บทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่

Thai army and cybersecurity policy for non-traditional threats

Yuttasak Raksereepitak[1] & Sirilak Tantayakul[2]

ยุทธศักดิ์ รักเสรีพิทักษ์ & ศิริลักษม์ ตันตยกุล

Corresponding author: 6314832039@rumail.ru.ac.th

Received: 07/08/65 Revised: 09/08/65 Accepted: 09/08/65

บทคัดย่อ

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยเก็บข้อมูลจากเอกสารและงานวิจัยที่เกี่ยวข้อง และจากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญ จำนวน 10 คน โดยมีวัตถุประสงค์เพื่อศึกษา 1. สภาพปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทย 2. ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ และ 3. แนวคิดและข้อเสนอแนะในการพัฒนาและปรับปรุงนโยบาย มาตรการทางกฎหมาย และระเบียบปฏิบัติ ในการป้องกันภัยคุกคามทางไซเบอร์ ผลการวิจัยพบว่า สภาพปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยแบ่งออกเป็น 2 ปัญหาใหญ่ ได้แก่ 1) ความไม่พร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2) ความไม่พร้อมในการรับมือปรากฏการณ์อำนาจแฝงจากโซเชียลมีเดีย และการสูญเสีย

---

[1] นักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

[2] คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

อธิปไตยไซเบอร์ของชาติ ในส่วนของความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จากผลการวิเคราะห์ขีดความสามารถด้านไซเบอร์ พบว่า ประเทศไทยมีขีดความสามารถด้านไซเบอร์โดยรวม อยู่ที่ระดับ 1.95 หมายความว่า ไทยจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ในทุกมิติ

คำสำคัญ: ความมั่นคงทางไซเบอร์; นโยบายสาธารณะ; สงครามรูปแบบใหม่

Abstract

This research is a qualitative research. Data were collected from related documents and from the interviews with 10 key informants. The purposes of studying were to study 1. cyber threats in Thailand 2. cybersecurity readiness and 3. concepts and recommendations for policy development and improvement, legal measures and regulations to protect against cyber threats. The results showed that the problem of cyber threats in Thailand is divided into 2 major problems, namely; 1) not being ready to prevent and secure cyber threats and maintain cybersecurity at the national level and 2) not being ready for cyber threats, coping with the hidden power phenomenon from social media and the loss of national cyber sovereignty. In terms of readiness for cyber security, according to the results of cyber capability analysis, Thailand's overall cyber capability is at 1.95, meaning that Thailand needs to develop its cyber capabilities in all dimensions.

Key words: cyber security; public policy; modern warfare

บทนำ

ปัจจุบันการทำสงครามไม่จำเป็นต้องมีอาวุธยุทโธปกรณ์ที่ล้ำสมัย หรือประสิทธิภาพในการทำลายล้างสูงเท่านั้น แต่ยังใช้วิธีการโจมตีทางไซเบอร์และการเข้าครอบงำทางความคิด ทัศนคติของผู้คนผ่านทางโซเชียลมีเดียด้วย ส่งผลให้กองทัพสามารถโจมตีฝ่ายตรงข้ามได้อย่างทันการณ์ ไม่มีการสูญเสียทางกายภาพ ไม่ต้องใช้งบประมาณในการซื้ออุยทโธปกรณ์ราคาสูง เพียงแค่มีความเชี่ยวชาญในการใช้โซเชียลมีเดียเป็นอาวุธ (Weaponization of social media) ก็สามารถเอาชนะศัตรูได้อย่างรวดเร็ว อีกทั้งปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ และภัยคุกคามรูปแบบใหม่ อาทิ การก่อการร้ายสากล อาชญากรรมข้ามชาติ การก่อความไม่สงบในพื้นที่ต่างๆ มีแนวโน้มทวีความรุนแรง ซึ่งเป็นผลมาจากความก้าวหน้า และการเปลี่ยนแปลงแบบก้าวกระโดดของเทคโนโลยีดิจิทัล เช่น สิ่งต่างๆ ถูกเชื่อมโยงสู่เครือข่ายอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายสื่อสารได้ เป็นต้น นอกจากนี้อำนาจของสารสนเทศและสื่อมัลติมีเดียกลายเป็นภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อการตัดสินใจในระดับชาติ ส่งผลให้มิติการรักษาความมั่นคงปลอดภัยของกองทัพ จึงมิได้มีเพียงทางพื้นดิน อากาศ น้ำ และอวกาศ เท่านั้น แต่ยังรวมถึงมิติไซเบอร์ด้วย

อย่างไรก็ตาม ภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างต่อเนื่องและมีความรุนแรงเพิ่มขึ้น สร้างความเสียหายให้แก่ประชาชน สังคม ตลอดจนประเทศชาติ โดยไม่เว้นแม้แต่ประเทศที่พัฒนาแล้ว หรือประเทศที่กำลังพัฒนา ดังจะเห็นได้จากเหตุการณ์สำคัญที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานของประเทศ ยกตัวอย่างเหตุการณ์ช่วงเดือนพฤษภาคม พ.ศ. 2564 มีการโจมตีทางไซเบอร์ครั้งใหญ่ที่เกิดขึ้นกับบริษัทท่อส่งน้ำมันรายใหญ่ของสหรัฐอเมริกา “Colonial Pipeline” ถูกโจมตีด้วย Ransomware หรือมัลแวร์เรียกค่าไถ่ ทำให้

ต้องหยุดการขนส่งน้ำมันบางส่วนลงชั่วคราวเพื่อแก้ไขปัญหาดังกล่าว สร้างความเสียหายเป็นอย่างมากต่อบริษัทและลูกค้า การโจมตีโดย Ransomware ที่เกิดขึ้นกับบริษัทท่อส่งน้ำมันดังกล่าวนั้น เป็นการปฏิบัติการของอาชญากรรมข้ามชาติที่จู่โจมเป้าหมายที่เป็นองค์กรหรือหน่วยงานโครงสร้างพื้นฐานสำคัญยิ่งยวด จากเหตุการณ์ดังกล่าว ไม่ได้เกิดขึ้นเป็นครั้งแรก หากแต่เกิดขึ้นมาแล้วในหลายประเทศทั่วโลกตลอดหลายปีที่ผ่านมา จึงเป็นที่มาและเป็นสาเหตุที่ประเทศต่างๆ ทั่วโลก จำเป็นต้องมีกฎหมายด้านไซเบอร์ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ด้วยเหตุการณ์ที่กล่าวมาแล้วในตอนต้น อาชญากรไซเบอร์มีเป้าหมายโจมตีหน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศต่างๆ ทำให้รัฐบาลไทยได้ออกนโยบายสาธารณะทางไซเบอร์ (สิทธิพันธ์ พุทธหุน, 2564) ซึ่งก็คือ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ออกมาประกาศใช้ ซึ่งบังคับใช้เฉพาะกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)

ดังนั้น กองทัพบก ในฐานะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย ในมิติด้านความมั่นคง จึงเล็งเห็นความสำคัญที่จะต้องมีความพร้อมในการเผชิญกับภัยคุกคามทั้งแบบดั้งเดิม และภัยคุกคามรูปแบบใหม่ ที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยตรงทั้งทางเศรษฐกิจ สังคมจิตวิทยา และการทหาร ในลักษณะที่ภัยคุกคามได้ทวีความรุนแรงเพิ่มขึ้นตามลำดับจากปัจจัยบวกของกระแสโลกาภิวัตน์ และความก้าวหน้าของการสื่อสารและเทคโนโลยีสารสนเทศ ซึ่งกองทัพบกมีบทบาทหลัก 2 ประการ คือ ประการที่ 1 การเตรียมกำลังและพัฒนากองทัพบกให้มีความทันสมัยสามารถ

เผชิญกับสถานการณ์ด้านความมั่นคงที่เปลี่ยนแปลงไป โดยจัดเตรียมและเสริมสร้างขีดความสามารถในด้านต่าง ๆ ได้แก่ ด้านโครงสร้างกำลัง ด้านความพร้อมรบ ด้านความต่อเนื่องในการรบ และด้านความทันสมัย และประการที่ 2 การใช้กำลังกองทัพบกควบคุมบังคับบัญชาและอำนวยการในการปฏิบัติตามพันธกิจต่าง ๆ จึงจำเป็นอย่างยิ่งที่จะต้องศึกษาและวิเคราะห์สภาพปัญหาแนวโน้มของภัยคุกคามทางไซเบอร์ กฎหมายด้านความมั่นคง กฎ ระเบียบอื่นๆ ที่เกี่ยวข้องของประเทศไทย รวมถึง ประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพ เพื่อกำหนดเป็นนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ และจัดทำข้อเสนอแนะในการปรับปรุงกฎหมายไซเบอร์ และระเบียบปฏิบัติในการป้องกันภัยคุกคามทางไซเบอร์ของประเทศไทยต่อไป

วิธีดำเนินการวิจัย

การวิจัยเรื่อง บทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่ มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาภัยคุกคามทางไซเบอร์ ความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย และแนวคิดและข้อเสนอแนะในการพัฒนาและปรับปรุงนโยบาย มาตรการทางกฎหมาย และระเบียบปฏิบัติ ในการป้องกันภัยคุกคามทางไซเบอร์ การวิจัยครั้งนี้ ใช้วิธีการวิจัยเชิงคุณภาพ โดยการใช้แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูล และศึกษารวบรวมข้อมูลจากเอกสาร ทฤษฎี แนวคิด และผลงานการวิจัยที่เกี่ยวข้องโดยใช้กรอบแนวคิดที่กำหนดไว้เป็นแนวทางในการศึกษา

ประชากรและผู้ให้ข้อมูลสำคัญ

ในการวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ โดยผู้วิจัยได้เก็บข้อมูลจากกลุ่มตัวอย่างด้วยการสัมภาษณ์แบบมีโครงสร้าง หรือการสัมภาษณ์แบบเป็น

ทางการ ผู้ให้ข้อมูลสำคัญ ได้แก่ ผู้เชี่ยวชาญ หรือผู้ทรงคุณวุฒิที่มีประสบการณ์การทำงานด้านการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ทำหน้าที่รับผิดชอบกำหนดนโยบายและมาตรการต่างๆ ของประเทศไทย รวมถึงผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ หรือผู้ทรงคุณวุฒิของกองทัพบก และนักวิชาการ รวมทั้งหมด 10 ท่าน เพื่อการรวบรวมข้อมูลจากการวิเคราะห์และเสนอข้อมูลความคิดเห็นของผู้เชี่ยวชาญด้านนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาศัยกรอบแนวคิดที่กำหนดไว้เป็นแนวทางในการศึกษา

ขอบเขตด้านเนื้อหา

ในการวิจัยผู้วิจัยเลือกใช้วิธีการวิจัย โดยการวิจัยเอกสาร เป็นการรวบรวมข้อมูลจากเอกสารทางวิชาการ ตำรา รายงานการวิจัย วิทยานิพนธ์ เอกสารทางราชการที่เกี่ยวข้องกับประเด็นนโยบายสาธารณะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การวิจัยเชิงคุณภาพ โดยผู้วิจัยมีนิยามศัพท์เฉพาะในการศึกษาวิจัย ดังนี้

ภัยคุกคามรูปแบบใหม่ (Non-Traditional threats) หมายถึง ภัยคุกคามในทุกๆ มิติที่ไม่ใช่ภัยคุกคามเฉพาะมิติด้านทางการทหารเท่านั้น ดังตัวอย่างเช่น ปัญหาโลกร้อนที่ก่อให้เกิดการเปลี่ยนแปลงทางสิ่งแวดล้อมที่มีผลกระทบต่อความเป็นอยู่ของมวลมนุษยชาติ และระบบนิเวศน์ หรือการเคลื่อนย้ายทุนจากบรรษัทข้ามชาติที่ส่งผลให้ประเทศบางประเทศล้มละลายได้ภายในชั่วข้ามคืน หรือการก่อการร้าย และการก่อความไม่สงบที่กระทำต่อผู้บริสุทธิ์ด้วยความรุนแรงและความหวาดกลัว หรือการค้ามนุษย์ข้ามชาติ เป็นต้น

สงครามผสมผสาน (Hybrid Warfare) หมายถึง สงครามที่ใช้วิธีการผสมผสานกันของเครื่องมือทั้งจากสงครามตามแบบ และสงครามไม่ตามแบบ ที่จะประกอบด้วย 8 องค์ประกอบหลัก คือ กองกำลังทหารปกติ, กำลังทหารรบพิเศษ, กองกำลังที่ไม่ใช่ทหาร, การสนับสนุนจากประชาชนในท้องถิ่น, สงครามข้อมูลข่าวสารและการโฆษณาชวนเชื่อ, การทูต, การโจมตีด้านไซเบอร์ และสงครามเศรษฐกิจ

สงครามสมัยใหม่ (Modern Warfare) หมายถึง การสงครามที่ใช้แนวความคิด วิธีการ และเทคโนโลยีด้านการทหารที่พัฒนาในห้วงตั้งแต่ท้ายสงครามโลกครั้งที่ 2 เป็นต้นมา จนถึงปัจจุบัน โดยในระหว่างท้ายศตวรรษที่ 19 ถึงต้นศตวรรษที่ 20 แนวความคิดและวิธีการทำสงครามได้มีความซับซ้อนมากขึ้น เนื่องจากมีภัยคุกคามที่ซับซ้อน และนำเทคโนโลยีสารสนเทศขั้นสูงมาร่วมปฏิบัติ

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง โดยภัยคุกคามทางไซเบอร์ ที่เป็นประเด็นสำคัญมี 2 มิติ ได้แก่ การโจมตีทางไซเบอร์ และการครอบงำทางไซเบอร์

ภัยคุกคามรูปแบบใหม่ (Non-Traditional threats) หมายถึง ภัยคุกคามในทุกๆ มิติที่ไม่ใช่ภัยคุกคามเฉพาะมิติด้านทางการทหารเท่านั้น ดัง

ตัวอย่างเช่น ปัญหาโลกร้อนที่ก่อให้เกิดการเปลี่ยนแปลงทางสิ่งแวดล้อมที่มีผลกระทบต่อความเป็นอยู่ของมวลมนุษยชาติ และระบบนิเวศน์ หรือการเคลื่อนย้ายทุนจากบรรษัทข้ามชาติที่ส่งผลให้ประเทศบางประเทศล้มละลายได้ภายในชั่วข้ามคืน หรือการก่อการร้าย และการก่อความไม่สงบที่กระทำต่อผู้บริสุทธิ์ด้วยความรุนแรงและความหวาดกลัว หรือการค้ามนุษย์ข้ามชาติ เป็นต้น

การโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง การโจมตีฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง ทำลาย หรือควบคุม การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมไปถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้ามด้วย

การครอบงำทางไซเบอร์ (Cyber Dominance) หมายถึง การถูกชี้นำหรือครอบงำทางความคิดโดยไม่รู้ตัวจากอำนาจของสารสนเทศและสื่อมัลติมีเดีย รวมถึงการสร้างกระแสเทียมบนสื่อสังคมออนไลน์ เช่น การปั่นกระแสด้วยแฮชแท็ก (#HashTag) การโพสต์ข่าวลือเทียม (False rumor) การสร้างข่าวปลอม (Fake News) เป็นต้น ซึ่งส่งผลกระทบต่อความคิดเห็น ความเชื่อ และการตอบสนองของประชาชนโดยรวม

เครื่องมือที่ใช้ในการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยได้ใช้การสัมภาษณ์แบบมีโครงสร้างเป็นเครื่องมือในการเก็บรวบรวมข้อมูลเชิงคุณภาพด้วยการการสัมภาษณ์แบบเจาะลึกจากผู้ให้ข้อมูลสำคัญโดยเป็นผู้เชี่ยวชาญด้านต่างๆ 10 ท่าน เป็นการสัมภาษณ์เดี่ยว โดยใช้แบบสัมภาษณ์แบบมีโครงสร้างไม่ชี้นำ ประกอบด้วยประเด็นคำถาม ดังนี้

ประเด็นที่ 1 สภาพปัญหาและภัยคุกคามทางไซเบอร์ ในมิติการโจมตีทางไซเบอร์ และมิติการครอบงำทางไซเบอร์ ที่มีผลกระทบต่อความมั่นคงของประเทศไทย

ประเด็นที่ 2 การประเมินความพร้อมในด้านกฎหมาย หรือเครื่องมือเพื่อจัดการกับภัยคุกคามทางไซเบอร์ ของประเทศไทย

ประเด็นที่ 3 ข้อเสนอแนะด้านนโยบาย/มาตรการ/แนวทาง ในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ ของประเทศไทย

ผลการวิจัยและอภิปรายผล

ผลการวิจัยเอกสาร

ผู้วิจัยได้ทำการศึกษาแนวคิดในการประเมินความพร้อมด้านไซเบอร์ของประเทศไทย โดยใช้กรอบแนวคิดของ National Cybersecurity Capacity Maturity Model (CMM) แห่ง University of Oxford (Global Cybersecurity Capacity Centre, 2016) มาประยุกต์ใช้ให้เหมาะสมกับสถานการณ์ปัจจุบันและสภาวะแวดล้อมของประเทศไทย ตามบริบทของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่งคง ซึ่งแบ่งออกเป็น 5 มิติ (แต่ละมิติ คะแนนเต็ม 5 คะแนน) สามารถสรุปผลได้ดังนี้

มิติที่ 1 หน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ จากการศึกษา พบว่า ประเทศไทย มีการประกาศโครงสร้างหน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ ภายใต้ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ มีการกำหนดคณะกรรมการฯ และอำนาจหน้าที่รับผิดชอบอย่างชัดเจน

และมีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง ทั้งภาครัฐและเอกชน (บางส่วน) จึงคิดเป็น 3.5 คะแนน

มิติที่ 2 หน่วยงานป้องกันการครอบงำทางไซเบอร์ จากการศึกษา พบว่า ประเทศไทยยังไม่มีหน่วยงานที่รับผิดชอบการป้องกันการครอบงำทางไซเบอร์โดยตรง ปัจจุบันมีศูนย์ต่อต้านข่าวปลอมประเทศไทย สังกัดกระทรวงดิจิทัลเศรษฐกิจและสังคม และกองบัญชาการตำรวจไซเบอร์ เท่านั้น จึงคิดเป็น 1 คะแนน

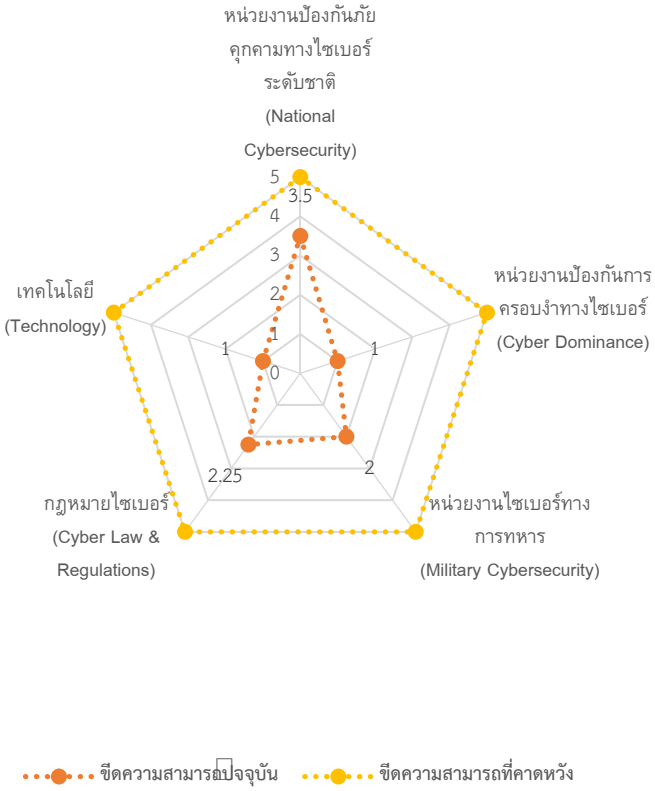
มิติที่ 3 หน่วยงานไซเบอร์ทางการทหาร จากการศึกษา พบว่า ประเทศไทยมีโครงสร้างพิเศษ ได้แก่ 5 ศูนย์ไซเบอร์ สังกัดกระทรวงกลาโหม แต่ยังไม่มีการกำหนดภารกิจด้านการครอบงำทางไซเบอร์ (เชิงรับ/เชิงรุก) ที่ชัดเจน จึงคิดเป็น 2 คะแนน

มิติที่ 4 กฎหมายไซเบอร์ จากการศึกษา พบว่า ประเทศไทยมีการบังคับใช้กฎหมายด้านไซเบอร์ ได้แก่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และ พ.ร.บ. คุ้มครองส่วนบุคคลฯ จึงคิดเป็น 2.25 คะแนน

มิติที่ 5 เทคโนโลยี จากการศึกษา พบว่า ประเทศไทยยังไม่มีการพัฒนาแพลตฟอร์มดิจิทัล หรือเป็นเจ้าของแฟลตฟอร์ม จึงคิดเป็น 1 คะแนน

จากผลการวิเคราะห์ขีดความสามารถด้านไซเบอร์ ของประเทศไทย แสดงให้เห็นว่า ประเทศไทย มีขีดความสามารถด้านไซเบอร์โดยรวม อยู่ที่ระดับ “1.95” หมายความว่า ประเทศไทยจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ในทุกๆ มิติ ซึ่งเป็นระดับที่เข้าใกล้ ระดับ 2 กล่าวคือ เป็นระดับที่เริ่มปรากฏ

โครงสร้างให้เป็นรูปธรรม แต่ยังไม่เริ่มกำหนดรายละเอียดขอบเขตที่ชัดเจน สามารถแสดงผลตามแผนภาพดังนี้



ภาพ 1 การวิเคราะห์ขีดความสามารถด้านไซเบอร์ ของประเทศไทย

ผลการวิจัยเชิงคุณภาพ

ผู้วิจัยได้สรุปผลการวิจัยแยกเป็น 3 ประเด็น เพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย ดังนี้

ประเด็นที่ 1 สภาพปัญหาและภัยคุกคามทางไซเบอร์ ในมิติการโจมตีทางไซเบอร์ และมิติการครอบงำทางไซเบอร์ ที่มีผลกระทบต่อความมั่นคงของประเทศไทย

จากผลการวิจัย พบว่า ภัยคุกคามทางไซเบอร์ในปัจจุบันทวีความรุนแรงและเพิ่มจำนวนมากขึ้นอย่างมีนัยสำคัญ เช่น การส่ง SMS ปลอม เพื่อ Phishing หรือแก๊ง Call Center เป็นต้น จากสถิติการรับแจ้งความคดีอาชญากรรมทางเทคโนโลยีมีแนวโน้มเพิ่มขึ้นทุกๆ ปี ส่วนสถิติจำนวนคดีที่มีการจับกุมอาชญากรรมทางเทคโนโลยีก็เพิ่มขึ้นด้วยเช่นกัน ประเด็นที่น่าสนใจคือ ภัยคุกคามที่เกิดจากการครอบงำทางไซเบอร์ ที่ควบคุมได้ยาก จึงเป็นเรื่องที่ประเทศไทยต้องกังวล เนื่องจากกฎหมายยังไม่ครอบคลุมการกระทำผิดทุกประเภท ด้วยเนื้อหาแนวดรามา (Drama) ที่ยังเป็นจุดสนใจและได้รับความนิยมในประเด็นของ SLVR บนสื่อออนไลน์ ประกอบด้วย S-Sex คือ การแสดงเรื่องราวทางเพศที่ไม่เหมาะสม ลามก อนาจาร หยาบโลน, L-Language คือ ภาษาที่ไม่เหมาะสม ใช้ถ้อยคำหยาบคาย รุนแรง ดูหมิ่นเหยียดหยาม, V-Violence คือ ความรุนแรงทางร่างกาย เช่น การทำร้ายร่างกาย การทารุณกรรม ความโหดเหี้ยม การฆ่าฟัน การทำลายล้าง และ R-Representation คือ การใช้ภาพตัวแทน คือ การใช้ตัวละครแสดงเพื่อสื่อความหมายในเชิงดูถูก เหยียดหยาม ล้อเลียน เยาะเย้ย ก่อให้เกิดความเกลียดชัง เกิดอคติ การแบ่งแยก

ถึงแม้ว่าจะมีการควบคุมหรือวางกฎเกณฑ์ต่างๆ แต่ผู้ผลิตสื่อก็ยังมิใคร่ตระหนักถึงผลกระทบที่จะเกิดตามมาสักเท่าใดนัก ยิ่งเป็นข่าวที่ถูกวิพากษ์วิจารณ์ยิ่งเป็นการกระตุ้นยอดวิว มีผู้ใช้งาน (User) เข้ามารับชมเพิ่มขึ้น มีโอกาสได้รับค่าโฆษณามากขึ้นตามไปอีก ซึ่งนับว่าคุ้มในแง่การตลาด แต่จริยธรรมและศีลธรรมของสื่อกลับเสื่อมถอยอย่างยิ่ง

ประเด็นที่ 2 การประเมินความพร้อมในด้านกฎหมาย หรือเครื่องมือเพื่อจัดการกับภัยคุกคามทางไซเบอร์ ของประเทศไทย

การวิจัยครั้งนี้ ใช้กรอบแนวคิดของ National Cybersecurity Capacity Maturity Model (CMM) เป็นต้นแบบ แบ่งออกเป็น 5 มิติ (Domain) สามารถสรุปผลการวิจัยได้ดังนี้

มิติที่ 1 หน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ พบว่าประเทศไทย มีหน่วยงานของรัฐบาลที่รับผิดชอบด้านความมั่นคงไซเบอร์จำนวน 8 หน่วยงานหลัก พร้อมด้วย 3 คณะทำงานฯ โดยแต่ละหน่วยรับผิดชอบตั้งแต่ระดับนโยบาย การปฏิบัติในแต่ละสายงานของตนเอง รวมถึงการกำหนดแนวทาง หรือมาตรการด้านความมั่นคงไซเบอร์ เพื่อให้การปฏิบัติของแต่ละหน่วยงานมีการประสานสอดคล้อง ทั้งนี้ ประเทศไทยได้มีการแต่งตั้งรองนายกรัฐมนตรี ให้ดำรงตำแหน่ง ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Director) มีหน้าที่ในการให้คำปรึกษานายกรัฐมนตรี ในเรื่องของความมั่นคงไซเบอร์ รวมถึงมีหน้าที่ประสานงาน/กำกับดูแลให้หน่วยงานที่เกี่ยวข้องปฏิบัติในทิศทางเดียวกัน

มิติที่ 2 หน่วยงานป้องกันการครอบงำทางไซเบอร์ พบว่า ประเทศไทยควรจัดตั้งหน่วยงานกำกับดูแลด้านครอบงำทางไซเบอร์โดยเฉพาะ เพื่อทำหน้าที่จัดระเบียบทั้งแพลตฟอร์ม ผู้ผลิตเนื้อหา และผู้ใช้งาน ให้ปฏิบัติตามที่กฎหมายกำหนด

มิติที่ 3 หน่วยงานไซเบอร์ทางการทหาร พบว่า กองทัพควรมีหน่วยงานต่อต้านการโจมตีทางไซเบอร์ที่มีภารกิจในการเฝ้าระวัง แจ้งเตือน ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ หรือการโจมตีด้านไซเบอร์ เพื่อให้สามารถปฏิบัติการเชิงรุกและเชิงรับ รวมถึง หน่วยงานต่อต้านการครอบงำทางไซเบอร์ทำหน้าที่ ตรวจสอบ ติดตามร่องรอยการกระทำต่างๆ ที่บันทึกไว้บนสื่อสังคมออนไลน์ หรืออินเทอร์เน็ต (Digital Footprint) เพื่อตรวจสอบ ประเมิน วิเคราะห์ทัศนคติ ติดตามกลุ่มเครือข่ายของบุคคลในสังคม รวมถึง การกวาดข้อมูลจากสื่อสังคมออนไลน์ เพื่อวิเคราะห์พฤติกรรม และทำนายแนวโน้มต่างๆ ที่เป็นภัยคุกคามทางไซเบอร์

มิติที่ 4 กฎหมายไซเบอร์ พบว่า กรณีศึกษาด้านกฎหมายไซเบอร์ของต่างประเทศ ที่มุ่งเน้นการแก้ปัญหาการครอบงำทางไซเบอร์ เช่น สหภาพยุโรป กำหนดให้ผู้ให้บริการสื่อสังคมออนไลน์ ต้องลบ โฆษณาชวนเชื่อ แนวคิดนิยมความรุนแรง การก่อการร้าย ภายใน 1 ชั่วโมง หลังจากตรวจพบ มีค่าปรับ 4% ของรายได้ หรือบราซิล มีกฎหมาย Law PLS2630/2020 (Anti-Fake news Act) มีข้อบังคับให้โซเชียลมิเดียและแอพพลิเคชั่นส่งข้อความต้องเก็บข้อมูลระบุตัวตนของผู้ใช้งาน ติดตามและเก็บ Logs ของผู้ใช้งาน รัฐสามารถสั่งห้ามการ Broadcast ได้ และรัฐสามารถค้น Logs DB แบบระยะไกล หรือสิงคโปร์ มีแนว

ปฏิบัติควบคุม “เนื้อหาต้องห้าม” บนอินเทอร์เน็ต และกฎหมาย Protection from online falsehoods and manipulation act 2019 (POFMA) เพื่อจัดการกับการเผยแพร่ข่าวปลอม และการปลุกปั่นในโลกออนไลน์ ซึ่งมีโทษปรับไม่เกิน 1 ล้านเหรียญสิงคโปร์ และจำคุกสูงสุดไม่เกิน 10 ปี หรือออสเตรเลีย มีกฎหมายการเข้ารหัสข้อมูล (Assistance and access act – AAA) ที่ช่วยให้เจ้าหน้าที่รัฐหรือตำรวจเข้าถึงข้อมูลที่เข้ารหัส หรือเป็นความลับของผู้ใช้งาน เพื่อประโยชน์ต่อการสืบสวนคดี และรับมือกับเครือข่ายการก่ออาชญากรรมทางไซเบอร์ ดังนั้นเมื่อพิจารณาแล้วประเทศไทยจึงควรปรับปรุงกฎหมายไซเบอร์

มิติที่ 5 เทคโนโลยี เป็นขีดความสามารถด้านการใช้เทคโนโลยีที่มีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ พบว่า ประเทศไทยควรสร้างแพลตฟอร์ม Social Media หรือแอพพลิเคชั่นสำหรับคนไทย เพื่อลดการพึ่งพาแอพพลิเคชั่นจากต่างประเทศ

ประเด็นที่ 3 ข้อเสนอแนะด้านนโยบาย/มาตรการ/แนวทาง ในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ ของประเทศไทย

จากผลการวิจัย พบว่า การกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรทบทวน และปรับปรุง โดยจำแนกออกตามองค์กรที่มีบทบาทเป็นผู้นำของการขับเคลื่อนยุทธศาสตร์ รวมถึงรัฐบาลควรใช้กลไกหน่วยงานภาครัฐ เช่น สกมช. กมช. ดศ. สมช. เป็นต้น ร่วมกับผู้เชี่ยวชาญนักวิชาการ ในการขับเคลื่อนแผนปฏิบัติการและโครงการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

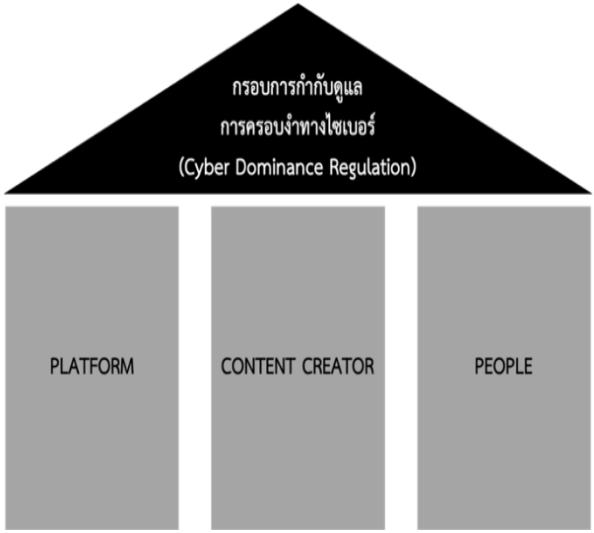
ข้อเสนอแนะ

การวิจัยครั้งนี้ ได้เสนอ กรอบแนวคิดการกำกับดูแลภัยคุกคามทางไซเบอร์ ในมิติการครอบงำทางไซเบอร์เป็นหลัก ในการพัฒนาและปรับปรุงนโยบาย มาตรการทางกฎหมาย และระเบียบปฏิบัติ โดยแบ่งออกเป็น 3 เสาหลัก ได้แก่

เสาที่ 1 แพลตฟอร์ม (Platform) หมายถึง แพลตฟอร์มดิจิทัล สื่อสังคมออนไลน์ หรือเทคโนโลยีด้านความมั่นคง เพื่อใช้เป็นเครื่องมือสำคัญในการรับมือการภัยคุกคามทางไซเบอร์ ยกตัวอย่างแพลตฟอร์มที่เป็นที่นิยมในประเทศไทย เช่น เฟซบุ๊ก (Facebook), ไลน์ (Line), ทวิตเตอร์ (Twitter), อินสตาแกรม (Instagram), ยูทูป (YouTube), คลับเฮาส์ (Clubhouse), ติ๊กต๊อก (Tiktok), วิกิพีเดีย (Wikipedia) เป็นต้น

เสาที่ 2 ผู้ผลิตเนื้อหาออนไลน์ (Content Creator) หมายถึง ผู้สร้างสรรค์และผลิตเนื้อหาบนสื่อต่างๆ ทั้งสื่อออฟไลน์ และออนไลน์ โดยมีจุดประสงค์ในการสื่อสารเนื้อหาเหล่านั้นกับกลุ่มผู้ติดตามลูกค้า (Target Audience) บนช่องทางของพวกเขา โดย Content Creator จะเป็นผู้เล่าเรื่องผ่านการเขียน การทำวิดีโอ หรือการทำรูปภาพกราฟิกในหัวข้อที่เชี่ยวชาญ หรือสนใจเป็นพิเศษและใช้เรื่องราวเหล่านั้นพูดคุยกับกลุ่มผู้ติดตาม หรือแม้แต่ดึงดูดผู้ติดตามใหม่ๆ ซึ่ง Content Creator มีชื่อเรียกหลากหลายรูปแบบ เช่น Influencer, Blogger หรือ Vlogger, Freelance หรือนักผลิตคอนเทนต์ในองค์กร (In-House) เป็นต้น นอกจากนี้ ยังรวมถึงสำนักข่าวออนไลน์ (Official)

เสาที่ 3 ผู้ใช้ (People) หมายถึง ผู้ใช้งานโซเชียลมีเดียทุกๆ ชนิด รวมถึง ผู้บริโภคสื่อออนไลน์ในทุกๆ แพลตฟอร์ม



ภาพ 2 กรอบการกำกับดูแลภัยคุกคามทางไซเบอร์ ในมิติการครอบงำทางไซเบอร์

ข้อเสนอแนะ ตามกรอบการกำกับดูแลภัยคุกคามทางไซเบอร์ มีดังต่อไปนี้

เสาที่ 1 แพลตฟอร์ม (Platform) มีข้อเสนอแนะ ดังนี้

1) สร้างแพลตฟอร์ม social media หรือแอพพลิเคชั่นสำหรับคนไทย จะเห็นได้จากปรากฏการณ์ “นโยบายคนละครึ่ง” ทำให้คนไทยเข้าถึงเทคโนโลยี

ดิจิทัลผ่านแอพฯ “เป๋าตัง” ซึ่งเป็นจุดเริ่มต้นที่ดีในการต่อยอดแอพฯ “เป๋าตัง” ไปสู่ซูเปอร์แอพ (Super App) ที่รวมบริการต่าง ๆ ของภาครัฐ หรือเปิดให้บริการดิจิทัลโดยเอกชนเข้ามาเชื่อมต่อระบบกับแอพฯ “เป๋าตัง” ซึ่งเป็นอีวอลเล็ต (E-Wallet) เพื่อชำระค่าสินค้าบริการ เริ่มจากบริการภาครัฐ เช่น ชำระค่าสาธารณูปโภค ค่าน้ำ ค่าไฟ ชำระภาษี ต่อทะเบียนรถยนต์ เป็นต้น ก่อนต่อยอดไปสู่การเป็นโครงสร้างพื้นฐานการชำระเงินให้กับภาคธุรกิจและเอสเอ็มอี เพื่อลดการพึ่งพาแอพพลิเคชั่นจากต่างประเทศ

2) กำหนดให้เจ้าของแพลตฟอร์มดิจิทัล หรือผู้ให้บริการสื่อสังคมออนไลน์ ในฐานะผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor) จำเป็นต้องจัดเก็บข้อมูลต่าง ๆ ภายในประเทศ เช่น ข้อมูลระบุตัวตนของผู้ใช้งาน, ข้อมูลประวัติการใช้งาน (Logs) ของผู้ใช้งาน เป็นต้น รวมถึงต้องประมวลผลข้อมูลภายในประเทศเท่านั้น

3) ผู้ให้บริการแพลตฟอร์มดิจิทัล/สื่อสังคมออนไลน์ จะต้องจัดตั้งอยู่ภายในประเทศ (ที่อยู่ติดต่อทางกายภาพในประเทศไทย)

4) ผู้ให้บริการแพลตฟอร์มดิจิทัล/สื่อสังคมออนไลน์ ต้องจัดประเภทและควบคุมเนื้อหาที่เผยแพร่ให้เป็นไปตามที่กฎหมายกำหนด หากผู้รับบริการ (User) ได้รับผลกระทบจากการเผยแพร่เนื้อหาที่ไม่เหมาะสม ผู้ให้บริการฯ จำเป็นต้องรับผิดชอบในการชดใช้ค่าเสียหาย และการดำเนินคดีตามกฎหมายที่เกี่ยวข้อง

5) เจ้าของบัญชี มีสิทธิ์ขอไม่ให้ เข้าถึง / เปิดเผย / ค้นหาข้อมูลส่วนบุคคล บนแพลตฟอร์มดิจิทัลได้

6) กองทัพบกควรพัฒนาแพลตฟอร์มดิจิทัลด้านสื่อสังคมออนไลน์และการติดต่อสื่อสารเป็นของหน่วยงานเอง เนื่องจากปัจจุบัน ทบ. มีแอพพลิเคชั่นบนมือถือ “Smart Soldier” จึงสามารถต่อยอดเป็น Super App ให้สามารถเข้าถึงกลุ่มเป้าหมายและนำข้อมูลมาวิเคราะห์เพื่อจัดนำนโยบายให้ตอบสนองความต้องการของกำลังพลและประชาชน

เสาที่ 2 ผู้ผลิตเนื้อหาออนไลน์ มีข้อเสนอแนะ ดังนี้

1) จัดตั้งหน่วยงานกำกับดูแลผู้ผลิตเนื้อหาออนไลน์โดยเฉพาะ เพื่อทำหน้าที่จัดระเบียบให้เป็นไปตามที่กฎหมายกำหนด

2) ออกกฎหมายเพื่อกำกับดูแลผู้ผลิตเนื้อหาสื่อ (Influencer) โดยเริ่มต้นจากการคัดกรองเพื่อติดตามกลุ่มคนดังที่เป็น Influencer โดยมีจำนวนผู้ติดตามบนสื่อสังคมออนไลน์ อยู่ในระดับ 1 แสนคนขึ้นไปจนถึงหลักล้าน เช่น ดารา เซเลบริตี้ ไฮโซ เป็นต้น เป็นการสร้างความตระหนักรู้ที่เป็นแบบ Mass Awareness

3) กองทัพบกได้มีการฝึกอบรมการสร้างการรับรู้การใช้งานสื่อสังคมออนไลน์อย่างสร้างสรรค์ โดยการคัดเลือกกำลังผลที่มีศักยภาพด้านการผลิตและเผยแพร่สื่อ เพื่อเป็นเครือข่าย Influencer ทั้งกำลังพล ครอบครัว และชุมชน เช่น โครงการมัคคุเทศก์น้อย ที่ได้นำลูกหลานกำลังพลมาเข้าค่ายกิจกรรมผลิตสื่อและประชาสัมพันธ์บนช่องทางออนไลน์ เป็นต้น

เสาที่ 3 ผู้ใช้ (People) มีข้อเสนอแนะ ดังนี้

1) กำหนดบทลงโทษทางกฎหมายให้เข้มงวด / เพิ่มค่าปรับ เมื่อเป็นการกระทำความผิดที่มุ่งเน้นไปที่การครอบงำทางไซเบอร์ เช่น เอาผิดกับบุคคล

ที่ลงข้อความที่ก่อให้เกิดความเกลียดชังทางอินเทอร์เน็ต (Hate Speech), การกลั่นแกล้งบุคคลทางสื่อโซเชียล (Cyber Bullying) เป็นต้น

2) การสร้างการตระหนักรู้การเข้าใจดิจิทัลให้แก่ประชาชน โดยมีกระบวนการสร้างความร่วมมือและภาคีเครือข่ายระหว่างหน่วยงานด้านการศึกษา เช่น กระทรวงศึกษาธิการ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นต้น กับหน่วยงานเอกชน เพื่อผลิตสื่อการเรียนรู้ ตำรา หนังสือสำหรับพลเมืองไทย บรรจุเป็นหลักสูตรในสถานศึกษา และเผยแพร่สร้างการรับรู้ผ่านกิจกรรมและสื่อออนไลน์

3) ประเทศไทยสามารถใช้มาตรการสารนิเทศของกองทัพบก เป็น sandbox ขยายการนำนโยบายไปสู่การปฏิบัติต่อหน่วยงานความมั่นคงในเหล่าทัพอื่นๆ เช่น กองทัพเรือ กองทัพอากาศ และสำนักงานตำรวจแห่งชาติ เป็นต้น

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1) ควรศึกษาแนวทางการปรับปรุงขั้นตอน (Protocol) กระบวนการ (Process) ในการดำเนินคดีทางกฎหมายไซเบอร์ ให้ครอบคลุมพื้นที่กำกับดูแลทั้งในประเทศและต่างประเทศ

2) ควรศึกษาแนวทางการจัดทำมาตรฐาน และการปรับกลยุทธ์ในการรับมือกับสงครามสมัยใหม่และการใช้ระบบมาตรฐานทางไซเบอร์ อาทิ ISO27001

3) ควรศึกษาแนวทางในการจัดเก็บเงินจากแพลตฟอร์มโซเชียลมีเดียต่างประเทศ เนื่องจากการที่บริษัทเอกชนดำเนินการแสวงหากำไร โดยใช้โครงสร้างพื้นฐานของรัฐ บริษัทเหล่านี้ควรมีหน้าที่จ่ายเงินให้กับรัฐในอัตราที่

เหมาะสม ในกรณีของไทยแพลตฟอร์มโซเชียลมีเดียที่ใช้โครงสร้างพื้นฐานโทรคมนาคมของไทยก็ควรจ่ายเงินให้กับรัฐไทย

4) ควรศึกษามิติอำนาจของสังคมเครือข่าย (Network Society) มีข้อพิจารณาอยู่ 4 ประการ คือ 1. Network 2. กฎ ระเบียบของแพลตฟอร์มดิจิทัล 3. Influencer และ 4. เจ้าของแพลตฟอร์ม

เอกสารอ้างอิง

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, พฤษภาคม 27). *ราชกิจจานุเบกษา. 136*(69 ก), 20-51

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562, พฤษภาคม 27). *ราชกิจจานุเบกษา. 136*(69 ก), 52-95.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (2550, มิถุนายน 18). *ราชกิจจานุเบกษา. 124* (27 ก), 4-13.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560. (2560, มกราคม 24). *ราชกิจจานุเบกษา. 134*(10 ก), 24-35.

สิทธิพันธ์ พุทธหุน. (2564). *เอกสารประกอบการบรรยายวิชาการกำหนดและการวิเคราะห์นโยบายสาธารณะ*. กรุงเทพมหานคร: มหาวิทยาลัยรามคำแหง, โครงการรัฐประศาสนศาสตรมหาบัณฑิต.

Global Cybersecurity Capacity Centre. (2016). *Cybersecurity capacity maturity model for nations (CMM)*. Revised Edition. Oxford, United Kingdom: University of Oxford.