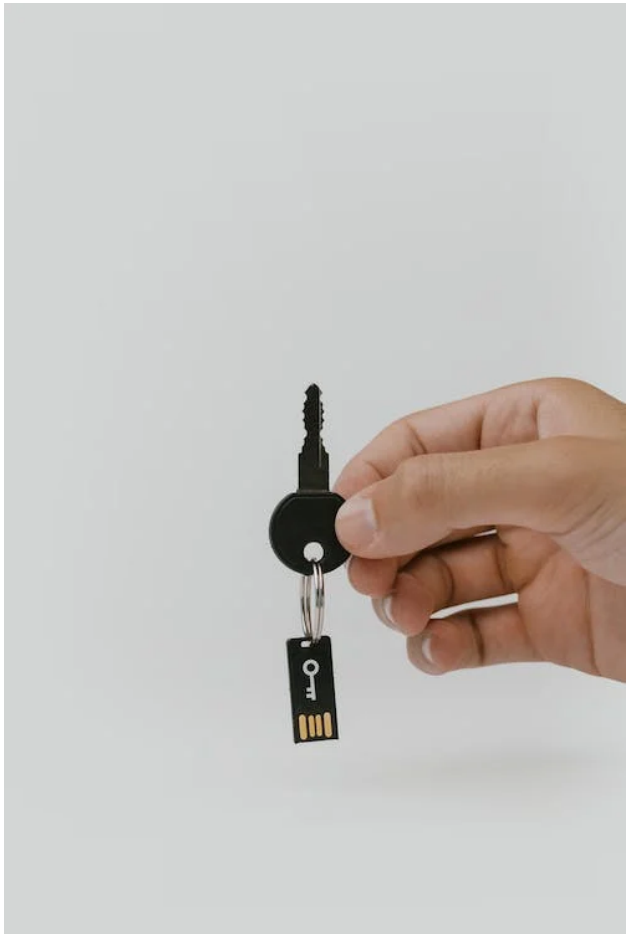
เส้นทางการเตรียมความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) ของประเทศไทย: เข้าใจอุปสรรค และค้นหาวิธีแก้ไข

อาจารย์ปวีร์ เจนวีระนนท์ อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ แบ่งปันมุมมองของเขา และสะท้อนถึงประเด็นว่าประเทศไทยสามารถที่จะปรับตัวอย่างไรในการรับมือกับลักษณะภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่พัฒนาอย่างรวดเร็ว บทความนี้สร้างขึ้นจากงานวิจัยล่าสุดของ *Tech For Good Institute (TFGI)* เกี่ยวกับความพร้อมในการรับมือภัยคุกคามไซเบอร์ *(Cyber resilience)*

อ่านงานวิจัยของ TFGI ได้ที่นี่



โดยอาจารย์ปวีร์ เจนวีระนนท์ อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ประเทศไทย

งานศึกษาเรื่อง Towards a Resilient Cyberspace in Southeast Asia ได้มีข้อเสนอเกี่ยว

กับกรอบความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber Resilience Framework) เพื่อส่งเสริมเศรษฐกิจดิจิทัลที่ปลอดภัย มั่นคง และยืดหยุ่นในภูมิภาค โดยได้ให้คำนิยาม กำหนดความหมายของความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) หรือยืดหยุ่นทางไซเบอร์ ระบุ

ส่วนที่สามารถทำให้ดีขึ้นได้ และแนะนำการเพิ่มการลงทุนในผู้คน กระบวนการ และเทคโนโลยี กรอบ หรือแนวทางดังกล่าวสามารถใช้ในการอ้างอิงเพื่อกำหนดแผนงานทางไซเบอร์ในอนาคตและสนับสนุนกลยุทธ์ระยะยาว ในบริบทของประเทศไทย กรอบ หรือแนวทางนี้สามารถนำไปใช้เพื่อพัฒนานโยบายเชิงปฏิบัติที่ส่งเสริมเศรษฐกิจดิจิทัลที่ปลอดภัย และยืดหยุ่นได้

ภูมิทัศน์ของความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) ในประเทศไทย

เช่นเดียวกับประเทศอื่น ๆ ในภูมิภาค ประเทศไทยไม่อาจหลีกเลี่ยงจากความเสี่ยง และความท้าทายที่เกิดจากภัยคุกคามทางไซเบอร์ จากข้อมูลของธนาคารแห่งประเทศไทย (ธปท.) เห็นได้ว่าประเทศไทยมีความเปราะบางในการรับมือทางไซเบอร์ โดยเบื้องต้นนั้นสาเหตุมาจากในเรื่องของบุคลากรภาคการธนาคาร และการเงินมีความก้าวหน้าอย่างมากในด้านความยืดหยุ่น อย่างไรก็ดีภาคส่วนอื่น เช่น อุตสาหกรรมด้านการดูแลสุขภาพก็ยังอยู่ในระยะเริ่มต้นของการพัฒนาการป้องกัน เพื่อลดช่องว่างในเรื่องของความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) ดังกล่าว ก็มีการริเริ่มเช่นกรอบ Cyber Resilience Assessment Framework (CRAF) และโครงการยกระดับทักษะที่มีเป้าหมายเพื่อเพิ่มขีดความสามารถของประเทศไทย อย่างไรก็ตาม เพื่อขับเคลื่อนประเทศไทยให้ก้าวไปข้างหน้าบนเส้นทางสู่ความยืดหยุ่นทางไซเบอร์ ผู้มีส่วนเกี่ยวของหลักในเรื่องเศรษฐกิจดิจิทัลจะต้องพิจารณาสิ่งที่ต้องดำเนินการอย่างเร่งด่วนตามลำดับความสำคัญ

1. การพัฒนานโยบายความปลอดภัยทางไซเบอร์ และกรอบการกำกับดูแลที่เหมาะสม

การพัฒนากลยุทธ์เกี่ยวกับความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ และสามารถยืดหยุ่นปรับเปลี่ยนได้มีความสำคัญอย่างยิ่งสำหรับประเทศไทย กลยุทธ์นี้ควรสอดคล้องกับบรรทัดฐานสากล ส่งเสริมบทบาทของผู้ให้บริการด้านไอทีในการต่อสู้กับภัยคุกคามทางไซเบอร์ และสร้างระบบนิเวศที่ส่งเสริมนวัตกรรม และนำเสนอทางออกในเรื่องของความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพสำหรับผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญ และผู้เข้าร่วมในตลาด (market participants)ความท้าทายนี้ไม่ได้เกิดขึ้นเฉพาะในประเทศไทย แต่ส่งผลกระทบต่อหลายประเทศทั่วโลก

การออกกฎหมายเพื่อส่งเสริมความปลอดภัยทางไซเบอร์เป็นความท้าทายที่สำคัญ สิ่งสำคัญคือต้องจัดการกับข้อกังวลเกี่ยวกับการเข้าถึงข้อมูลของรัฐบาล และสร้างความมั่นใจว่าระบบตรวจสอบและถ่วงดุลเข้มแข็ง เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต และอาจผิดกฎหมาย การสร้างสมดุลอย่างระมัดระวังเป็นสิ่งจำเป็น เพื่อให้อำนาจแก่เจ้าหน้าที่อย่างพอเหมาะ เพื่อวัตถุประสงค์ด้านความมั่นคงของชาติ และการบังคับใช้กฎหมาย ในขณะเดียวกันก็ป้องกันการใช้อำนาจอย่างไม่ถูกต้องที่อาจจะเกิดขึ้นได้

ดังนั้น รากฐานที่มั่นคงสำหรับเศรษฐกิจดิจิทัลจึงอยู่ในกรอบการกำกับดูแลที่ครอบคลุมอุตสาหกรรมต่าง ๆ จำเป็นต้องมีความเข้าใจที่ชัดเจน และความมั่นใจเกี่ยวกับการบังคับใช้กฎหมายและมาตรการต่าง ๆ ของรัฐบาล ความโปร่งใสผ่านการออกระเบียบ กฎเกณฑ์ หรือแนวปฏิบัติเป็นสิ่งสำคัญ ซึ่งความสมบูรณ์ของนโยบายนั้นต้องใช้เวลา และการประเมินอย่างสม่ำเสมอเป็นสิ่งจำเป็นเพื่อให้แน่ใจถึงความเกี่ยวข้อง และประสิทธิผลที่ต่อเนื่อง

นอกจากนี้ ทางการไทยควรพิจารณานำแนวปฏิบัติ หรือมาตรฐานที่เป็นที่ยอมรับทั่วโลก เช่นกรอบ NIST Cybersecurity Framework (CSF) และ TFGI's resilience framework มาพัฒนาเป็นกรอบแนวทางของตนเอง ซึ่งจะทำให้สามารถสร้างกรอบการรับมือ และประเมินความยืดหยุ่นของภาครัฐที่ครอบคลุม การนำกรอบเหล่านี้ไปใช้จะช่วยให้หน่วยงานภาครัฐของไทยมีวิธีการที่สอดคล้องกันในการประเมินมาตรการรับมือทางไซเบอร์ และระบุประเด็นที่น่ากังวล นอกจากนี้ สิ่งสำคัญคือต้องปรับกรอบให้สอดคล้องกับข้อกำหนด และมาตรฐานที่เกี่ยวข้องกับไซเบอร์อื่น ๆ รวมถึงข้อกำหนดและมาตรฐานภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (the General Data Protection Regulation (GDPR)), the Security of Network and Information Systems (NIS) Directive และมาตรฐานอื่น ๆ ที่บังคับใช้ นอกเหนือจากกรอบ NIST Cybersecurity Framework (CSF) และ TFGI's resilience Framework

แม้ว่าจะมีเครื่องมือทางกฎหมายที่พัฒนาขึ้นในช่วงหลายปีที่ผ่านมาซึ่งสะท้อนถึงนโยบายความปลอดภัยทางไซเบอร์ (เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น) และถูกบังคับใช้กับภาคส่วนที่แตกต่างกันออกไป อย่างไรก็ตาม ยังไม่เห็นความพยายามในการที่จะทำให้เครื่องมือทางกฎหมายเหล่านี้เป็นอันหนึ่งอันเดียวกันในการส่งเสริมยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทยโดยรวม

เพื่อปรับปรุงท่าทีด้านความมั่นคงปลอดภัยทางไซเบอร์โดยรวมของประเทศไทย จำเป็นอย่างยิ่งที่จะต้องบูรณาการ และประสานเครื่องมือทางกฎหมายที่มีอยู่ให้เป็นกรอบการทำงานที่เป็นเอกภาพ นอกจากนี้ การใช้ประโยชน์จากแนวปฏิบัติที่เป็นที่ยอมรับทั่วโลกเป็นสิ่งสำคัญเพื่อหลีกเลี่ยงความพยายามที่ซ้ำซ้อน เติมเต็มช่องว่างในแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ และเพิ่มขีดความสามารถในเรื่องความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience)

2. การเสริมสร้างความร่วมมือระหว่างภาครัฐ และเอกชน และส่งเสริมความร่วมมือในประเทศ และต่างประเทศ

ประเทศไทยต้องสร้างสภาพแวดล้อมของตลาดที่เปิดกว้างสำหรับผู้ให้บริการเทคโนโลยีที่เสนอแนวทางการแก้ปัญหา (solutions) การรักษาความปลอดภัยที่เชื่อถือได้สำหรับทั้งรัฐบาล และโครงสร้างพื้นฐานที่สำคัญ

การร่วมมือกันเป็นสิ่งสำคัญสู่ความก้าวหน้า สิ่งนี้ต้องการกฎระเบียบที่สอดคล้องกับรูปแบบธุรกิจในอุตสาหกรรมต่างๆ เพื่อเสริมสร้างความปลอดภัยและความยืดหยุ่น (resilience) รัฐบาลจำเป็นต้องสร้างความสัมพันธ์แบบร่วมมือกับผู้เข้าร่วมในตลาด แสวงหาความเชี่ยวชาญของเขา และเข้าใจในความสามารถ และความเต็มใจที่จะมีส่วนร่วม นี่เป็นสิ่งสำคัญ ในขณะที่รัฐบาลดำเนินมาตรการเพื่อป้องกันการโจมตีทางไซเบอร์ในอนาคต รวมถึงการปรับใช้โครงสร้างพื้นฐานดิจิทัล การเพิ่มขีดความสามารถด้านข่าวกรองภัยคุกคาม และการปรับปรุงการป้องกันปลายทาง (endpoint protection)

นอกจากนี้ ความร่วมมือระหว่างหน่วยงานระหว่างหน่วยงานรัฐบาล และกระทรวงต่าง ๆ เป็นสิ่งจำเป็น กฎระเบียบสำหรับภาคส่วนต่าง ๆ เช่น การธนาคาร การเงิน การขนส่ง และสาธารณูปโภค

อาจแตกต่างกันไป ในขณะที่ผู้ให้บริการด้านไอที และคลาวด์มักจะดำเนินการในลักษณะข้าม หรือหลายภาคส่วน และเขตอำนาจศาล การทำให้แน่ใจถึงความสอดคล้องต้องกันของกฎระเบียบเหล่านี้เป็นสิ่งสำคัญเพื่อหลีกเลี่ยงความขัดแย้งที่อาจจะเกิดขึ้นได้

ประการสุดท้าย ความร่วมมือระหว่างประเทศระหว่างประเทศ พันธมิตร และคู่ค้าที่มีแนวคิดเดียวกันมีความสำคัญ เนื่องจากทางออก หรือข้อเสนอเกี่ยวกับความปลอดภัยทางไซเบอร์ และภัยคุกคามอยู่เหนือพรมแดน (มีลักษณะที่เกี่ยวพันกันระหว่างประเทศ) ความร่วมมือในระดับนานาชาติจึงมีความสำคัญ

3. **ส่งเสริมทักษะด้านดิจิทัล และเพิ่มพูนความรู้ทางไซเบอร์**

ความต้องการมืออาชีพที่มีทักษะสูงในภาคส่วนความปลอดภัยทางไซเบอร์ของไทย เน้นย้ำถึงความจำเป็นในการบ่มเพาะความเชี่ยวชาญด้านดิจิทัล และเพิ่มพูนความรู้ทางไซเบอร์ การเชื่อมช่องว่างของทักษะผ่านโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ที่มีการดำเนินการ ปรับใช้อย่างเหมาะสม เป็นสิ่งจำเป็น และเพิ่มโอกาสที่ดีในการลงทุน

นอกจากนี้ การส่งเสริมการมีส่วนร่วมของผู้หญิงในการศึกษาด้านวิทยาการคอมพิวเตอร์ที่มากขึ้น ก็สามารถช่วยขยายกำลังคนได้ นอกจากนี้ ควรมีโอกาสสำหรับบุคคลที่ทำงานมาถึงช่วงกลางอาชีพ (mid-career individuals) ในการเปลี่ยนสายอาชีพไปสู่สายอาชีพทางด้านเทคโนโลยีเช่นเดียวกับแนวโน้มที่พบในประเทศสหรัฐอเมริกา

เพื่อให้บรรลุเป้าหมายเหล่านี้ รัฐบาลไทย ควรลงทุนในโครงการฝึกอบรม และพัฒนาเพื่อเพิ่มพูนความชำนาญของบุคลากรด้านไอทีในหน่วยงานภาครัฐ และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญ (CII) การร่วมมือกับผู้ให้บริการบุคคลที่สาม และส่งเสริมการแบ่งปันความรู้ระหว่างหน่วยงานที่เกี่ยวข้องก็มีความสำคัญต่อการพัฒนาทักษะดิจิทัล และปรับปรุงความรู้ทางไซเบอร์

ในขอบเขตของการรักษาความปลอดภัยทางไซเบอร์ ทักษะที่สำคัญสามประการได้กลายเป็นสิ่งสำคัญยิ่ง ประการแรก ความเชี่ยวชาญในการประมวลผลแบบคลาวด์ (cloud computing) เป็นสิ่งที่ต้องมี เนื่องจากมีการพึ่งพาที่เก็บข้อมูลดิจิทัลเพิ่มขึ้น ทักษะที่สำคัญที่สุดประการที่สองคือการวิเคราะห์ข่าวกรองภัยคุกคาม ซึ่งทำให้คนทำงานสามารถ คาดการณ์และตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ประการสุดท้าย การประเมินความเสี่ยงก็มีความสำคัญต่อความปลอดภัยในโลกไซเบอร์ เพื่อทำความเข้าใจ และลดช่องโหว่ และภัยคุกคามที่อาจเกิดขึ้น

4. ให้จัดสรรงบประมาณเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศ

รัฐบาลต้องจัดสรรเงินทุนสำหรับงานต่างๆ ที่จำเป็นต่อการบรรลุวัตถุประสงค์ดังกล่าวข้างต้น งานเหล่านี้รวมถึงแต่ไม่จำกัดเพียงการขยายบุคลากรด้านความปลอดภัยทางไซเบอร์ การเพิ่มความสามารถด้านวิทยาการข้อมูล และข่าวกรองภายในภาครัฐ และการจัดตั้งหน่วยงานเฉพาะ หรือหน่วย

งานป้องกันเพื่อตอบโต้การโจมตีทางไซเบอร์ รัฐบาลควรจัดลำดับความสำคัญ และให้ความสำคัญในเรื่องของการลงทุนในมาตรการรักษาความปลอดภัยทางไซเบอร์

รัฐบาลไทยควรพิจารณาแก้ไขพระราชบัญญัติการจัดซื้อจัดจ้างภาครัฐเพื่อให้เจ้าหน้าที่มีความยืดหยุ่นมากขึ้นในการดำเนินโครงการพัฒนาที่มีประสิทธิภาพ นอกจากนี้ แนวทางปฏิบัติที่ชัดเจนยังจำเป็นเพื่อให้แน่ใจว่ามีการบังคับใช้กฎหมายเป็นไปในทิศทางเดียวกัน สม่ำเสมอ และยังเป็นการสร้างความมั่นใจแก่ผู้ให้บริการด้านไอที

โดยสรุป เส้นทางสู่ความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) ของประเทศไทยจำเป็นต้องมีแนวทางที่ครอบคลุม ซึ่งรวมถึง การพัฒนานโยบาย และกรอบความปลอดภัยทางไซเบอร์ที่เหมาะสม ส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนโดยเน้นที่การฝึกฝนทักษะด้านดิจิทัล และให้ความสำคัญกับการลงทุนเพื่อเตรียมการในด้านความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience)โดยใช้มาตรการเหล่านี้ และส่งเสริมระบบนิเวศความร่วมมือ ประเทศไทยจะสามารถทำงานเพื่อมุ่งสู่เศรษฐกิจดิจิทัลที่ปลอดภัย ซึ่งจะช่วยให้เกิดสังคมดิจิทัลที่ทุกภาคส่วนเชื่อมั่น

เกี่ยวกับผู้เขียน

อาจารย์ปวีร์ เจนวีระนนท์ เป็นอาจารย์ประจำที่คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ประเทศไทย เขายังเป็นนักวิจัยที่ศูนย์วิจัยว่าด้วยการเงินทางเลือก (Cambridge Centre for Alternative Finance (CCAF)) **ที่คณะบริหารธุรกิจ มหาวิทยาลัยเคมบริดจ์** (Judge Business School, University of Cambridge) **ก่อนหน้านี้ เขาดำรงตำแหน่งเป็นผู้เชี่ยวชาญทางด้านกฎเกณฑ์เศรษฐกิจดิจิทัลของกลุ่มธนาคารโลก** (World Bank Group) **เป็นที่ปรึกษาให้กับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์** (ETDA) **ในโครงการเกี่ยวกับการกำกับดูแลเทคโนโลยีเกิดใหม่ (เทคโนโลยีบล็อกเชน) และบริการการพิสูจน์ยืนยันตัวตนทางดิจิทัล นอกจากนี้เขายังเป็นอดีตคณะกรรมการสมาคมฟินเทคประเทศไทย**