บทสรุปเชิงนโยบาย
POLICY BRIEF

ฉบับที่ 2
ปี 2568

กลุ่มงานวิจัยและพัฒนา สำนักวิชาการ
สำนักงานเลขาธิการสภาผู้แทนราษฎร

ภัยคุกคามไซเบอร์ในภาครัฐ ความท้าทายใหม่ในยุคดิจิทัล

จัดทำโดย
นางสาวบูชิตา ไวทยานนท์
วิทยากรชำนาญการพิเศษ

ภัยคุกคามไซเบอร์ในภาครัฐ: ความท้าทายใหม่ในยุคดิจิทัล

ประเด็นสำคัญ

- การปกป้องโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure Protection) โดยภาครัฐให้ความสำคัญกับการปกป้องโครงสร้างพื้นฐานทางดิจิทัล เช่น ระบบไฟฟ้า น้ำประปา สาธารณสุข และการเงิน เนื่องจากเป็นเป้าหมายที่อาจถูกโจมตีจากภัยคุกคามไซเบอร์ ซึ่งอาจส่งผลกระทบต่อความมั่นคงของประเทศ
- การพัฒนาบุคลากรและทักษะความรู้ด้านไซเบอร์ ควรมีการส่งเสริมการพัฒนาบุคลากรที่มีทักษะด้านความปลอดภัยทางไซเบอร์ เพื่อให้สามารถรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ รวมถึงความสร้างความตระหนักรู้ให้แก่สังคม
- กฎหมายและมาตรการควบคุมทางไซเบอร์ ภาครัฐได้ออกกฎหมายต่าง ๆ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และนโยบายด้านความปลอดภัยทางไซเบอร์ เพื่อป้องกันและจัดการกับการโจมตีทางไซเบอร์ รวมถึงมาตรการการกำกับดูแลการใช้เทคโนโลยีอย่างถูกต้อง
- ความร่วมมือระหว่างประเทศ ประเทศไทยเน้นย้ำความร่วมมือกับประเทศต่าง ๆ และองค์กรระหว่างประเทศ เพื่อเป็นการแบ่งปันข้อมูลข่าวสาร การพัฒนามาตรการการรับมือและการป้องกันภัยคุกคามไซเบอร์
- การจัดการเหตุการณ์และการรับมือกับภัยคุกคามไซเบอร์ โดยการพัฒนาศูนย์ตอบสนองต่อภัยคุกคามไซเบอร์ในประเทศไทย เพื่อให้ภาครัฐสามารถติดตามและรับมือกับเหตุการณ์โจมตีทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ
- ข้อเสนอแนะที่สำคัญ คือ การกำหนดกรอบนโยบายไซเบอร์ที่ครอบคลุมและบังคับใช้อย่างชัดเจน ประเทศไทยควรพัฒนากฎหมายและแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมทุกภาคส่วน พร้อมทั้งกำหนดมาตรฐานการป้องกันภัยไซเบอร์สำหรับหน่วยงานภาครัฐและองค์กรเอกชน โดยให้ความสำคัญกับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และจัดตั้งระบบติดตามภัยคุกคามทางไซเบอร์ที่สามารถดำเนินการได้ในระดับชาติอย่างเป็นรูปธรรม

1. บทนำ

ในยุคที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในทุกด้านของชีวิต ส่งผลต่อการทำงานของภาครัฐที่จำเป็นต้องมีการเปลี่ยนแปลง รัฐบาลและหน่วยงานภาครัฐต่าง ๆ ได้มีการนำเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) มาใช้ในการบริหารจัดการข้อมูล รวมถึงการให้บริการสาธารณะผ่านระบบดิจิทัล เช่น ระบบฐานข้อมูลประชาชน ระบบการเงินภาครัฐและระบบการติดต่อราชการออนไลน์ ความสะดวกในการให้บริการและการบริหารจัดการข้อมูลดังกล่าว ช่วยเสริมประสิทธิภาพและความโปร่งใสของภาครัฐ ทำให้เกิดความเสี่ยงในการเผชิญกับภัยคุกคามไซเบอร์ที่เพิ่มมากขึ้นเช่นกัน

ภัยคุกคามไซเบอร์ในภาครัฐเป็นปัญหาที่นับวันจะทวีความรุนแรงขึ้น การโจมตีไซเบอร์จากแฮกเกอร์ไม่เพียงแต่ส่งผลกระทบต่อความมั่นคงของระบบสารสนเทศเท่านั้น แต่ยังมีผลกระทบโดยตรงต่อความปลอดภัยของข้อมูลสำคัญของประเทศ การโจมตีที่มุ่งเป้าไปยังหน่วยงานของรัฐ อาจทำให้ข้อมูล

ที่สำคัญรั่วไหล หรือระบบบริการของรัฐหยุดชะงัก ซึ่งเป็นอุปสรรคต่อการบริหารจัดการภาครัฐอย่างมีประสิทธิภาพ

ประเทศไทยเผชิญกับภัยคุกคามไซเบอร์มาอย่างต่อเนื่อง มีรายงานการโจมตีไซเบอร์หลายครั้งที่มุ่งเป้าไปยังหน่วยงานภาครัฐในลักษณะต่าง ๆ เช่น การโจมตีด้วยแรนซัมแวร์ (Ransomware) ที่เข้ารหัสข้อมูลและเรียกค่าไถ่ หรือการโจมตีแบบปฏิเสธการให้บริการ (DDoS) ที่ทำให้ระบบล่ม ส่งผลกระทบต่อการให้บริการแก่ประชาชน นอกจากนี้ การละเมิดข้อมูลส่วนบุคคลจากฐานข้อมูลของรัฐก็เป็นประเด็นสำคัญซึ่งอาจก่อให้เกิดความเสียหายต่อภาพลักษณ์และความเชื่อมั่นของประชาชนในการให้บริการของภาครัฐ

2. สถานการณ์ปัจจุบันเกี่ยวกับการป้องกันภัยคุกคามไซเบอร์

สถานการณ์ปัจจุบัน

สำนักงานสภาความมั่นแห่งชาติ ได้กำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 เป็นแนวนโยบายระดับชาติฉบับแรกของประเทศไทย เพื่อรองรับสังคมที่ก้าวเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบ โดยมีเป้าประสงค์หลักเพื่อสร้างความพร้อมให้กับประเทศไทยสามารถรับมือกับภัยคุกคามไซเบอร์ได้อย่างครอบคลุมและรอบด้านโดยรวมมากที่สุดเท่าที่สภาวะแวดล้อมและทรัพยากรเอื้ออำนวย และมุ่งเน้นการมีกลไกกลางในการบริหารจัดการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐาน และการสร้างความตระหนักรู้ให้ทุกภาคส่วนเตรียมพร้อมรับมือตลอดจนความร่วมมือจากต่างประเทศทั้งในระดับภูมิภาคและระดับโลก

สถานการณ์ความพร้อมของประเทศไทยเกี่ยวกับการรับมือและจัดการความเสี่ยงกับภัยคุกคามทางไซเบอร์ยังมีข้อจำกัดในหลายด้าน ในขณะที่ความซับซ้อนของภัยคุกคามที่เกิดขึ้นมีความแปลกใหม่ตลอดเวลา สามารถพบได้จากเหตุการณ์การค้นพบช่องโหว่ในระบบปฏิบัติการแอปพลิเคชัน หรือแม้แต่ซอฟต์แวร์ของอุปกรณ์ประเภท IoT (Internet of Things) ที่เริ่มมีการใช้งานอย่างแพร่หลายในช่วงหลายปีที่ผ่านมา ทำให้แฮกเกอร์สามารถลักลอบติดตั้งมัลแวร์หรือโปรแกรมประสงค์ร้ายบนคอมพิวเตอร์ที่มีช่องโหว่และฝังรหัสอันตราย สามารถสร้างความเสียหายให้กับข้อมูลของเหยื่อ เช่น WannaCry Ransomware ซึ่งเป็นมัลแวร์เรียกค่าไถ่ข้อมูลด้วยการเข้ารหัสลับ ทำให้ผู้ใช้ไม่สามารถเปิดข้อมูลใช้งานได้ สามารถแพร่กระจายได้ด้วยตัวเองผ่านการโจมตีช่องโหว่ของระบบปฏิบัติการ Windows ทำให้การระบาดเป็นไปอย่างรวดเร็วในวงกว้างกว่าเดิม หรือ Mirai Botnet ซึ่งเป็นมัลแวร์โจมตีอุปกรณ์ประเภท IoT ที่แฮกเกอร์สามารถสั่งการให้โจมตีระบบคอมพิวเตอร์ของผู้อื่นที่อยู่ในเครือข่ายคอมพิวเตอร์ในลักษณะ DDoS (Distributed Denial-of-Service) ทำให้บริการเครือข่ายอินเทอร์เน็ตและบริการที่ตกเป็นเป้าโจมตีขาดสภาพความพร้อมให้บริการ

สภาพปัญหาและแนวโน้มของภัยคุกคามไซเบอร์

1) ปัจจุบันเทคโนโลยีของอุปกรณ์อิเล็กทรอนิกส์ก้าวหน้าไปมาก อุปกรณ์สื่อสารที่สามารถเข้าถึงอินเทอร์เน็ตมีขนาดเล็กลง หรือมีให้เลือกใช้ได้หลากหลาย และมีอุปกรณ์ที่ใช้ในชีวิตประจำวันที่ต้องอาศัยอินเทอร์เน็ตมากขึ้น เช่น โทรศัพท์ จีพีเอส กล้องถ่ายรูป อุปกรณ์การแพทย์ จึงเป็นจุดอ่อนที่ทำให้เสี่ยงต่อการเกิดภัยทางไซเบอร์ได้ง่ายขึ้น ไม่ว่าผู้ใช้งานหรือผู้โจมตีจะอยู่ ณ สถานที่ใดของโลก อีกทั้งพบว่าผู้ใช้งานมักให้ความสำคัญกับความปลอดภัยเป็นอันดับรอง และเน้นความสะดวกสบายเป็นหลัก

2) ความเสี่ยงต่อการถูกโจมตีในหลายลักษณะทั้งต่อโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ไฟฟ้า ประปา ท่อก๊าซ โดยใช้มัลแวร์โจมตีระบบตรวจสอบและควบคุมการทำงานของระบบสาธารณูปโภคหรือต่อบริการสาธารณะ เช่น การข่มขู่โจมตี ระงับการให้บริการเว็บไซต์โดยใช้เทคนิค DoS/DDoS (Denial of Service/Distributed Denial of Service) ฯลฯ จนประชาชนไม่สามารถเข้าถึงเว็บไซต์ที่ต้องการใช้บริการได้

รวมถึงการส่งมัลแวร์ประเภท Ransomware ไปเข้ารหัสลับเอกสารสำคัญในคอมพิวเตอร์ของเหยื่อ เพื่อเรียกร้องให้จ่ายค่าไถ่ก็เป็นการโจมตีอีกลักษณะหนึ่ง

3) ตลาดการเงินโลกไร้พรมแดนซึ่งเป็นผลจากเทคโนโลยีและนวัตกรรมทางการเงินมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการพัฒนาเครื่องมือทางการเงินใหม่ ๆ เช่น Application ทางการเงิน Crowd Funding และ Financial Platform ฯลฯ รวมทั้งต้องเตรียมความพร้อมในด้านต่าง ๆ เพื่อรองรับต่อการเปลี่ยนแปลงที่เกิดขึ้น เช่น การปรับปรุงกฎระเบียบในการกำกับดูแลภาคการเงิน การสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการในเรื่องความปลอดภัยของข้อมูลส่วนตัวผ่านระบบเทคโนโลยีสารสนเทศ การป้องกันความเสี่ยงจากความเชื่อมโยงทางการเงิน การเคลื่อนย้ายเงินทุนและปริมาณธุรกรรมที่เพิ่มขึ้น

4) หน่วยงานภายในประเทศยังไม่ให้ความสำคัญกับการวางแผนรับมือและซ้อมทั้งก่อนเกิดเหตุ ขณะเกิดเหตุ และหลังเกิดเหตุที่ได้มาตรฐาน โดยเฉพาะความสามารถในการฟื้นตัว (Resilience) หลังเกิดภัยคุกคามทางไซเบอร์ ซึ่งมีความสำคัญอย่างยิ่งต่อการรักษาความต่อเนื่องของการปฏิบัติการในมิติต่าง ๆ โดยจะช่วยลดผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ให้น้อยลง

5) การก่อการร้ายไซเบอร์และการทำสงครามไซเบอร์ (Cyber terrorism/Cyber warfare) ไทยเป็นประเทศหนึ่งที่มีความเสี่ยงในการเป็นพื้นที่กระทำการก่อการร้ายทางไซเบอร์โดยรัฐ หรือบุคคล/กลุ่มบุคคล ตลอดจนกลุ่มผู้ก่อการร้าย ซึ่งการก่อการร้ายทางไซเบอร์ยังหมายรวมถึงการนำสื่อออนไลน์ไปใช้เป็นเครื่องมือในการเผยแพร่แนวคิดที่นิยมการใช้ความรุนแรงหรือการสอนการก่อการร้าย การจัดหาอาวุธและวัสดุที่ใช้ประกอบเป็นอาวุธ รวมทั้งสอนวิธีการทำ การหาสมาชิกมาร่วมอุดมการณ์และก่อการอีกด้วย สำหรับไทยนั้นต้องคอยเฝ้าระวังกลุ่มเสี่ยงที่อาจถูกชักจูงไปในการดังกล่าว และในด้าน Cyber Warfare นั้น ซึ่งไทยต้องพัฒนาขีดความสามารถในการควบคุมมิติทางไซเบอร์ที่จะมีผลต่อการทำสงคราม เพื่อสามารถปกป้องผลประโยชน์แห่งชาติ และรักษาความมั่นคงแห่งชาติที่เกิดจากภัยคุกคามในรูปแบบใหม่นี้

6) ปัญหาการขาดความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะการใช้อินเทอร์เน็ต พบว่าผู้ใช้งานอินเทอร์เน็ตมักให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยเป็นอันดับรองและเน้นความสะดวกสบายเป็นหลัก จึงต้องสร้างความตระหนักรู้ให้กับประชาชนทั่วไปและผู้ใช้งานอินเทอร์เน็ตในทุกระดับให้ทราบถึงภัยคุกคามทางไซเบอร์และวิธีรับมือกับปัญหานี้

7) การแพร่ระบาดของภัยไซเบอร์ ทำให้เกิดความเสี่ยงด้านความปลอดภัยไซเบอร์ตามมาอีกหลายรูปแบบ เช่น การสร้างความเสียหายแก่ระบบ การจารกรรมข้อมูลบนระบบคอมพิวเตอร์ (ข้อมูลการค้า การเงิน หรือข้อมูลส่วนตัว) หรือแม้แต่การโจมตีโครงสร้างพื้นฐานที่มีความสำคัญที่สามารถทำให้ระบบเศรษฐกิจหยุดชะงักและได้รับความเสียหายหรือเกิดอันตรายต่อชีวิตและทรัพย์สินของประชาชน โดยที่ภัยไซเบอร์เหล่านี้ล้วนแล้วแต่พัฒนาอย่างรวดเร็วตามความก้าวหน้าของเทคโนโลยี

3. การประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ของประเทศไทย

การประเมินความพร้อมในการรับมือภัยคุกคามไซเบอร์ ทำให้ทราบถึงระดับความเสี่ยงของภัยคุกคามไซเบอร์ อันจะนำไปสู่การกำหนดแนวทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสม สามารถแบ่งออกเป็น 5 ด้านหลัก ๆ ดังนี้

1) ความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ ประเทศไทยให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์มาอย่างต่อเนื่อง โดยมีกฎหมายที่กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แบ่งออกเป็น 3 กลุ่ม ได้แก่ (1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดมาตรการสำคัญ ๆ ด้านความมั่นคงปลอดภัยเอาไว้ เพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือ

เมื่อมีการใช้ระบบคอมพิวเตอร์หรือระบบอินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งครอบคลุมทั้งในการพาณิชย์อิเล็กทรอนิกส์ รวมถึงการให้บริการทางอิเล็กทรอนิกส์ของรัฐ หรือในงานรัฐบาลอิเล็กทรอนิกส์นั้น มีความมั่นคงปลอดภัย ตลอดจนกำหนดให้หน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure Protection) ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย ต่อมาได้มีการตรากฎหมายจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ซึ่งได้กำหนดอำนาจหน้าที่สำคัญเพิ่มเติมอีกประการ คือ การยกระดับทักษะผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งทำหน้าที่ดูแลศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT) (2) กฎหมายระดับอนุบัญญัติหรือกฎหมายลูกที่กำหนดมาตรการในการกำกับดูแลตลาดเงินโดยธนาคารแห่งประเทศไทยและตลาดทุนโดยสำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย รวมทั้งในการกำกับดูแลธุรกิจประกันภัยโดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อให้บริการของผู้ประกอบการในภาคเศรษฐกิจที่มีการกำกับดูแลให้มีความมั่นคงปลอดภัย และ (3) กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์ โดยมีกองป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษกระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศ ภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นหน่วยงานรองรับการดำเนินงาน

2) ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์ แม้ประเทศไทยจะให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มากขึ้นตามลำดับ และได้มีการดำเนินงานของหน่วยงานปฏิบัติหลาย ๆ หน่วยงาน เช่น การทำงานของศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ (The Computer Emergency Response Team) หรือไทยเซิร์ต (ThaiCERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ช่วยในการปกป้องและประสานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ และเริ่มมีการทำงานในรูปแบบ CERT ในองค์กรที่ทำหน้าที่กำกับดูแลองค์การภาคเอกชนบ้างแล้วก็ตาม หรือมีการดำเนินงานของกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษกระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือธนาคารแห่งประเทศไทย แต่รูปแบบการทำงานดังกล่าวก็เป็นการทำงานในเชิงป้องกันและตั้งรับเมื่อมีภัยคุกคามทางไซเบอร์เท่านั้น จึงได้มีการจัดตั้งศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม หรือกองทัพไทย เพื่อรับมือกับภัยคุกคามทางไซเบอร์ในเชิงรุกให้มากขึ้น ทั้งนี้ ในภาพรวมของประเทศยังจำเป็นต้องผลักดันให้มีกลไกการประสานงานและเชื่อมโยงระหว่างฝ่ายนโยบายกับหน่วยงานปฏิบัติ และมีการดำเนินการอย่างเป็นรูปธรรม โดยเฉพาะในงานด้านการข่าวและการข่าวกรองทางไซเบอร์ที่มีส่วนสำคัญอย่างมากต่อการปฏิบัติภารกิจของเจ้าหน้าที่ในด้านการติดตามประเมินสถานการณ์และตัดสินใจ อีกทั้งจำเป็นต้องเพิ่มกลไกในการตรวจสอบและติดตามประเมินผล ซึ่งประเทศไทยยังไม่มีหน่วยงานหลักที่มีอำนาจและหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยตรง จึงมีความจำเป็นอย่างยิ่งที่ต้องมีศูนย์กลางในการดำเนินการเรื่องดังกล่าว เพื่อให้สามารถ

ยกระดับการป้องกันและรับมือกับภัยคุกคามและการโจมตีทางไซเบอร์ที่มีแนวโน้มว่าจะซับซ้อน และมีความรุนแรงเพิ่มมากขึ้นตามลำดับ

3) ความพร้อมด้านบุคลากร ถือเป็นสิ่งที่สำคัญอย่างยิ่ง ทั้งในด้านความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ระดับนโยบายและปฏิบัติ และด้านความรู้ความเชี่ยวชาญเฉพาะทาง ซึ่งประเทศไทยควรกำหนดทิศทางและให้ความสำคัญกับการส่งเสริมและสนับสนุนการพัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามที่อาจเกิดขึ้นในรูปแบบต่าง ๆ ได้อย่างครอบคลุมและมีประสิทธิภาพ

4) ความพร้อมของระบบและเทคโนโลยี ประเทศไทยยังขาดระบบการบริหารจัดการเครือข่ายเพื่อเสริมความมั่นคงของประเทศและยังต้องพึ่งพาต่างประเทศอย่างสูงในด้านนี้ ภาครัฐจึงควรหันมาให้ความสำคัญกับการพัฒนาระบบและเทคโนโลยีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง เพื่อลดการพึ่งพาต่างชาติและเพื่อการรักษาผลประโยชน์ของชาติและความมั่นคงของชาติอย่างรอบคอบ รัดกุม และได้มาตรฐาน ควบคู่ไปกับการเสริมสร้างระบบและเทคโนโลยีที่นำเข้ามาจากต่างประเทศ

5) ความพร้อมด้านงานสืบสวน งานข่าวและข่าวกรองทางไซเบอร์ ปัจจุบันยังขาดการบูรณาการและการให้ความสำคัญกับการพัฒนาขีดความสามารถศักยภาพด้านงานข่าวกรองทางไซเบอร์ ซึ่งมีส่วนสำคัญอย่างยิ่งในการทำความเข้าใจกับภัยคุกคามรูปแบบใหม่ ๆ โดยเฉพาะภัยคุกคามทางไซเบอร์ อันจะช่วยเสริมงานด้านการสืบสวนและงานข่าวโดยรวมอีกด้วย

4. แนวปฏิบัติที่ดีในการป้องกันและรับมือภัยคุกคามไซเบอร์ของต่างประเทศ

การเชื่อมโยงประเทศต่าง ๆ ในโลกไซเบอร์สเปซ (Cyber Space) มีผลกระทบต่อความมั่นคงของประเทศในระดับนานาชาติมากขึ้น จึงทำให้หลายประเทศทั่วโลกให้ความสนใจในการกำหนดนโยบายความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้เกิดความเสี่ยงน้อยที่สุดในการใช้ระบบเทคโนโลยีดิจิทัลในการขับเคลื่อนเศรษฐกิจ สังคมและการเมือง ภาครัฐจำเป็นต้องเรียนรู้บทเรียนแนวคิดการทำงานของหลากหลายประเทศในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งมีเงื่อนไขความสำเร็จในการขับเคลื่อนการป้องกันภัยคุกคามทางไซเบอร์ที่แตกต่างกัน เพื่อนำมาปรับใช้ในบริบทของประเทศไทย จากกรณีตัวอย่างการป้องกันภัยคุกคามทางไซเบอร์ของประเทศสหรัฐอเมริกา จีน และเกาหลีใต้ โดยมีรายละเอียดดังนี้

1) กรณีศึกษาของประเทศสหรัฐอเมริกา ได้มีการอนุมัติใช้กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์มากถึง 5 ฉบับ ได้แก่ ฉบับแรก คือ กฎหมาย National Cybersecurity and Critical Infrastructure Protection Act of 2014 (NCCIPA) ยกระดับศูนย์บูรณาการความมั่นคงปลอดภัยไซเบอร์และการสื่อสารแห่งชาติ (National Cybersecurity and Communications Integration Center: NCCIC) ซึ่งอยู่ใต้สังกัดของกระทรวงความมั่นคงในประเทศ (Homeland Security) ให้เป็นศูนย์กลางการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ระหว่างภาครัฐกับภาคเอกชน ฉบับที่สอง คือ Cybersecurity Enhancement Act of 2014 มอบอำนาจให้สถาบันหลักของประเทศซึ่งเป็นผู้กำหนดมาตรฐานด้านเทคโนโลยี คือ National Institute of Standards and Technology's (NIST) สนับสนุนและอำนวยความสะดวกให้กับภาคเอกชน ในการพัฒนามาตรฐานไซเบอร์และธรรมเนียมปฏิบัติอันเป็นเลิศ (Best Practices) สำหรับโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เช่น ระบบธนาคาร ขนส่ง และพลังงาน ซึ่งหากถูกโจมตีทางไซเบอร์ย่อมเกิดความเสียหายมหาศาล NIST ในฐานะองค์กรภาครัฐทำหน้าที่เพียงสนับสนุนเท่านั้น ซึ่งกฎหมายไม่ให้บังคับว่าเอกชนต้องใช้มาตรฐานใดมาตรฐานหนึ่งเพื่อเปิดโอกาสให้มีการพัฒนาอย่างเป็นอิสระ และไม่เปิดช่องให้มีการเอื้อประโยชน์แก่บริษัทใดบริษัทหนึ่งเป็นการเฉพาะ และ

กฎหมายใหม่เพิ่มเติมอีก 3 ฉบับ ที่มุ่งเน้นไปที่การปรับปรุงระดับความปลอดภัยของระบบของรัฐและพัฒนาบุคลากร ซึ่งสหรัฐอเมริกาเน้นปรับปรุงมาตรฐานความปลอดภัยของระบบ การแลกเปลี่ยนข้อมูลที่เกี่ยวกับภัยคุกคามไซเบอร์ และศักยภาพของเจ้าหน้าที่ โดยทั้งหมดอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลและมีกลไกตรวจสอบถ่วงดุลทุกขั้นตอน รวมทั้งรายงานผลการดำเนินงานประจำปีต่อกรรมาธิการในสภา

2) กรณีศึกษาของประเทศจีน ให้ความสำคัญกับการปกป้องความมั่นคงไซเบอร์และระบบโครงสร้างพื้นฐาน อันนำมาสู่การออกกฎหมายความปลอดภัยทางไซเบอร์ในปัจจุบัน อาทิ โทรคมนาคม การจัดการน้ำ ธนาคารและการเงิน พลังงาน การคมนาคมและไฟฟ้า รวมถึงสิ่งอื่น ๆ ซึ่งหากถูกทำลาย ทำให้เสียหาย หรือเกิดการรั่วไหล จะทำให้เกิดผลเสียมหาศาลต่อความมั่นคงของชาติ สวัสดิการสาธารณะ ความเป็นอยู่ของประชาชน หรือประโยชน์สาธารณะของประเทศ โดยกฎหมายความปลอดภัยทางไซเบอร์มีความคล้ายคลึงกับกฎหมายต่อต้านการก่อการร้ายของประเทศจีนเป็นอย่างยิ่ง ซึ่งบังคับให้ผู้ประกอบกิจการโทรคมนาคมและผู้ให้บริการทางอินเทอร์เน็ตต้องส่งมอบวิธีการถอดรหัสข้อมูลรักษาความปลอดภัยและความช่วยเหลือทางเทคนิคต่าง ๆ ให้แก่รัฐบาลเพื่อป้องกันและสืบสวนกิจกรรมของผู้ก่อการร้าย โดยรัฐบาลจีนจะอ้างว่ากฎหมายต่อต้านการก่อร้ายร้ายมิได้เรียกร้องให้บริษัทต้องจัดทำช่องทางลัดแก่รัฐบาลแต่อย่างใด โดยในกฎหมายความปลอดภัยทางไซเบอร์ บริษัทอินเทอร์เน็ตต่างชาติซึ่งอยู่นอกเขตอำนาจศาลของจีนต้องให้ความร่วมมือกับรัฐบาลจีนในการให้ความช่วยเหลือด้านการถอดรหัสข้อมูลหรือสร้างช่องทางพิเศษให้แก่รัฐบาลในการเข้าถึงข้อมูลส่วนบุคคล อีกทั้ง กฎหมายฉบับนี้ยังไม่ได้กำหนดขอบเขตการใช้กฎหมายนี้แต่เพียงในเฉพาะกรณีที่จำเป็นหรือวางแนวปฏิบัติให้แก่เจ้าหน้าที่รัฐในการใช้อำนาจเท่านั้น

3) กรณีศึกษาของประเทศเกาหลีใต้ มีหน่วยงาน Korea Internet Security Agency หรือ KISA เป็นหน่วยงานภายใต้กระทรวงวิทยาศาสตร์ ไอซีทีและแผนงานอนาคต (Ministry of Science, ICT and Future Planning: MSIP) ซึ่งดูแลศูนย์การรักษาความมั่นคงปลอดภัยอินเทอร์เน็ตเกาหลีใต้ หรือ Korea Internet Security Center (KISC) รวมถึงศูนย์ประสานงานการตอบโต้ฉุกเฉินด้านคอมพิวเตอร์ประเทศเกาหลี หรือ KrCERT/CC (Korea Computer Emergency Response Team Coordination Center) ซึ่งเป็นหน่วยงานประเภท CERT ขนาดใหญ่ มีบุคลากรด้านเทคนิคจำนวนมากทำหน้าที่ในการบริหารและจัดการความมั่นคงปลอดภัยของเครือข่ายอินเทอร์เน็ตของเกาหลีใต้ในหลายด้าน อาทิ การวิจัยและวิเคราะห์เหตุภัยคุกคามและการโจมตีทางไซเบอร์ การรับแจ้งเหตุและประสานการจัดการกับภัยคุกคามในเครือข่ายอินเทอร์เน็ตได้อย่างทันท่วงที รวมถึงทำหน้าที่เผยแพร่และส่งเสริมการสร้างความตระหนัก และพัฒนาทักษะบุคลากรด้านเทคนิคในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร เป็นต้น นอกจากนี้ KISA ยังมีหน้าที่ในการประชาสัมพันธ์ ฝึกอบรม Security Awareness ให้แก่ผู้ใช้งานหรือ End-User เพื่อให้เกิดความเข้าใจเรื่อง Information Security ในระดับที่สามารถป้องกันตนเองได้ โดย KISA ได้ออกหนังสือเกี่ยวกับความปลอดภัยข้อมูล และจัดงานสัมมนาด้านการป้องกันความปลอดภัยข้อมูลทุกปีในชื่องาน Information Security Week เพื่อเป็นการสร้างความเข้าใจด้านการรักษาความปลอดภัยข้อมูลให้กับสังคมของหน่วยงาน ผู้ใช้ระบบสารสนเทศและอินเทอร์เน็ต ให้เห็นถึงความสำคัญของการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ รวมทั้งเกาหลีใต้ยังได้มีการประกาศใช้นโยบายแผนแม่บทระบบสารสนเทศของประเทศเกาหลีใต้ที่เรียกว่า IT839 Strategy เพื่อผลักดันประเทศเกาหลีใต้ให้เป็นผู้นำในโลกสารสนเทศต่อไป

กล่าวโดยสรุปได้ว่า แนวคิดการป้องกันภัยคุกคามทางไซเบอร์ของสหรัฐอเมริกาเป็นการรักษาโครงสร้างระบบอินเทอร์เน็ต ขณะที่แนวคิดการป้องกันภัยคุกคามทางไซเบอร์ของเกาหลีใต้ให้ความสำคัญการคุ้มครองดูแลผู้ใช้งานและพัฒนาเทคโนโลยีในโลกอนาคต และการป้องกันภัยคุกคามทางไซเบอร์ของจีนมุ่งเน้นที่การรักษาความมั่นคงของรัฐเป็นสำคัญ ดังนั้น แนวทางการป้องกันภัยคุกคามไซเบอร์ของแต่ละประเทศนั้นจึงมีเอกลักษณ์ที่แตกต่างกัน ซึ่งรัฐบาลไทยสามารถนำแนวคิดในแต่ละด้านของแต่ละประเทศมาประยุกต์และเตรียมพร้อมรับมือภัยคุกคามไซเบอร์ เพื่อให้ประเทศไทยสามารถแข่งขันในโลกยุคดิจิทัลและระบบอินเทอร์เน็ตที่มีความสำคัญในการขับเคลื่อนสังคม เศรษฐกิจและการเมืองของประเทศ โดยมุ่งเน้นการรักษาความปลอดภัยข้อมูลเป็นสิ่งสำคัญ

5. แนวทางแก้ไขการป้องกันภัยคุกคามไซเบอร์

ปัจจุบันการทำงานผ่านเครือข่ายสารสนเทศและอินเทอร์เน็ตในประเทศไทย หลายองค์กรทั้งหน่วยงานรัฐและภาคเอกชนเริ่มปรับตัวยอมรับมากขึ้น ผ่านการสื่อสารออนไลน์และระบบเทคโนโลยีสารสนเทศขับเคลื่อนการทำงาน มีความคล่องตัว สะดวกและรวดเร็ว อย่างไรก็ตาม การทำงานผ่านระบบออนไลน์ทำให้ต้องเสี่ยงต่อความปลอดภัยทางไซเบอร์ของผู้ปฏิบัติงาน โดยพบว่ามีปัญหามากที่สุดในเรื่องความไม่ปลอดภัยของการทำงานที่มีการเชื่อมต่อจากภายนอกเข้าสู่องค์กร ซึ่งอาชญากรทางไซเบอร์สามารถเข้ามาแสวงหาผลประโยชน์ โดยมีรูปแบบเปลี่ยนแปลงไปตามความสนใจในช่วงเวลานั้น ๆ ของผู้ใช้ระบบออนไลน์และสร้างความเสียหายให้กับองค์กรได้ ไม่ว่าจะเป็นความเสียหายทางมูลค่าด้านการเงิน ความเสียหายทางด้านข้อมูล ซึ่งอาจส่งผลกระทบให้ภาพลักษณ์ขององค์กรขาดความน่าเชื่อถือ โดยภัยคุกคามทางไซเบอร์จากการปฏิบัติงานผ่านเครือข่ายสารสนเทศและอินเทอร์เน็ต เป็นภัยคุกคามที่เปิดช่องให้อาชญากรไซเบอร์เข้ามาสู่ระบบคอมพิวเตอร์ขององค์กรได้ ซึ่งจะต้องพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และปัญหาภัยคุกคามทางไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วยการใช้เทคโนโลยีดิจิทัลและนวัตกรรม โดยจะต้องทำการพัฒนาศักยภาพของบุคลากรด้านเทคนิคเชิงลึก ต้องอาศัยการฝึกฝนทักษะความเชี่ยวชาญ เพื่อให้มีศักยภาพในการป้องกัน ตรวจสอบ วิเคราะห์ ติดตาม และรับมือภัยไซเบอร์ในรูปแบบใหม่ ๆ และการสร้างความตระหนักรู้ ความเข้าใจพื้นฐานในการใช้งานระบบสารสนเทศและอินเทอร์เน็ตให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ให้กับทุกคนในองค์กรให้ปลอดภัยและปฏิบัติตัวได้อย่างถูกต้อง โดยภาครัฐจะต้องกำหนดมาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ดังนั้น ภาครัฐจึงจำเป็นต้องป้องกันและลดความเสี่ยงลงให้มากที่สุด ด้วยการดำเนินการที่ครอบคลุม ดังนี้ 1) ให้ความรู้และสร้างความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ 2) สร้างความตระหนักในการใช้งานเทคโนโลยีดิจิทัลและระบบอินเทอร์เน็ตให้กับประชาชนและทุกภาคส่วนที่เกี่ยวข้อง 3) สร้างขีดความสามารถและส่งเสริมการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานที่เกี่ยวข้อง และ 4) สนับสนุนให้มีการศึกษาและวิจัยการพัฒนาการแก้ปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อรับมือกับภัยคุกคามรูปแบบใหม่และเป็นการยกระดับการทำงานให้มีความเป็นมาตรฐานเทียบเท่าระดับสากลและเกิดความคุ้มค่าสูงสุด

6. บทสรุปและข้อเสนอแนะ

การกำหนดมาตรการและแนวทางด้านความมั่นคงปลอดภัยไว้ในกฎหมายที่เกี่ยวข้อง โดยให้ความสำคัญในด้านการป้องกันหรือลดความเสี่ยง การสร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และการกำหนดฐานความผิดและบทลงโทษ ซึ่งอาจครอบคลุมเพียงบางมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น จึงจำเป็นต้องยกระดับความเข้มแข็งเพื่อเตรียมความพร้อมของประเทศด้านดังกล่าวให้ครอบคลุมถึงมิติของการเฝ้าระวังภัยคุกคาม หรือการดำเนินการใด ๆ ที่จำเป็นเมื่อมีการโจมตี หรือเมื่อเกิดวิกฤติต่อความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการกำหนดมาตรการในการทำงานร่วมกันระหว่างหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ทั้งในภาครัฐและเอกชน เมื่อต้องเผชิญกับการโจมตี หรือภาวะวิกฤติดังกล่าวที่อาจส่งผลกระทบอย่างมีนัยสำคัญและรุนแรง อันส่งผลกระทบต่อความมั่นคงของประเทศได้ นอกจากนี้ ประเทศไทยยังขาดแนวทางปฏิบัติ และบรรทัดฐานในการบริหารจัดการไซเบอร์สเปซที่ชัดเจนในระดับภูมิภาคและระดับระหว่างประเทศ ซึ่งรัฐควรให้ความสำคัญกับการสนับสนุนให้มีบรรทัดฐานและแนวทางปฏิบัติระหว่างประเทศที่เป็นที่ยอมรับ ดังนั้น จึงจำเป็นต้องมีการผลักดันการจัดทำกรอบนโยบายหรือยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อส่งเสริมความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกันความขัดแย้งทางไซเบอร์ระหว่างรัฐอันอาจเกิดขึ้นได้ในอนาคต รวมทั้งปกป้องคุ้มครองบริการภาครัฐแม้จะโดนภัยคุกคามทางไซเบอร์แต่ยังสามารถรับมือไม่ให้เกิดความเสียหายในวงกว้างของสังคม และสามารถให้บริการประชาชนได้อย่างต่อเนื่องและมีประสิทธิภาพได้

1. ข้อเสนอแนะเชิงนโยบาย

หน่วยงานภาครัฐ ภาคธุรกิจ และภาคประชาชน ควรมีการพัฒนาความรู้และทักษะเทคโนโลยีในการรับมือและป้องกันภัยคุกคามไซเบอร์อย่างสม่ำเสมอ เพื่อให้ทุกคนตระหนักถึงความเสี่ยงของข้อมูลและการป้องกันภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ เป็นการส่งเสริมและสนับสนุนการแลกเปลี่ยนความรู้ในการป้องกันภัยคุกคามไซเบอร์ระหว่างหน่วยงานรัฐกับภาคเอกชน จะก่อให้เกิดการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อการพัฒนาระบบสารสนเทศด้านการแลกเปลี่ยนข้อมูลของหน่วยงาน ส่งผลให้ข้อมูลมีความถูกต้องแม่นยำ และเป็นข้อมูลที่มีคุณภาพ เพื่อให้หน่วยงานที่เกี่ยวข้องมีแผนรับมือภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ควรจัดตั้งระบบติดตามภัยคุกคามทางไซเบอร์ที่สามารถดำเนินการได้ในระดับชาติอย่างเป็นรูปธรรม ดังนี้

1) จัดตั้งหน่วยงานกลางด้านความมั่นคงไซเบอร์ (Cybersecurity Authority) เพื่อประสานงานกับหน่วยงานต่าง ๆ ในการป้องกันและรับมือกับภัยคุกคามไซเบอร์ เช่น การจัดทำกรอบนโยบาย การประเมินความเสี่ยงและการฝึกซ้อมรับมือกับเหตุการณ์

2) ออกกฎหมายและระเบียบข้อบังคับที่ทันสมัย ปรับปรุงและพัฒนากฎหมายเกี่ยวกับความปลอดภัยไซเบอร์ให้ทันต่อสถานการณ์ รวมถึงกำหนดบทลงโทษที่ชัดเจนสำหรับการกระทำผิดในโลกไซเบอร์ เช่น การละเมิดข้อมูลส่วนบุคคล การโจมตีระบบคอมพิวเตอร์และการหลอกลวงทางดิจิทัล

3) สร้างระบบสำรองข้อมูล (Backup) และแผนฟื้นฟูระบบ (Disaster Recovery) เพื่อให้สามารถกลับมาใช้งานได้อย่างรวดเร็วในกรณีเกิดการโจมตี เช่น การโจมตีแบบเรียกค่าไถ่ (Ransomware)

4) สนับสนุนการพัฒนาความรู้และทรัพยากรบุคคลด้านไซเบอร์ จัดทำแผนพัฒนาบุคลากรให้มีความเชี่ยวชาญเฉพาะด้าน เช่น การอบรมเจ้าหน้าที่ IT และเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ เพื่อให้มีทักษะและความพร้อมในการรับมือกับการโจมตีรูปแบบใหม่

2. ข้อเสนอแนะเชิงปฏิบัติ

การป้องกันภัยคุกคามทางไซเบอร์เป็นสิ่งจำเป็นที่ทุกภาคส่วนจะต้องมีส่วนช่วยในการรักษาความปลอดภัยและป้องกันภัยคุกคามที่อาจเกิดขึ้นกับตนเองหรือหน่วยงาน อันเนื่องจากการพึ่งพาระบบออนไลน์และเทคโนโลยีดิจิทัลในการดำเนินชีวิตและการปฏิบัติงาน ซึ่งนับวันจะกลายเป็นภัยคุกคามร้ายแรงมากขึ้น ดังนั้น ภาครัฐจึงจำเป็นต้องป้องกันและลดความเสี่ยงลงให้มากที่สุด ด้วยการดำเนินการที่ครอบคลุมดังนี้

1) เพิ่มระบบการตรวจจับและตอบสนองภัยคุกคามไซเบอร์ (Threat Detection and Response) ติดตั้งระบบที่สามารถตรวจจับการโจมตีไซเบอร์แบบเรียลไทม์ พร้อมทั้งพัฒนากระบวนการตอบสนองที่รวดเร็ว เช่น การกู้คืนข้อมูลและการปิดกั้นการเข้าถึงของผู้ไม่ประสงค์ดี

2) ประเมินความเสี่ยงอย่างสม่ำเสมอ จัดทำการประเมินความเสี่ยงทางไซเบอร์สำหรับระบบของหน่วยงานรัฐเป็นระยะ เช่น การตรวจสอบช่องโหว่ของระบบ การทดสอบเจาะระบบ (Penetration Testing) และการวิเคราะห์ภัยคุกคาม (Threat Intelligence)

3) กำหนดมาตรฐานความปลอดภัยทางไซเบอร์ระดับชาติ พัฒนามาตรฐานความปลอดภัยไซเบอร์ที่ชัดเจน เช่น การใช้ระบบป้องกันข้อมูลและเครือข่าย การจัดการสิทธิ์การเข้าถึง และการสำรองข้อมูล เพื่อลดช่องโหว่ในโครงสร้างพื้นฐานของรัฐ

4) ฝึกซ้อมสถานการณ์จำลอง (Cybersecurity Drills) จำลองการโจมตีทางไซเบอร์ในหน่วยงานรัฐ เพื่อเตรียมความพร้อมและปรับปรุงกระบวนการปฏิบัติงานเมื่อเผชิญกับเหตุการณ์จริง

5) ส่งเสริมการใช้เครื่องมือเข้ารหัสและการยืนยันตัวตนแบบหลายขั้นตอน (Encryption and Multi-Factor Authentication) สนับสนุนการใช้เทคโนโลยีเข้ารหัสข้อมูลสำคัญและระบบยืนยันตัวตนแบบหลายปัจจัย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

บรรณานุกรม

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. **ควรระวังความปลอดภัยจาก 'อาชญากรไซเบอร์' ช่วงวิกฤติโควิด 19**. สืบค้นเมื่อวันที่ 19 กุมภาพันธ์ 2568, จาก https://tcsd.go.th/ควรระวังปลอดภัยจาก/

กุณฑลี รื่นรมย์. **แนวทางการเขียนงานวิชาการ ประเภทงานวิจัย 2564**. สืบค้นเมื่อวันที่ 19 กุมภาพันธ์ 2568, จาก https://webs.rmutl.ac.th/assets/upload/files/2021/07/20210727103523_75666.pdf

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภาระยะ 4 ปี (พ.ศ. 2562-2565). **นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา**. สืบค้นเมื่อวันที่ 21 กุมภาพันธ์ 2568, จาก https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=70952&filename=gennews_section9

คมชัดลึกออนไลน์. **ภัยคุกคามไซเบอร์ ไทยพุ่ง สกมช. ยกระดับความปลอดภัยป้องกันแฮกเกอร์**. สืบค้นเมื่อวันที่ 19 กุมภาพันธ์ 2568, จากhttps://www.komchadluek.net/news/economic/538875

ปรีดี นุกุลสมปรารถนา. **Critical Thinking สิ่งจำเป็นสำหรับการทำงานยุคใหม่**. สืบค้นเมื่อวันที่ 12 กุมภาพันธ์ 2568, จาก https://www.popticles.com/business/critical-thinking-for-today-work/

ผู้จัดการออนไลน์. **DSI ดึงเยาวชนร่วมเป็นหูเป็นตาจับอาชญากรรมทางเน็ต**. สืบค้นเมื่อวันที่ 14 กุมภาพันธ์ 2568, จาก https://mgronline.com/crime/detail/9510000093187

ราชกิจจานุเบกษา. **พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**. สืบค้นเมื่อวันที่ 12 กุมภาพันธ์ 2568, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PD

ราชกิจจานุเบกษา. **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**. สืบค้นเมื่อวันที่ 12 กุมภาพันธ์ 2568, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

ราชกิจจานุเบกษา. **พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550**. สืบค้นเมื่อวันที่ 21 กุมภาพันธ์ 2568, จาก https://citcoms.nu.ac.th/wp-content/uploads/2018/03/law-computer2550.pdf

ศูนย์ไซเบอร์กองทัพบก. **ประวัติศูนย์ไซเบอร์กองทัพบก**. สืบค้นเมื่อวันที่ 21 กุมภาพันธ์ 2568, จาก https://cyber.rta.mi.th/about.php

สรณันท์ จิวะสุรัตน์ และ ชัยชนะ มิตรพันธ์. **ความเป็นมาของไทยเซิร์ต จากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที**. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). สืบค้นเมื่อวันที่ 4 กุมภาพันธ์ 2568, จาก https://www.thaicert.or.th/papers/general/2012/pa2012ge001.html

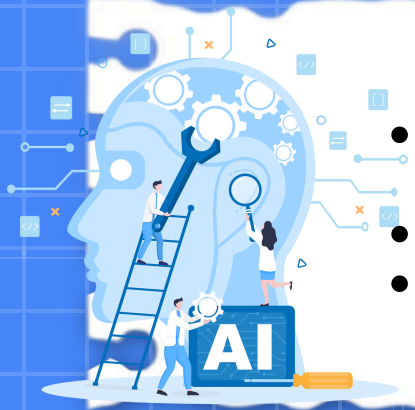
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. **สถิติภัยคุกคาม ประจำปี พ.ศ. 2565**. สืบค้นเมื่อวันที่ 10 กุมภาพันธ์ 2568, จาก https://www.etda.or.th/th/Our-Service/thaicert/ stat.aspx

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). ประวัติความเป็นมา. สืบค้นเมื่อวันที่ 1 กุมภาพันธ์ 2568, จาก https://www.dga.or.th/th/profile/810/

ภัยคุกคามไซเบอร์ในภาครัฐ
ความท้าทายใหม่ในยุคดิจิทัล

ภัยคุกคามไซเบอร์ในภาครัฐ

- การโจมตีทางไซเบอร์ที่มุ่งเป้าไปยังภาครัฐ เช่น การขโมยข้อมูล การโจมตีแบบ DDos และการเจาะระบบสำคัญ
- ความเสี่ยงต่อข้อมูลส่วนบุคคล โครงสร้างพื้นฐานสำคัญ และความมั่นคงของประเทศ



แนวปฏิบัติที่ดีของต่างประเทศ

- สหรัฐอเมริกา : ตั้ง CISA (Cybersecurity and Infrastructure Security Agency)
- จีน : ใช้ระบบเฝ้าระวังที่เข้มงวด (Great Firewall)
- เกาหลีใต้ : สร้าง Cyber Command และลงทุนในระบบ Ai

ข้อเสนอแนะเพื่อป้องกันภัยคุกคามไซเบอร์

- เสริมสร้างความร่วมมือระหว่างประเทศ
- พัฒนาบุคลากรด้านไซเบอร์
- ใช้ Ai และ Machine Learning
- ปรับปรุงกฎหมายให้สอดคล้องกับภัยคุกคามใหม่ ๆ
- สนับสนุนการพัฒนาระบบป้องกันไซเบอร์ที่ทันสมัย

- ภัยคุกคามไซเบอร์ในภาครัฐเป็นความท้าทายสำคัญในยุคดิจิทัล
- ทุกประเทศต้องเสริมสร้างมาตรการป้องกันในทุกมิติ ตั้งแต่เทคโนโลยี กฎหมาย และความร่วมมือระหว่างประเทศ

ความปลอดภัยไซเบอร์วันนี้
คือความมั่นคงของประเทศในอนาคต