ภาครัฐกับการจัดการความมั่นคงไซเบอร์ในยุคโลกาภิวัตน์*

GOVERNMENT AND CYBERSECURITY MANAGEMENT IN THE ERA OF GLOBALIZATION

อรพินทร์ พญาพิทักษ์สกุล
Oraphin Phayaphithaksakun
นักวิชาการอิสระ
Independent Scholar
Corresponding Author E-mail: 6701104234@mcu.ac.th

บทคัดย่อ

บทความได้วิเคราะห์ถึงบทบาทที่หลากหลายและครอบคลุมของภาครัฐในการรับมือกับความท้าทายเหล่านี้ เริ่มตั้งแต่การกำหนดยุทธศาสตร์และนโยบายด้านความมั่นคงไซเบอร์แห่งชาติ รวมถึงการออกกฎหมายและข้อบังคับที่จำเป็นเพื่อสร้างกรอบการดำเนินงานที่ชัดเจนและมีประสิทธิภาพ นอกจากนี้ ภาครัฐยังมีหน้าที่สำคัญในการสร้างและบริหารจัดการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ได้รับการปกป้องสูงสุด พร้อมทั้งพัฒนาขีดความสามารถและบุคลากรผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ โดยการลงทุนในการฝึกอบรมและจัดตั้งหน่วยงานเฉพาะทางอย่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ที่พร้อมรับมือกับภัยคุกคามยิ่งไปกว่านั้น การจัดการความมั่นคงไซเบอร์ที่ประสบความสำเร็จยังต้องอาศัยความร่วมมือที่แข็งแกร่งทั้งภายในประเทศระหว่างภาครัฐ ภาคเอกชน และสถาบันการศึกษา รวมถึงความร่วมมือระหว่างประเทศในการแลกเปลี่ยนข้อมูลข่าวสารและประสานงานในการสืบสวนอาชญากรรมไซเบอร์ข้ามชาติ ที่สำคัญ คือ ภาครัฐต้องมีบทบาทเชิงรุกในการสร้างความตระหนักรู้และให้ความรู้แก่สาธารณะ เพื่อให้ประชาชนตระหนักถึงภัยคุกคามและเป็นส่วนหนึ่งของแนวทางการป้องกัน ดังนั้น การบริหารจัดการความมั่นคงไซเบอร์ในยุคปัจจุบันเป็นภารกิจที่ซับซ้อนและต่อเนื่อง ภาครัฐจำเป็นต้องดำเนินการอย่างบูรณาการในทุกมิติที่กล่าวมา เพื่อสร้างภูมิคุ้มกันทางไซเบอร์ที่เข้มแข็ง ยืดหยุ่นและพร้อมรับมือกับการเปลี่ยนแปลง อันจะนำไปสู่การพัฒนาประเทศอย่างมั่นคงและยั่งยืนในยุคดิจิทัล

คำสำคัญ: บทบาทของภาครัฐ; การจัดการความมั่นคงไซเบอร์; ยุคโลกาภิวัตน์

Abstract

The article analyzed the diverse and comprehensive roles of the government in addressing these challenges, starting from the formulation of national cybersecurity strategies and policies, to the enactment of necessary laws and regulations to create a clear and effective operational framework. In addition, the government has an important role in creating and managing critical information infrastructure to ensure maximum protection, as well as developing cybersecurity capabilities and personnel by investing in training and establishing specialized agencies such as the Computer Security Coordination Center that are ready to deal with threats. Furthermore, successful cybersecurity management requires strong domestic cooperation between the government, private sector, and educational institutions, as well as

*Received October 26, 2025; Revised February 9, 2026; Accepted February 19, 2026

international cooperation in exchanging information and coordinating the investigation of transnational cybercrime. Importantly, the government must play a proactive role in raising awareness and educating the public so that they are aware of the threats and are part of the prevention approach. Therefore, cybersecurity management in the present era is a complex and continuous task. The government must take integrated action in all the aforementioned dimensions to create strong, resilient cyber immunity and be ready to cope with changes, which will lead to stable and sustainable national development in the digital age.

Keywords: The Role of Government; Cyber Security Management; Globalization Era

บทนำ

ในศตวรรษที่ 21 การปฏิวัติด้านเทคโนโลยีดิจิทัลได้แผ่ขยายอิทธิพลไปทั่วทุกมุมโลก สร้างสรรค์ยุคสมัยที่เรียกว่า ยุคโลกาภิวัตน์ดิจิทัล หรือที่มักเรียกโดยย่อว่า ยุคโลกาภิวัตน์ ซึ่งเป็นช่วงเวลาที่ข้อมูลข่าวสาร การสื่อสาร และการทำธุรกรรมต่าง ๆ สามารถเดินทางข้ามพรมแดนได้อย่างไร้ข้อจำกัด ด้วยความเร็วและประสิทธิภาพที่ไม่เคยมีมาก่อน อินเทอร์เน็ตได้กลายเป็นเส้นเลือดใหญ่หล่อเลี้ยงเศรษฐกิจ สังคม และการเมืองโลก ทำให้โลกเชื่อมโยงกันในลักษณะที่เรียกว่า “โลกไร้พรมแดน” (Borderless World) อย่างไรก็ตาม เหรียญย่อมมีสองด้านเสมอ ความก้าวหน้าทางเทคโนโลยีดิจิทัลที่มาพร้อมกับความสะดวกสบายและโอกาสทางเศรษฐกิจมหาศาล ก็ได้นำมาซึ่งความท้าทายใหม่ที่ไม่เคยเกิดขึ้นมาก่อน นั่นคือ ภัยคุกคามทางไซเบอร์ ภัยคุกคามเหล่านี้มีความแตกต่างจากภัยคุกคามแบบดั้งเดิมอย่างสิ้นเชิง เนื่องจากไม่จำกัดอยู่แค่ในขอบเขตทางภูมิศาสตร์ แต่สามารถแพร่กระจายและสร้างความเสียหายได้ทั่วโลกภายในพริบตาเดียว ตั้งแต่การโจมตีระบบโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ระบบพลังงาน ระบบคมนาคม ระบบการเงิน ที่อาจนำไปสู่ภาวะล่มสลายทางเศรษฐกิจและการหยุดชะงักของบริการสาธารณะ ไปจนถึงการจารกรรมข้อมูลภาครัฐที่อาจกระทบต่อความมั่นคงของชาติ การรั่วไหลของข้อมูลส่วนบุคคลที่ส่งผลต่อความเป็นส่วนตัวและการดำเนินชีวิตของประชาชน การก่อกวนระบบการเงินเพื่อแสวงหาผลประโยชน์ที่ผิดกฎหมาย หรือแม้แต่การบิดเบือนข้อมูล (Disinformation) และการสร้างข่าวปลอม (Fake News) เพื่อปลุกปั่น สร้างความแตกแยกในสังคม และบ่อนทำลายความน่าเชื่อถือของรัฐบาล ภัยคุกคามเหล่านี้ล้วนเป็นภัยคุกคามที่ไม่ปรากฏรูปธรรม แต่มีผลกระทบที่จับต้องได้และร้ายแรงยิ่งกว่าที่เคยเป็นมา (Broda & Strömbäck, 2024)

ในบริบทของยุคโลกาภิวัตน์นี้ ภาครัฐ ในฐานะผู้มีบทบาทสำคัญสูงสุดในการธำรงไว้ซึ่งความมั่นคงของชาติ การรักษาความสงบเรียบร้อย และการปกป้องผลประโยชน์ของประชาชน จึงต้องเผชิญกับภารกิจอันหนักอึ้งในการบริหารจัดการและรับมือกับ ความมั่นคงไซเบอร์ ที่นับวันจะทวีความซับซ้อนและรุนแรงขึ้น ภาครัฐไม่สามารถมองข้ามความท้าทายนี้ได้อีกต่อไป เพราะความมั่นคงไซเบอร์ได้กลายเป็นองค์ประกอบสำคัญของความมั่นคงแห่งชาติอย่างแยกไม่ออก การขาดความพร้อมหรือการละเลยต่อภัยคุกคามทางไซเบอร์อาจส่งผลให้ประเทศชาติเผชิญกับความเสี่ยงอันใหญ่หลวง ทั้งในมิติทางเศรษฐกิจ สังคม การเมืองและการต่างประเทศ (ไอริน โรจน์รักษ์, 2568)

การกำหนดยุทธศาสตร์และนโยบายด้านความมั่นคงไซเบอร์แห่งชาติ การวางรากฐานที่มั่นคงผ่านวิสัยทัศน์ นโยบาย และแผนปฏิบัติการที่ชัดเจน เพื่อกำหนดทิศทางและเป้าหมายในการปกป้องประเทศจากภัยคุกคามไซเบอร์ในระยะยาว การพัฒนากฎหมายและข้อบังคับที่เกี่ยวข้อง การสร้างกรอบกฎหมายที่ทันสมัยและครอบคลุม เพื่อรองรับการบังคับใช้ การป้องปรามอาชญากรรมไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล การเสริมสร้างขีดความสามารถและพัฒนาบุคลากร การลงทุนในการพัฒนากำลังคนที่มีความรู้

ความเชี่ยวชาญด้านไซเบอร์ รวมถึงการสร้างโครงสร้างพื้นฐานทางเทคโนโลยีที่จำเป็น เพื่อให้สามารถตรวจจับ ป้องกัน และตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ (ปรัชญา จำนงค์, 2566) การสร้างความร่วมมือระหว่างประเทศและภาคเอกชน การตระหนักถึงความจำเป็นในการทำงานร่วมกันกับพันธมิตรระหว่างประเทศเพื่อแลกเปลี่ยนข้อมูลข่าวสาร ประสบการณ์ และร่วมกันรับมือกับภัยคุกคามข้ามพรมแดนรวมถึงการส่งเสริมความร่วมมือกับภาคเอกชนซึ่งเป็นผู้มีส่วนสำคัญในการพัฒนานวัตกรรมและให้บริการด้านไซเบอร์ การสร้างความตระหนักรู้และส่งเสริมการมีส่วนร่วมของภาคประชาชน การให้ความรู้แก่ประชาชนถึงความสำคัญของความมั่นคงไซเบอร์และแนวทางการป้องกันตนเอง เพื่อให้ทุกคนเป็นส่วนหนึ่งของเครือข่ายความมั่นคงไซเบอร์ที่เข้มแข็งของประเทศ (โกวิทย์ พวงงาม, 2555)

ดังนั้น การวิเคราะห์ประเด็นเหล่านี้อย่างลึกซึ้งจะช่วยให้ผู้อ่านเข้าใจถึงความท้าทายที่ซับซ้อนและแนวทางที่ภาครัฐกำลังดำเนินการเพื่อรับมือกับภัยคุกคามไซเบอร์ในยุคโลกาภิวัตน์ และท้ายที่สุด ความสำคัญของการที่ประเทศไทยจะต้องมีการบริหารจัดการความมั่นคงไซเบอร์ที่แข็งแกร่งและยืดหยุ่น เพื่อให้สามารถก้าวข้ามความท้าทายและคว้าโอกาสที่มาพร้อมกับโลกดิจิทัลได้อย่างมั่นคง ปลอดภัย และยั่งยืนสำหรับคนรุ่นต่อไป

บทบาทของภาครัฐกับการจัดการความมั่นคงไซเบอร์

ในยุคโลกาภิวัตน์ที่เทคโนโลยีดิจิทัลเป็นหัวใจสำคัญของการดำเนินชีวิต การจัดการความมั่นคงไซเบอร์จึงมิใช่เพียงภาระหน้าที่ แต่เป็น พันธกิจหลัก ของภาครัฐทั่วโลก เพื่อธำรงไว้ซึ่งเสถียรภาพและความอยู่รอดของประเทศชาติ ภัยคุกคามไซเบอร์ในปัจจุบันมิได้จำกัดอยู่แค่การโจมตีทางเทคนิค แต่ยังรวมถึงการโจมตีทางสังคม การเมือง และเศรษฐกิจ ทำให้บทบาทของภาครัฐในการบริหารจัดการความมั่นคงไซเบอร์มีความซับซ้อนและต้องครอบคลุมในหลายมิติ บทบาทเหล่านี้สามารถสรุปได้เป็นประเด็นหลักดังต่อไปนี้ (สัญญา เคนาภูมิ, 2561)

1. การกำหนดนโยบายและยุทธศาสตร์แห่งชาติ (Policy and Strategy Formulation) หัวใจของการจัดการความมั่นคงไซเบอร์ที่มีประสิทธิภาพคือการมีนโยบายและยุทธศาสตร์ระดับชาติที่ชัดเจนและครอบคลุมภาครัฐมีหน้าที่ (ธนภูมิ ชาติดี และถิรวุฒิ แสงมณีเดช, 2567) ดังนี้

1.1 วิเคราะห์และประเมินภัยคุกคาม ทำความเข้าใจภาพรวมของภัยคุกคามไซเบอร์ ทั้งในระดับโลกและระดับประเทศ รวมถึงแนวโน้มของเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นในอนาคต (พิธุวรรณ กิติคุณ, 2561)

1.2 กำหนดยุทธศาสตร์ชาติ พัฒนาแผนยุทธศาสตร์ที่กำหนดวิสัยทัศน์ เป้าหมาย และทิศทางระยะยาวในการป้องกัน ตอบสนอง และฟื้นฟูจากภัยคุกคามไซเบอร์ โดยต้องสอดคล้องกับนโยบายความมั่นคงแห่งชาติโดยรวม

1.3 ออกกฎหมายและข้อบังคับ ตรากฎหมายที่เกี่ยวข้องกับความมั่นคงไซเบอร์ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมถึงการออกกฎระเบียบ ข้อบังคับ และมาตรฐานต่าง ๆ ที่เกี่ยวข้อง เพื่อสร้างกรอบการดำเนินงานที่ชัดเจนและมีผลบังคับใช้

1.4 จัดสรรงบประมาณและทรัพยากร พิจารณาจัดสรรงบประมาณและทรัพยากรที่เพียงพอสำหรับการลงทุนในโครงสร้างพื้นฐานด้านไซเบอร์ การวิจัยและพัฒนา การฝึกอบรมบุคลากรและการดำเนินงานตามแผนยุทธศาสตร์

2. การสร้างและบริหารจัดการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure Protection - CIIP) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) คือระบบและเครือข่าย

คอมพิวเตอร์ที่จำเป็นต่อการดำเนินงานของประเทศ เช่น ระบบพลังงาน โทรคมนาคม การเงิน สาธารณสุข และการขนส่ง ภาครัฐมีบทบาทสำคัญในการระบุและจำแนก CII กำหนดว่าอะไรคือโครงสร้างพื้นฐานสำคัญที่ต้องได้รับการปกป้องเป็นพิเศษ เนื่องจากหากถูกโจมตีจะส่งผลกระทบอย่างร้ายแรงต่อประเทศ วางมาตรการป้องกันและตอบสนอง กำหนดและบังคับใช้มาตรการรักษาความมั่นคงปลอดภัยสำหรับ CII โดยเฉพาะ รวมถึงการวางแผนฉุกเฉินและแผนการกู้คืนระบบเมื่อเกิดเหตุการณ์โจมตี และกำกับดูแลและตรวจสอบ ตรวจสอบให้แน่ใจว่าผู้ประกอบการ CII ทั้งภาครัฐและเอกชนปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยที่กำหนด (สมบัติ ธำรงธัญวงศ์, 2546)

3. การพัฒนาขีดความสามารถและบุคลากร (Capability and Human Resource Development) การมีนโยบายที่ดีจะไม่สมบูรณ์หากขาดบุคลากรที่มีความสามารถภาครัฐจึงต้องให้ความสำคัญ ได้แก่

3.1 พัฒนาบุคลากรเฉพาะทาง ลงทุนในการฝึกอบรมและพัฒนาผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ ทั้งในภาครัฐและภาคการศึกษา เพื่อให้มีจำนวนเพียงพอและมีทักษะที่ทันสมัยต่อภัยคุกคามที่เปลี่ยนแปลงไป (Klijn et al., 2010)

3.2 จัดตั้งหน่วยงานเฉพาะกิจ จัดตั้งหน่วยงานหรือศูนย์ปฏิบัติการด้านความมั่นคงไซเบอร์ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (CSIRT/CERT) เพื่อเป็นศูนย์กลางในการเฝ้าระวัง ตรวจจับ ตอบสนอง และแก้ไขปัญหาภัยคุกคามไซเบอร์

3.3 ส่งเสริมการวิจัยและพัฒนา (R&D) สนับสนุนการวิจัยและพัฒนาเทคโนโลยีและนวัตกรรมใหม่ ๆ ด้านความมั่นคงไซเบอร์ เพื่อให้ประเทศมีความสามารถในการพึ่งพาตนเองและก้าวทันเทคโนโลยีระดับโลก

4. การสร้างความร่วมมือและความร่วมมือระหว่างประเทศ (Collaboration and International Cooperation) ภัยคุกคามไซเบอร์ไร้พรมแดน ทำให้การรับมือต้องอาศัยความร่วมมือ ภาครัฐมีบทบาทสำคัญในการสร้างความร่วมมือภายในประเทศ ส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานภาครัฐด้วยกัน ภาคเอกชน สถาบันการศึกษา และภาคประชาสังคม เพื่อแลกเปลี่ยนข้อมูล ประสบการณ์ และทรัพยากรและสร้างความร่วมมือระหว่างประเทศ เข้าร่วมเป็นภาคีในสนธิสัญญาและข้อตกลงระหว่างประเทศที่เกี่ยวข้องกับความมั่นคงไซเบอร์ แลกเปลี่ยนข้อมูลภัยคุกคาม และร่วมมือในการดำเนินคดีอาชญากรรมไซเบอร์ข้ามชาติกับนานาประเทศ (Jampani, 2025)

5. การสร้างความตระหนักรู้และการให้ความรู้แก่สาธารณะ (Public Awareness and Education) ความมั่นคงไซเบอร์ไม่ใช่แค่เรื่องของภาครัฐ แต่เป็นเรื่องของทุกคน ภาครัฐจึงต้องรณรงค์สร้างความตระหนักรู้ให้ความรู้แก่ประชาชนทั่วไปและภาคธุรกิจถึงความสำคัญของความมั่นคงไซเบอร์ ภัยคุกคามที่อาจพบเจอและแนวทางการป้องกันตนเองเบื้องต้น เช่น การใช้รหัสผ่านที่รัดกุม การระมัดระวังการคลิกลิงก์แปลกปลอม และการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ และส่งเสริมการศึกษาด้านไซเบอร์ บรรจุเนื้อหาเกี่ยวกับความมั่นคงไซเบอร์ในหลักสูตรการศึกษาตั้งแต่ระดับประถมจนถึงอุดมศึกษา เพื่อสร้างพลเมืองดิจิทัลที่มีความรู้ความเข้าใจและสามารถรับมือกับภัยคุกคามได้ (กาญจนา นครคง และธนัสถา โรจนตระกูล, 2567)

6. การตอบสนองต่อเหตุการณ์และการกู้คืนระบบ (Incident Response and Recovery) เมื่อเกิดเหตุการณ์โจมตีทางไซเบอร์ ภาครัฐมีหน้าที่ในการจัดตั้งทีมตอบสนองเหตุการณ์ มีทีมงานที่พร้อมปฏิบัติการตลอด 24 ชั่วโมง เพื่อตรวจจับ วิเคราะห์ และตอบสนองต่อการโจมตีได้อย่างทันท่วงที และมีการวางแผนการกู้คืนระบบ มีแผนการกู้คืนระบบและข้อมูลที่ชัดเจน เพื่อให้ระบบที่ถูกโจมตีสามารถกลับมาทำงานได้โดยเร็วที่สุดและลดผลกระทบต่อการให้บริการสาธารณะ (สุพรรัตน์ วงศ์ดุสิตบุรี, 2566)

ดังนั้น บทบาทของภาครัฐในการจัดการความมั่นคงไซเบอร์ในยุคโลกาภิวัตน์นั้นมีความหลากหลายและครอบคลุม ตั้งแต่การวางแผนเชิงยุทธศาสตร์ การออกกฎหมาย การพัฒนาบุคลากร การสร้างความร่วมมือ

ไปจนถึงการให้ความรู้แก่ประชาชน การที่ประเทศจะก้าวไปข้างหน้าในโลกดิจิทัลได้อย่างมั่นคงและปลอดภัยนั้นขึ้นอยู่กับความสามารถของภาครัฐในการปรับตัว สร้างสรรค์ และบูรณาการบทบาทเหล่านี้ให้เป็นระบบเดียวกัน เพื่อสร้างภูมิต้านทานทางไซเบอร์ที่แข็งแกร่งและยั่งยืน

แนวทางการพัฒนาภาครัฐกับการจัดการความมั่นคงไซเบอร์

การจัดการความมั่นคงไซเบอร์ในยุคโลกาภิวัตน์ไม่ใช่เพียงแค่การติดตั้งโปรแกรมป้องกันไวรัสหรือไฟร์วอลล์อีกต่อไป แต่เป็นการสร้างภูมิคุ้มกันทางไซเบอร์ที่แข็งแกร่งและยืดหยุ่นครอบคลุมทุกมิติของประเทศ สำหรับประเทศไทย ภาครัฐได้ตระหนักถึงความสำคัญนี้และมีความพยายามในการพัฒนาขีดความสามารถด้านความมั่นคงไซเบอร์มาอย่างต่อเนื่อง อย่างไรก็ตาม ท่ามกลางภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงรวดเร็วและซับซ้อนขึ้นเรื่อย ๆ (ศาสตรา โตอ่อน, 2549) ภาครัฐไทยจำเป็นต้องเร่งปรับปรุงและพัฒนาแนวทางการจัดการความมั่นคงไซเบอร์ให้ทันสมัยและมีประสิทธิภาพมากยิ่งขึ้น โดยสามารถสรุปแนวทางการพัฒนาที่สำคัญได้ดังนี้

1. การยกระดับกฎหมายและนโยบายให้ทันสมัยและบังคับใช้จริงจัง แม้ประเทศไทยจะมีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (พ.ร.บ. ไซเบอร์) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) แล้ว แต่การบังคับใช้และการปรับปรุงให้สอดคล้องกับสถานการณ์ที่เปลี่ยนไปเป็นสิ่งสำคัญยิ่ง ต้องมีการทบทวนและปรับปรุงกฎหมายอย่างต่อเนื่อง เพราะภัยคุกคามไซเบอร์มีการพัฒนาอย่างรวดเร็ว กฎหมายจึงต้องมีความยืดหยุ่นและสามารถปรับปรุงแก้ไขให้ทันกับรูปแบบการโจมตีใหม่ ๆ เช่น การโจมตีด้วยปัญญาประดิษฐ์ (AI) หรือควอนตัมคอมพิวติง (Quantum Computing) มีการออกกฎหมายลำดับรองและมาตรฐานที่ชัดเจน กำหนดแนวปฏิบัติ กฎเกณฑ์ และมาตรฐานทางเทคนิคที่ชัดเจนและเป็นรูปธรรม เพื่อให้หน่วยงานภาครัฐและเอกชนสามารถนำไปปฏิบัติได้อย่างถูกต้องและมีประสิทธิภาพ มีการสร้างกลไกการบังคับใช้ที่มีประสิทธิภาพ เสริมสร้างศักยภาพของหน่วยงานผู้บังคับใช้กฎหมาย เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ให้มีอำนาจ บุคลากร และเครื่องมือที่เพียงพอในการดำเนินคดีและบังคับใช้กฎหมายได้อย่างจริงจังและรวดเร็ว และมีการกำหนดมาตรการลงโทษที่เด็ดขาด เพื่อป้องปรามผู้กระทำผิดและสร้างความตระหนักถึงผลกระทบจากการโจมตีทางไซเบอร์

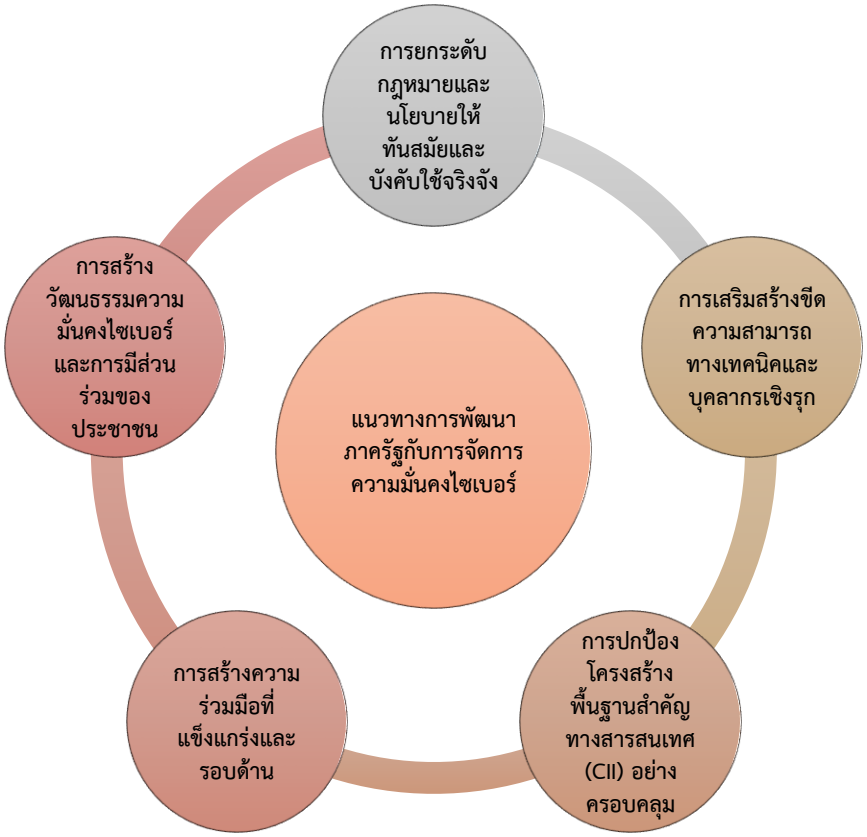
2. การเสริมสร้างขีดความสามารถทางเทคนิคและบุคลากรเชิงรุก การลงทุนในเทคโนโลยีและบุคลากรคือ หัวใจสำคัญของการป้องกันและตอบสนองต่อภัยคุกคาม พัฒนาบุคลากรไซเบอร์อย่างเร่งด่วน ลงทุนในการฝึกอบรมบุคลากรทั้งภาครัฐและเอกชนให้มีความรู้ความสามารถด้านความมั่นคงไซเบอร์ในระดับที่หลากหลาย ตั้งแต่ระดับผู้ใช้งานทั่วไปไปจนถึงผู้เชี่ยวชาญด้านการวิเคราะห์มัลแวร์ การเจาะระบบป้องกัน (Penetration Testing) และการตอบสนองต่อเหตุการณ์ (Incident Response) โดยอาจร่วมมือกับสถาบันการศึกษาและภาคเอกชน จัดตั้งศูนย์ปฏิบัติการความมั่นคงไซเบอร์ที่เข้มแข็ง (SOC/CSIRT) พัฒนาศูนย์ปฏิบัติการและศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CSIRT/CERT) ให้มีขีดความสามารถในการเฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพตลอด 24 ชั่วโมง นำเทคโนโลยีขั้นสูงมาประยุกต์ใช้ พิจารณานำเทคโนโลยีใหม่ ๆ เช่น ปัญญาประดิษฐ์ (AI) และ Machine Learning มาใช้ในการวิเคราะห์ข้อมูลภัยคุกคาม การตรวจจับความผิดปกติ และการคาดการณ์การโจมตี และส่งเสริมการวิจัยและพัฒนา สนับสนุนการวิจัยและพัฒนาเทคโนโลยีและนวัตกรรมด้านความมั่นคงไซเบอร์ภายในประเทศ เพื่อลดการพึ่งพาเทคโนโลยีจากต่างประเทศและสร้างความสามารถในการพึ่งพาตนเอง

3. การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) อย่างครอบคลุม CII เป็นเป้าหมายหลักของการโจมตีที่มุ่งหวังผลกระทบในวงกว้าง ภาครัฐต้องให้ความสำคัญเป็นพิเศษ ระบุและจัดลำดับความสำคัญของ CII ทบทวนและระบุประเภทของ CII ที่สำคัญอย่างต่อเนื่อง โดยพิจารณาจากผลกระทบหากถูกโจมตี กำหนดมาตรฐานความปลอดภัยเฉพาะสำหรับ CII ออกมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยที่เข้มงวดและเป็นไปตามหลักสากลสำหรับ CII แต่ละประเภท ตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ กำหนดให้ผู้ดูแล CII ทั้งภาครัฐและเอกชนต้องมีการประเมินความเสี่ยงและทดสอบระบบความปลอดภัยอย่างสม่ำเสมอ และรายงานผลต่อหน่วยงานกำกับดูแล วางแผนการกู้คืนระบบและการจัดการเหตุการณ์ฉุกเฉิน พัฒนาแผนการตอบสนองเหตุการณ์ (Incident Response Plan) และแผนการกู้คืนระบบ (Disaster Recovery Plan) ที่มีประสิทธิภาพสำหรับ CII ทุกประเภท เพื่อลดเวลาการหยุดชะงักและผลกระทบจากการโจมตี

4. การสร้างความร่วมมือที่แข็งแกร่งและรอบด้าน ความมั่นคงไซเบอร์เป็นเรื่องที่ต้องอาศัยความร่วมมือจากทุกภาคส่วน ความร่วมมือภาครัฐและเอกชน (Public-Private Partnership - PPP) ส่งเสริมการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชน โดยเฉพาะผู้ประกอบการ CII เพื่อแลกเปลี่ยนข้อมูลภัยคุกคาม ประสบการณ์ และร่วมกันพัฒนากลยุทธ์การป้องกัน ความร่วมมือระหว่างประเทศ สร้างเครือข่ายและขยายความร่วมมือกับประเทศต่าง ๆ ทั้งในระดับภูมิภาคและระดับโลก เพื่อแลกเปลี่ยนข่าวกรองภัยคุกคาม การประสานงานในการสืบสวนอาชญากรรมไซเบอร์ข้ามชาติ และการร่วมกันพัฒนากฎหมายและแนวปฏิบัติสากล ความร่วมมือกับภาคประชาสังคมและสถาบันการศึกษา สนับสนุนบทบาทของภาคประชาสังคมในการเฝ้าระวังและให้ความรู้แก่ประชาชน รวมถึงการร่วมมือกับสถาบันการศึกษาในการผลิตบุคลากรและทำการวิจัย

5. การสร้างวัฒนธรรมความมั่นคงไซเบอร์และการมีส่วนร่วมของประชาชน การสร้างความตระหนักรู้เป็นพื้นฐานสำคัญในการลดความเสี่ยง รณรงค์และให้ความรู้แก่ประชาชนอย่างต่อเนื่อง จัดกิจกรรมรณรงค์เผยแพร่ข้อมูล และให้ความรู้เกี่ยวกับภัยคุกคามไซเบอร์และแนวทางการป้องกันตนเองที่เข้าใจง่ายและเข้าถึงได้ทุกกลุ่มเป้าหมาย เช่น การระมัดระวังฟิชชิ่ง (Phishing) การใช้รหัสผ่านที่ปลอดภัย และการติดตั้งโปรแกรมป้องกันมัลแวร์ ส่งเสริมการศึกษาด้านดิจิทัลและไซเบอร์ บรรจุหลักสูตรด้านความปลอดภัยไซเบอร์และทักษะดิจิทัลที่จำเป็นไว้ในระบบการศึกษาทุกระดับ เพื่อสร้างพลเมืองดิจิทัลที่มีความรู้และภูมิคุ้มกัน สร้างช่องทางการรายงานภัยคุกคาม จัดให้มีช่องทางที่ง่ายและสะดวกสำหรับประชาชนในการรายงานเหตุการณ์ภัยคุกคามไซเบอร์ที่พบเจอ เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถรับทราบและตอบสนองได้อย่างรวดเร็ว

ดังนั้น การพัฒนาภาครัฐไทยกับการจัดการความมั่นคงไซเบอร์ในยุคโลกาภิวัตน์ต้องอาศัยการบูรณาการแนวทางที่หลากหลายและครอบคลุมทุกมิติ ตั้งแต่การยกระดับกรอบกฎหมาย การเสริมสร้างขีดความสามารถของบุคลากรและเทคโนโลยี การปกป้องโครงสร้างพื้นฐานที่สำคัญ การสร้างความร่วมมือที่แข็งแกร่ง ไปจนถึงการสร้างวัฒนธรรมความมั่นคงไซเบอร์ในหมู่ประชาชน การดำเนินการอย่างจริงจังและต่อเนื่องในทุก ๆ ด้าน จะช่วยให้ประเทศไทยสามารถสร้างภูมิคุ้มกันทางไซเบอร์ที่เข้มแข็ง พัฒนาเศรษฐกิจดิจิทัลได้อย่างมั่นใจ และธำรงไว้ซึ่งความมั่นคงของชาติในยุคที่โลกเชื่อมโยงกันอย่างไร้พรมแดนได้อย่างยั่งยืน สรุปเป็นองค์ความรู้ใหม่ดังภาพที่ 1



ภาพที่ 1 องค์ความรู้ใหม่

สรุป

ภาครัฐมีบทบาทที่ครอบคลุมและหลากหลายในการสร้างภูมิคุ้มกันทางไซเบอร์ให้กับประเทศ โดยสามารถสรุปหน้าที่หลักได้ดังนี้ การกำหนดนโยบายและยุทธศาสตร์แห่งชาติ คือ รากฐานสำคัญในการวางทิศทาง วิสัยทัศน์ และเป้าหมายระยะยาวในการรับมือกับภัยคุกคามไซเบอร์ รวมถึงการออกกฎหมายและข้อบังคับที่ทันสมัยและบังคับใช้ได้จริง เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นเครื่องมือทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ การสร้างและบริหารจัดการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ภาครัฐมีหน้าที่ในการระบุ กำหนดมาตรฐาน และกำกับดูแลการรักษาความมั่นคงปลอดภัยของระบบและเครือข่ายที่สำคัญต่อการดำเนินงานของประเทศ ไม่ว่าจะเป็นระบบพลังงาน การเงิน หรือโทรคมนาคม เพื่อป้องกันผลกระทบที่ร้ายแรงหากถูกโจมตี การพัฒนาขีดความสามารถและบุคลากร การลงทุนในการสร้างบุคลากรที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงไซเบอร์ ทั้งในภาครัฐและภาคเอกชน รวมถึงการจัดตั้งหน่วยงานเฉพาะกิจอย่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CSIRT/CERT) เป็นสิ่งจำเป็นเพื่อเสริมสร้างความสามารถในการตรวจจับ ตอบสนอง และแก้ไขปัญหา การสร้างความร่วมมือและความร่วมมือระหว่างประเทศ เนื่องจากภัยคุกคามไซเบอร์ไร้พรมแดน การทำงานร่วมกันทั้งภายในประเทศระหว่างภาครัฐ เอกชน สถาบันการศึกษา และการสร้างความร่วมมือกับนานาชาติในการแลกเปลี่ยนข้อมูลข่าวสาร การประสานงานในการสืบสวนคดี และการร่วมกันพัฒนากฎกติการะหว่างประเทศ จึงเป็นหัวใจสำคัญ การสร้างความตระหนักรู้และการให้ความรู้แก่สาธารณะ ความมั่นคงไซเบอร์ไม่ใช่เรื่องของภาครัฐเพียงลำพัง

การสร้างความตระหนักรู้ให้แก่ประชาชนทั่วไปเกี่ยวกับภัยคุกคามและวิธีการป้องกันตนเอง รวมถึงการส่งเสริมการศึกษาด้านไซเบอร์ในทุกระดับ จะช่วยสร้างพลเมืองดิจิทัลที่มีความเข้าใจและร่วมเป็นส่วนหนึ่งของการปกป้องประเทศ

แนวทางการพัฒนาภาครัฐไทยกับการจัดการความมั่นคงไซเบอร์ สำหรับประเทศไทย การพัฒนาความมั่นคงไซเบอร์ของภาครัฐต้องมุ่งเน้นไปที่การดำเนินการเชิงรุกและบูรณาการในหลายมิติ ยกระดับกฎหมายและนโยบายให้ทันสมัยและบังคับใช้จริงจัง ทบทวนและปรับปรุงกฎหมายอย่างต่อเนื่องให้เท่าทันกับรูปแบบภัยคุกคามใหม่ ๆ พร้อมทั้งออกกฎหมายลำดับรองและมาตรฐานที่ชัดเจน และเสริมสร้างกลไกการบังคับใช้กฎหมายให้มีประสิทธิภาพ เสริมสร้างขีดความสามารถทางเทคนิคและบุคลากรเชิงรุก เร่งพัฒนาบุคลากรไซเบอร์ผ่านการฝึกอบรม การจัดตั้งศูนย์ปฏิบัติการความมั่นคงไซเบอร์ที่เข้มแข็ง และการนำเทคโนโลยีขั้นสูงมาประยุกต์ใช้เพื่อการป้องกันและตรวจจับภัยคุกคาม ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างครอบคลุม ระบุและจัดลำดับความสำคัญของ CII อย่างต่อเนื่อง กำหนดมาตรฐานความปลอดภัยเฉพาะทางและบังคับใช้การตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ สร้างความร่วมมือที่แข็งแกร่งและรอบด้าน ส่งเสริมความร่วมมือระหว่างภาครัฐ-เอกชน-สถาบันการศึกษาในประเทศ และขยายความร่วมมือกับนานาชาติในการแลกเปลี่ยนข้อมูลข่าวกรองและร่วมมือในการรับมือกับอาชญากรรมไซเบอร์ข้ามชาติ สร้างวัฒนธรรมความมั่นคงไซเบอร์และการมีส่วนร่วมของประชาชน รณรงค์และให้ความรู้แก่ประชาชนอย่างต่อเนื่องเพื่อสร้างความตระหนักรู้และส่งเสริมให้ทุกคนเป็นส่วนหนึ่งของการป้องกันภัยคุกคามไซเบอร์

ดังนั้น การจัดการความมั่นคงไซเบอร์ในยุคโลกาภิวัตน์ถือเป็นภารกิจสำคัญที่ไม่สามารถประนีประนอมได้ของภาครัฐ การที่ประเทศไทยจะสามารถก้าวผ่านความท้าทายในโลกดิจิทัล และคว้าโอกาสในการพัฒนาเศรษฐกิจและสังคมดิจิทัลได้อย่างมั่นคงและยั่งยืนนั้น ขึ้นอยู่กับความสามารถของภาครัฐในการปรับตัว สร้างสรรค์ และบูรณาการความร่วมมือจากทุกภาคส่วน เพื่อสร้างภูมิคุ้มกันทางไซเบอร์ที่เข้มแข็ง ยืดหยุ่น และพร้อมรับมือกับภัยคุกคามในทุกรูปแบบ การลงทุนในความมั่นคงไซเบอร์วันนี้ คือการลงทุนในอนาคตที่ปลอดภัยและเจริญรุ่งเรืองของประเทศชาติ

เอกสารอ้างอิง

กาญจนา นครคง และธนัสถา โรจนตระกูล. (2567). ระบบอุปถัมภ์กับปัญหาการบริหารงานภาครัฐ. วารสารสหวิทยาการนวัตกรรมปริทรรศน์, 7(4), 452-465.

โกวิทย์ พวงงาม. (2555). การปกครองท้องถิ่นไทย : หลักการและมิติใหม่ในอนาคต (พิมพ์ครั้งที่ 8). กรุงเทพฯ: วิญญูชน.

ธนภูมิ ชาติดี และถิรวุฒิ แสงมณีเดช. (2567). การจัดการบริการสาธารณะแนวใหม่ด้านการส่งเสริมสุขภาพสำหรับผู้สูงอายุของภาครัฐในระดับท้องถิ่นด้วยการวิเคราะห์อภิมาน. วารสารมหาจุฬานาครทรรศน์, 11(4), 142-152.

ปรัชญา จำนงค์. (2566). นวัตกรรมการบริหารจัดการงานบริการขององค์กรปกครองส่วนท้องถิ่น ในจังหวัดนครปฐม. วารสารนวัตกรรมการศึกษาและการวิจัย, 7(4), 1402-1413.

พิธุวรรณ กิติคุณ. (2561). ห้องปฏิบัติการนวัตกรรมภาครัฐ (Government Innovation Lab: Gov Lab). เอกสารวิชาการอิเล็กทรอนิกส์ เล่มที่ 1-16. กรุงเทพฯ: สำนักงานเลขาธิการสภาผู้แทนราษฎร.

ศาสตรา โตอ่อน. (2549). การปฏิรูปการเมืองเพื่อความอยู่เย็นเป็นสุขในยุคโลกาภิวัตน์. สืบค้น 8 สิงหาคม 2568, จาก http://www.public-law.net/publaw/view.aspx?id=1004

สมบัติ ธำรงธัญวงศ์. (2546). การเมือง : แนวความคิดและการพัฒนา. กรุงเทพฯ: สถาบันบัณฑิตพัฒนาบริหารศาสตร์.

สัญญา เคนาภูมิ. (2561). กระบวนทัศน์การจัดการบริการสาธารณะแนวใหม่. วารสารมนุษยศาสตร์และสังคมศาสตร์มหาวิทยาลัยราชภัฏอุบลราชธานี, 9(1), 181-197.

สุพรรัตน์ วงศ์ดุสิตบุรี. (2566). การบริหารจัดการของผู้นำสมัยใหม่ในยุคดิจิทัลของเทศบาลเมืองพัทยา. วารสาร มจร พุทธปัญญาปริทรรศน์, 8(1), 136-148.

ไอริน โรจน์รักษ์. (2568). ยุทธศาสตร์การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์: ก้าวต่อไปกับพลวัตของสังคมที่เปลี่ยนแปลง. วารสารธรรมศาสตร์, 44(2), 197-216.

Broda, E. & Strömbäck, J. (2024). Misinformation, Disinformation, and Fake News: Lessons from An Interdisciplinary, Systematic Literature Review. Annals of the International Communication Association, 48(2), 139–166.

Jampani, S. K. (2025). Cross-Border Cybersecurity Collaboration: Building A Global Framework for Threat. World Journal of Advanced Engineering Technology and Sciences, 14(2), 001–010.

Klijn, E. H. et al. (2010). The Impact of Network Management on Outcomes in Governance Networks. Public Administration, 88(4), 1063-1082.