พลวัตความมั่นคงทางไซเบอร์ของประเทศไทย

กนกนก โพธิ์หอม [1]

บทนำ

ปัจจุบันเทคโนโลยีทางไซเบอร์ได้มีการพัฒนาไปอย่างก้าวกระโดด ซึ่งพื้นที่ไซเบอร์ได้กลายเป็นปัจจัยหนึ่งสำหรับการดำรงชีวิตของคนในสังคม เมื่อเทคโนโลยีมีการพัฒนามากขึ้น การเข้าถึงเทคโนโลยีของผู้คนจึงเป็นไปได้โดยสะดวกมากขึ้นตาม โดยเทคโนโลยีทางไซเบอร์ที่พัฒนาและเป็นที่นิยมอย่างมากในปัจจุบัน ได้แก่ เทคโนโลยีทางไซเบอร์ในการค้นหาข้อมูล (Search Engine) เช่น Google Yahoo เป็นต้น เทคโนโลยีไซเบอร์ในรูปแบบพื้นที่ทางสังคม อาทิ Facebook, Twitter, Instagram, Line, Youtube หรือ ระบบการประชุมทางไกล (Video Conferencing) ที่กลายมาเป็นช่องทางการติดต่อสื่อสารระหว่างหน่วยงานในสภาวการณ์ปัจจุบัน ซึ่งเมื่อประชาชนสามารถใช้พื้นที่ทางไซเบอร์ในการทำกิจกรรมต่างๆ เช่น การพบปะสังสรรค์ การเสพข่าวสาร – สื่อบันเทิง รวมไปถึงการทำธุรกรรมทางการเงิน ส่งผลให้รัฐจำเป็นจะต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยให้กับพื้นที่ทางไซเบอร์กับเหตุการณ์ที่มีโอกาสเกิดขึ้นได้ไม่ว่าจะเป็นการโจรกรรมข้อมูลทางไซเบอร์ การทำลายข้อมูลทางไซเบอร์ รวมไปถึงการใช้พื้นที่ทางไซเบอร์ในการก่ออาชญากรรม หรือวินาศกรรม เป็นต้น เพื่อเป็นการประกันความปลอดภัยต่อประชาชนและเป็นการรักษาอธิปไตยในพื้นที่ทางไซเบอร์ของประเทศไทย

บริบททางไซเบอร์ของประเทศไทย

นับตั้งแต่กระแสของโลกาภิวัตน์ (Globalization) ที่ทำให้เกิดการกระชับแน่นของบริบทโลกทั้งเวลาและสถานที่ที่มีความต่างกัน (Time and Space Compression) มีความเข้มข้นขึ้นในช่วงสองทศวรรษที่ผ่านมา โลกได้มีการพัฒนาเทคโนโลยีโดยเฉพาะเทคโนโลยีทางไซเบอร์อย่างมาก เพื่อสร้างความสะดวกสบายและทางเลือกสำหรับ

[1] นักวิเคราะห์นโยบายและแผนปฏิบัติการ กองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ สำนักงานสภาความมั่นคงแห่งชาติ, รัฐศาสตรบัณฑิต (การระหว่างประเทศ) คณะรัฐศาสตร์และรัฐประศาสนศาสตร์ มหาวิทยาลัยเชียงใหม่

การใช้ชีวิตประจำวัน ในส่วนของประเทศไทย การพัฒนาทางเทคโนโลยีไม่ว่าจะเป็นการพัฒนาของเทคโนโลยีด้านการสื่อสาร เทคโนโลยีด้านพื้นที่สังคมออนไลน์ หรือแม้กระทั่งเกมออนไลน์เกิดการพัฒนามากขึ้นจนสามารถเข้าถึงผู้คนได้อย่างง่ายดาย หลายเทคโนโลยีได้กลายมาเป็นธุรกิจและอุตสาหกรรมการผลิตที่สำคัญของประเทศ เช่น การผลิตชิ้นส่วนอิเล็กทรอนิกส์ ธุรกิจโทรคมนาคม สารสนเทศ หรืออุตสาหกรรมเกมออนไลน์ เป็นต้น โดยจากปี 2562 ที่ประเทศไทยมีสถิติของผู้ใช้อินเทอร์เน็ตมากกว่า 47.5 ล้านคน หรือ ประมาณร้อยละ 70 ของประชากรในประเทศไทย [2] โดยครอบคลุมการใช้งานหลายรูปแบบทั้งการใช้งานแบบส่วนตัว การใช้งานในเชิงธุรกิจหรือการใช้งานในหน่วยงานของรัฐ

การที่พื้นที่ทางไซเบอร์ถูกใช้ประโยชน์อย่างแพร่หลาย ความพยายามในการใช้ช่องทางดังกล่าวเพื่อแสวงหาประโยชน์ก็เพิ่มขึ้นตามไปด้วยเนื่องจากพื้นที่ทางไซเบอร์เป็นพื้นที่เสมือนที่มูลค่าสูง อีกทั้งรัฐยังไม่ได้มีเครื่องมือในการป้องกันการกระทำผิดในพื้นที่ทางไซเบอร์ที่มีประสิทธิภาพมากนัก จึงส่งผลให้เกิดการถูกคุกคามหรือก่ออาชญากรรมในพื้นที่ทางไซเบอร์ ซึ่งประเทศไทยถูกจัดให้อยู่ในอันดับที่ 4 ของโลกในการแจ้งเหตุภัยคุกคามทางไซเบอร์ ซึ่งขึ้นจากอันดับที่ 6 จากปีก่อนหน้า โดยภัยคุกคามทางไซเบอร์ทั่วโลกรูปแบบต่าง ๆ ในปี 2563 เกิดขึ้นแล้วจำนวนกว่า 1,744 ครั้ง ในช่วง 8 เดือนที่ผ่านมา และมีแนวโน้มเพิ่มมากขึ้นอย่างต่อเนื่อง [3] จากการที่บุคคลมีการเชื่อมโยงกับพื้นที่ทางไซเบอร์มากขึ้น โดยความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามไซเบอร์เป็นสาเหตุและปัจจัยหลักที่ส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจ คุณภาพชีวิต หรือความมั่นคงของประเทศ ตลอดจนนโยบายของรัฐบาลที่กำลังขับเคลื่อนสู่ยุคเศรษฐกิจดิจิทัล หรือ ไทยแลนด์ 4.0

[2] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, (2563), ETDA เผย ปี 62 คนไทยใช้อินเทอร์เน็ตเพิ่มขึ้นเฉลี่ย 10 ชั่วโมง 22 นาที Gen Y ครองแชมป์ 5 ปีซ้อน, (ออนไลน์), https://www.etda.or.th/th/NEWS/ETDA-Revealed-Thailand-Internet-User-Behavior-2019.aspx สืบค้นเมื่อวันที่ 30 มีนาคม 2564

[3] DEPA, (2563), ดีป้า-ม.ศรีปทุม-อินโฟเฟด ผนึกกำลังปั้นขุนพล Cyber Security, (ออนไลน์), https://www.depa.or.th/th/article-view/20201117_04, สืบค้นเมื่อวันที่ 30 มีนาคม 2564

ภัยคุกคามทางไซเบอร์ต่อประเทศไทย

ประเทศไทยได้ตระหนักถึงปัญหาของความมั่นคงทางไซเบอร์ที่เพิ่มความสำคัญขึ้น ซึ่งจะสังเกตได้จากการมีกฎหมายที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ หรือการมีหน่วยงานด้านความมั่นคงทางไซเบอร์ โดยรัฐบาลได้มีวิสัยทัศน์ในการรับมือกับภัยคุกคามรูปแบบใหม่ที่มีการเปลี่ยนแปลงอย่างรวดเร็วทันต่อการขับเคลื่อนของโลกสมัยใหม่[4] สำหรับปัญหาด้านความมั่นคงทางไซเบอร์นั้น ประเทศไทยเป็นประเทศหนึ่งที่มีความเสี่ยงที่จะตกเป็นพื้นที่กระทำการก่อการร้ายทางไซเบอร์โดยรัฐ บุคคล หรือกลุ่มบุคคล ตลอดจนผู้ก่อการร้าย ซึ่งการก่อการร้ายทางไซเบอร์ยังหมายรวมไปถึงการนำสื่อออนไลน์ไปใช้เป็นเครื่องมือในการเผยแพร่แนวคิดที่นิยมการใช้ความรุนแรง หรือการสอนการก่อการร้าย การจัดหาอาวุธและวัสดุที่ใช้ประกอบเป็นอาวุธ รวมทั้งสอนวิธีการทำ การหาสมาชิกเพื่อมาร่วมอุดมการณ์การก่อการร้ายอีกด้วย

โดยประเด็นปัญหาที่กล่าวมาข้างต้น ส่งผลให้ประเทศไทยต้องพัฒนาขีดความสามารถในการควบคุมพื้นที่ทางไซเบอร์ที่จะก่อให้เกิดความมั่นคงทางไซเบอร์ที่เพิ่มมากขึ้น การเตรียมพร้อมนี้อาจรวมไปถึงเหตุการณ์ที่อาจเกิดขึ้นในอนาคต อย่างเช่นการทำสงครามทางไซเบอร์ ซึ่งหากประเทศไทยมีการดำเนินการอย่างเหมาะสม ก็จะทำให้สามารถปกป้องผลประโยชน์แห่งชาติได้ ปัญหาอีกประการหนึ่ง คือ ปัญหาการขาดความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะการใช้อินเทอร์เน็ต ที่มักจะให้ความสำคัญกับความมั่นคงทางไซเบอร์เป็นลำดับรอง ซึ่งจะส่งผลต่อความมั่นคงทางไซเบอร์ในภาพรวม โดยประเทศไทยได้ดำเนินการคือการเฝ้าระวังภัยคุกคามในรูปแบบใหม่ที่จะสร้างความเสียหายให้แก่ประเทศและสร้างความเดือดร้อนแก่ประชาชนที่ใช้งาน หากข้อมูลด้านความมั่นคงถูกเข้าถึงได้โดยปราศจากความยินยอมของภาครัฐจะส่งผลทำให้ขาดเสถียรภาพด้านความมั่นคง

---

[4] สำนักงานพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, (2561), ยุทธศาสตร์ชาติ พ.ศ. 2561-2580, กรุงเทพฯ: สำนักงานพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

มุมมองด้านความมั่นคงทางไซเบอร์

เนื่องจากความเปลี่ยนแปลงของเทคโนโลยีและกระแสโลกาภิวัตน์ ส่งผลต่อความสำคัญของการใช้พื้นที่ทางไซเบอร์ในโลก ในมุมมองของรัฐ พื้นที่ทางไซเบอร์จะมีความเสี่ยงที่จะเป็นภัยคุกคามของรัฐอย่างแน่นอน เนื่องจากการใช้พื้นที่ทางไซเบอร์ทั่วโลกถูกเชื่อมต่อกันอย่างสมบูรณ์ จึงทำให้เกิดมูลค่าทางเศรษฐกิจ [5] ที่สามารถนับได้ว่าจะเป็นผลประโยชน์แห่งชาติได้ จากมุมมองดังกล่าว สามารถมองความมั่นคงทางไซเบอร์ตามแนวคิด “การทำให้เป็นความมั่นคง” (Securitization) โดยการที่รัฐจะระบุให้ประเด็นใดเป็นประเด็นความมั่นคงที่รัฐต้องให้ความสำคัญนั้น ประเด็นดังกล่าวจะต้องเป็นสิ่งที่เกิดขึ้นอย่างเป็นสากล และมีแนวโน้มจะเกิดขึ้นในประเทศไทยด้วย และจำเป็นจะต้องมีการนิยามให้ชัดเจนว่าเรื่องหรือประเด็นใดที่จะถือว่าเป็นภัยความมั่นคง เป็นภัยความมั่นคงในรูปแบบใด และภัยความมั่นคงนี้จะทำให้รัฐเสียผลประโยชน์แห่งชาติอย่างไรได้บ้าง [6]

สำหรับการกำหนดคำนิยามของความมั่นคงทางไซเบอร์ของประเทศไทย มีการกำหนดคำนิยามจากหน่วยงานพลเรือนและหน่วยงานทหาร โดยหน่วยงานพลเรือนได้กำหนดคำนิยามแบบกว้าง เพื่อให้เป็นการฉายภาพของความมั่นคงทางไซเบอร์ในภาพรวม คือ การกระทำความผิดหรือทำลายความมั่นคงของประเทศผ่านระบบคอมพิวเตอร์ ในขณะที่การกำหนดคำนิยามของกองทัพก็กำหนดไว้ในภาพรวมเช่นเดียวกัน โดยหมายถึงการกระทำหรือดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมีจุดมุ่งหมายเพื่อประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง [7] ด้วยเหตุนี้ จึงส่งผลทำให้ทำหน้าที่ความรับผิดชอบของกองทัพในการกำกับดูแลประเด็นด้านความมั่นคงทางไซเบอร์จึงมีความคลุมเครือจนทำให้เกิดการดำเนินงานที่ทับซ้อนกันระหว่างหน่วยงานพลเรือนกับหน่วยงานทหาร เช่น การเจาะข้อมูลของหน่วยงานต่าง ๆ ในประเทศ การใช้พื้นที่ทางไซเบอร์

[5] วรรณภา ทองแดง, (2563), ผลกระทบเศรษฐกิจดิจิทัล: การขยายตัวของรายจ่ายสาธารณะ ด้านการศึกษาและภัยคุกคามทางไซเบอร์, วารสารมนุษยศาสตร์สังคมศาสตร์ 37 (2) พฤษภาคม - สิงหาคม 2563 ของแก่น: มหาวิทยาลัยขอนแก่น

[6] Buzan B, Waever O (2003) Regions and powers: the structure of international security. Cambridge University Press, Cambridge p25.

[7] สำนักงานเลขาธิการสภาผู้แทนราษฎร, (2560), ศูนย์ไซเบอร์กองทัพบก, (ออนไลน์), https://library2.parliament.go.th/ebook/content-issue/2560/hi2560-021.pdf, สืบค้นเมื่อวันที่ 30 มีนาคม 2564

ในการกล่าวร้ายหรือทำให้เสียชื่อเสียงแก่บุคคลหรือกลุ่มบุคคล เป็นต้น โดยระบบดังกล่าวอาจพิจารณาว่าการกระทำดังกล่าวอยู่ในขอบเขตความรับผิดชอบของแต่ละหน่วยงาน ในขณะที่กองทัพเองอาจพิจารณาว่าการโจมตีนั้นจะส่งผลกระทบต่อความมั่นคงทางไซเบอร์ของประเทศ ซึ่งกองทัพจำเป็นจะต้องเข้ามาจัดการ แต่ปัญหาที่เกิดขึ้นตามมาก็คือการระบุหน่วยรับผิดชอบในการจัดการปัญหาภัยคุกคามทางไซเบอร์ว่าควรจะเป็นหน่วยงานพลเรือนหรือหน่วยงานทางทหาร ซึ่งจะนำไปสู่ปัญหาในการทับซ้อนทางอำนาจของหน่วยงานที่จะเป็นข้อจำกัดของกระบวนการการจัดการภัยคุกคามทางไซเบอร์ภายในประเทศไทย

บริบทด้านความมั่นคงทางไซเบอร์ของประเทศไทย

บริบทที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ของประเทศไทยในภาพรวมนั้น แม้ว่าจะมีความทับซ้อนในการทำงานระหว่างหน่วยพลเรือนกับหน่วยทหาร แต่การดำเนินการในเบื้องต้นจะเป็นการกำหนดมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่มีลักษณะเป็นองค์รวม ที่จะเน้นไปที่การให้ความรู้พื้นฐานเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ และวิธีการป้องกันไม่ให้ตกอยู่ในสถานการณ์เสี่ยงที่จะได้รับผลกระทบจากภัยคุกคามที่เกิดขึ้น โดยให้ความสำคัญต่อภัยคุกคามที่เกิดขึ้นในการทำธุรกรรม หรือการกระทำที่ส่งผลกระทบต่อระบบเศรษฐกิจและต่อหน่วยงานโดยตรง ซึ่งรูปแบบของภัยคุกคามที่เกิดขึ้นในลักษณะนี้ ผู้กระทำการมักจะเป็นบุคคลหรือกลุ่มบุคคลที่มีจุดประสงค์ของการดำเนินการเพื่อผลประโยชน์เท่านั้น ไม่ได้เป็นการกระทำที่มุ่งหวังจะทำลายความมั่นคงในระดับรัฐ และการดำเนินการต่าง ๆ ยังอยู่ในประเทศไทย จึงนับว่าเหตุการณ์ในลักษณะดังกล่าวเป็นภัยคุกคามภายในรัฐ (Intra State Threat) โดยหน่วยงานที่เกี่ยวข้องสามารถดำเนินการจัดการตามระดับความร้ายแรงของความผิด และสามารถดำเนินการได้อย่างเต็มที่โดยไม่ต้องกังวลว่าการจัดการดังกล่าวจะเป็นการละเมิดอธิปไตยของรัฐอื่น ในกรณีนี้ประเทศไทยถือว่ามีมุมมองต่อความมั่นคงทางไซเบอร์แตกต่างจากประเทศอื่น ๆ ที่มุ่งเน้นการป้องกันภัยคุกคามทางไซเบอร์ที่มาจากภายนอกประเทศ (Inter State Threat)

การจัดการกับภัยคุกคามทางไซเบอร์ของประเทศไทย

1. การจัดการกับภัยคุกคามทางไซเบอร์ด้านกฎหมาย

หน่วยงานที่ดูแลด้านความมั่นคงทางไซเบอร์ได้รับการวางกรอบการทำงานตั้งแต่ยุทธศาสตร์ชาติ และ แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นด้านความมั่นคง พ.ศ. 2561 – 2580 ที่เป็นกรอบการดำเนินการด้านความมั่นคงทางไซเบอร์ของประเทศไทยผ่านยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017 – 2021) [8] ซึ่งเป็นแนวนโยบายระดับชาติฉบับแรกของไทยในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อมเอื้ออำนวย โดยมุ่งเน้นให้มีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างพื้นฐานสำคัญ การสร้างความตระหนักในทุกภาคส่วน และการสร้างความร่วมมือกับต่างประเทศ และการจัดทำพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [9] การตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น

2. การจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานพลเรือน

หากจะทำการวิเคราะห์ถึงการดำเนินการเกี่ยวกับการจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานพลเรือนในประเทศไทยนั้นอาจกล่าวได้ว่าประเทศไทยนั้นนับว่ามีความพร้อมในระดับหนึ่งสำหรับการป้องกันภัยคุกคามทางไซเบอร์ในระดับต้นหรือปานกลาง โดยที่ภัยคุกคามทางไซเบอร์ในระดับต้น (Low Level Threat) ที่เป็นภัยคุกคามที่เกิดขึ้นจากการกระทำของบุคคลหรือกลุ่มบุคคลที่มีจุดมุ่งหมายของการดำเนินการเพื่อตอบสนองความต้องการส่วนตัว และภัยคุกคามทางไซเบอร์ระดับปานกลาง (Medium Level Crime) คือ การกระทำทางไซเบอร์โดยบุคคลหรือกลุ่มบุคคลที่ผ่านการวางแผนไว้เป็นอย่างดี โดยอาจเป็นการกระทำของกลุ่มก่อการร้ายที่มีความต้องการที่จะสร้างความเสียหายให้แก่รัฐในระดับที่ไม่รุนแรงมากนัก [10] ซึ่งภัยคุกคามทางไซเบอร์รูปแบบดังกล่าวเป็นลักษณะของภัยคุกคามทางไซเบอร์ที่ประเทศไทยเคยประสบมาแล้ว โดยเฉพาะอย่างยิ่งภัยคุกคามทางไซเบอร์ในระดับต้นที่สามารถพบเห็นได้อยู่บ่อยครั้ง ลักษณะของภัยคุกคามทางไซเบอร์ทั้งสองลักษณะที่กล่าวไปข้างต้น เป็นสิ่งที่หน่วยงานด้านความมั่นคงของประเทศไทยสามารถดำเนินการป้องกันได้อย่างมีประสิทธิภาพ โดยในระยะแรกมีการดำเนินการจากหน่วยงานในกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเมื่อมี พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ขึ้นมา ก็ได้มีการโอนอำนาจหน้าที่ด้านความมั่นคงทางไซเบอร์ให้กับหน่วยงานตามกฎหมายต่อไป

---

[8] สำนักงานสภาความมั่นคงแห่งชาติ, (2561), ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017 – 2021), กรุงเทพฯ: สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา

[9] ราชกิจจานุเบกษา, (2562), พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กรุงเทพฯ: สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา

[10] Steven Bucci, (2012), Cyber Security Evangelist and Subject Matter Expert Consultant, Washington: Washington post

สำหรับในปี 2562 ได้มีการจัดตั้งหน่วยงานในการดูแลรักษาความมั่นคงทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติและประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ [11]

ในส่วนบทบาทของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น สมช. เป็นหน่วยรับผิดชอบหลักในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 ซึ่งได้มีการขยายระยะเวลาถึงปี 2565 เพื่อให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ อีกทั้งได้รับมอบหมายให้ปฏิบัติหน้าที่หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIs) ด้านความมั่นคงของรัฐ (Security Regulator) และเป็นหน่วยงานหลักในการบริหารจัดการภัยคุกคามทางไซเบอร์ในระดับวิกฤต (Cyber Threat Crisis Level) ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [12]

3. การจัดการกับภัยคุกคามทางไซเบอร์ของหน่วยงานทหาร

กองทัพเป็นตัวแสดงหลักที่มีความสำคัญในการจัดการกับภัยคุกคามทางไซเบอร์ของประเทศไทย เนื่องจากกองทัพเป็นหน่วยงานที่มีหน้าที่ในการกำกับดูแลประเด็นที่มีความเกี่ยวข้องกับความมั่นคง โดยเฉพาะอย่างยิ่งความมั่นคงที่อาจส่งผลกระทบต่อความมั่นคงในภาพรวมของรัฐได้ ด้วยเหตุนี้จึงเป็นสาเหตุที่ทำให้ภารกิจการดำเนินงาน

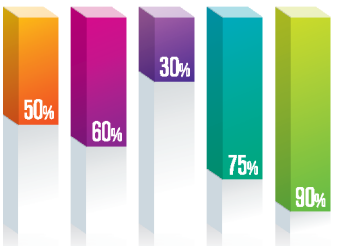
[11] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, (2563), เกี่ยวกับ สก.มช. https://www.mdes.go.th/mission/detail/2481-%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%81%E0%B8%B1%E0%B8%9A-%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A-. สืบค้นเมื่อวันที่ 2 เมษายน 2564

[12] มาตรา 67 ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วย สภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

เกี่ยวกับเรื่องความมั่นคงทางไซเบอร์ของหน่วยงานกองทัพที่ดูมีความชัดเจนมากกว่าหน่วยงานพลเรือน อย่างไรก็ตามอ้างอิงจากวัตถุประสงค์การดำเนินงานที่มีความเกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ จะได้เห็นว่าหน่วยงานภายใต้สังกัดกองทัพจะให้ความสำคัญไปที่ประเด็นหลัก คือ การรักษาความมั่นคงภายในองค์กร [13] การดำเนินงานในส่วนนี้เป็นความพยายามของกองทัพในการที่จะรักษาความมั่นคงของฐานข้อมูล เว็บไซต์ รวมถึงพื้นที่ทางไซเบอร์ของกองทัพให้มีความปลอดภัย ปราศจากการเจาะเข้าระบบจากภายนอกและการรักษาความมั่นคงของสถาบันหลักของชาติ ซึ่งประเด็นนี้จะถูกให้ความสำคัญมากเป็นพิเศษกว่าประเด็นอื่น โดยอาจมีสาเหตุมาจากอุดมการณ์ของกองทัพที่จะปกป้องสถาบันหลักของชาติ

ในการรักษาความมั่นคงด้านไซเบอร์ในประเทศนั้น กองทัพอาจมองว่าเป็นหน้าที่ของกองทัพที่ต้องเป็นหน่วยรับผิดชอบในการดำเนินการ และกองทัพไทยได้มีปฏิบัติการในด้านความมั่นคงทางไซเบอร์ต่าง ๆ ซึ่งเป็นการปฏิบัติงานที่ข้ามขอบเขตของหน่วยงานพลเรือน เช่น กระทรวงดิจิทัลฯ หรือ สกมช. ในกรณีนี้กองทัพได้อ้างถึงประเด็นการรักษาความมั่นคงของประเทศ เพื่อสร้างความชอบธรรมในการดำเนินการด้านความมั่นคงทางไซเบอร์ อย่างไรก็ตาม มุมมองที่หน่วยงานทางทหารมีต่อประเด็นการรักษาความมั่นคงทางไซเบอร์มีความแตกต่างจากหน่วยงานพลเรือนอยู่ค่อนข้างมาก เนื่องจากหน่วยงานทางทหารจะมีการให้ความสำคัญกับการดำเนินการจัดการกับภัยคุกคามภายในประเทศเป็นหลัก ในขณะที่หน่วยงานพลเรือนจะให้ความสำคัญกับภัยคุกคามที่มาจากภายนอกประเทศ และมองว่าภัยคุกคามจากนอกประเทศเป็นอันตรายและส่งผลกระทบมากกว่าภัยคุกคามจากภายในประเทศ

สำหรับข้อจำกัดของการดำเนินงานด้านไซเบอร์ของกองทัพ คือ กระแสต่อต้านจากประชาชน เนื่องจากบริบทปัจจุบันที่ประชาชนมีความไม่พอใจในการดำเนินการของหน่วยงานทางทหารอยู่ค่อนข้างมาก โดยความพยายามของรัฐบาลไทยในช่วงก่อนหน้านี้ที่มีความพยายามจะผลักดันระบบอินเทอร์เน็ตภายในประเทศไทยให้เป็นไปในรูปแบบของ Single Gateway เช่นเดียวกับประเทศจีน [14] หรือการมีปฏิบัติการข่าวสาร (Information Operation) ขึ้นในสื่อสังคมออนไลน์ [15] ที่ก่อให้เกิดความไม่พอใจและกระแสต่อต้านจากประชาชนอย่างรุนแรง ส่งผลต่อการดำเนินการจัดการกับภัยคุกคามทางไซเบอร์ของกองทัพไทยที่จะถูกจับตามองจากประชาชนอย่างเข้มงวด ซึ่งสาเหตุนี้อาจเป็นปัจจัยสำคัญที่ส่งผลต่อการดำเนินงานด้านความมั่นคงทางไซเบอร์ของกองทัพในอนาคต



[13] พล.ต.ฤทธี อินทราวุธ, (2557), ศูนย์ไซเบอร์กองทัพบก, เขี้ยวเล็บ หรือ เสือกระดาษ, (ออนไลน์), http://rittee1834.blogspot.com/2014/12/blog-post.html, สืบค้นเมื่อวันที่ 2 เมษายน 2564

[14] สำนักงานเลขาธิการสภาผู้แทนราษฎร, (2559), การใช้ทางผ่านทางอินเตอร์เน็ตช่องทางเดียว (Single Gateway), (ออนไลน์), https://library2.parliament.go.th/ebook/content-issue/2559/hi2559-020.pdf, สืบค้นเมื่อวันที่ 2 เมษายน 2564

[15] THE MOMENTUM, (2563), การฉ้อฉลเชิงอำนาจ'(2): สงครามจิตวิทยากับประชาชน, (ออนไลน์), https://themomentum.co/citizen2-0-information-operations/, สืบค้นเมื่อวันที่ 2 เมษายน 2564

ผลลัพธ์ของการดำเนินการจัดการภัยคุกคามทางไซเบอร์

ประเทศไทยมีการจัดการดูแลด้านความมั่นคงทางไซเบอร์ในหลากหลายมิติโดยผลลัพธ์จากการจัดการทางไซเบอร์นั้นหน่วยงานที่เกี่ยวข้องกับชีวิตประจำวันของประชาชนได้มีการป้องกันการเจาะข้อมูล การฝึกอบรมต่าง ๆ ที่เกี่ยวข้องกับการป้องกันทางไซเบอร์ และในด้านหน่วยทางทหารได้มีการฝึกอบรมและทำระบบป้องกันทางไซเบอร์ แต่ในสังคมกลับไม่สามารถรับรู้ได้ถึงระบบป้องกันหรือการป้องกันได้อย่างชัดเจน ซึ่งภาครัฐได้มองว่าพื้นที่ทางไซเบอร์จำเป็นจะต้องได้รับการปกป้องกลายมาเป็นประเด็นด้านความมั่นคงตามแนวคิดของการทำให้เป็นความมั่นคง (Securitization) อย่างไรก็ตาม ประเทศไทยยังมีความพร้อมในการรับมือกับภัยความมั่นคงทางไซเบอร์ที่ยังไม่เพียงพอ เนื่องจากยังขาดผู้เชี่ยวชาญด้านไซเบอร์ โดยมีสาเหตุมากจาก 1) ค่าตอบแทนที่ไม่มากพอ 2) การโดนภาคเอกชนดึงตัวไปทำงาน 3) ความก้าวหน้าทางอาชีพที่ไม่ชัดเจน และ 4) บุคลากรด้านไซเบอร์ขาดแคลนทั่วโลก ถึงแม้ว่าจะมีการอบรมในเรื่องของความมั่นคงทางไซเบอร์ แต่ความเชี่ยวชาญของผู้ที่ทำงานในหน่วยงานดังกล่าวก็ยังมีไม่เพียงพอในการจัดการความมั่นคงทางไซเบอร์ทั้งหมดของประเทศไทย

สรุป

กล่าวโดยสรุปคือ การเปลี่ยนแปลงทางด้านเทคโนโลยีที่เกิดขึ้นในปัจจุบันรวมถึงแนวโน้มของการพัฒนาเทคโนโลยีในอนาคตทำให้ประเด็นของความมั่นคงทางไซเบอร์เป็นหนึ่งในประเด็นด้านความมั่นคงที่ทุกภาคส่วนจำเป็นจะต้องให้ความสำคัญ โดยเฉพาะอย่างยิ่งหน่วยงานที่เกี่ยวข้องกับความมั่นคง แต่ในปัจจุบันปัญหาที่พบเกี่ยวกับการดำเนินการจัดการด้านความมั่นคงทางไซเบอร์ในประเทศไทย ในประเทศไทยจะเป็นปัญหาที่เกิดขึ้นที่เกิดจากการให้คำนิยามของความมั่นคงทางไซเบอร์ ที่อาจมีความแตกต่างกันของแต่ละหน่วยงาน ดังนั้น จึงควรมีการบูรณาการข้อมูลเพื่อให้ความเข้าใจที่ตรงกัน นอกจากนี้หน่วยงานด้านความมั่นคงควรดำเนินการสร้างความเข้าใจกับภาคประชาชน เพื่อให้ได้รับความร่วมมือจากประชาชนอย่างเต็มที่ เพื่อให้การดำเนินงานของหน่วยงานเป็นไปอย่างสะดวกมากขึ้น ประกอบกับในปัจจุบันหน่วยงานด้านความมั่นคงมีภาพลักษณ์ที่ไม่ดีนักในมุมมองของประชาชน ดังนั้น จึงควรที่จะดำเนินการเสริมสร้างการรับรู้ ความเข้าใจและความน่าเชื่อถือในการดำเนินงานแก่ประชาชน เพื่อให้สามารถดำเนินการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและลดแรงต่อต้านจากภาคประชาชน

เอกสารอ้างอิง

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, (2563), เกี่ยวกับ สกมช. https://www.mdes.go.th/mission/detail/2481-%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%81%E0%B8%B1%E0%B8%9A-%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A-. สืบค้นเมื่อวันที่ 2 เมษายน 2564

พล.ต. ฤทธี อินทราวุธ, (2557), ศูนย์ไซเบอร์กองทัพบก เขี้ยวเล็บ หรือ เสือกระดาษ, (ออนไลน์), http://rittee1834.blogspot.com/2014/12/blog-post.html, สืบค้นเมื่อวันที่ 2 เมษายน 2564

ราชกิจจานุเบกษา, (2562), พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กรุงเทพฯ: สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา

วรรณภา ทองแดง, (2563), ผลกระทบเศรษฐกิจดิจิทัล: การขยายตัวของรายจ่ายสาธารณะ ด้านการศึกษาและภัยคุกคามทางไซเบอร์, วารสารมนุษยศาสตร์สังคมศาสตร์ 37 (2) พฤษภาคม - สิงหาคม 2563 ขอนแก่น: มหาวิทยาลัยขอนแก่น

สำนักงานพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, (2561), ยุทธศาสตร์ชาติ พ.ศ. 2561-2580, กรุงเทพฯ: สำนักงานพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, (2563), ETDA เผย ปี 62 คนไทยใช้อินเทอร์เน็ตเพิ่มขึ้นเฉลี่ย 10 ชั่วโมง 22 นาที Gen Y ครองแชมป์ 5 ปีซ้อน, (ออนไลน์), https://www.etda.or.th/th/NEWS/ETDA-Revealed-Thailand-Internet-User-Behavior-2019.aspx สืบค้นเมื่อวันที่ 30 มีนาคม 2564

สำนักงานเลขาธิการสภาผู้แทนราษฎร, (2559), การใช้ทางผ่านทางอินเตอร์เน็ตช่องทางเดียว (Single Gateway), (ออนไลน์), https://library2.parliament.go.th/ebook/content-issue/2559/hi2559-020.pdf, สืบค้นเมื่อวันที่ 2 เมษายน 2564

_____, (2560), ศูนย์ไซเบอร์กองทัพบก, (ออนไลน์), https://library2.parliament.go.th/ebook/content-issue/2560/hi2560-021.pdf, สืบค้นเมื่อวันที่ 30 มีนาคม 2564

สำนักงานสภาความมั่นคงแห่งชาติ, (2561), ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017 – 2021), กรุงเทพฯ: สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา

DEPA, (2563), ดีป้า-ม.ศรีปทุม-อินโฟเฟด ผนึกกำลังปั้นขุนพล Cyber Security, (ออนไลน์), https://www.depa.or.th/th/article-view/20201117_04, สืบค้นเมื่อวันที่ 30 มีนาคม 2564

THE MOMENTUM, (2563), การฉ้อฉลเชิงอำนาจ'(2): สงครามจิตวิทยากับประชาชน, (ออนไลน์), https://themomentum.co/citizen2-0-information-operations/, สืบค้นเมื่อวันที่ 2 เมษายน 2564

Buzan B, Waever O (2003) Regions and powers: the structure of international security. Cambridge University Press, Cambridge

Steven Bucci, (2012), Cyber Security Evangelist and Subject Matter Expert Consultant, Washington: Washington post

ฑภิพร สุพร, อาจารย์คณะรัฐศาสตร์และรัฐประศาสนศาสตร์ มหาวิทยาลัยเชียงใหม่ สัมภาษณ์เมื่อวันที่ 10 มีนาคม 2562