบอร์ในรูปแบบต่าง ๆ เช่น การสร้างเว็บไซต์ปลอมเพื่อหลอกเอาข้อมูลส่วนบุคคล การแฮกข้อมูล และการหลอกเอาทรัพย์สิน เป็นต้น

ปัจจัยที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยี

อาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์ เป็นปรากฏการณ์ที่เพิ่มขึ้นอย่างต่อเนื่องในประเทศไทย สาเหตุหลักมาจากการเปลี่ยนแปลงของสังคมสู่ยุคดิจิทัล ซึ่งส่งผลให้เกิดช่องว่างและโอกาสในการกระทำผิดผ่านระบบเทคโนโลยีสารสนเทศ การวิเคราะห์ปัจจัยที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรม

ทางเทคโนโลยีในประเทศไทยสามารถแบ่งออกเป็นหลายด้าน ได้แก่ ปัจจัยทางเทคโนโลยี ปัจจัยทางสังคมและพฤติกรรมผู้ใช้งานคอมพิวเตอร์ ปัจจัยทางกฎหมาย และปัจจัยด้านการบังคับใช้กฎหมาย ดังนี้

1. ปัจจัยทางเทคโนโลยี การแพร่หลายของเทคโนโลยีสารสนเทศและการเชื่อมโยงของเครือข่ายอินเทอร์เน็ตทั่วโลก ทำให้เกิดโอกาสในการกระทำผิดที่ง่ายและรวดเร็วขึ้น การกระจายตัวของระบบอินเทอร์เน็ต และความสามารถในการติดตามสอดส่องบุคคลทั้งแบบคนจำนวนน้อยสอดส่องคนจำนวนมาก (Panopticism) และแบบคนจำนวนมากสอดส่องคนจำนวนน้อย (Synopticism) รวมถึงการทิ้งร่องรอยทางข้อมูล (Digital footprint) ของผู้ใช้งานอินเทอร์เน็ต ทำให้ผู้กระทำผิดสามารถใช้ข้อมูลเหล่านี้ในการก่ออาชญากรรมได้ง่ายขึ้น

2. ปัจจัยทางสังคมและพฤติกรรมผู้ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตมีบทบาทสำคัญในการเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยี การขาดความรู้ด้านความปลอดภัยไซเบอร์ การไม่ตระหนักถึงภัยคุกคาม และการมีบุคลิกภาพที่ขาดจิตสำนึกในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เป็นปัจจัยที่ทำให้ผู้ใช้งานตกเป็นเหยื่ออาชญากรรมไซเบอร์ได้ง่าย

3. ปัจจัยทางกฎหมาย เนื่องจากกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในประเทศไทยยังไม่ทันสมัยและไม่สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ขาดการบูรณาการระหว่างหน่วยงานที่เกี่ยวข้อง และการขาดความรู้ ความเข้าใจ รวมถึงทัศนคติในด้านลบของเจ้าหน้าที่ที่เกี่ยวข้อง เป็นอุปสรรคต่อการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ

4. ปัจจัยด้านการบังคับใช้กฎหมายที่ไม่เข้มงวดและขาดประสิทธิภาพ เป็นอีกปัจจัยหนึ่งที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยี การขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง และการขาดทรัพยากรในการตรวจสอบและติดตามผู้กระทำผิด ทำให้การป้องกันและปราบปรามอาชญากรรมไซเบอร์เป็นไปอย่างล่าช้าและไม่ทันต่อเหตุการณ์

การเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยีในประเทศไทยเป็นผลมาจากปัจจัยหลายด้านที่เกี่ยวข้องกัน การแก้ไขปัญหานี้จำเป็นต้องมีการบูรณาการระหว่างภาครัฐ ภาคเอกชน และประชาชนในการพัฒนาความรู้ด้านความปลอดภัยไซเบอร์ การปรับปรุงกฎหมายให้ทันสมัย และการเสริมสร้างศักยภาพของหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ

ผลกระทบของอาชญากรรมทางเทคโนโลยี

ในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญในชีวิตประจำวันของประชาชน อาชญากรรมทางเทคโนโลยี (Cybercrime) ได้กลายเป็นภัยคุกคามที่ส่งผลกระทบอย่างรุนแรงและหลากหลายมิติ ทั้งในระดับบุคคล องค์กร และสังคมโดยรวม การกระทำผิดในลักษณะนี้มีความซับซ้อนและยากต่อการตรวจสอบ เนื่องจากสามารถกระทำได้โดยไม่จำกัดสถานที่และเวลา รวมถึงมีการแพร่ขยายผลกระทบได้อย่างรวดเร็วผ่านเครือข่ายอินเทอร์เน็ต

1. ผลกระทบต่อบุคคล บุคคลทั่วไปมักตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ เช่น การหลอกลวงทางออนไลน์ การขโมยข้อมูลส่วนบุคคล และการโจมตีระบบคอมพิวเตอร์ ผลกระทบที่เกิดขึ้นไม่เพียงแต่ทำให้สูญเสียทรัพย์สิน แต่ยังส่งผลต่อสุขภาพจิตและความเชื่อมั่นในการใช้เทคโนโลยี โดยเฉพาะกลุ่มวัยทำงานที่มีอายุระหว่าง 30-44 ปี ซึ่งเป็นกลุ่มที่มีแนวโน้มตกเป็นเหยื่อมากที่สุด

2. ผลกระทบต่อองค์กรและภาคธุรกิจ องค์กรและภาคธุรกิจต้องเผชิญกับความเสี่ยงจากอาชญากรรมทางเทคโนโลยีที่อาจส่งผลต่อความมั่นคงของระบบข้อมูลและความเชื่อมั่นของลูกค้า การโจมตีในรูปแบบต่าง ๆ เช่น การโจมตีด้วยมัลแวร์ การแฮกระบบ หรือการเรียกค่าไถ่ข้อมูล สามารถทำให้ระบบการดำเนินงานหยุดชะงัก และก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างมหาศาล รวมถึงการละเมิดข้อมูลส่วนบุคคลยังอาจทำให้องค์กรต้องเผชิญกับการฟ้องร้องและการเสียชื่อเสียง

3. ผลกระทบต่อภาครัฐและความมั่นคงของประเทศ อาชญากรรมทางเทคโนโลยีมีผลกระทบต่อความมั่นคงของประเทศในหลายด้าน การโจมตีระบบของหน่วยงานรัฐ เช่น การแฮกข้อมูลของหน่วยงานราชการ หรือการโจมตีโครงสร้างพื้นฐานที่สำคัญ อาจส่งผลต่อความเชื่อมั่นของประชาชนและความมั่นคงของประเทศ โดยการแพร่กระจายข้อมูลเท็จหรือข่าวปลอมผ่านสื่อออนไลน์ยังสามารถกระตุ้นความไม่สงบในสังคมและบ่อนทำลายความเชื่อมั่นในรัฐบาล

4. ผลกระทบต่อโครงสร้างสังคมและวัฒนธรรม การแพร่กระจายของอาชญากรรมทางเทคโนโลยีส่งผลต่อพฤติกรรมและค่านิยมของสังคม ผู้คนเริ่มมีความระแวงและไม่ไว้วางใจในการใช้เทคโนโลยีและสื่อออนไลน์ นอกจากนี้ การกลั่นแกล้งทางไซเบอร์ (Cyberbullying) และการเข้าถึงเนื้อหาที่ไม่เหมาะสมยังส่งผลต่อพัฒนาการและสุขภาพจิตของเด็กและเยาวชน การเปลี่ยนแปลงพฤติกรรมดังกล่าวอาจนำไปสู่การลดลงของความสัมพันธ์ทางสังคมและการเสื่อมถอยของวัฒนธรรมที่เคยมีอยู่

5. ผลกระทบต่อระบบกฎหมายและการบังคับใช้กฎหมาย อาชญากรรมทางเทคโนโลยีมีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ทำให้ระบบกฎหมายและการบังคับใช้กฎหมายต้องเผชิญกับความท้าทายในการปรับตัว การขาดความรู้และความเข้าใจในเทคโนโลยีของเจ้าหน้าที่ที่เกี่ยวข้อง รวมถึงการขาดเครื่องมือและทรัพยากรที่เพียงพอ ทำให้การดำเนินคดีและการบังคับใช้กฎหมายอาจไม่สามารถตอบสนองต่อสถานการณ์ได้อย่างมีประสิทธิภาพ

กรณีศึกษานโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ

สหรัฐอเมริกา

สหรัฐอเมริกานับเป็นประเทศต้นแบบในด้านการพัฒนาและปรับปรุงนโยบายเพื่อรับมือกับอาชญากรรมทางเทคโนโลยีอย่างเป็นระบบ โดยมีพัฒนาการของกฎหมาย ความร่วมมือระหว่างหน่วยงานและกลยุทธ์ระดับชาติที่สามารถปรับตัวตามลักษณะของอาชญากรรมทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

1. กฎหมายสำคัญด้านอาชญากรรมทางเทคโนโลยี

1.1 The Computer Fraud and Abuse Act (CFAA) พระราชบัญญัติฉบับนี้มีผลบังคับใช้ตั้งแต่ ค.ศ. 1986 เพื่อรับมือกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ถูกแก้ไขหลายครั้งเพื่อให้ทันสมัยตามพฤติกรรมอาชญากรรมที่เปลี่ยนไป โดยเฉพาะประเด็นเกี่ยวกับ hacking, phishing และการทำลายระบบข้อมูล (สุชาดา วิไลรัตน์, 2564) จุดเด่นของ CFAA คือ การครอบคลุมทั้งการกระทำที่ตั้งใจและไม่ได้ตั้งใจ ซึ่งช่วยให้หน่วยงานสามารถดำเนินคดีได้อย่างยืดหยุ่น

1.2 USA PATRIOT Act หลังเหตุการณ์การโจมตีที่ก่อให้เกิดการสูญเสียชีวิตและความเสียหายมากที่สุดในประวัติศาสตร์ของสหรัฐอเมริกา (September 11 Attacks) รัฐบาลสหรัฐอเมริกาได้ตรากฎหมายฉบับนี้ซึ่งมีผลกระทบโดยตรงต่ออาชญากรรมไซเบอร์ กำหนดให้อำนาจหน่วยงานด้านความมั่นคงสามารถ

ตรวจสอบข้อมูลดิจิทัลเพื่อวัตถุประสงค์ด้านความมั่นคง และกำหนดบทลงโทษใหม่ต่อการใช้เทคโนโลยีเพื่อสนับสนุนการก่อการร้าย (ณรงค์ กุลนิเทศ, สมศักดิ์ หน่องพงษ์, วรธัช วิชชุวาณิชย์, และ ณิช วงศ์ส่องจ้า, 2556)

1.3 Cybersecurity Information Sharing Act (CISA Act) เป็นกฎหมายที่ส่งเสริมให้หน่วยงานภาครัฐและเอกชนแบ่งปันข้อมูลอาชญากรรมทางเทคโนโลยีระหว่างกัน โดยไม่ต้องกังวลเรื่องความรับผิดทางกฎหมาย ซึ่งเป็นกลไกที่สำคัญในการสร้างระบบเตือนภัยล่วงหน้าและเพิ่มความต้านทานทางไซเบอร์ในระดับชาติ

2. หน่วยงานหลักด้านความมั่นคงไซเบอร์

2.1 Federal Bureau of Investigation (FBI) Cyber Division หน่วยงานหลักด้านการบังคับใช้กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ มีอำนาจสืบสวนสอบสวนการโจมตีระบบคอมพิวเตอร์ทั้งในระดับประเทศและข้ามชาติ (Federal Bureau of Investigation, n.d.) มีความร่วมมือกับองค์กรระดับนานาชาติ เช่น Interpol และ Europol

2.2 Cybersecurity and Infrastructure Security Agency (CISA) หน่วยงานอิสระภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ (U.S. Department of Homeland Security: DHS) มีภารกิจหลักในการวิเคราะห์ภัยคุกคาม สนับสนุนภาครัฐและเอกชนในการป้องกันระบบโครงสร้างพื้นฐานสำคัญของประเทศจากการโจมตีไซเบอร์ (Cybersecurity and Infrastructure Security Agency, n.d.)

2.3 National Security Agency (NSA) ทำหน้าที่ในด้านข่าวกรองและการปฏิบัติการทางไซเบอร์ โดยมีขีดความสามารถในการติดตามภัยคุกคามในระดับสูง รวมถึงการวางกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

3. ยุทธศาสตร์ระดับชาติและกลไกการบูรณาการ

3.1 National Cyber Strategy เอกสารยุทธศาสตร์ของทำเนียบขาวมีเป้าหมายในการกระจายความรับผิดชอบให้แก่ภาคเอกชน ส่งเสริมให้มีการออกแบบระบบเทคโนโลยีที่ปลอดภัยโดยหลักการตั้งต้น (Secure by Design) พร้อมกับการส่งเสริมความยืดหยุ่นของระบบโครงสร้างพื้นฐานที่สำคัญทั่วประเทศ (National Cyber Strategy, 2023)

3.2 Multi-Stakeholder Model สหรัฐอเมริกาดำเนินกลยุทธ์ที่เน้นความร่วมมือแบบภาคีหลายฝ่าย (multi-stakeholder) โดยมีภาคธุรกิจ องค์กรไม่แสวงหากำไร และสถาบันการศึกษาเข้ามามีบทบาทในการกำหนดมาตรฐานความปลอดภัยและร่วมออกแบบนโยบาย

สหภาพยุโรป

สหภาพยุโรป (European Union: EU) เป็นภูมิภาคที่มีบทบาทสำคัญในการกำหนดมาตรฐานและกรอบนโยบายด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีแนวทางที่เน้นการคุ้มครองสิทธิของประชาชน ความโปร่งใส และความร่วมมือระหว่างประเทศสมาชิกในฐานะรัฐอธิปไตยที่ผสานนโยบายกลางเข้ากับกลไกในระดับชาติอย่างเป็นระบบ

1. กฎหมายสำคัญด้านอาชญากรรมทางเทคโนโลยี

1.1 General Data Protection Regulation (GDPR) เป็นกฎหมายที่มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม ค.ศ. 2018 มีจุดมุ่งหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรปและกำหนดมาตรฐานระดับสูงเกี่ยวกับการเก็บ การประมวลผล และการถ่ายโอนข้อมูลส่วนบุคคลทั้งภายในและภายนอกสหภาพยุโรป จุดเด่นของ GDPR คือ บทลงโทษสูงสุดถึง 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ทั่วโลกขององค์กร หากไม่ปฏิบัติตามข้อกำหนด

1.2 NIS Directive (Directive on Security of Network and Information Systems) กฎหมายนี้มีผลบังคับใช้ตั้งแต่ ค.ศ. 2016 เป็นกฎหมายฉบับแรกของสหภาพยุโรปที่ว่าด้วยมาตรฐานด้านความปลอดภัยทางไซเบอร์ โดยกำหนดให้ประเทศสมาชิกต้องมีหน่วยงานรับผิดชอบด้านความมั่นคงไซเบอร์ (National CSIRT) และผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญต้องรายงานเหตุการณ์ด้านความปลอดภัย (กระทรวงการต่างประเทศ, 2568)

2. หน่วยงานหลักด้านความมั่นคงไซเบอร์

2.1 European Union Agency for Cybersecurity (ENISA) ซึ่งมีภารกิจหลักในการให้คำปรึกษาทางวิชาการ สนับสนุนการกำหนดนโยบายความปลอดภัยทางไซเบอร์ และส่งเสริมการสร้างศักยภาพบุคลากรในประเทศสมาชิก ENISA ยังมีบทบาทในการจัดทำแนวทางปฏิบัติร่วมและการประเมินความเสี่ยงสำหรับระบบโครงสร้างพื้นฐานที่สำคัญในระดับภูมิภาค (European Union Agency for Cybersecurity, n.d.)

2.2 Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU) มีหน้าที่ตรวจสอบอาชญากรรมทางเทคโนโลยีที่อาจกระทบต่อหน่วยงานของสหภาพยุโรป โดยเฉพาะในสถาบันและองค์กรของสหภาพยุโรป เช่น European Parliament และEuropean Commission เป็นต้น (Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies, n.d.)

2.3 Data Protection Authorities (DPAs) ในแต่ละประเทศสมาชิกจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นหน่วยงานกำกับดูแลการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรปและให้คำปรึกษาด้านสิทธิส่วนบุคคล รวมถึงรับเรื่องร้องเรียนจากประชาชน (ณัฏฐวุฒิ แก้ววิเชียร, 2563)

3. ยุทธศาสตร์ระดับชาติและกลไกการบูรณาการ

3.1 Cybersecurity Strategy of the EU เอกสารยุทธศาสตร์ฉบับนี้เสนอแนวทางการสร้างภูมิคุ้มกันในโลกดิจิทัล (Digital Resilience) และอธิปไตยทางไซเบอร์ (Cybersecurity Sovereignty) โดยเน้นการปกป้องโครงสร้างพื้นฐานที่สำคัญ การยกระดับความสามารถของประเทศสมาชิก และการเป็นผู้นำด้านมาตรฐานไซเบอร์ระดับโลก (กระทรวงการต่างประเทศ, 2568)

3.2 ความร่วมมือระหว่างประเทศสมาชิกสหภาพยุโรป โดยส่งเสริมการแลกเปลี่ยนข้อมูลภัยคุกคามผ่านกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป (European Cybersecurity Competence Centre: ECCC) และการร่วมมือระหว่างหน่วยงานที่ดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์และยกระดับหน่วยบริการความมั่นคงปลอดภัยและการจัดการปัญหาด้านไซเบอร์ (CSIRTs Network) เพื่อให้การแจ้งเตือนภัยไซเบอร์มีความรวดเร็วและแม่นยำ

ตารางที่ 1 การเปรียบเทียบนโยบายไซเบอร์ของสหภาพยุโรปและสหรัฐอเมริกา

ประเด็นนโยบาย	สหภาพยุโรป (EU)	สหรัฐอเมริกา (USA)
กฎหมายหลัก	- GDPR (General Data Protection Regulation): กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวด - NIS Directive: กำกับดูแลความมั่นคงของระบบเครือข่ายและสารสนเทศ	- CFAA (Computer Fraud and Abuse Act): ป้องกันอาชญากรรมทางคอมพิวเตอร์ - PATRIOT Act: ให้อำนาจการเฝ้าระวังเพื่อความมั่นคง - CISA Act: ส่งเสริมการแบ่งปันข้อมูลภัยทางไซเบอร์
การคุ้มครองข้อมูล	- ให้ความสำคัญกับสิทธิของเจ้าของข้อมูล - ผู้ใช้มีสิทธิในการเข้าถึง แก้ไข และลบข้อมูลส่วนบุคคล - การใช้งานข้อมูลต้องโปร่งใสและมีความยินยอมอย่างชัดเจน	- มุ่งเน้นความมั่นคงของรัฐและการต่อต้านการก่อการร้าย - มีข้อยกเว้นให้หน่วยงานรัฐเข้าถึงข้อมูลเพื่อการสอบสวน
หน่วยงานหลัก	- ENISA (European Union Agency for Cybersecurity) - CERT-EU (Computer Emergency Response Team - EU) - Data Protection Authorities (DPAs)	- FBI (Federal Bureau of Investigation) - CISA (Cybersecurity and Infrastructure Security Agency) - NSA (National Security Agency)
ความร่วมมือระหว่างประเทศ	- มีการเชื่อมโยงภายในผ่าน CSIRTs Network และ EU Cybersecurity Act - ส่งเสริมความร่วมมือระดับข้ามพรมแดนในกลุ่มสมาชิก EU	- มีการร่วมมือทวิภาคีหรือผ่านพันธมิตรอย่าง NATO โดยเน้นอธิปไตยทางไซเบอร์ (Cyber Sovereignty) และความมั่นคงภายในประเทศ
การมีส่วนร่วมของพลเมือง	- ส่งเสริมสิทธิของประชาชนให้เข้าถึงร้องเรียน และควบคุมข้อมูลตนเอง - มีหน่วยงานรับเรื่องร้องเรียนอย่างเป็นระบบ	- เน้นให้ภาคเอกชนเป็นแกนนำ เช่น บริษัทที่ประกอบกิจการด้านเทคโนโลยีขนาดใหญ่ - บทบาทพลเมืองโดยตรงมีค่อนข้างจำกัด

จากการศึกษาพบว่า นโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของสหภาพยุโรปและสหรัฐอเมริกาแตกต่างกันในระดับแนวคิดและโครงสร้าง สหภาพยุโรปมีแนวโน้มปกป้องสิทธิด้วยกรอบกฎหมายที่เข้มงวดและกลไกการมีส่วนร่วมของประชาชนที่ชัดเจน ขณะที่สหรัฐอเมริกาเน้นความมั่นคงและความยืดหยุ่นในการบริหารจัดการภัยคุกคาม ผ่านหน่วยงานความมั่นคงและการร่วมมือกับภาคเอกชน แม้แนวทางทั้งสองจะมีข้อดีข้อด้อยต่างกัน แต่สิ่งสำคัญ คือ การสร้างสมดุลระหว่างเสรีภาพส่วนบุคคลและความมั่นคงของประเทศ ซึ่งเป็นโจทย์สำคัญที่ทุกประเทศต้องเผชิญในยุคดิจิทัล

สิงคโปร์

สิงคโปร์เป็นประเทศที่ได้รับการยอมรับว่าเป็นหนึ่งในผู้นำด้านนโยบายความมั่นคงทางเทคโนโลยีในภูมิภาคเอเชียตะวันออกเฉียงใต้ แม้จะเป็นประเทศขนาดเล็กที่มีทรัพยากรจำกัด แต่สิงคโปร์ได้ใช้จุดแข็งด้านการบริหารจัดการเชิงกลยุทธ์ การวางแผนเชิงนโยบายที่มุ่งเน้นผลสัมฤทธิ์ และการบูรณาการนโยบายดิจิทัลกับความมั่นคงของรัฐอย่างสอดคล้องกัน สามารถวิเคราะห์โครงสร้างนโยบาย กฎหมาย กลไกบริหาร และบทเรียนจากนโยบายของสิงคโปร์ที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (สภาองค์กรของผู้บริโภค, 2568; อมรรัตน์ อินนุมาตร, 2566; สราวุธ ปิติยาศักดิ์, และวราภรณ์ วนาพิทักษ์, 2564) ดังนี้

1. กฎหมายสำคัญด้านอาชญากรรมทางเทคโนโลยี

1.1 Cybersecurity Act 2018 กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ มีผลบังคับใช้เมื่อวันที่ 2 มีนาคม ค.ศ. 2018 เป็นกฎหมายหลักที่ควบคุมการปฏิบัติงานและความรับผิดชอบในการเสริมสร้างการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) รวมถึงการให้สิทธิแก่หน่วยงานรัฐในการเข้าตรวจสอบและสั่งการในกรณีที่มีเหตุการณ์คุกคามระบบคอมพิวเตอร์ของประเทศ โดยกฎหมายนี้ครอบคลุมทั้งภาครัฐและเอกชน และกำหนดโทษที่ชัดเจนหากมีการละเมิดมาตรฐานด้านไซเบอร์ (Cybersecurity Act 2018, 2022)

1.2 Personal Data Protection Act (PDPA) นอกจากกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) สิงคโปร์ยังมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งควบคุมการเก็บ ใช้ และเผยแพร่ข้อมูลส่วนบุคคล โดยเน้นความโปร่งใส ความยินยอม และสิทธิของเจ้าของข้อมูล

2. หน่วยงานหลักด้านความมั่นคงไซเบอร์

2.1 Cyber Security Agency of Singapore (CSA) หน่วยงานหลักด้านความมั่นคงไซเบอร์ของประเทศ ทำหน้าที่วางนโยบาย กำกับดูแลงานด้านความมั่นคงไซเบอร์โดยภาพรวม ตรวจสอบภัยคุกคามประสานงานกับภาคส่วนต่าง ๆ โดยขึ้นตรงต่อสำนักนายกรัฐมนตรี และเผยแพร่ความรู้เกี่ยวกับ Cyber Hygiene ในกลุ่มประชาชนทั่วไป

2.2 SingCERT ทีมตอบสนองเหตุการณ์ด้านไซเบอร์ของประเทศ มีหน้าที่รับแจ้งเหตุ วิเคราะห์ความเสี่ยง และออกคำแนะนำฉุกเฉินให้กับองค์กรและประชาชนทั่วไป

3. ยุทธศาสตร์ระดับชาติและกลไกการบูรณาการ

3.1 Singapore Cybersecurity Strategy 2021 ยุทธศาสตร์ของสิงคโปร์เป็นเครื่องมือสำคัญในการสำรวจการขยายขอบเขต การกำกับดูแลของรัฐ ภายใต้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดให้มี 4 เสาหลัก คือ 1) การเสริมสร้างระบบป้องกัน 2) การสร้างความเชื่อมั่นและวางระบบไว้ล่วงหน้า 3) การส่งเสริมเศรษฐกิจไซเบอร์ และ 4) การเป็นผู้นำด้านความร่วมมือระหว่างประเทศ โดยกำหนดเป้าหมายการเตรียมพร้อมตั้งแต่ภาคธุรกิจไปจนถึงภาคประชาชน

3.2 Smart Nation Initiative นโยบายรัฐบาลที่เน้นการบูรณาการเทคโนโลยีดิจิทัลในทุกมิติของการดำรงชีวิต เช่น E-payment, Digital Identity, Intelligent Transport System ฯลฯ โดยมีหน่วยงานด้านความมั่นคงไซเบอร์ (CSA) เป็นผู้ออกแบบระบบรักษาความปลอดภัยแบบเชิงรุก (Proactive Cybersecurity)

แนวปฏิบัติที่ดีจากประเทศเกาหลีใต้และญี่ปุ่น

ประเทศเกาหลีใต้และญี่ปุ่นเป็นสองประเทศในภูมิภาคเอเชียตะวันออกที่ได้รับการยอมรับว่ามีความก้าวหน้าด้านเทคโนโลยีและระบบการจัดการภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพสูง ทั้งสองประเทศประสบกับภัยคุกคามทางเทคโนโลยีจากภายในและภายนอกมาอย่างต่อเนื่อง จึงได้พัฒนานโยบาย กลไกการบริหารและกฎหมายที่ตอบสนองต่ออาชญากรรมทางเทคโนโลยีอย่างหลากหลาย จากการศึกษาพบแนวปฏิบัติที่ดีจากประเทศเกาหลีใต้และญี่ปุ่น โดยมุ่งวิเคราะห์โครงสร้างนโยบายและกลไกบูรณาการ ซึ่งอาจนำมาปรับใช้ในบริบทของประเทศไทยได้อย่างเหมาะสม

1. เกาหลีใต้ มีความก้าวหน้าทางดิจิทัลสูง แต่ขณะเดียวกันก็เป็นเป้าหมายสำคัญของภัยคุกคามทางไซเบอร์ โดยเฉพาะจากเกาหลีเหนือซึ่งอยู่ในสภาวะความตึงเครียดทางการเมืองกับเกาหลีใต้มาอย่างยาวนาน (สำนักข่าวอิศรา, 2567) รายงานประจำปีของศูนย์ความมั่นคงทางไซเบอร์แห่งชาติ (NCSC) เกาหลีใต้เปิดเผยว่า ใน ค.ศ. 2021 กลุ่มแฮกเกอร์ที่เกี่ยวข้องกับหน่วยข่าวกรองทหารของเกาหลีเหนือได้พยายามเจาะและขโมยข้อมูลจากหน่วยงานสำคัญของเกาหลีใต้ เช่น กระทรวงกลาโหม กรมการต่างประเทศ กระทรวงการรวมชาติ ฯลฯ การโจมตีเหล่านี้มุ่งข้อมูลด้านความมั่นคงและนโยบาย ซึ่งถือเป็นภัยคุกคามระดับชาติที่เกาหลีใต้ต้องให้ความสำคัญในการรับมืออย่างเร่งด่วน นอกจากภัยจากเกาหลีเหนือแล้ว เกาหลีใต้ยังเผชิญกับการโจมตีทางไซเบอร์โดยกลุ่มอาชญากรไซเบอร์ระหว่างประเทศ ไม่ว่าจะเป็นการเจาะระบบเพื่อขโมยทรัพย์สินดิจิทัล (เช่น การแฮ็กคริปโตเคอร์เรนซี) หรือการปล่อยมัลแวร์ทำลายข้อมูลโครงสร้างพื้นฐานสำคัญของเกาหลีใต้ เช่น ระบบธนาคาร พลังงาน และโทรคมนาคม ล้วนเคยถูกโจมตีมาแล้วทั้งสิ้น ศูนย์ความมั่นคงไซเบอร์ฯ เกาหลีใต้รายงานว่า จำนวนการโจมตีไซเบอร์ต่อองค์กรรัฐและเอกชนเพิ่มขึ้นร้อยละ 9 ในครึ่งแรกของ ค.ศ. 2021 (ฟีลิกซ์ คิม, 2565) รูปแบบการโจมตีมีความหลากหลาย ตั้งแต่การโจมตีเว็บไซต์ของหน่วยงานรัฐไปจนถึงการแพร่ไวรัสในเครือข่ายบริษัทเอกชน ความต่อเนื่องของภัยคุกคามดังกล่าวทำให้เกาหลีใต้ต้องพัฒนาระบบ เตือนภัยไซเบอร์ล่วงหน้า และเครือข่ายแบ่งปันข้อมูลภัยคุกคามที่ครอบคลุมทั่วทั้งภาครัฐและโครงสร้างพื้นฐานสำคัญ โดยเกาหลีใต้มีมาตรการในการรับมือภัยคุกคามไซเบอร์ ดังนี้

1.1 กรอบกฎหมายและนโยบายหลัก เกาหลีใต้มีพระราชบัญญัติที่เกี่ยวข้องกับความมั่นคงไซเบอร์หลายฉบับ โดยเฉพาะ “Act on Promotion of Information and Communications Network Utilization and Information Protection: Network Act” ซึ่งเป็นกฎหมายหลักที่ควบคุมความปลอดภัยแก่ผู้ให้บริการในช่องทางออนไลน์ รวมถึงผู้ค้าขายในระบบ E-Commerce ซึ่งให้ความเข้มงวดในเรื่องการเก็บการใช้ และการโอนย้ายข้อมูลส่วนบุคคลของผู้บริโภค รวมถึงกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความปลอดภัยสารสนเทศภาครัฐ (Personal Information Protection Act: PIPA) เพื่อให้ครอบคลุมภัยรูปแบบใหม่ เช่น อาชญากรรมบนเครือข่ายสังคมออนไลน์และการโจมตีโครงสร้างพื้นฐานดิจิทัล นอกจากนี้ รัฐบาลเกาหลีใต้ยังส่งเสริมมาตรฐานความปลอดภัยไซเบอร์ในภาคส่วนต่าง ๆ โดยล่าสุดได้ดำเนินโครงการรับรองความปลอดภัยระบบคลาวด์ (Cloud Security Certification) สำหรับบริการคลาวด์ที่หน่วยงานรัฐใช้งานทั้งหมด เพื่อยกระดับความมั่นคงของการประมวลผลข้อมูลภาครัฐบนคลาวด์ ส่วนภาคเอกชนนั้น กระทรวงวิทยาศาสตร์และ ICT ของเกาหลีใต้ได้ออกแนวทางให้บริษัทที่ดูแลข้อมูลประชาชนจำนวนมากต้องปฏิบัติตามมาตรการความปลอดภัยขั้นต่ำ เช่น การเข้ารหัสข้อมูลสำคัญ และ การสำรองระบบอย่างสม่ำเสมอ นอกจากนั้น เกาหลีใต้ยังเตรียมเปิดตัวระบบรับรองความปลอดภัยของอุปกรณ์ IoT เพื่อให้แน่ใจว่าอุปกรณ์ IoT และแอพพลิเคชันในมือถือที่เกี่ยวข้องมีความปลอดภัยตั้งแต่ขั้นตอนการพัฒนา

การกำหนดมาตรฐานและกรอบกฎหมายที่ทันสมัยเช่นนี้มีส่วนช่วยลดช่องโหว่และยกระดับภูมิคุ้มกันไซเบอร์โดยรวมของประเทศ (ศิริกัญญา ดุสิตนานนท์, 2565)

1.2 หน่วยงานหลักด้านความมั่นคงไซเบอร์ คือ (1) Korea Internet & Security Agency (KISA) เป็นหน่วยงานหลักที่รับผิดชอบด้านการพัฒนาและบริหารระบบความปลอดภัยทางอินเทอร์เน็ต รวมถึงการพัฒนาเทคโนโลยีด้านการเข้ารหัสและการตรวจสอบภัยคุกคาม (2) National Intelligence Service (NIS) เพื่อดูแลการป้องกันภัยไซเบอร์ในระดับโครงสร้างพื้นฐานชาติแบบเบ็ดเสร็จ ศูนย์นี้ทำหน้าที่เฝ้าระวังวิเคราะห์การโจมตี และประเมินมาตรการรักษาความปลอดภัยของหน่วยงานหลายร้อยแห่งทั่วประเทศ และ (3) Korea Cyber Command หน่วยงานด้านความมั่นคงไซเบอร์ของกระทรวงกลาโหม มีหน้าที่ป้องกันการโจมตีที่เกี่ยวข้องกับความมั่นคงแห่งชาติ

1.3 ยุทธศาสตร์เชิงรุกและนวัตกรรม เกาหลีใต้เน้นการใช้เทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ (AI) การวิเคราะห์ Big Data และ Blockchain ในการคาดการณ์และป้องกันภัยไซเบอร์ โดยมีการพัฒนาระบบเตือนภัยล่วงหน้า (Early Warning System) สำหรับโครงสร้างพื้นฐานด้านพลังงาน โทรคมนาคม และการเงิน

2. ญี่ปุ่น ต้องเผชิญภัยคุกคามไซเบอร์หลากหลายรูปแบบ โดยเฉพาะการโจมตีที่มาจากประเทศคู่แข่งและองค์กรอาชญากรรมไซเบอร์ข้ามชาติ รัฐบาลญี่ปุ่นได้ระบุในยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565–2567) ว่า จีน รัสเซีย และเกาหลีเหนือ เป็นแหล่งภัยคุกคามทางไซเบอร์หลักที่พุ่งเป้าโจมตีญี่ปุ่น (สำนักงานข่าวกรองแห่งชาติ, 2564) เช่น การจารกรรมข้อมูลความลับทางทหารและการทูต และการก่อกวนโครงสร้างพื้นฐานสำคัญ นอกจากนี้ ยังเกิดเหตุโจมตีทางไซเบอร์ต่อหน่วยงานและบริษัทของประเทศญี่ปุ่นอยู่เรื่อย ๆ เช่น การแฮกข้อมูลองค์การสำรวจอวกาศญี่ปุ่น (JAXA) ซึ่งทำให้ข้อมูลเทคโนโลยีด้านอวกาศรั่วไหลและตกอยู่ในความเสี่ยง (สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา, 2566) เหตุการณ์เหล่านี้ชี้ให้เห็นว่าญี่ปุ่นยังคงเป็นเป้าหมายของทั้งการโจมตีโดยรัฐ (เช่น หน่วยข่าวกรองเกาหลีเหนือ) และการโจมตีโดยอาชญากรไซเบอร์ที่มุ่งหวังผลประโยชน์ทางการเงิน เช่น การโจมตีด้วยมัลแวร์เรียกค่าไถ่ในภาคธุรกิจและโครงข่ายขนส่งสาธารณะ (ตรรกวิทย์ มิ่งขวัญ, 2568) ภัยคุกคามไซเบอร์ที่สำคัญอีกด้านหนึ่ง คือ การโจมตีโครงสร้างพื้นฐานสำคัญของญี่ปุ่น ไม่ว่าจะเป็นระบบไฟฟ้า การคมนาคมขนส่ง หรือบริการการเงินการธนาคาร เครือข่ายสาธารณูปโภคเหล่านี้ตกเป็นเป้าหมายของการโจมตีแบบ Distributed Denial-of-Service (DDoS) และมัลแวร์ที่มุ่งสร้างความเสียหายเป็นวงกว้าง โดยกรณีที่เกิดขึ้น ได้แก่ การโจมตีเว็บไซต์รัฐบาลญี่ปุ่นกว่า 20 แห่งโดยกลุ่มแฮกเกอร์ (Killnet) ที่ได้รับการสนับสนุนจากรัสเซีย (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์, 2565) รวมถึงการโจมตีระบบสารสนเทศของสายการบินเจแปนแอร์ไลน์ (JAL) ซึ่งส่งผลกระทบต่อการให้บริการด้านการบิน (ไซเบอร์ ดีเฟนส์, 2567) แม้บางเหตุการณ์จะไม่เปิดเผยผู้กระทำที่แน่ชัด แต่รัฐบาลญี่ปุ่นมองว่าภัยคุกคามเหล่านี้มีแนวโน้มเพิ่มขึ้นทั้งทางปริมาณและความซับซ้อน (สำนักงานข่าวกรองแห่งชาติ, 2564) จึงต้องจับตาและเตรียมมาตรการเชิงรุกเพื่อป้องกันล่วงหน้า โดยญี่ปุ่นมีมาตรการในการรับมือภัยคุกคามไซเบอร์ ดังนี้

2.1 กรอบกฎหมายหลัก ญี่ปุ่นออกกฎหมายและนโยบายใหม่ ๆ เพื่อรับมือภัยไซเบอร์ที่ทวีความรุนแรงขึ้นใน ค.ศ. 2014 ญี่ปุ่นได้ประกาศใช้พระราชบัญญัติพื้นฐานว่าด้วยความมั่นคงไซเบอร์ (Basic Cybersecurity Act) ซึ่งเป็นกรอบวางนโยบายการรักษาความปลอดภัยไซเบอร์ระดับชาติ และใน ค.ศ. 2025 คณะรัฐมนตรีญี่ปุ่นได้เห็นชอบร่างกฎหมายการป้องกันทางไซเบอร์เชิงรุก โดยอนุญาตให้หน่วยงานรัฐสามารถ

ดำเนินการเชิงรุกต่อเซิร์ฟเวอร์ของผู้โจมตีก่อนที่จะสร้างความเสียหายร้ายแรง กฎหมายใหม่นี้กำหนดให้ตำรวจและกองกำลังป้องกันตนเองสามารถเข้าถึงและยับยั้งเซิร์ฟเวอร์ต้นทางของการโจมตี ได้ภายใต้การอนุมัติของหน่วยงานอิสระที่จัดตั้งขึ้นมาเฉพาะ เพื่อสร้างสมดุลระหว่างความมั่นคงและสิทธิเสรีภาพ นอกจากนี้ ยังมีการจัดตั้งตำแหน่งเจ้าหน้าที่ไซเบอร์ประจำคณะรัฐมนตรี (Chief Cybersecurity Officer) เทียบเท่าปลัดกระทรวงเพื่อบูรณาการนโยบายไซเบอร์ของหน่วยงานต่าง ๆ ให้เป็นเอกภาพ (ตรรกวิทย์ มิ่งขวัญ, 2568) มาตรการทางกฎหมายและนโยบายเหล่านี้สะท้อนถึงความมุ่งมั่นของญี่ปุ่นในการปรับปรุงกรอบการรับมือภัยไซเบอร์ให้ทันต่อสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็ว

2.2 หน่วยงานหลักด้านความมั่นคงไซเบอร์ คือ (1) National Center of Incident Readiness and Strategy for Cybersecurity (NISC) เป็นหน่วยงานภายใต้สำนักนายกรัฐมนตรีของญี่ปุ่น มีบทบาทในการกำหนดนโยบายและยุทธศาสตร์ระดับชาติด้านความมั่นคงไซเบอร์ รวมถึงประสานงานกับหน่วยงานต่าง ๆ เพื่อเสริมสร้างความมั่นคงในโลกดิจิทัล (2) Cybersecurity Strategic Headquarters หน่วยงานนี้ตั้งอยู่ภายใต้สำนักนายกรัฐมนตรี มีหน้าที่กำหนดนโยบายระดับสูงและบูรณาการการดำเนินงานของหน่วยงานต่าง ๆ เพื่อเสริมสร้างความมั่นคงไซเบอร์ของประเทศ และ (3) Japan Computer Emergency Response Team (JPCERT/CC) เป็นทีมตอบสนองเหตุการณ์ฉุกเฉินด้านความมั่นคงไซเบอร์ของญี่ปุ่น ทำงานร่วมกับองค์กรระหว่างประเทศในการเฝ้าระวังและตอบสนองต่ออาชญากรรมทางเทคโนโลยี (National Center of Incident Readiness and Strategy for Cybersecurity, 2024)

2.3 แนวทางการส่งเสริมการมีส่วนร่วม ญี่ปุ่นเน้นการสร้างวัฒนธรรมความมั่นคงไซเบอร์โดยบูรณาการหลักสูตรความปลอดภัยไซเบอร์ในระดับการศึกษาขั้นพื้นฐานจนถึงมหาวิทยาลัย นอกจากนี้ยังมีเดือนแห่งการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Month) ซึ่งจัดกิจกรรมสร้างความรู้แก่ประชาชนในรูปแบบหลากหลาย

ตารางที่ 2 การเปรียบเทียบนโยบายไซเบอร์ของเกาหลีใต้และญี่ปุ่น

ประเด็นนโยบาย	เกาหลีใต้	ญี่ปุ่น
กฎหมายหลัก	- PIPA (Personal Information Protection Act) - Information and Network Act	- Basic Act on Cybersecurity - APPI (Act on the Protection of Personal Information)
หน่วยงานหลัก	- KISA (Korea Internet & Security Agency) - NIS (National Intelligence Service) - Cyber Command	- NISC (National center of Incident readiness and Strategy for Cybersecurity) - Strategic Headquarters for Cybersecurity - JPCERT (Japan Computer Emergency Response Team)

ประเด็นนโยบาย	เกาหลีใต้	ญี่ปุ่น
แนวทางเทคโนโลยี	- ใช้ AI, Blockchain, และ Big Data อย่างเข้มข้นในการป้องกันและตรวจจับอาชญากรรมทางเทคโนโลยี	- มุ่งเน้นการจัดการความเสี่ยงและการคุ้มครองข้อมูลเป็นหลัก
ความร่วมมือภาคเอกชน	- ระดับสูง โดยเฉพาะการแบ่งปันข้อมูล Treat Intelligence กับบริษัทเทคโนโลยี	- ระดับปานกลาง แต่มีการร่วมมือกันอย่างต่อเนื่อง โดยเฉพาะในบริษัทเทคโนโลยีขนาดใหญ่
การส่งเสริมประชาชน	- มีการฝึกอบรมเชิงลึกด้าน Cyber Hygiene และสร้างความไซเบอร์ในระดับบุคคล	- ผสมผสานความรู้ด้านไซเบอร์เข้าสู่ระบบการศึกษาเพื่อปลูกฝังระดับเยาวชน

จากการศึกษาพบว่า เกาหลีใต้และญี่ปุ่นแม้มีแนวทางที่แตกต่างกัน แต่มีลักษณะร่วมกัน คือ การบูรณาการภาครัฐ ภาคเอกชน และประชาชนเข้าด้วยกันในการสร้างความมั่นคงทางไซเบอร์ โดยการผสานแนวทางเทคโนโลยีของเกาหลีใต้และแนวคิดการสร้างวัฒนธรรมของญี่ปุ่นจะช่วยยกระดับศักยภาพด้านนโยบายไซเบอร์ของไทยให้ทันกับภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วและมีความซับซ้อนมากยิ่งขึ้น

การวิเคราะห์เปรียบเทียบเชิงระบบเกี่ยวกับนโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี

การดำเนินนโยบายในการรับมือกับอาชญากรรมทางเทคโนโลยีอย่างครอบคลุม การวิเคราะห์เชิงเปรียบเทียบเชิงระบบจึงมีความสำคัญอย่างยิ่งในการทำความเข้าใจโครงสร้าง กลไก และแนวทางปฏิบัติที่หลากหลายของประเทศต่าง ๆ ผู้เขียนขอนำเสนอสังเคราะห์ข้อมูลจากประเทศต้นแบบที่ได้ศึกษามาแล้ว ได้แก่ สหรัฐอเมริกา สหภาพยุโรป สิงคโปร์ เกาหลีใต้ และญี่ปุ่น โดยใช้กรอบวิเคราะห์ 5 ด้าน ได้แก่ 1) กฎหมายหลัก 2) โครงสร้างหน่วยงาน 3) การคุ้มครองสิทธิส่วนบุคคล 4) การมีส่วนร่วมของภาคส่วนต่าง ๆ และ 5) กลยุทธ์ในการรับมือภัยคุกคามใหม่

1. กฎหมายหลัก ประเทศส่วนใหญ่ต่างมีกฎหมายเฉพาะที่ควบคุมอาชญากรรมไซเบอร์ เช่น CFAA ในสหรัฐอเมริกา GDPR และ NIS Directive ในสหภาพยุโรป Cybersecurity Act ในสิงคโปร์ PIPA ในเกาหลีใต้ และ Basic Act on Cybersecurity ในญี่ปุ่น โดยกฎหมายเหล่านี้มักมีจุดร่วม คือ การกำหนดความผิด การบังคับให้รายงานเหตุการณ์ไซเบอร์ และการให้สิทธิแก่หน่วยงานในการดำเนินการในสถานการณ์ฉุกเฉิน อย่างไรก็ตาม สหภาพยุโรปให้ความสำคัญกับสิทธิส่วนบุคคลสูงที่สุด ขณะที่สหรัฐอเมริกามีแนวโน้มยืดหยุ่นเพื่อความมั่นคง

2. โครงสร้างหน่วยงานและกลไกการบริหารของประเทศที่ศึกษามีการจัดตั้งหน่วยงานกลางเพื่อบริหารนโยบายไซเบอร์ เช่น CISA ในสหรัฐอเมริกา ENISA ในสหภาพยุโรป CSA ในสิงคโปร์ KISA ในเกาหลีใต้ และ NISC ในญี่ปุ่น โดยประเทศที่มีโครงสร้างรวมศูนย์และให้อำนาจสูงต่อหน่วยงานกลาง เช่น สิงคโปร์และเกาหลีใต้ มักมีความคล่องตัวในการตอบสนองภัยคุกคาม ในขณะที่สหภาพยุโรปมีการกระจายอำนาจให้แก่ประเทศสมาชิก ส่งผลให้การดำเนินงานอาจมีความล่าช้าแต่ยึดหลักประชาธิปไตยมากกว่า

3. การคุ้มครองสิทธิส่วนบุคคล แนวทางของประเทศที่ศึกษาสะท้อนความแตกต่างของค่านิยมในแต่ละสังคมอย่างชัดเจน โดยสหภาพยุโรปให้ความสำคัญสูงสุดกับสิทธิส่วนบุคคลผ่าน GDPR ญี่ปุ่นและเกาหลีใต้เน้นความสมดุลระหว่างสิทธิส่วนบุคคลและความมั่นคง ในขณะที่สหรัฐอเมริกามักถูกวิจารณ์ว่าให้ความสำคัญกับการสอดส่องเพื่อความมั่นคงมากเกินไป และสิงคโปร์มีข้อยกเว้นจำนวนมากต่อการเข้าถึงข้อมูลโดยหน่วยงานของรัฐ

4. การมีส่วนร่วมของภาคส่วนต่าง ๆ สหรัฐอเมริกาและเกาหลีใต้มีการสนับสนุนภาคเอกชนให้เข้ามามีส่วนร่วมในระบบความมั่นคงทางไซเบอร์อย่างชัดเจน เช่น การแบ่งปัน Threat Intelligence และการฝึกซ้อมร่วม ญี่ปุ่นเน้นการบูรณาการกับระบบการศึกษา ส่วนสหภาพยุโรปเปิดช่องให้ภาคประชาสังคมเข้าร่วมกำหนดนโยบาย สิงคโปร์มีกลไก Public-Private Partnership ที่มีประสิทธิภาพมากและใช้แนวทาง One Government Approach ในการประสานงาน

5. กลยุทธ์ในการรับมือกับภัยคุกคาม สหรัฐอเมริกาและเกาหลีใต้เน้นการใช้ AI Big Data และเทคโนโลยีการวิเคราะห์เชิงลึกเพื่อป้องกันภัยคุกคามล่วงหน้า ญี่ปุ่นเน้นการเตรียมความพร้อมและการสร้างวัฒนธรรมไซเบอร์ สิงคโปร์ใช้แนวทาง Proactive Security ขณะที่สหภาพยุโรปมุ่งเน้นการจัดการความเสี่ยงและกำหนดมาตรฐานระดับสากล

ตารางที่ 3 การเปรียบเทียบนโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี 5 ประเทศ

ด้าน	สหรัฐอเมริกา	สหภาพยุโรป	สิงคโปร์	เกาหลีใต้	ญี่ปุ่น
กฎหมายหลัก	CFAA, CISA	GDPR, NIS	Cybersecurity Act, PDPA	PIPA, Network Act	Basic Act, APPI
หน่วยงานหลัก	CISA, FBI	ENISA, CERT-EU	CSA, SingCERT	KISA, NIS NISC, JPCERT	NISC, JPCERT
โครงสร้างบริหาร	รวมศูนย์	การจายอำนาจ	รวมศูนย์	รวมศูนย์	กึ่งรวมศูนย์
สิทธิส่วนบุคคล	ยืดหยุ่น	เข้มงวด	ปานกลาง	ปานกลาง	สมดุล
การมีส่วนร่วม	ภาคเอกชนเป็นแกนหลัก	ภาคประชาชนและ Non-governmental organization (NGO)	เอกชนและภาครัฐ	เอกชนและภาครัฐ	การศึกษาและภาครัฐ
กลยุทธ์ในการรับมือ	AI, เชิงรุก (Proactive)	การประเมินความเสี่ยง (Risk-Based)	เชิงรุก + PPP (Public-Private Partnership)	AI + ระบบอัตโนมัติ (Automation)	วัฒนธรรม + การจัดการความเสี่ยง

จากการศึกษาการเปรียบเทียบนโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของสหรัฐอเมริกา สหภาพยุโรป สิงคโปร์ เกาหลีใต้ และญี่ปุ่น แสดงให้เห็นถึงแนวทางการจัดการอาชญากรรมทางเทคโนโลยีที่แตกต่างกันตามบริบทของแต่ละประเทศ โดยสหรัฐอเมริกาเน้นด้านความมั่นคงของรัฐ มีโครงสร้างแบบรวมศูนย์ผ่านหน่วยงานสำคัญอย่าง CISA และ FBI มีกฎหมาย CFAA และ CISA เป็นเครื่องมือหลัก และให้ภาคเอกชนมีบทบาทสูงในเชิงกลยุทธ์ โดยเฉพาะการใช้ AI แบบเชิงรุก ขณะที่สหภาพยุโรปให้ความสำคัญกับสิทธิส่วนบุคคลอย่างสูงผ่านกฎหมาย GDPR และมีการกระจายอำนาจบริหาร โดยเปิดพื้นที่ให้ภาคประชาชนและ NGO เข้ามามีส่วนร่วม กลยุทธ์เน้นการประเมินความเสี่ยงและความโปร่งใส สิงคโปร์ใช้โครงสร้างรวมศูนย์คล้ายสหรัฐฯ แต่เน้นการประสานความร่วมมือระหว่างภาครัฐและเอกชน (PPP) อย่างเป็นระบบ เกาหลีใต้มุ่งเน้นเทคโนโลยีอัจฉริยะ เช่น AI และระบบอัตโนมัติ ภายใต้การบริหารแบบรวมศูนย์ โดยเน้นบทบาทร่วมของรัฐและเอกชนอย่างชัดเจน ขณะที่ญี่ปุ่นมีโครงสร้างกึ่งรวมศูนย์ โดยหน่วยงานหลักอย่าง NISC และ JPCERT ร่วมมือกับภาคการศึกษาในการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ถึงแม้แต่ละประเทศจะมีโครงสร้าง กฎหมาย และกลยุทธ์ที่แตกต่างกัน แต่ต่างมุ่งหวังเป้าหมายเดียวกันคือการเสริมสร้างระบบความมั่นคงไซเบอร์ที่ยั่งยืน สอดคล้องกับบริบทของประเทศตนเอง และสร้างสมดุลระหว่างความมั่นคงกับสิทธิของประชาชน

ข้อเสนอแนะเชิงนโยบายสำหรับประเทศไทย

จากการวิเคราะห์เชิงเปรียบเทียบแนวนโยบายของต่างประเทศในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า ประเทศไทยแม้จะมีการดำเนินงานที่ก้าวหน้าในบางด้าน แต่ยังขาดโครงสร้างเชิงนโยบายที่เป็นระบบ ครอบคลุม และมีประสิทธิภาพเพียงพอในการรับมือกับภัยคุกคามที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ดังนั้น ข้อเสนอเชิงนโยบายต่อไปนี้จึงมีวัตถุประสงค์เพื่อยกระดับขีดความสามารถของประเทศใน 5 มิติ ได้แก่ 1) การจัดตั้งโครงสร้างกลางที่มีประสิทธิภาพ 2) การปรับปรุงกฎหมายและกลไกทางกฎหมาย 3) การเสริมสร้างศักยภาพบุคลากรและวัฒนธรรมความมั่นคงไซเบอร์ 4) การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี และ 5) การส่งเสริมความร่วมมือในระดับภูมิภาคและนานาชาติ (สำนักงานพัฒนารัฐบาลดิจิทัล, 2567) ดังนี้

1. การจัดตั้งหน่วยงานกลางด้านความมั่นคงไซเบอร์ ประเทศไทยควรจัดตั้งหน่วยงานกลางที่มีอำนาจหน้าที่ชัดเจนคล้ายกับ CSA ของสิงคโปร์ หรือ NISC ของญี่ปุ่น โดยให้มีสถานะเป็นหน่วยงานอิสระภายใต้สำนักนายกรัฐมนตรี ทำหน้าที่วางแผนยุทธศาสตร์ กำกับ ดูแล และประสานความร่วมมือกับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน โดยควรมีกฎหมายรองรับที่ให้อำนาจในการตรวจสอบ ควบคุม และเข้าถึงข้อมูลที่จำเป็นในภาวะฉุกเฉิน

2. การปรับปรุงกฎหมายให้ทันสมัยและสอดคล้องกับสากล แม้ว่าปัจจุบันประเทศไทยจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว แต่ยังมีช่องว่างหลายประการ เช่น การกำหนดนิยามของอาชญากรรมทางเทคโนโลยี การแบ่งแยกระหว่างภัยคุกคามทั่วไปกับภัยต่อโครงสร้างพื้นฐานสำคัญ การขาดกลไกการรายงานเหตุการณ์ไซเบอร์ภาคบังคับ ฯลฯ ควรมีการตรากฎหมายเฉพาะ เช่น กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของไทย ที่มีทั้งมาตรการบังคับใช้และกลไกคุ้มครองสิทธิพลเมืองอย่างสมดุล

3. การเสริมสร้างศักยภาพบุคลากรและวัฒนธรรมไซเบอร์ ควรพัฒนาหลักสูตร Cybersecurity Studies ตั้งแต่ระดับมัธยมจนถึงระดับอุดมศึกษา ร่วมกับการจัดตั้งศูนย์ฝึกอบรมเชิงลึกระดับภูมิภาค (Cybersecurity Training Hub) รวมถึงการให้ทุนวิจัยแก่สถาบันการศึกษาที่เน้นการพัฒนาเทคโนโลยีป้องกันภัยคุกคาม เช่น ระบบที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ (Threat Intelligence Platform) หรือระบบจำลองกลยุทธ์ด้านไซเบอร์ (Cyber Range Simulator) ที่ใช้ฝึกซ้อมเชิงปฏิบัติการ

4. การยกระดับโครงสร้างพื้นฐานทางเทคโนโลยี รัฐบาลควรลงทุนในการจัดตั้งระบบเตือนภัยล่วงหน้า (Early Warning System) สำหรับอาชญากรรมทางเทคโนโลยีต่อโครงสร้างพื้นฐานสำคัญ เช่น ระบบพลังงาน การเงิน การสื่อสาร และสาธารณสุข โดยใช้เทคโนโลยี AI และ Big Data ร่วมกับการออกแบบระบบที่มีความปลอดภัยโดยหลักการตั้งต้น (Secure by Design) ตามแนวทางของสหรัฐอเมริกา

5. การส่งเสริมความร่วมมือระดับภูมิภาคและนานาชาติ ประเทศไทยควรขยายความร่วมมือกับองค์กรระดับภูมิภาค เช่น ASEAN-Japan Cybersecurity Centre และกับกลุ่มประเทศ CLMV (Cambodia, Laos, Myanmar and Vietnam) ผ่านการลงนามในบันทึกความเข้าใจ (MOU) การเข้าร่วมโครงการ CERT ระดับสากล เช่น FIRST, APCERT และการแลกเปลี่ยนบุคลากรกับประเทศที่มีความเชี่ยวชาญ เช่น สิงคโปร์ เกาหลีใต้ และญี่ปุ่น

อย่างไรก็ตาม นโยบายการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของประเทศไทยยังขาดลักษณะ Cyber Governance ที่ชัดเจน กล่าวคือ ยังไม่มีระบบการบริหารจัดการแบบองค์รวมที่เชื่อมโยงทุกภาคส่วนเข้าด้วยกัน ในขณะที่อาชญากรรมทางเทคโนโลยีกำลังพัฒนาในลักษณะเครือข่ายระหว่างประเทศและมีศักยภาพที่จะก่อให้เกิดวิกฤตระดับประเทศ การพัฒนาเพียงมาตรการป้องกันเฉพาะจุดหรือการตอบโต้เฉพาะกิจจึงไม่เพียงพอ ประเทศไทยจำเป็นต้องมีวิสัยทัศน์และยุทธศาสตร์ทางไซเบอร์ระยะยาวที่เน้นความยืดหยุ่น (Resilience) และความสามารถในการฟื้นตัว (Recovery) จากวิกฤต โดยเน้นการมีส่วนร่วมของพลเมือง การให้ความรู้แก่เยาวชน และการยกระดับภาคเอกชนให้มีบทบาทในฐานะพันธมิตรด้านความมั่นคงของประเทศ

บรรณานุกรม

ภาษาไทย

กระทรวงการต่างประเทศ. (2568). **สหภาพยุโรปผ่านข้อกฎหมายไซเบอร์ความปลอดภัยสำหรับผลิตภัณฑ์ดิจิทัลที่เชื่อมต่อกับอินเทอร์เน็ต**. สืบค้น 17 เมษายน 2568 จาก https://globthailand.com/austria-06022024/

กฤษฎา แสงเจริญทรัพย์. (2566). **ความเป็นไปได้และแนวทางการป้องกันอาชญากรรมโดยการใช้เทคโนโลยี: ศึกษากรณีการป้องกันการทุจริตคอร์รัปชั่นในประเทศไทย.** สืบค้น 14 เมษายน 2568 จาก https://so05.tci-thaijo.org/index.php/QLLJ/article/download/269008/181036/1073489

กิตติมา คงสำรวย, สราวุธ ปิตาศักดิ์, และวราภรณ์ วนาพิทักษ์. (2567). **หลักความยินยอมในกฎหมายคุ้มครองข้อมูลส่วนบุคคล: การศึกษาเปรียบเทียบกฎหมายของสหภาพยุโรป สาธารณรัฐเกาหลี และราชอาณาจักรไทย.** สืบค้น 25 เมษายน 2568 จากhttps://ojs.lib.buu.ac.th/index.php/law/article/view/10094/9141

ไซเบอร์ ดีเฟนส์. (2567). **ระบบของสายการบินเจแปนแอร์ไลน์ถูกโจมตีทางไซเบอร์ส่งผลกระทบต่อการปฏิบัติการบิน.** สืบค้น 25 เมษายน 2568 จาก https://cyberdefense.co.th/japan-airlines-system-hit-cyberattack/

ณรงค์ กุลนิเทศ, สมศักดิ์ หน่องพงษ์, วรธัช วิชชุวาณิชย์, และณิช วงศ์ส่องจ้า. (2556). **เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์.** มหาวิทยาลัยราชภัฏสวนสุนันทา.

ณัฏฐวุฒิ แก้ววิเชียร. (2563). การเสริมสร้างความร่วมมือด้านความมั่นคงไซเบอร์ระหว่างประเทศ: กรณีศึกษายุโรป. **วารสารรัฐศาสตร์และรัฐประศาสนศาสตร์ มหาวิทยาลัยเชียงใหม่**, 11(2), 67-82.

ตรรกวิทย์ มิ่งขวัญ. (2568). **รัฐบาลญี่ปุ่นจัดทำสรุปสาระสำคัญของร่างกฎหมายการใช้ระบบป้องกันทางไซเบอร์แบบเชิงรุก .** สืบค้น 25 เมษายน 2568 จาก https://web.parliament.go.th/view/16/รายละเอียดข่าว/การเมือง_ประมวลข่าวต่างประเทศ/5300/TH-TH

ทูตนิวเคลียร์เกาหลีใต้ จี้ไทยร่วมมือหยุดโครงการอาวุธ-ภัยคุกคามไซเบอร์เกาหลีเหนือ**.** (2567). **สำนักข่าวอิศรา.** สืบค้น 24 เมษายน 2568 จาก https://www.isranews.org/article/isranews-news/125587-isranews-UrgeNorthKorea.html

นวลน้อย ตรีรัตน์. (2567). **ภัยคุกคามทางออนไลน์: ปัญหาและความท้าทาย.** สืบค้น 15 เมษายน 2568 จาก https://www.econ.chula.ac.th/download/research/Nualnoi/01-นวลน้อย-บทสังเคราะห์ภัยออนไลน์.pdf

ปิยอร เปลี่ยนผดุง, กฤษฎา ใจแก้วทิ, ณัฐ สุขเวชวรกิจ, และ พรณัชชา ทับพันบุบผา. (2567). **กฎหมายและหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในการควบคุม ป้องกัน และปราบปรามอาชญากรรมทางการเงินออนไลน์ในประเทศไทย.** สืบค้น 14 เมษายน 2568 จาก https://www.econ.chula.ac.th/download/research/Nualnoi/03-ปิยอร-กฎหมายควบคุม%20ป้องกัน%20และปราบปรามอาชญากรรมออนไลน์-final.pdf

ฟีลิกซ์ คิม. (2565). **เกาหลีใต้ยกระดับการป้องกันทางไซเบอร์จากแฮกเกอร์ในเกาหลีเหนือและประเทศอื่น ๆ.** สืบค้น 14 เมษายน 2568 จาก https://ipdefenseforum.com/th/2022/01/เกาหลีใต้ยกระดับการป้อ/

รณกร วาพันสุ, และจิรวุฒิ ลิปิพันธ์. (2566). **อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีการฟิชชิ่งที่เกี่ยวข้องกับการฉ้อโกงประชาชน.** สืบค้น 14 เมษายน 2568 จาก https://grad.dpu.ac.th/upload/content/files/year12-2/12-8.pdf

ศ.ชัชนันท์ ลีระเติมพงษ์. (2564). **แผนปฏิบัติการป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี: จัดการศึกษาแบบใหม่ของตำรวจ ระยะ 5 ปี (พ.ศ. 2564-2568).** สืบค้น 14 เมษายน 2568 จาก https://sscthailand.org/assets/mobileapp/stdjob/1407.pdf

ศิริกัญญา ดุสิตนานนท์. (2565). **ปัญหาและข้อเสนอแนะในการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.** สืบค้น 14 เมษายน 2568 จาก https://ejournals.swu.ac.th/index.php/JOS/article/view/14420/12256/50825

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์. (2565). **เว็บไซต์ของรัฐบาลญี่ปุ่นโดนโจมตีทางไซเบอร์.** สืบค้น 25 เมษายน 2568 จาก https://ctf.in.th/ncert/1553/

สภาองค์กรของผู้บริโภค. (2568). **ป้องกันภัยออนไลน์ เทียบมาตรการ ยุโรปอเมริกา-สิงคโปร์-ไทย**. สืบค้น 14 เมษายน 2568 จาก https://www.tcc.or.th/cybercrime-policy-comparative/

สราวุธ ปิติยาศักดิ์, และวราภรณ์ วนาพิทักษ์. (2564). **มาตรการทางกฎหมายในการกำกับดูแลข่าวลวงบนสื่อสังคมออนไลน์: ศึกษาเปรียบเทียบกฎหมายของราชอาณาจักรไทยกับสาธารณรัฐสิงคโปร์.** สืบค้น 14 เมษายน 2568 https://so04.tci-thaijo.org/index.php/stou-sms-pr/article/view/250080

สัจจะ โชคบุญส่งสวัสดิ์. (2566). **แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์.** สืบค้น 14 เมษายน 2568 จาก https://www.ocsc.go.th/?attachment_id=87343

สำนักข่าวกรองแห่งชาติ. (2564). **แผนยุทธศาสตร์ทางไซเบอร์ของญี่ปุ่นระบุว่าจีน รัสเซีย และเกาหลีเหนือเป็นภัยคุกคามทางไซเบอร์.** สืบค้น 25 เมษายน 2568 จาก https://www.nia.go.th/cyber/cyberpage/560/

สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา. (2566). **องค์การสำรวจอวกาศญี่ปุ่นหรือ JAXA ถูกโจมตีจากภัยคุกคามทางไซเบอร์.** สืบค้น 25 เมษายน 2568 จาก https://www.uni.net.th/index.php/news/4562/

สำนักงานพัฒนารัฐบาลดิจิทัล. (2567). **นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570).** สืบค้น 21 เมษายน 2568 จาก https://www.dga.or.th/document/105565/

สุชาดา วิไลรัตน์. (2564). นโยบายความมั่นคงทางไซเบอร์ในประเทศพัฒนาแล้ว: แนวโน้มสำคัญ. **วารสารรัฐศาสตร์**, 41(2), 55–73.

อมรรัตน์ อินนุมาตร. (2566). **กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน: ศึกษากรณีพระราชบัญญัติการรักษาความมั่นคงไซเบอร์ พ.ศ. 2562 .** สืบค้น 24 เมษายน 2568 จาก https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:314741

อรรคภพ รอดจินดา. (2566). **สถานการณ์และแนวทางการป้องกันอาชญากรรมคอมพิวเตอร์.** สืบค้น 10 เมษายน 2568 จาก https://www.onlb.go.th/about/featured-articles/5143-a5143

ภาษาอังกฤษ

Cybersecurity Act 2018. (2022). Retrieved April 22, 2025 from https://sso.agc.gov.sg/Act/CA2018?ViewType=Pdf&_=20230130140832

Cybersecurity and Infrastructure Security Agency. (n.d.). Retrieved April 17, 2025 from https://www.cisa.gov/

Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies. (n.d.). Retrieved April 22, 2025 from https://cert.europa.eu/about-us

European Union Agency for Cybersecurity. (n.d.). Retrieved April 18, 2025 from https://www.enisa.europa.eu/topics/cyber-threats

Federal Bureau of Investigation. (n.d.). Retrieved April 18, 2025 from https://www.fbi.gov/investigate/cyber

National Center of Incident Readiness and Strategy for Cybersecurity. (2024). Retrieved April 19, 2025 from https://www.nisc.go.jp/eng/pdf/overview_of_cybersecurity2024_en.pdf

National Cyber Strategy. (2023). Retrieved April 19, 2025 from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

ปก

วุฒิสภา. (2568). **รัฐเร่งออกกฎหมายปราบปรามแก๊งคอลเซ็นเตอร์ ผ่านร่างแก้ไขพระราชกำหนด (พ.ร.ก.) มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี.** สืบค้น 21 เมษายน 2568 จาก https://www.senate.go.th/view/386/News/Highlight/267/TH-TH