



รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง การแก้ไขปัญหายัยคุกคามทางไซเบอร์ภายใต้นโยบาย
และแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติระยะต่อไป
(พ.ศ. 2571-2575)

จัดทำโดย นายรพี โล่ชัยยะกุล
รหัส 17003

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูต รุ่นที่ 17 ปี 2569
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ
ลิขสิทธิ์ของกระทรวงการต่างประเทศ



รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง การแก้ไขปัญหาย้ายคุกคามทางไซเบอร์ภายใต้นโยบาย
และแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติระยะต่อไป
(พ.ศ. 2571-2575)

จัดทำโดย นายรพี โล่ชัยยะกุล
รหัส 17003

หลักสูตรนักบริหารการทูต รุ่นที่ 17 ปี 2569
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ
รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา



เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูตของกระทรวงการต่างประเทศ

ลงชื่อ.....

(เอกอัครราชทูต ดร.จริย์วัฒน์ สันตะบุตร)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(เอกอัครราชทูตปัญญรักษ์ พูลทรัพย์)

อาจารย์ที่ปรึกษา

ลงชื่อ.....

(ศาสตราจารย์กิตติคุณ ดร.ไชยวัฒน์ คำชู)

อาจารย์ที่ปรึกษา

บทสรุปสำหรับผู้บริหาร

รายงานการศึกษาฉบับนี้มุ่งศึกษาการแก้ไขปัญหากลไกความทางไซเบอร์ เพื่อจัดทำข้อเสนอสำหรับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติระยะต่อไป (พ.ศ. 2571-2575) โดยมีวัตถุประสงค์เพื่อศึกษารูปแบบ วิธีการ สถานการณ์ และผลกระทบของกลไกความทางไซเบอร์ต่อความมั่นคงของชาติ ตลอดจนเสนอแนวทางเชิงนโยบายที่เหมาะสมกับบริบทของประเทศไทย การศึกษาใช้ระเบียบวิธีเชิงคุณภาพแบบพรรณนาเชิงวิเคราะห์ โดยรวบรวมข้อมูลจากกฎหมาย เอกสารนโยบาย รายงานสถานการณ์ งานวิชาการ และกรณีศึกษาแนวปฏิบัติที่ดีของต่างประเทศ รวมทั้งพิจารณาความร่วมมือในกรอบอาเซียน สหประชาชาติ และความร่วมมือกับประเทศคู่สัมพันธ์ที่สำคัญ

ผลการศึกษาพบว่า กลไกความทางไซเบอร์ได้พัฒนาจากปัญหาด้านความมั่นคงปลอดภัยของระบบสารสนเทศไปสู่เครื่องมือเชิงยุทธศาสตร์ที่รัฐ อาชญากร และตัวแสดงที่มีใช้รัฐสามารถนำมาใช้เพื่อการจารกรรม การก่ออาชญากรรม การบ่อนทำลายโครงสร้างพื้นฐานสำคัญ การสร้างอิทธิพล และการสนับสนุนปฏิบัติการทางทหาร ภัยดังกล่าวมีลักษณะข้ามพรมแดน เกิดขึ้นอย่างรวดเร็ว ระบุตัวผู้กระทำได้ยาก และสามารถสร้างผลกระทบต่อเศรษฐกิจ สังคม การเมือง การต่างประเทศ และความมั่นคงของชาติได้พร้อมกัน อย่างไรก็ตาม การดำเนินงานของไทยในปัจจุบันยังให้น้ำหนักกับการตรวจจับ ป้องกัน และรับมือเหตุในเชิงเทคนิคเป็นหลัก ทำให้ยังไม่สามารถเชื่อมโยงเหตุการณ์ทางไซเบอร์กับตัวแสดง เจตนา และวัตถุประสงค์เชิงยุทธศาสตร์ได้อย่างเป็นระบบ

ข้อจำกัดสำคัญที่พบ ได้แก่ การขาดกลไกประเมินกลไกความทางไซเบอร์และการระบุตัวผู้กระทำ การไม่มีชุดเครื่องมือตอบสนองเชิงนโยบายที่พร้อมใช้ การทำงานและข้อมูลที่กระจุกกระจายอยู่ในหลายหน่วยงาน ตลอดจนการพึ่งพาความร่วมมือทวิภาคีกับมหาอำนาจมากกว่ากลไกพหุภาคี นอกจากนี้ ไทยยังใช้ประโยชน์จากสถานะประเทศขนาดกลาง ที่ตั้งของศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงไซเบอร์ และความสัมพันธ์ที่สมดุลกับประเทศมหาอำนาจได้ไม่เต็มศักยภาพ ขณะที่กรณีศึกษาของสหราชอาณาจักร ญี่ปุ่น สิงคโปร์ เนเธอร์แลนด์ และประเทศอื่น ๆ แสดงให้เห็นว่า การเพิ่มขีดความสามารถเชิงรุกต้องดำเนินควบคู่กับการแบ่งบทบาทหน่วยงานที่ชัดเจน กรอบกฎหมาย ความโปร่งใส และกลไกกำกับตรวจสอบที่มีประสิทธิภาพ

ผลการศึกษาข้างต้นนำไปสู่การมีข้อเสนอเชิงนโยบายหลัก คือ ไทยต้องเพิ่มกรอบการมองกลไกความทางไซเบอร์จากปัญหาเชิงเทคนิคไปสู่ปัญหาเชิงการเมืองและยุทธศาสตร์ โดยบูรณาการ

การดำเนินงานในสี่มิติ ได้แก่ ความมั่นคงปลอดภัยไซเบอร์ การทูตไซเบอร์ การป้องกันประเทศทางไซเบอร์ และการปราบปรามอาชญากรรมทางไซเบอร์ พร้อมเร่งพัฒนากำลังคนและอุตสาหกรรมภายในประเทศ ยกกระตือรือร้นการคุ้มครองโครงสร้างพื้นฐานสำคัญ จัดทำรายงานประเมินภัยคุกคามระดับชาติประจำปี พัฒนาขีดความสามารถในการระบุตัวผู้กระทำ จัดทำชุดมาตรการตอบสนองที่ได้สัดส่วน สร้างกลไกแลกเปลี่ยนข้อมูลระหว่างรัฐ เอกชน และภาควิชาการ ตลอดจนเตรียมรับมือความเสี่ยงจากปัญญาประดิษฐ์และเทคโนโลยีควอนตัมที่กำลังคืบคลานเข้ามาในระยะเวลานี้

การขับเคลื่อนการดำเนินงานในระยะต่อไป ควรให้สภาความมั่นคงแห่งชาติกำกับนโยบายในภาพรวม โดยมีสำนักงานสภาความมั่นคงแห่งชาติเป็นเจ้าภาพประสานภารกิจข้ามหน่วยงาน ผ่านกลไกอำนวยการร่วมที่กำหนด ส่วนตัวชี้วัดผลการดำเนินงานควรเน้นผลลัพธ์ด้านขีดความสามารถ ความรวดเร็วในการตัดสินใจและประสิทธิผลของการตอบสนอง ทั้งนี้ ความสำเร็จของนโยบายขึ้นอยู่กับเจตจำนงทางการเมือง การจัดสรรงบประมาณและบุคลากรอย่างเพียงพอ รวมถึงความไว้วางใจของประชาชนต่อการใช้อำนาจรัฐอย่างโปร่งใส รับผิดชอบ และตรวจสอบได้ ทั้งหมดนี้จะส่งผลให้ไทยเปลี่ยนจากการตั้งรับไปสู่การดำเนินนโยบายไซเบอร์เชิงรุกอย่างมีความรับผิดชอบ และสามารถรักษาผลประโยชน์แห่งชาติได้อย่างมั่นคงและยั่งยืนในระยะยาว

กิตติกรรมประกาศ

รายงานการศึกษาฉบับนี้ เป็นความพยายามที่จะศึกษาเพิ่มเติมเกี่ยวกับการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของไทยในกรอบนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติระยะต่อไป (พ.ศ. 2571-2575) ซึ่งขณะนี้สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ในฐานะหน่วยรับผิดชอบการจัดทำนโยบายฉบับนี้ตามพระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. 2559 อยู่ระหว่างนำร่างนโยบายเสนอกลไกที่เกี่ยวข้องพิจารณาให้ความเห็นชอบก่อนประกาศใช้อย่างเป็นทางการในปีงบประมาณ พ.ศ. 2571 ต่อไป

ดังนั้น ผู้เขียนจึงขอใช้โอกาสที่ได้จัดทำรายงานการศึกษาส่วนบุคคลในการศึกษาหลักสูตรนักบริหารการทูต (นบท.) รุ่นที่ 17 เสนอมุมมองหรือแนวคิดเพิ่มเติมเกี่ยวกับปัญหานี้ในอีกแง่มุมหนึ่งนอกเหนือจากที่เป็นผู้รับผิดชอบกำกับดูแลงานไซเบอร์ด้านความมั่นคงในประเด็นภัยคุกคามข้ามชาติที่ สมช. รับผิดชอบในระดับนโยบาย ซึ่งในการจัดทำรายงานจำเป็นต้องได้รับการสนับสนุนหรือความช่วยเหลือด้านข้อมูลหรืออื่น ๆ จากผู้ที่เกี่ยวข้อง โดยเฉพาะผู้ร่วมงานที่ สมช. อย่างรอบด้านที่สุดในรอบระยะเวลาอันจำกัด จึงต้องขอขอบคุณทุกท่านตามที่ได้กล่าวมาเป็นอย่างสูงไว้ ณ ที่นี้

อนึ่ง คงต้องกล่าวขอบคุณท่านอาจารย์ที่ปรึกษาทุกท่านที่กรุณาให้คำแนะนำที่ช่วยให้การจัดทำรายงานเป็นไปด้วยความเรียบร้อย ตลอดจนเจ้าหน้าที่ประจำหลักสูตรที่ให้ความเอื้อเฟื้อช่วยเหลือผู้เขียนเป็นอย่างดี และหวังว่ารายงานนี้น่าจะเป็นประโยชน์กับผู้อ่านตามความเห็นสมควรต่อไป

รพี โล่ชัยยะกุล

กันยายน 2569

สารบัญ

บทสรุปสำหรับผู้บริหาร	ง
กิตติกรรมประกาศ	ฉ
สารบัญ	ช
บทที่ 1 บทนำ	1
1.1 ภูมิหลัง และความสำคัญของหัวข้อที่จะศึกษา	1
1.2 การวิเคราะห์ความสำคัญเชิงยุทธศาสตร์ของส่วนราชการ	12
บทที่ 2 การวิเคราะห์ประเด็นศึกษาและผลการศึกษา	17
2.1 การกำหนดประเด็นศึกษา	17
2.2 การวิเคราะห์ประเด็นศึกษา	19
2.3 สรุปผลการศึกษา	35
บทที่ 3 ข้อเสนอ	38
3.1 ข้อเสนอเชิงนโยบาย	38
3.2 ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ	43
บรรณานุกรม	48
ภาคผนวก	55
ประวัติผู้เขียน	57

บทที่ 1

บทนำ

ความมั่นคงของรัฐในห้วงหลายทศวรรษที่ผ่านมาได้เปลี่ยนผ่านจากกรอบความมั่นคงรูปแบบเก่าที่ให้น้ำหนักกับภัยคุกคามทางทหารระหว่างรัฐ การรุกรานดินแดน และการแข่งขันสะสมกำลังรบ ไปสู่กรอบความมั่นคงรูปแบบใหม่ที่ตัวแสดงมีได้จำกัดอยู่เพียงรัฐ ขอบเขตของภัยไม่ผูกติดกับพรมแดน และเส้นแบ่งระหว่างความมั่นคงภายในกับความมั่นคงภายนอกพรั่นเลือนลง¹

เอกสารยุทธศาสตร์ของไทยได้สะท้อนการเปลี่ยนผ่านดังกล่าวมาระยะหนึ่งแล้ว โดยยุทธศาสตร์กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2560-2564 ได้จำแนกภัยคุกคามรูปแบบใหม่ไว้ถึงเก้าประเภทซึ่งมีภัยคุกคามทางไซเบอร์รวมอยู่ด้วย² ในบรรดาภัยคุกคามรูปแบบใหม่เหล่านี้ ภัยคุกคามทางไซเบอร์มีลักษณะเฉพาะที่ทำให้ต้องได้รับความสนใจเป็นพิเศษ กล่าวคือ เป็นภัยที่แทรกอยู่ในโครงสร้างพื้นฐานและกิจกรรมทางเศรษฐกิจและสังคมแทบทุกด้าน สามารถถูกใช้เป็นเครื่องมือของทั้งอาชญากร กลุ่มก่อการร้าย และรัฐผู้กระทำการ รายงานฉบับนี้จึงมุ่งศึกษาการกำหนดนโยบายเพื่อรับมือภัยคุกคามทางไซเบอร์ในฐานะประเด็นความมั่นคงที่มีมิติทั้งทางเทคนิค เศรษฐกิจ สังคม และการเมืองระหว่างประเทศ

1.1 ภูมิหลัง และความสำคัญของหัวข้อที่จะศึกษา

1.1.1 ความหมายของความมั่นคงปลอดภัยไซเบอร์ และนิยามภัยคุกคามทางไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security หรือ Cybersecurity) ในความหมายพื้นฐานที่สุด หมายถึง การธำรงรักษาคุณสมบัติสามประการของสารสนเทศและระบบสารสนเทศ อันได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ซึ่งวงการวิชาการและวิชาชีพเรียกรวมกันว่า "CIA Triad" กรอบแนวคิดนี้ทำหน้าที่เป็นเกณฑ์ตัดสินว่าเหตุการณ์ใดถือเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย เพราะทุกครั้งที่

¹ คณะที่ปรึกษาของสภาความมั่นคงแห่งชาติด้านการข่าวกรอง, “การประเมินกำลังอำนาจของชาติ (National Power) และภัยคุกคามรูปแบบใหม่,” วารสารมุมมองความมั่นคง ฉบับที่ 7 (มิถุนายน-กันยายน 2564): 5-16.

² กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, ยุทธศาสตร์กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2560-2564, [ออนไลน์], 2560, แหล่งที่มา: https://isoc.go.th/uploads/ITA/O4/O4_ยุทธศาสตร์_กอ_รมน.2560-2564 [12 สิงหาคม 2569].

คุณสมบัติข้อใดข้อหนึ่งถูกระทบ ระบบย่อมเกิดความสูญเสียหรือเสียหายต่อผู้ใช้งานทันที ตำราที่เกี่ยวข้องในภาษาไทย อธิบายตรงกันว่า ความปลอดภัยของคอมพิวเตอร์ คือ การรักษาความลับ ความถูกต้อง และความพร้อมใช้ของทรัพยากรระบบสารสนเทศ ตั้งแต่ระดับฮาร์ดแวร์ขึ้นไป³ ครอบคลุม (1) ฮาร์ดแวร์และอุปกรณ์ทางกายภาพ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล อุปกรณ์จัดเก็บข้อมูล (2) อุปกรณ์ปลายทาง เช่น โทรศัพท์เคลื่อนที่ แท็บเล็ต และอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) ที่เชื่อมต่อถึงกันผ่านระบบเครือข่าย สามารถแลกเปลี่ยนข้อมูลหรือเชื่อมต่อกันได้อย่างอัจฉริยะ และรองรับการควบคุมอัตโนมัติ (3) เฟิร์มแวร์และระบบปฏิบัติการ (4) ข้อมูล และ (5) ผู้ใช้งาน กระบวนการทำงาน และนโยบายหรือการกำกับดูแลขององค์กร

การรักษาความลับ หมายถึง การทำให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่เข้าถึงข้อมูลได้ การละเมิดคุณสมบัติข้อนี้จึงปรากฏในรูปของการจารกรรมข้อมูล การลักลอบดักจับสัญญาณ และการนำข้อมูลส่วนบุคคลออกไปเผยแพร่หรือซื้อขาย ในบริบทของไทยเหตุการณ์ข้อมูลผู้ป่วยและข้อมูลประชาชนรั่วไหลจากระบบของหน่วยงานรัฐหลายครั้งในช่วง พ.ศ. 2564-2568 สะท้อนการสูญเสียคุณสมบัติข้อนี้อย่างชัดเจน⁴

ความถูกต้องครบถ้วน หมายถึง การทำให้ข้อมูลและระบบไม่ถูกแก้ไขเปลี่ยนแปลง โดยผู้ที่ไม่มีความสิทธิ ภัยที่กระทบคุณสมบัติข้อนี้จึงมีได้จำกัดอยู่เพียงการลบหรือแก้ไขตัวเลขในฐานข้อมูล หากยังรวมถึงการแทรกแซงคำสั่งควบคุมเครื่องจักรในโรงงานอุตสาหกรรมและระบบควบคุมโครงสร้างพื้นฐานสำคัญ ซึ่งอาจสร้างผลกระทบทางกายภาพต่อชีวิตและทรัพย์สินได้โดยตรง

ความพร้อมใช้งาน หมายถึง การทำให้ผู้ใช้ที่มีสิทธิสามารถเข้าถึงระบบและข้อมูลได้ เมื่อจำเป็น การโจมตีแบบปฏิเสธการให้บริการ (Distributed Denial of Service-DDoS) และมัลแวร์เรียกค่าไถ่ (Ransomware) เป็นตัวอย่างที่ชัดเจนที่สุดของการทำลายคุณสมบัติข้อนี้ เพราะทั้งสองรูปแบบมุ่งทำให้บริการหยุดชะงักมากกว่ามุ่งขโมยข้อมูล และเมื่อบริการที่หยุดชะงัก เป็นบริการสาธารณะ ผลกระทบย่อมขยายจากระดับองค์กรไปสู่ระดับสังคมอย่างรวดเร็ว

ดังนั้น ภัยคุกคามทางไซเบอร์ (Cyber Threat) จึงนิยามได้ว่า คือ การกระทำใด ๆ ที่มุ่งทำลายคุณสมบัติทั้งสามประการข้างต้น ซึ่งไทยได้บัญญัตินิยามดังกล่าวไว้เป็นกฎหมายแล้วโดย มาตรา 3 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดว่า "ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมีมุ่งทำให้เกิดการประทุษร้าย

³ มหาวิทยาลัยสุโขทัยธรรมาธิราช, ความมั่นคงปลอดภัยของระบบสารสนเทศ, เอกสารการสอนชุดวิชา 96101 หน่วยที่ 14, [ออนไลน์], 2566, แหล่งที่มา: <https://www.stou.ac.th/Schools/sst/main/Subject96101/96101-14.pdf> [12 สิงหาคม 2569].

⁴ ประชาไท, ข้อมูลคนไทยหลุดซ้ำ ๆ หน่วยงานไทยยังถูกโจมตีหนัก 1 ปี 3 เดือน ไทยเจอภัยกว่า 2,700 ครั้ง, [ออนไลน์], 2568, แหล่งที่มา: <https://prachatai.com/journal/2025/04/112536> [12 สิงหาคม 2569].

ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง⁵

พระราชบัญญัติฉบับเดียวกันยังจำแนกระดับความรุนแรงของภัยคุกคามออกเป็นสามระดับ ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ พร้อมกำหนดกลไกการยกระดับและการประสานงานที่แตกต่างกันในแต่ละระดับ นอกจากนี้ กฎหมายยังกำหนดให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ต้องจัดทำแผนพร้อมรับมือ มีเจ้าหน้าที่เผชิญเหตุ และรายงานเหตุผ่านกลไกกลางของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)⁶

นิยามตามกฎหมายไทยจึงตั้งอยู่บนฐานคิดเชิงเทคนิคเป็นด้านหลัก กล่าวคือกฎหมายอธิบายภัยคุกคามผ่าน "วิธีการกระทำ" และ "ผลกระทบต่อระบบ" มากกว่าจะอธิบายผ่าน "ตัวแสดง" และ "แรงจูงใจเชิงยุทธศาสตร์" ที่อยู่เบื้องหลังการกระทำนั้น ลักษณะเช่นนี้เหมาะสมอย่างยิ่งสำหรับการบังคับใช้กฎหมายและการปฏิบัติการเผชิญเหตุ แต่กลับไม่เพียงพอต่อการวิเคราะห์เชิงนโยบาย เพราะการรับมือภัยที่รัฐต่างชาติอยู่เบื้องหลังย่อมต้องอาศัยความเข้าใจ แรงจูงใจ หรือเจตนาของรัฐอื่น ไม่ใช่เพียงเข้าใจว่ารัฐนั้นใช้ช่องโหว่ใด ประเด็นศึกษาของรายงานฉบับนี้จึงเริ่มต้นจากช่องว่างดังกล่าวนี้

1.1.2 พัฒนาการของภัยคุกคามทางไซเบอร์

การตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ต่อรัฐ มีรากฐานมาจากการข่าวกรองสัญญาณ (Signals Intelligence: SIGINT) ในช่วงสงครามโลกครั้งที่สอง เมื่อฝ่ายสัมพันธมิตรจัดตั้งหน่วยงานถอดรหัสที่ Bletchley Park ในอังกฤษ เพื่อถอดรหัสเครื่อง Enigma ของเยอรมนี และสหรัฐอเมริกาพัฒนาขีดความสามารถแบบเดียวกันเพื่อสนับสนุนปฏิบัติการภูมิภาคเอเชียแปซิฟิก ความสำเร็จดังกล่าวสร้างบทเรียนเชิงยุทธศาสตร์ที่ตกทอดมาถึงปัจจุบันสองประการ ประการแรก คือ การเข้าถึงการสื่อสารของฝ่ายตรงข้ามอาจสร้างความได้เปรียบชี้ขาดผลของสงครามได้ และประการที่สอง คือ การใช้ขีดความสามารถเช่นนี้ต้องอาศัยความลับอย่างยิ่งยวด เพราะทันทีที่ฝ่ายตรงข้ามรู้ว่ารหัสถูกถอดได้ความได้เปรียบที่เคยได้รับอาจหายไป หลักการทั้งสองข้อนี้ยังคงกำกับพฤติกรรมของรัฐในพื้นที่ไซเบอร์จนถึงทุกวันนี้ และอธิบายว่าเหตุใดหน่วยข่าวกรองสัญญาณอย่างสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกา (National Security Agency: NSA) และสำนักงานสื่อสารรัฐบาลสหราชอาณาจักร

⁵ สำนักเลขาธิการคณะรัฐมนตรี, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, [ออนไลน์], 2562, หน้า 21-22, แหล่งที่มา: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF [12 สิงหาคม 2569].

⁶ สำนักเลขาธิการคณะรัฐมนตรี, อ้างแล้ว เจริญรทที่ 5, หน้า 28-35.

อาณาจักร (Government Communications Headquarters: GCHQ) จึงกลายเป็นแกนกลางของขีดความสามารถไซเบอร์ของทั้งสองประเทศ

การจารกรรมทางไซเบอร์จึงเป็นรูปแบบแรก และยังคงเป็นรูปแบบที่แพร่หลายที่สุดของการใช้ขีดความสามารถไซเบอร์โดยรัฐ กรณีที่สะท้อนภาพนี้ได้ชัดเจน คือ การเจาะระบบซอฟต์แวร์บริหารเครือข่ายของบริษัท SolarWinds ที่ถูกเปิดเผยเมื่อ พ.ศ. 2563 ซึ่งผู้โจมตีแทรกโค้ดประสงค์ร้ายเข้าไปในระบบของหน่วยงานสหรัฐฯ ส่งผลให้สามารถเข้าถึงเครือข่ายของผู้ใช้งานกว่า 18,000 ราย รวมถึงหน่วยงานรัฐบาลกลางสหรัฐฯ หลายแห่ง เหตุการณ์นี้แสดงให้เห็นว่า การจารกรรมสมัยใหม่ไม่จำเป็นต้องเจาะเป้าหมายโดยตรง แต่สามารถเจาะผ่านอุปกรณ์หรือซอฟต์แวร์ที่องค์กรสำคัญต้องพึ่งพาได้⁷

การใช้เครื่องมือไซเบอร์เพื่อก่อวินาศกรรมโครงสร้างพื้นฐานของรัฐอื่น ปรากฏชัดครั้งแรกในกรณีเอสโตเนียเมื่อ พ.ศ. 2550 ในเดือนเมษายนปีนั้น รัฐบาลเอสโตเนียตัดสินใจย้ายอนุสาวรีย์ทหารโซเวียตออกจากใจกลางกรุงทาลลินน์ (Tallinn) ซึ่งสร้างความไม่พอใจอย่างรุนแรงต่อรัสเซีย และกลุ่มผู้ใช้อินเทอร์เน็ตที่ฝักใฝ่รัสเซีย หลังจากนั้นเว็บไซต์ของรัฐบาล กระทรวงต่าง ๆ ธนาคาร และสื่อมวลชนของเอสโตเนียถูกโจมตีแบบปฏิเสธการให้บริการอย่างต่อเนื่องเป็นเวลาหลายสัปดาห์ ผลกระทบสำคัญ คือ บริการสาธารณะและบริการทางการเงินของประเทศที่พึ่งพาระบบดิจิทัลอย่างสูงต้องหยุดชะงักเป็นระยะ และทำให้จุดแข็งด้านรัฐบาลดิจิทัลของเอสโตเนียกลับกลายเป็นจุดอ่อนในทันที กรณีนี้เป็นครั้งแรกที่ประชาคมระหว่างประเทศตระหนักว่า การโจมตีทางไซเบอร์สามารถถูกใช้เป็นเครื่องมือกดดันทางการเมืองระหว่างรัฐได้จริง⁸

การก่อวินาศกรรมทางไซเบอร์ที่สร้างความเสียหายทางกายภาพ ปรากฏขึ้นในกรณี Stuxnet เมื่อ พ.ศ. 2553 นักวิเคราะห์เชื่อว่าสหรัฐฯ และอิสราเอลร่วมกันพัฒนามัลแวร์ประเภทตัวหนอน (Worm) ในกรณีดังกล่าวภายใต้ปฏิบัติการชื่อ Olympic Games เพื่อแทรกซึมเข้าไปในระบบควบคุมเชิงอุตสาหกรรมของโรงงานเสริมสมรรถนะยูเรเนียมที่เมืองนาทานซ์ (Natanz) ในอิหร่าน มัลแวร์ดังกล่าวถูกออกแบบให้เรียนรู้พฤติกรรมปกติของระบบก่อน แล้วจึงค่อย ๆ สั่งให้เครื่องหมุนเหวี่ยงแยกยูเรเนียมทำงานผิดปกติจนเสียหาย ขณะเดียวกันก็ส่งข้อมูลปลอมกลับไปยังห้องควบคุมเพื่อมิให้ผู้ปฏิบัติงานสังเกตเห็นความผิดปกติ ผลกระทบสำคัญ คือ โครงการนิวเคลียร์ของอิหร่านล่าช้าออกไปประมาณหกเดือนถึงสองปี และความล่าช้าดังกล่าวเมื่อประกอบกับมาตรการกดดันทางเศรษฐกิจได้เพิ่มอำนาจต่อรองให้สหรัฐฯ จนนำไปสู่การเจรจาข้อตกลงนิวเคลียร์ใน พ.ศ.

⁷ ภาณุทัต วัชรภรณ์, “ความขัดแย้งทางไซเบอร์ในมุมมองเชิงยุทธศาสตร์,” วารสารมุมมองความมั่นคง ฉบับที่ 18 (กุมภาพันธ์-พฤษภาคม 2568): 41.

⁸ ภาณุทัต วัชรภรณ์, “เทคโนโลยีสารสนเทศและการสื่อสารกับการเมืองระหว่างประเทศ: การเปลี่ยนแปลงอำนาจรัฐและระเบียบระหว่างประเทศในศตวรรษที่ยี่สิบเอ็ด,” วารสารมุมมองความมั่นคง ฉบับที่ 11 (ตุลาคม 2565-มกราคม 2566): 32.

2558 กรณีนี้จึงเป็นตัวอย่างที่ชัดเจนที่สุดว่า เครื่องมือไซเบอร์ถูกใช้เพื่อ "กำหนดทิศทางการการณ" (shaping) ทางการเมืองระหว่างประเทศได้อย่างไร^{9 10}

การโจมตีระบบไฟฟ้าของยูเครนใน พ.ศ. 2558 และ 2559 ยกระดับความรุนแรงของภัยรูปแบบนี้ขึ้นไปอีกขั้น ในเหตุการณ์เดือนธันวาคม 2558 ผู้โจมตีใช้อีเมลหลอกลวงแบบเจาะจงเป้าหมายเพื่อวางมัลแวร์ BlackEnergy แล้วเข้าควบคุมระบบ SCADA ของการไฟฟ้ายูเครน ส่งผลให้สถานีไฟฟ้าย่อยกว่า 30 แห่ง หยุดทำงาน และประชาชนกว่า 230,000 คน ไม่มีไฟฟ้าใช้นานถึงหกชั่วโมงท่ามกลางอากาศหนาวเย็น¹¹

กรณีล่าสุดที่ยืนยันว่า ภัยรูปแบบนี้ยังคงดำเนินอยู่ คือ การโจมตีโรงไฟฟ้าแห่งหนึ่งในสหราชอาณาจักร เมื่อเดือนสิงหาคม พ.ศ. 2569 โดยมีรายงานว่า กลุ่มผู้โจมตีที่เชื่อมโยงกับรัฐบาลอิหร่านสามารถทำให้โรงไฟฟ้าดังกล่าวหยุดเดินเครื่องนานถึงสี่วัน ซึ่งเชื่อว่าเป็นครั้งแรกที่การโจมตีทางไซเบอร์ประสบความสำเร็จในการปิดโรงไฟฟ้าในสหราชอาณาจักร ทางสหราชอาณาจักรปฏิเสธที่จะเปิดเผยว่าเป็นโรงไฟฟ้าแห่งใดโดยอ้างเหตุผลด้านความมั่นคง แต่ระบุว่าเป็นโรงไฟฟ้าขนาดเล็กและไม่ส่งผลกระทบต่อการผลิตและจ่ายไฟฟ้าของประเทศในภาพรวม¹²

เหตุการณ์ดังกล่าวนี้เกิดขึ้นในห้วงเวลาเดียวกับการโจมตีโครงสร้างพื้นฐานด้านน้ำของสหรัฐฯ ซึ่งส่งผลกระทบต่อ 12 รัฐ โดยโรงบำบัดน้ำเสียหลายสิบแห่งได้รับผลกระทบ เกิดน้ำท่วมและแรงดันน้ำประปาตกลง จนบางพื้นที่ต้องแนะนำให้ประชาชนตม้่น้ำก่อนดื่ม โดยแหล่งข่าวในรัฐบาลสหรัฐฯ ยืนยันภายหลังว่าภัยดังกล่าวน่าจะมีต้นทางจากกรุงเตหะราน ทั้งนี้ อิหร่านได้ยกระดับการโจมตีทางไซเบอร์ต่อประเทศตะวันตกอย่างมีนัยสำคัญท่ามกลางความขัดแย้งในภูมิภาคตะวันออกกลาง โดยเฉพาะหลังจากที่สหรัฐฯ และอิสราเอลเริ่มปฏิบัติการโจมตีทางอากาศในเดือนกุมภาพันธ์ กรณีนี้จึงสะท้อนว่าการก่อวินาศกรรมโครงสร้างพื้นฐานยังถูกใช้เป็นเครื่องมือส่งสัญญาณและกดดันทางการเมืองระหว่างรัฐ มากกว่าจะมุ่งสร้างความเสียหายทางกายภาพในวงกว้าง¹³

รูปแบบถัดมาคือการใช้ขีดความสามารถไซเบอร์เพื่อทำลายองค์กรสำคัญในรัฐอื่นเพื่อตอบโต้ทางการเมือง กรณีบริษัทน้ำมันแห่งชาติซาอุดีอาระเบีย (Saudi Aramco) เมื่อเดือนสิงหาคม พ.ศ. 2555 เป็นตัวอย่างที่ชัดเจน ผู้โจมตีปล่อยมัลแวร์ชื่อ Shamoon ซึ่งลบข้อมูลและเขียนทับ

⁹ ฐิติมาศ ศรีสุข, “สงครามไซเบอร์กับการนิยามใหม่ของการทำสงครามในการเมืองระหว่างประเทศยุคความมั่นคง ฉบับที่ 11 (ตุลาคม 2565-มกราคม 2566): 59.

¹⁰ ภาณุทัต วัชรภรณ์. อ้างแล้ว เชิงอรรถที่ 7, หน้า 48.

¹¹ ฐิติมาศ ศรีสุข, อ้างแล้ว เชิงอรรถที่ 9, หน้า 60-61.

¹² The Telegraph, Iran shut down British power plant in unprecedented cyber attack, [Online], 2026, Available from: <https://www.telegraph.co.uk/news/2026/08/22/iranian-hackers-shut-down-uk-power-plant/> [2026, August 25].

¹³ The Telegraph, อ้างแล้ว เชิงอรรถที่ 12.

ส่วนบันทึกการเริ่มระบบ (Master Boot Record: MBR) ของเครื่องคอมพิวเตอร์ราว 30,000 เครื่องในเวลาไล่เลี่ยกัน ทำให้เครื่องทั้งหมดใช้การไม่ได้ ผลกระทบสำคัญ คือ บริษัทพลังงานที่ใหญ่ที่สุดแห่งหนึ่งของโลกต้องหยุดกระบวนการทางธุรกิจและกลับไปใช้กระดาษเป็นเวลากว่าหนึ่งสัปดาห์ และต้องจัดหาฮาร์ดดิสก์ใหม่จำนวนมหาศาลเพื่อกู้คืนระบบ กลุ่มที่เรียกตนเองว่า Cutting Sword of Justice อ้างความรับผิดชอบ ขณะที่หน่วยข่าวกรองสหรัฐฯ ระบุว่าอิหร่านอยู่เบื้องหลัง¹⁴

กรณีบริษัท Las Vegas Sands เมื่อเดือนกุมภาพันธ์ พ.ศ. 2557 แสดงให้เห็นว่า ถ้อยแถลงทางการเมืองของบุคคลเอกชนก็อาจนำมาซึ่งการตอบโต้ทางไซเบอร์จากรัฐได้ นาย Sheldon Adelson เจ้าของกลุ่มธุรกิจคาสิโนดังกล่าวได้กล่าวในเวทีสาธารณะว่า สหรัฐฯ ควรใช้อาวุธนิวเคลียร์กับอิหร่าน หลังจากนั้นไม่นานผู้โจมตีที่เชื่อว่าเชื่อมโยงกับอิหร่านได้ปล่อยมัลแวร์ทำลายข้อมูลในเครือข่ายของบริษัท จนเซิร์ฟเวอร์ในลาสเวกัสเสียหายราวสามในสี่ และสร้างความเสียหายในการกู้คืนระบบราว 40 ล้านดอลลาร์สหรัฐฯ ผู้โจมตียังยึดหน้าเว็บไซต์ของบริษัทเพื่อเผยแพร่ข้อความเตือนในเชิงการเมือง ผลกระทบเชิงนโยบายที่สำคัญ คือ กรณีนี้ทำให้สหรัฐฯ ตระหนักว่าภาคเอกชนอาจตกเป็นเป้าหมายแทนรัฐได้ และการป้องกันประเทศทางไซเบอร์จึงไม่อาจจำกัดอยู่เพียงเครือข่ายของภาครัฐ¹⁵

กรณีบริษัท Sony Pictures เมื่อปลาย พ.ศ. 2557 เป็นตัวอย่างของการใช้เครื่องมือไซเบอร์เพื่อ "ส่งสัญญาณ" (signaling) ทางการเมือง กลุ่มแฮกเกอร์ที่เรียกตนเองว่า Guardians of Peace เจาะฐานข้อมูลของบริษัทขโมยและลบข้อมูลสำคัญ เผยแพร่อีเมลภายในของผู้บริหาร และทำให้ระบบคอมพิวเตอร์ของทั้งบริษัทใช้การไม่ได้ แรงจูงใจเชื่อมโยงกับการที่บริษัทเตรียมฉายภาพยนตร์ที่มีเนื้อหาเสียดสีผู้นำเกาหลีเหนือ ผลกระทบสำคัญมิได้อยู่ที่มูลค่าความเสียหายทางการเงินเท่านั้น แต่อยู่ที่การที่บริษัทตัดสินใจชะลอการฉายภาพยนตร์ในระยะแรก ซึ่งเท่ากับว่า รัฐหนึ่งสามารถใช้เครื่องมือไซเบอร์บีบบังคับให้เอกชนในอีกรัฐหนึ่งเปลี่ยนพฤติกรรมได้สำเร็จ และเป็นการข่มขู่ผู้ที่คิดจะกระทำการทำนองเดียวกันไปพร้อมกัน^{16 17}

พัฒนาการอีกรูปแบบหนึ่งคือ การใช้ขีดความสามารถไซเบอร์เพื่อแสวงหารายได้ โดยรัฐที่ถูกคว่ำบาตรจากนานาชาติ กลุ่ม Lazarus ซึ่งเชื่อมโยงกับรัฐบาลเกาหลีเหนือเป็นตัวอย่างที่

¹⁴ Council on Foreign Relations, Compromise of Saudi Aramco and RasGas, [Online], 2012, Available from: <https://www.cfr.org/cyber-operations/compromise-of-saudi-aramco-and-rasgas> [2026, August 12].

¹⁵ Bloomberg, Iranian Hackers Hit Sheldon Adelson's Sands Casino in Las Vegas, [Online], 2014, Available from: <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas> [2026, August 12].

¹⁶ ภาณุทัต วัชรภรณ์, อั้งแล้ว เฆนอร์รที่ 8, หน้า 31.

¹⁷ ภาณุทัต วัชรภรณ์, อั้งแล้ว เฆนอร์รที่ 7, หน้า 44.

ชัดเจนที่สุด กลุ่มนี้ก่อเหตุตั้งแต่การโจรกรรมเงินจากธนาคารกลางบังกลาเทศผ่านระบบ SWIFT ใน พ.ศ. 2559 การแพร่กระจายมัลแวร์เรียกค่าไถ่ WannaCry ใน พ.ศ. 2560 ไปจนถึงการโจรกรรมสินทรัพย์ดิจิทัลจากศูนย์ซื้อขายคริปโทเคอร์เรนซี ByBit มูลค่ากว่า 1,500 ล้านดอลลาร์สหรัฐ เมื่อเดือนกุมภาพันธ์ พ.ศ. 2568 ซึ่งถือเป็นการโจรกรรมสินทรัพย์ดิจิทัลครั้งใหญ่ที่สุดในประวัติศาสตร์¹⁸ ผลกระทบเชิงยุทธศาสตร์ที่สำคัญ คือ รายได้จากอาชญากรรมไซเบอร์ยังกลายเป็นแหล่งทุนสำคัญที่หล่อเลี้ยงโครงการขีปนาวุธและนิวเคลียร์ของเกาหลีเหนือ ทำให้มาตรการคว่ำบาตรทางเศรษฐกิจแบบดั้งเดิมมีประสิทธิภาพลดลงอย่างมีนัยสำคัญ^{19 20}

รูปแบบล่าสุดที่สร้างความกังวลมากที่สุด คือ การวางฐานเข้าถึงระบบล่วงหน้า (pre-positioning) โดยไม่ก่อความเสียหายในทันที กลุ่ม Volt Typhoon ซึ่งหน่วยงานความมั่นคงของสหรัฐฯ ระบุว่า ได้รับการสนับสนุนจากรัฐบาลจีน ได้แทรกซึมเข้าสู่เครือข่ายเทคโนโลยีสารสนเทศขององค์กรโครงสร้างพื้นฐานสำคัญในภาคโทรคมนาคม พลังงาน คมนาคม และการประปาของสหรัฐฯ ตั้งแต่ราวกลาง พ.ศ. 2564 โดยใช้เทคนิค “living off the land” ซึ่งอาศัยเครื่องมือที่มีอยู่ในระบบปฏิบัติการอยู่แล้วแทนการติดตั้งมัลแวร์ ทำให้ตรวจจับได้ยากอย่างยิ่ง ผลกระทบเชิงยุทธศาสตร์ที่สำคัญ คือ การฝังตัวดังกล่าวมิได้มุ่งจารกรรมข้อมูล แต่มุ่งเตรียมความพร้อมสำหรับการก่อวินาศกรรมหรือทำลายระบบในห้วงที่เกิดความตึงเครียดทางภูมิรัฐศาสตร์ในอนาคต ซึ่งเท่ากับเป็นการสร้างอำนาจต่อรองไว้ล่วงหน้าโดยที่ฝ่ายป้องกันอาจไม่รู้ตัว^{21 22}

ในห้วงห้าปีข้างหน้า ปัญญาประดิษฐ์ (Artificial Intelligence: AI) สามารถทำให้ภัยไซเบอร์รุนแรงและซับซ้อนยิ่งขึ้นได้ เพราะเทคโนโลยีนี้สามารถลดกำแพงความเชี่ยวชาญที่ผู้โจมตีต้องมี ทำให้ผู้ที่มิมีทักษะจำกัดสามารถสร้างมัลแวร์อีเมลหลอกลวงที่แนบเนียนและเสียงหรือภาพปลอมได้ในต้นทุนต่ำ ขณะเดียวกัน AI ยังสามารถเพิ่มความเร็วและความแม่นยำในการค้นหาช่องโหว่ และ

¹⁸ Techsauce Team, สรุปเหตุการณ์ ByBit โดนแฮก คดีโจรกรรมคริปโตครั้งใหญ่ที่สุดในประวัติศาสตร์ กลุ่มแฮกเกอร์คือใครและทำไมต้องแฮก?, [ออนไลน์], 2568, แหล่งที่มา: <https://techsauce.co/news/bybit-hacked-1-5-billion-crypto-loss> [12 สิงหาคม 2569].

¹⁹ จตุรวิทย์ เครือวานิชกิจ, รู้จัก Lazarus แฮกเกอร์มือฉกาจแห่งเกาหลีเหนือ, [ออนไลน์], 2569, แหล่งที่มา: <https://www.beartai.com/tech/features/1355154> [12 สิงหาคม 2569].

²⁰ THAIRATH Money, เกาหลีเหนือ ขึ้นแท่นแชมป์ถือครองบิตคอยน์อันดับ 3 ของโลกหลังทุ่มทุนปั้นแฮกเกอร์หัวกะทิไว้บ้าน, [ออนไลน์], 2568, แหล่งที่มา: https://www.thairath.co.th/money/tech_innovation/digital_assets/2848265 [12 สิงหาคม 2569].

²¹ Cybersecurity and Infrastructure Security Agency, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Cybersecurity Advisory AA24-038A, [Online], 2024, Available from: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> [2026, August 12].

²² Microsoft Threat Intelligence, Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques, [Online], 2023, Available from: <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/?msocid=1313e5844c506f7c33c9f2e84d0f6e88> [2026, August 12].

การกำหนดเป้าหมาย ซึ่งอาจทำให้ห้วงเวลาที่ฝ่ายป้องกันมีในการตอบสนองสั้นลงอย่างมาก เทคโนโลยีควอนตัม (Quantum)²³ สร้างความเสี่ยงในอีกลักษณะที่ต่างออกไป โดยแม้คอมพิวเตอร์ควอนตัมที่สามารถถอดรหัสซึ่งใช้ปกป้องข้อมูลในปัจจุบันจะยังไม่เกิดขึ้นจริงในระยะอันใกล้ แต่ผู้ไม่ประสงค์ดีสามารถลักลอบเก็บข้อมูลที่เข้ารหัสไว้ในวันนี้เพื่อถอดรหัสในภายหลัง ซึ่งเป็นความเสี่ยงที่เรียกว่า "เก็บเกี่ยววันนี้ ถอดรหัสภายหลัง" (harvest now, decrypt later) ความเสี่ยงนี้กระทบข้อมูลที่ต้องรักษาความลับเป็นเวลานาน เช่น ข้อมูลข่าวกรอง ข้อมูลสุขภาพ และข้อมูลทางการทูต ประเทศที่ก้าวหน้าจึงเริ่มวางแผนเปลี่ยนผ่านไปสู่วิทยาการรหัสที่ต้านทานควอนตัม (Post-Quantum Cryptography: PQC) แล้ว^{24 25}

พัฒนาการทั้งหมดข้างต้นชี้ไปในทิศทางเดียวกันว่า ภัยคุกคามทางไซเบอร์เคลื่อนตัวจากปัญหาทางเทคนิคขององค์กรไปสู่เครื่องมือทางการเมืองของรัฐอย่างชัดเจน ทุกกรณีที่ยกมาล้วนมีแรงจูงใจทางการเมือง ภูมิรัฐศาสตร์ หรือเศรษฐกิจการเมืองเป็นตัวขับเคลื่อน มิใช่เพียงความบกพร่องของระบบเท่านั้น ดังที่นักวิเคราะห์ชี้ว่า "การโจมตีทางไซเบอร์เป็นเพียงอาการของโรค" ซึ่งมีต้นตอมาจากความขัดแย้งระหว่างรัฐในพื้นที่กายภาพ การป้องกันและแก้ไขจึงต้องอาศัยทักษะทางการเมือง นำทักษะทางเทคนิค²⁶

1.1.3 ความพยายามของรัฐในการยับยั้งภัยคุกคามทางไซเบอร์

รัฐต่าง ๆ ตอบสนองต่อพัฒนาการข้างต้นด้วยการจัดตั้งหน่วยงานเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติเป็นลำดับแรก สหรัฐอเมริกาจัดตั้งหน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐาน (Cybersecurity and Infrastructure Security Agency: CISA) ใน พ.ศ. 2561 สหราชอาณาจักรจัดตั้งศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Centre: NCSC) ใน พ.ศ. 2559 และสิงคโปร์จัดตั้งหน่วยงานความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Agency: CSA) ใน พ.ศ. 2558 หน่วยงานเหล่านี้ทำหน้าที่ร่วมกันอย่างน้อยสามประการ ได้แก่ การเป็นศูนย์กลางการเฝ้าระวังและเผชิญเหตุระดับชาติ การกำหนดมาตรฐานและกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญ และการสื่อสารเตือนภัยต่อสาธารณะ

²³ เทคโนโลยีควอนตัม (Quantum Technology) คือ การประยุกต์ใช้คุณสมบัติของอนุภาคระดับควอนตัม เช่น การซ้อนทับของสถานะ (superposition) และการพัวพันเชิงควอนตัม (entanglement) มาประมวลผลข้อมูล คอมพิวเตอร์ควอนตัมจึงคำนวณปัญหาบางประเภทได้เร็วกว่าคอมพิวเตอร์แบบดั้งเดิมอย่างมีนัยสำคัญ ในทางความมั่นคงปลอดภัยไซเบอร์ นัยที่สำคัญที่สุดคือ อัลกอริทึมควอนตัม จะสามารถถอดรหัสระบบเข้ารหัสที่ใช้กันอยู่ในปัจจุบันได้

²⁴ โพสต์ทูเดย์, อย่าชะล่าใจ! ข้อมูลที่ปลอดภัยวันนี้ อาจโดนเจาะในอีก 5 ปี เมื่อ 'ควอนตัม' มาถึง, [ออนไลน์], 2569, แหล่งที่มา: <https://www.posttoday.com/smart-life/737916> [12 สิงหาคม 2569].

²⁵ กรุงเทพธุรกิจ, Q-Day ใกล้กว่าที่คิด! Red Hat แนะ 4 ขั้นตอนรับมือภัยถอดรหัส, [ออนไลน์], 2569, แหล่งที่มา: <https://www.bangkokbiznews.com/tech/ai/1246705> [12 สิงหาคม 2569].

²⁶ ภาณุทัต วัชรภรณ์, อ้างแล้ว เจริญพร 8, หน้า 33.

จุดที่ควรสังเกต คือ หน่วยงานเหล่านี้มิได้ทำหน้าที่เชิงเทคนิคเพียงอย่างเดียว หากยังทำหน้าที่แปลงข้อมูลทางเทคนิคให้เป็นสารสนเทศเชิงยุทธศาสตร์สำหรับผู้กำหนดนโยบายด้วย ตัวอย่างที่ชัดเจน คือ ประกาศเตือนภัยร่วมของ CISA และหน่วยงานพันธมิตรที่ระบุชื่อกลุ่มภัยคุกคามรัฐที่หนุนหลัง และเจตนาเชิงยุทธศาสตร์อย่างเปิดเผย เช่น ประกาศเรื่อง Volt Typhoon ที่กล่าวถึงข้างต้น ซึ่งเป็นเอกสารทางเทคนิคที่มีนัยทางการเมืองระหว่างประเทศอย่างสูง

ในระดับพหุภาคี ประชาคมระหว่างประเทศได้หารือประเด็นความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสารในเวทีสหประชาชาติภายใต้คณะกรรมการชุดที่ 1 ว่าด้วยการลดอาวุธและความมั่นคงระหว่างประเทศมาอย่างต่อเนื่อง กระบวนการดังกล่าวดำเนินผ่านสองกลไกหลัก คือ คณะผู้เชี่ยวชาญภาครัฐ (Group of Governmental Experts: GGE) ซึ่งมีสมาชิกจำกัด และ คณะทำงานปลายเปิด (Open-ended Working Group: OEWS) ซึ่งเปิดให้รัฐสมาชิกทุกประเทศเข้าร่วม ผลลัพธ์ที่สำคัญที่สุดของกระบวนการนี้ คือ รายงาน GGE พ.ศ. 2558 ซึ่งเสนอบรรทัดฐานโดยสมัครใจ 11 ประการ สำหรับพฤติกรรมที่มีความรับผิดชอบของรัฐในพื้นที่ไซเบอร์²⁷

บรรทัดฐานดังกล่าวได้พัฒนาจนกลายเป็นกรอบสหประชาชาติว่าด้วยพฤติกรรมที่มีความรับผิดชอบของรัฐในพื้นที่ไซเบอร์ (UN Framework on Responsible State Behavior in Cyberspace) ซึ่งประกอบด้วย เสาหลักสี่ประการ ได้แก่ การปรับใช้กฎหมายระหว่างประเทศที่มีอยู่ กับพื้นที่ไซเบอร์ การปฏิบัติตามบรรทัดฐานโดยสมัครใจ การดำเนินมาตรการสร้างความไว้วางใจ และการเสริมสร้างศักยภาพ บรรทัดฐานที่สำคัญต่อไทยเป็นพิเศษ ได้แก่ ข้อที่ห้ามิให้รัฐโจมตีโครงสร้างพื้นฐานสำคัญของรัฐอื่น ข้อที่ห้ามิให้รัฐปล่อยให้ดินแดนของตนถูกใช้เป็นฐานในการกระทำผิด และข้อที่กำหนดให้รัฐต้องตอบสนองต่อคำร้องขอความช่วยเหลือจากรัฐอื่น

ความก้าวหน้าล่าสุดของกระบวนการนี้เกิดขึ้นเมื่อวันที่ 11 กรกฎาคม พ.ศ. 2568 เมื่อรัฐสมาชิกสหประชาชาติรวมทั้งไทยร่วมรับรองการจัดตั้งกลไกถาวรด้านความมั่นคงทางไซเบอร์ (Global Mechanism) ในการประชุม OEWS สมัยเนื้อหาสาระครั้งที่ 11 ณ นครนิวยอร์ก กลไกใหม่นี้ นับเป็นครั้งแรกที่สหประชาชาติมีเวทีถาวรสำหรับหารือปัญหาความมั่นคงไซเบอร์ โดยมีภารกิจสำคัญ ครอบคลุมการเสริมสร้างขีดความสามารถของรัฐ การส่งเสริมการใช้เทคโนโลยีอย่างมีความรับผิดชอบ

²⁷ United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, [Online], 2015, Available from: <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf> [2026, August 12].

และการหารือเรื่องภัยคุกคาม การเข้าร่วมของไทยจึงเปิดโอกาสให้ไทยมีส่วนกำหนดกติการะหว่างประเทศแทนที่จะเป็นเพียงผู้รับกติกา²⁸

รัฐจำนวนมากยังได้เผยแพร่เอกสารแสดงท่าทีของประเทศต่อการตีความและปรับใช้กฎหมายระหว่างประเทศในมิติไซเบอร์ (national position papers) เอกสารเหล่านี้อธิบายว่ารัฐนั้นเห็นว่า การกระทำทางไซเบอร์ในระดับใดจึงถือเป็นการแทรกแซงกิจการภายใน การใช้กำลัง หรือการโจมตีด้วยอาวุธตามกฎหมายบัตรสหประชาชาติ การเผยแพร่ท่าทีดังกล่าวสร้างประโยชน์สองประการ คือ ช่วยลดความคลุมเครือในการตีความกฎหมายระหว่างประเทศ และช่วยส่งสัญญาณเส้นแบ่งที่รัฐนั้นยอมรับไม่ได้ให้ฝ่ายตรงข้ามทราบล่วงหน้า คู่มือ Tallinn Manual 2.0 ซึ่งจัดทำโดยคณะผู้เชี่ยวชาญอิสระเป็นเอกสารอ้างอิงที่ใช้กันแพร่หลายในการหารือประเด็นเหล่านี้ แม้จะมีได้มีสถานะผูกพันทางกฎหมายก็ตาม²⁹

การระบุตัวตนผู้กระทำการทางไซเบอร์และการกล่าวโทษอย่างเป็นทางการเป็นสาธารณะ (public attribution) กลายเป็นเครื่องมือเชิงนโยบายที่รัฐใช้เพิ่มขึ้นอย่างต่อเนื่อง กระบวนการนี้ประกอบด้วยขั้นตอนสามระดับขั้น ได้แก่ การระบุเชิงเทคนิคที่อาศัยหลักฐานทางนิติวิทยาศาสตร์ดิจิทัล การระบุเชิงข่าวกรองที่อาศัยแหล่งข่าวหลายแหล่งประกอบกัน และการตัดสินใจเชิงการเมืองว่าจะเปิดเผยหรือไม่และเมื่อใด สหภาพยุโรปได้ก้าวไปอีกขั้นด้วยการตั้งระบอบมาตรการจำกัดต่อการโจมตีทางไซเบอร์ และประกาศใช้มาตรการคว่ำบาตรบุคคลและองค์กรที่อยู่เบื้องหลังการโจมตีเป็นครั้งแรกเมื่อเดือนกรกฎาคม พ.ศ. 2563³⁰ ประเด็นสำคัญ คือ การกล่าวโทษสาธารณะเป็นการตัดสินใจทางการเมืองมิใช่ข้อสรุปทางเทคนิคเพียงอย่างเดียว รัฐอาจเลือกไม่กล่าวโทษแม้จะทราบตัวผู้กระทำการกล่าวโทษนั้นไม่สอดคล้องกับผลประโยชน์ในขณะนั้น

องค์การสนธิสัญญาแอตแลนติกเหนือ (North Atlantic Treaty Organization: NATO) ได้กำหนดเส้นแบ่ง (redline) ต่อภัยคุกคามทางไซเบอร์อย่างชัดเจน โดยประกาศตั้งแต่การประชุมสุดยอดที่เวลส์ใน พ.ศ. 2557 ว่า กฎหมายระหว่างประเทศปรับใช้กับพื้นที่ไซเบอร์ และการโจมตีทางไซเบอร์อาจนำไปสู่การใช้มาตรา 5 ว่าด้วยการป้องกันร่วมกันได้ ต่อมาในการประชุมสุดยอดที่กรุงวอร์ซอ พ.ศ. 2559 NATO ยอมรับว่า ไซเบอร์เป็นปริณทลปฏิบัติทางทหารเช่นเดียวกับ

²⁸ กระทรวงการต่างประเทศ, ไทยร่วมรับรองการจัดตั้งกลไกถาวรด้านความมั่นคงทางไซเบอร์ภายใต้กรอบสหประชาชาติ, [ออนไลน์], 2568, แหล่งที่มา: <https://www.mfa.go.th/th/content/th-endorses-global-mechanism-cyber-security-th> [12 สิงหาคม 2569].

²⁹ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge: Cambridge University Press, 2017).

³⁰ Council of the European Union, *EU Imposes the First Ever Sanctions against Cyber-Attacks*, press release, [Online], 2020, Available from: <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks> [2026, August 12].

ทางบก ทะเล และอากาศ การประกาศเช่นนี้ทำหน้าที่ป้องกันภัยด้วยการสร้างความไม่แน่นอนให้ฝ่ายตรงข้าม เพราะฝ่ายตรงข้ามไม่อาจคาดเดาได้ว่าการกระทำระดับใดจะกระตุ้นการตอบโต้ร่วมของพันธมิตร

ในด้านการป้องกันประเทศ สหรัฐฯ จัดตั้งกองบัญชาการไซเบอร์ (United States Cyber Command: USCYBERCOM) ตั้งแต่ พ.ศ. 2552 เพื่อทั้งป้องกันเครือข่ายของกระทรวงกลาโหม และเตรียมความพร้อมสำหรับปฏิบัติการเชิงรุก³¹ ต่อมาสหรัฐฯ ได้พัฒนาแนวคิด "การป้องกันเชิงรุกล่วงหน้า" (defend forward) และ "การปะทะอย่างต่อเนื่อง" (persistent engagement) ซึ่งตั้งอยู่บนสมมติฐานว่า พื้นที่ไซเบอร์เป็นปริภูมิแห่งการช่วงชิงความได้เปรียบมากกว่าปริภูมิแห่งการบีบบังคับ ดังนั้น การตอบโต้เป็นครั้งคราวจึงไม่เพียงพอ รัฐต้องดำเนินปฏิบัติการอย่างต่อเนื่องเพื่อสะสมความได้เปรียบและลดทอนขีดความสามารถของคู่แข่งตลอดเวลา

สหราชอาณาจักรพัฒนาแนวทางที่แตกต่างออกไปด้วยการจัดตั้งกองกำลังไซเบอร์แห่งชาติ (National Cyber Force: NCF) ใน พ.ศ. 2563 ซึ่งเป็นหน่วยงานร่วมระหว่างกระทรวงกลาโหม และ GCHQ NCF ประกาศหลักการ "การใช้อำนาจไซเบอร์อย่างมีความรับผิดชอบ" (responsible cyber power) ซึ่งเน้นว่า ปฏิบัติการเชิงรุกต้องเป็นไปตามกฎหมาย ได้สัดส่วน และอยู่ภายใต้การกำกับดูแล จุดเด่นของแนวทางนี้ คือ การแยกบทบาทอย่างชัดเจนระหว่างศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Centre: NCSC) ที่ทำหน้าที่ป้องกันอย่างเปิดเผย กับ NCF ที่ทำหน้าที่เชิงรุกอย่างเป็นความลับ ซึ่งช่วยรักษาความไว้วางใจของภาคเอกชนและประชาชนต่อหน่วยงานฝ่ายป้องกันได้

ญี่ปุ่นเป็นตัวอย่างล่าสุดของรัฐที่ปรับเปลี่ยนท่าทีจากการตั้งรับไปสู่การป้องกันเชิงรุก โดยรัฐสภาญี่ปุ่นได้ผ่านกฎหมายว่าด้วยการป้องกันไซเบอร์เชิงรุก (Active Cyber Defense Law: ACD Law) พ.ศ. 2568 กฎหมายฉบับนี้อ่อนุญาตให้หน่วยงานทหารและหน่วยงานบังคับใช้กฎหมายดำเนินมาตรการเชิงรุกเพื่อสกัดกั้นภัยคุกคามก่อนเข้าถึงเป้าหมาย กำหนดให้ผู้ประกอบการโครงสร้างพื้นฐานสำคัญต้องรายงานเหตุ และอนุญาตให้เก็บข้อมูลการสื่อสารในขอบเขตจำกัดเพื่อเฝ้าระวังภัย การเปลี่ยนแปลงนี้จึงมีนัยสำคัญเป็นพิเศษ เพราะขัดกับกรอบความมั่นคงแนวนานาชาติที่ญี่ปุ่นยึดถือมายาวนาน และแสดงว่าแม้รัฐที่ระมัดระวังที่สุดก็เห็นว่าการตั้งรับเพียงลำพังไม่เพียงพออีกต่อไป³²

ภาพรวมของความพยายามข้างต้นชี้ให้เห็นข้อสรุปสำคัญประการหนึ่ง คือ รัฐที่ก้าวหน้าด้านไซเบอร์ไม่ได้ใช้เครื่องมือทางเทคนิคเพียงอย่างเดียวในการรับมือภัยคุกคาม หากใช้

³¹ ภาณุทัต วัชรภรณ์, อ้าวแล้ว เจริญรอกที่ 8, หน้า 30.

³² Center for Cybersecurity Policy and Law, Japan's New Active Cyber Defense Law: A Strategic Evolution in National Cybersecurity, [Online], 2025, Available from: <https://www.centerforcybersecuritypolicy.org/insights-and-research/japans-new-active-cyber-defense-law-a-strategic-evolution-in-national-cybersecurity> [2026, August 12].

เครื่องมือทางการทูต กฎหมาย เศรษฐกิจ ข้าราชการ และการทหารประกอบกัน เป็นชุดเครื่องมือเชิงนโยบาย (policy toolbox) ที่เลือกใช้ได้ตามความรุนแรงของแต่ละสถานการณ์ การมีเครื่องมือที่หลากหลายทำให้รัฐตอบสนองได้อย่างได้สัดส่วนโดยไม่ต้องยกระดับความขัดแย้งเกินควร และทำให้การป้องปรามมีความน่าเชื่อถือมากขึ้น

อย่างไรก็ตาม ความพยายามของรัฐดังกล่าวมิได้หมายความว่า ปัญหาไซเบอร์เป็นเรื่องของหน่วยงานภาครัฐแต่เพียงฝ่ายเดียว เพราะโครงสร้างพื้นฐานสำคัญ ระบบการเงิน โรงพยาบาล และฐานข้อมูลส่วนบุคคลจำนวนมากอยู่ในความครอบครองของภาคเอกชน ภัยคุกคามจึงส่งผลกระทบโดยตรงต่อประชาชนในมิติความมั่นคงของมนุษย์ (human security) ทั้งความปลอดภัยในชีวิตและทรัพย์สิน ความเป็นส่วนตัว การเข้าถึงบริการสาธารณะ และความเชื่อมั่นต่อระบบดิจิทัล การแก้ไขปัญหาจึงต้องมองควบคู่กันทั้งมิติความมั่นคงของรัฐและความมั่นคงของมนุษย์ โดยอาศัยความร่วมมือระหว่างภาครัฐ ภาคเอกชน และประชาชน

1.2 การวิเคราะห์ความสำคัญเชิงยุทธศาสตร์ของส่วนราชการ

1.2.1 มาตรการที่ไทยได้ดำเนินการมา

ไทยได้พยายามปกป้องผลประโยชน์ของชาติในมิติไซเบอร์ด้วยการออกมาตรการหลายชั้นตลอดทศวรรษที่ผ่านมา มาตรการเหล่านี้ครอบคลุมตั้งแต่การตรากฎหมายเฉพาะการจัดทำยุทธศาสตร์ระดับชาติ การบรรจุประเด็นไซเบอร์ไว้ในนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ ไปจนถึงการจัดทำแผนปฏิบัติการเฉพาะด้าน ผลของความพยายามดังกล่าวสะท้อนออกมาในดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index: GCI) ซึ่งจัดโดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) โดยไทยได้รับการจัดอันดับอยู่ในกลุ่มระดับต้นของโลก³³

รากฐานทางกฎหมายที่สำคัญที่สุดคือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กฎหมายฉบับนี้จัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีนายกรัฐมนตรีเป็นประธาน และจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยปฏิบัติหลัก พร้อมกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) และหน้าที่ตามกฎหมายของหน่วยงานเหล่านั้น กฎหมายยังกำหนดกลไกการเผชิญเหตุตามระดับความรุนแรงของภัย ซึ่งถือเป็นการวางโครงสร้างพื้นฐานเชิงสถาบันที่จำเป็นสำหรับการรับมือภัยไซเบอร์ระดับชาติ

³³ Bangkok Bank InnoHub, ไซเบอร์แจ่มความสำเร็จ ไทยครองอันดับ 7 โลกด้านความปลอดภัยทางไซเบอร์, [ออนไลน์], 2567, แหล่งที่มา: <https://www.bangkokbankinnohub.com/th/thailand-ranks-7th-in-global-cybersecurity-index> [12 สิงหาคม 2569].

อย่างไรก็ตาม กระบวนการจัดทำกฎหมายฉบับนี้เคยถูกวิพากษ์วิจารณ์อย่างกว้างขวางในประเด็นความสมดุลระหว่างความมั่นคงกับสิทธิเสรีภาพ องค์กรภาคประชาสังคมตั้งข้อสังเกตว่า อำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลอาจถูกใช้เพื่อสอดส่องผู้เห็นต่างทางการเมือง³⁴ ขณะที่ผู้ตั้งข้อสังเกตว่าร่างกฎหมายในบางช่วงสะท้อนทัศนคติด้านความมั่นคงแบบเดิมมากกว่าหลักการความมั่นคงปลอดภัยไซเบอร์สากล³⁵ ข้อวิจารณ์เหล่านี้มีนัยสำคัญต่อรายงานฉบับนี้ เพราะแสดงว่าความไว้วางใจของสาธารณะเป็นเงื่อนไขที่ขาดไม่ได้ของนโยบายไซเบอร์ที่ยั่งยืน

ก่อนหน้าการตรากฎหมาย สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 ซึ่งถือเป็นเอกสารนโยบายฉบับแรกที่ระบุอย่างชัดเจนว่า ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามต่อความมั่นคงแห่งชาติ มิใช่เพียงปัญหาทางเทคนิค เอกสารฉบับนี้กำหนดกลยุทธ์หลักหกด้านและวางแนวทางการบูรณาการการทำงานระหว่างหน่วยงาน ซึ่งเป็นการยกระดับสถานะของประเด็นไซเบอร์ในสารบบนโยบายความมั่นคงของไทยอย่างมีนัยสำคัญ

ในระยะปัจจุบัน นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570) ได้บรรจุประเด็นไซเบอร์ไว้เป็นนโยบายและแผนความมั่นคงที่ 10 ว่าด้วยการป้องกันและแก้ไขปัญหามั่นคงทางไซเบอร์ โดยมี สมช. เป็นหน่วยงานเจ้าภาพ เป้าหมายที่กำหนดไว้ประกอบด้วย การเพิ่มประสิทธิภาพ การป้องกันการโจมตีทางไซเบอร์ การยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ และการลดการก่ออาชญากรรมทางไซเบอร์³⁶ นอกจากนี้ นโยบายและแผนฉบับดังกล่าวยังระบุประเด็นไซเบอร์ไว้ในบริบทความมั่นคงระดับโลกและระดับภูมิภาค โดยจัดให้พื้นที่ไซเบอร์และอวกาศเป็น "ปัจจัยเร่ง" ที่มีผลต่อภูมิรัฐศาสตร์ และภูมิเศรษฐศาสตร์ของไทย

ในระดับแผนปฏิบัติการ กมช. ได้ออกประกาศเรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565-2570 ซึ่งดำเนินการตามมาตรา 9 (1) แห่งพระราชบัญญัติฯ เพื่อใช้เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ³⁷

³⁴ iLaw, ร่าง พ.ร.บ.มั่นคงไซเบอร์ฯ 62: เปิดช่องเจ้าหน้าที่รัฐ 'สอดส่อง' คนเห็นต่างได้, [ออนไลน์], 2562, แหล่งที่มา: <https://www.ilaw.or.th/articles/3332> [12 สิงหาคม 2569].

³⁵ ThaiPublica, พ.ร.บ. ไซเบอร์: เมื่อหลักความมั่นคงไซเบอร์แพ้ทัศนคติ “ความมั่นคง 0.4”, [ออนไลน์], 2562, แหล่งที่มา: <https://thaipublica.org/2019/03/cybersecurity-principles-lost-national-security> [12 สิงหาคม 2569].

³⁶ สำนักงานสภาความมั่นคงแห่งชาติ, นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570), [ออนไลน์], 2566, หน้า 72-74, แหล่งที่มา: https://www.nsc.go.th/wp-content/uploads/2023/06/nsc_policy_66-70-2-.pdf [12 สิงหาคม 2569].

³⁷ สำนักเลขาธิการคณะรัฐมนตรี, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570), [ออนไลน์], 2565, แหล่งที่มา: https://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/303/T_0003.PDF [12 สิงหาคม 2569].

แผนฉบับนี้เน้นการยกระดับขีดความสามารถของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) การพัฒนากำลังคน การสร้างความตระหนักรู้ และการพัฒนากลไกเผชิญเหตุ ซึ่งล้วนเป็นภารกิจที่จำเป็นและสอดคล้องกับแนวปฏิบัติสากล

1.2.2 ข้อจำกัดจากการตีความปัญหาไซเบอร์ในเชิงเทคนิคเป็นด้านหลัก

แม้ไทยจะมีกฎหมาย นโยบาย และแผนครบถ้วนตามรูปแบบสากล แต่การดำเนินงานที่ผ่านมาสะท้อนว่าไทยยังคงตีความปัญหาไซเบอร์ในเชิงเทคนิคเป็นด้านหลัก หลักฐานที่ชัดเจนที่สุดปรากฏในวิธีการรายงานสถิติภัยคุกคามของ สกมช. ซึ่งจำแนกเหตุการณ์ตาม "รูปแบบทางเทคนิค" เป็นสำคัญ ได้แก่ ความพยายามในการบุกรุก การฉ้อโกง ความปลอดภัยของเนื้อหาข้อมูล การบุกรุกระบบ ความพร้อมใช้งานของระบบ และมัลแวร์ประเภทต่าง ๆ โดยในห้วง พ.ศ. 2567 ถึง ไตรมาสแรกของ พ.ศ. 2568 หน่วยงานรัฐและเอกชนไทยเผชิญเหตุรวม 2,724 ครั้ง โดยความพยายามในการบุกรุกมีจำนวนสูงสุดที่ 1,161 ครั้ง รองลงมา คือ การฉ้อโกง 716 ครั้ง^{38 39}

การจำแนกในลักษณะดังกล่าวมีประโยชน์ต่อฝ่ายปฏิบัติ แต่กลับไม่ตอบคำถามเชิงยุทธศาสตร์ที่ผู้กำหนดนโยบายจำเป็นต้องรู้ กล่าวคือ สถิติชุดนี้บอกได้ว่าไทยถูกโจมตี "ด้วยวิธีใด" และ "หน่วยงานประเภทใด" ถูกโจมตีบ่อยที่สุด แต่ไม่บอกว่า "ใคร" เป็นผู้โจมตี "เพราะเหตุใด" และเหตุการณ์เหล่านั้นเชื่อมโยงกับสถานการณ์ทางภูมิรัฐศาสตร์อย่างไร ยิ่งไปกว่านั้น การเผยแพร่สถิติของ สกมช. ยังไม่ได้แยกให้เห็นว่า หน่วยงานแต่ละประเภทเผชิญภัยรูปแบบใดบ้าง ทำให้ไม่อาจวิเคราะห์ได้ว่าภาคส่วนใดกำลังตกเป็นเป้าหมายเชิงยุทธศาสตร์⁴⁰

การเปรียบเทียบกับรายงานของประเทศอื่น ทำให้ช่องว่างนี้ปรากฏชัดยิ่งขึ้น รายงานการประเมินภัยคุกคามไซเบอร์แห่งชาติของแคนาดา (National Cyber Threat Assessment: NCTA) จำแนกภัยตาม "ตัวแสดง" และ "เจตนา" เป็นหลัก โดยได้ระบุชี้ตัวว่ารัฐใดที่ปฏิบัติการจารกรรม รัฐใดวางฐานเข้าถึงระบบโครงสร้างพื้นฐาน และกลุ่มอาชญากรใดทำหน้าที่เป็นตัวแทนของรัฐ⁴¹ ในทำนองเดียวกัน รายงานประจำปีของ NCSC สหราชอาณาจักร ระบุจำนวนเหตุการณ์ที่มีนัยสำคัญต่อความมั่นคงแห่งชาติแยกจากเหตุการณ์ทั่วไป พร้อมอธิบายบริบททาง

³⁸ ประชาไท, อ่วงแล้ว เจิงอรรถที่ 4.

³⁹ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, สถิติภัยคุกคามทางไซเบอร์, [ออนไลน์], 2569, แหล่งที่มา: <https://www.ncsa.or.th/policy/threat-statistics> [12 สิงหาคม 2569].

⁴⁰ ประชาไท, อ่วงแล้ว เจิงอรรถที่ 4.

⁴¹ Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025-2026, [Online], 2024, Available from: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf> [2026, August 12].

ภูมิรัฐศาสตร์ที่เกี่ยวข้อง⁴² การรายงานเช่นนี้ทำให้ผู้กำหนดนโยบายเห็นภาพว่า ประเทศกำลังเผชิญกับใคร ไม่ใช่เพียงเผชิญกับอะไร

ผลสืบเนื่องประการแรกของการรายงานเชิงเทคนิค คือ ผู้กำหนดนโยบายและผู้ปฏิบัติงานไม่สามารถมองเห็นภาพกว้างของแรงจูงใจของตัวแสดงภัยคุกคามได้ เมื่อเหตุการณ์การรั่วไหลของข้อมูล การเสนอขายช่องโหว่ของหน่วยงานภาครัฐบนเว็บมืด และการเจาะระบบหน่วยงานด้านความมั่นคง ถูกบันทึกไว้เป็นเพียง "การบุกรุกระบบ" จำนวนหนึ่ง โดยไม่มีการวิเคราะห์ว่าเหตุการณ์เหล่านั้นอาจเชื่อมโยงกันหรือมีตัวแสดงระดับรัฐอยู่เบื้องหลัง ระบบราชการย่อมสูญเสียโอกาสในการเตือนภัยเชิงยุทธศาสตร์ล่วงหน้า

ผลสืบเนื่องประการที่สอง คือ หน่วยงานมีแนวโน้มยึดติดกับการแก้ไขปัญหาล้วนในเชิงเทคนิค เมื่อภาพของปัญหาถูกนำเสนอในรูปของช่องโหว่และมัลแวร์ ทางออกที่ถูกเสนอย่อมเป็นการอุดช่องโหว่ ติดตั้งระบบป้องกัน และฝึกอบรมบุคลากร ซึ่งล้วนจำเป็นแต่ไม่เพียงพอ ทั้งที่ในความเป็นจริง ไทยสามารถนำเครื่องมือเชิงนโยบายอื่นมาสนับสนุนการป้องกันและป้องกันได้ เช่น การหยิบยกประเด็นขึ้นหารือในกรอบทวิภาคี การใช้กลไกความร่วมมือระหว่างประเทศเพื่อติดตามผู้กระทำผิด การประสานท่าทีกับประเทศที่มีจุดยืนใกล้เคียง หรือการกำหนดกรอบมาตรการตอบสนองไว้ล่วงหน้า

ผลสืบเนื่องประการที่สาม คือ การรับมือของไทยมีลักษณะตั้งรับเป็นด้านหลัก งานศึกษาเชิงวิชาการชี้ว่า การตอบสนองของไทยต่อเหตุการณ์ด้านไซเบอร์มักเกิดขึ้นหลังจากปัญหาปรากฏเป็นข่าวแล้ว และมักถูกกำหนดโดยแรงกดดันทางการเมืองหรือแรงกดดันจากภายนอกมากกว่าการวางแผนล่วงหน้า⁴³ ลักษณะเช่นนี้ทำให้ไทยเสียเปรียบเชิงยุทธศาสตร์ โดยในพื้นที่ไซเบอร์ฝ่ายโจมตีได้เปรียบฝ่ายป้องกันโดยธรรมชาติอยู่แล้ว กล่าวคือ ฝ่ายป้องกันต้องป้องกันให้ได้ทุกครั้ง ขณะที่ฝ่ายโจมตีต้องการเพียงช่องโหว่จุดเดียวในครั้งใดครั้งหนึ่ง

ผลสืบเนื่องประการสุดท้าย คือ นโยบายและแผนในระยะปัจจุบันยังไม่ได้เตรียมรองรับภัยรูปแบบใหม่จากปัญญาประดิษฐ์ (Artificial Intelligence: AI) และเทคโนโลยีควอนตัม (Quantum) อย่างเป็นระบบ การเปลี่ยนผ่านไปสู่วิทยาการรหัสที่ต้านทานควอนตัมเป็นภารกิจที่ต้องใช้เวลาหลายปี และต้องเริ่มจากการจัดทำบัญชีระบบเข้ารหัสทั้งหมดของประเทศ หากไทยไม่เริ่มดำเนินการในห้วง พ.ศ. 2571-2575 ข้อมูลที่ถูกลักลอบเก็บไว้ในวันนี้ย่อมมีความเสี่ยงที่จะถูก

⁴² National Cyber Security Centre, *NCSC Annual Review 2025*, [Online], 2025, Available from:

<https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-annual-review-2025.pdf> [2026, August 12].

⁴³ Surachanee "Hammerli" Sriyai, *Borderland Scam Centres and Cyber Threats: Policy Considerations for Thailand*,

[Online], 2025, pp. 8-9, Available from: <https://www.iseas.edu.sg/wp-content/uploads/2025/07/>

ISEAS_Perspective_2025_60.pdf [2026, August 12].

ถอดรหัสได้ในอนาคตในทำนองเดียวกัน การรับมือกับการโจมตีที่เสริมด้วย AI ต้องอาศัยการลงทุนด้านการตรวจจับอัตโนมัติและการพัฒนากำลังคนที่เข้าใจทั้งเทคโนโลยีและบริบทเชิงยุทธศาสตร์

ประเด็นศึกษาของรายงานฉบับนี้จึงสรุปได้ว่า ประเทศไทยมีโครงสร้างสถาบันและเครื่องมือทางกฎหมายที่เพียงพอในระดับหนึ่งแล้ว แต่ยังขาดกรอบการมองปัญหาที่เชื่อมโยงเหตุการณ์ทางไซเบอร์เข้ากับบริบททางการเมืองระหว่างประเทศ และยังขาดกลไกที่ทำให้หน่วยงานด้านเทคนิค ข้าราชการ การทูต การป้องกันประเทศ และการบังคับใช้กฎหมายทำงานร่วมกันได้อย่างเป็นระบบ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติในระยะต่อไป (พ.ศ. 2571-2575) จึงควรแก้ไขช่องว่างทั้งสองประการนี้เป็นลำดับแรก

บทที่ 2

การวิเคราะห์ประเด็นศึกษาและผลการศึกษา

2.1 การกำหนดประเด็นศึกษา

จากการสำรวจวรรณกรรมเกี่ยวข้องกับการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ พบว่าองค์ความรู้และการปฏิบัติของไทยแยกออกเป็นสองสายอย่างค่อนข้างชัดเจน สายแรก คือ ประเด็นด้านเทคนิคซึ่งเน้นการป้องกัน ตรวจจับ และเผชิญเหตุในระดับระบบและองค์กร ส่วนสายที่สอง คือ ประเด็นด้านนโยบายซึ่งเน้นการบริหารจัดการและการขับเคลื่อนยุทธศาสตร์ แผนงาน และโครงการของหน่วยงานที่เกี่ยวข้องทั้งฝ่ายพลเรือนและฝ่ายทหาร การแยกสายดังกล่าวมิได้เป็นเพียงการแบ่งงานทางวิชาการ หากสะท้อนโครงสร้างทางกฎหมายและสถาบันของไทยโดยตรง

สายที่หนึ่ง คือ ประเด็นด้านเทคนิค มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยรับผิดชอบหลักตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ภารกิจของหน่วยงานนี้ครอบคลุมการกำหนดมาตรฐานขั้นต่ำสำหรับหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ การเฝ้าระวังและแจ้งเตือน การประสานการเผชิญเหตุ และการพัฒนากำลังคนด้านไซเบอร์ วรรณกรรมในสายนี้จึงมุ่งวิเคราะห์ประสิทธิภาพของกลไกตามกฎหมาย ความพร้อมของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และปัญหาในทางปฏิบัติของการบังคับใช้

งานศึกษาในสายเทคนิคที่น่าสนใจ ได้แก่ งานที่วิเคราะห์ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของ สกมช. ซึ่งชี้ให้เห็นว่า แผนของหน่วยงานมีความครบถ้วนในเชิงโครงสร้าง แต่ยังเผชิญข้อจำกัดด้านทรัพยากรและการประสานงานข้ามหน่วยงาน⁴⁴ และงานที่วิเคราะห์มุมมองเชิงกฎหมายต่อความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน ซึ่งชี้ว่า ลักษณะข้ามพรมแดนของภัยไซเบอร์ ทำให้การบังคับใช้กฎหมายภายในประเทศเพียงลำพังไม่เพียงพอ⁴⁵

วรรณกรรมในสายนโยบายที่โดดเด่นที่สุด ปรากฏในวารสารมุมมองความมั่นคงของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ซึ่งจะได้กล่าวถึงโดยละเอียดต่อไป นอกจากนี้ ยังมีงานที่

⁴⁴ ธวัชชัย สุขสาย และ วสันต์ เกิดสวัสดิ์, มหายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของ สกมช., [ออนไลน์], 2566, แหล่งที่มา: https://so12.tci-thaijo.org/index.php/watmahasawat_jsc/article/view/771/640 [12 สิงหาคม 2569].

⁴⁵ สุธีราภรณ์ แสงจันทร์ศรี และ สลิลา กลั่นเรืองแสง, มุมมองเชิงกฎหมายต่อความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน, [ออนไลน์], 2564, แหล่งที่มา: <https://so02.tci-thaijo.org/index.php/ISSC/article/view/251833/169890> [12 สิงหาคม 2569].

วิเคราะห์บทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ในห้วง พ.ศ. 2560-2565 ซึ่งสะท้อนพัฒนาการของฝ่ายทหารในการสร้างขีดความสามารถด้านไซเบอร์⁴⁶ และรายงานข่าวเกี่ยวกับการที่กระทรวงกลาโหมเตรียมยกระดับหน่วยงานไซเบอร์ของกองทัพขึ้นเป็นกองบัญชาการ^{47 48}

ข้อค้นพบสำคัญจากการสำรวจวรรณกรรม คือ วรรณกรรมทั้งสองสายมีจุดเชื่อมต่อนาน้อยกว่าที่ควรจะเป็น งานในสายเทคนิคมักไม่วิเคราะห์แรงจูงใจเชิงยุทธศาสตร์ของตัวแสดง ขณะที่งานในสายนโยบายมักไม่ลงลึกถึงข้อจำกัดในทางปฏิบัติของหน่วยงานเทคนิค ช่องว่างนี้เองที่ทำให้การกำหนดนโยบายของไทยขาดสะพานเชื่อมระหว่างข้อมูลเชิงเทคนิคที่หน่วยงานปฏิบัติมีอยู่กับการตัดสินใจเชิงยุทธศาสตร์ที่ผู้กำหนดนโยบายต้องทำ ดังนั้น การจัดทำรายงานฉบับนี้จึงมุ่งเสนอประเด็นแนวทางเชื่อมสองสายดังกล่าวเข้าด้วยกัน โดยมีวัตถุประสงค์ ขอบเขต และวิธีการศึกษา ดังนี้

2.1.1 วัตถุประสงค์ของการศึกษา

- 1) ศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบของภัยคุกคามทางไซเบอร์
- 2) ศึกษาผลกระทบของภัยคุกคามทางไซเบอร์ ที่ส่งผลต่อความมั่นคงของชาติ
- 3) จัดทำข้อเสนอเชิงนโยบายและแนวทางการแก้ไขปัญหา ในระยะต่อไป

2.1.2 ขอบเขตการศึกษา

ศึกษาในรอบของการขับเคลื่อนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570) นำไปสู่การจัดทำข้อเสนอในห้วง พ.ศ. 2571-2575

2.1.3 วิธีการศึกษา

ใช้วิธีเชิงคุณภาพแบบพรรณนาเชิงวิเคราะห์ (descriptive analysis) ข้อมูลชั้นปฐมภูมิและทุติยภูมิจากเอกสารนโยบาย กฎหมาย รายงาน และข่าวสารที่เกี่ยวข้อง รวมถึงงานวิชาการและกรณีศึกษาต่างประเทศที่มีนัยสำคัญ

⁴⁶ รัชกร ภูริธรจินดา, เกรียงชัย ปิงประวดี, ณัฐพงศ์ บุญเหลือ และนิพนธ์ โชะเฮง, บทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2560-2565, [ออนไลน์], 2567, แหล่งที่มา: <https://so01.tci-thaijo.org/index.php/JDAR/article/download/275572/177933/1098471> [12 สิงหาคม 2569].

⁴⁷ ประชาไท, ก.กลาโหม เตรียมตั้งกองบัญชาการสงครามไซเบอร์, [ออนไลน์], 2567, แหล่งที่มา: <https://prachatai.com/journal/2024/05/109345> [12 สิงหาคม 2569].

⁴⁸ ไทยรัฐ, “กองทัพ” รุกตั้งหน่วยไซเบอร์ทหาร รับภัยคุกคาม เริ่มผลิตนักรบ 1 ต.ค. นี้, [ออนไลน์], 2567, แหล่งที่มา: <https://www.thairath.co.th/news/local/bangkok/2787536> [12 สิงหาคม 2569].

2.2 การวิเคราะห์ประเด็นศึกษา

2.2.1 แนวคิดและทฤษฎีเกี่ยวกับการแก้ปัญหาไซเบอร์ในเชิงรัฐศาสตร์

2.2.1.1 นักวิชาการเกี่ยวกับไซเบอร์

รายงานฉบับนี้ขอหยิบยกตัวบุคคลที่ได้รับการยอมรับโดยทั่วไป ดังนี้

1) Adam Segal เป็นนักวิชาการชาวอเมริกันประจำสภาความสัมพันธ์ระหว่างประเทศ (Council on Foreign Relations) สหรัฐฯ และเป็นผู้อำนวยการโครงการนโยบายดิจิทัลและพื้นที่ไซเบอร์ ผลงานสำคัญของเขา คือ หนังสือ *The Hacked World Order* ซึ่งเสนอว่า โลกได้ก้าวเข้าสู่ยุคที่รัฐใช้พื้นที่ไซเบอร์เป็นเวทีหลักในการต่อสู้ คำขाय ต่อรอง และแทรกแซงกันอย่างไม่เปิดเผยมากขึ้น⁴⁹ Segal เสนอให้มองภัยไซเบอร์ในฐานะการดำเนินนโยบายต่างประเทศรูปแบบหนึ่ง มิใช่ปัญหาความปลอดภัยของระบบสารสนเทศ เขาชี้ว่าโครงสร้างอำนาจในพื้นที่ไซเบอร์ไม่เป็นไปตามอำนาจในโลกกายภาพ เพราะทุกรัฐล้วนประจบและอาจตกเป็นเหยื่อได้เสมอ แม้แต่มหาอำนาจที่มีขีดความสามารถทางทหารสูงสุด

ข้อเสนอเชิงนโยบายของ Segal มีสามประการหลัก ประการแรก รัฐควรลงทุน ในการสร้างบรรทัดฐานระหว่างประเทศและกลไกกำกับดูแลอินเทอร์เน็ต แทนที่จะพึ่งพาการแข่งขันสะสมขีดความสามารถเพียงอย่างเดียว ประการที่สอง รัฐควรพัฒนาขีดความสามารถในการระบุตัวตนผู้กระทำการ เพราะการระบุตัวตนที่น่าเชื่อถือเป็นเงื่อนไขของการป้องปรามและการสร้างความรับผิดชอบ และประการที่สาม รัฐควรตระหนักว่าการแบ่งขั้วทางเทคโนโลยีระหว่างมหาอำนาจกำลังบีบให้ประเทศขนาดกลางต้องเลือกข้าง จึงต้องวางยุทธศาสตร์รักษาพื้นที่ทางเลือกของตนไว้ตั้งแต่เนิ่น ๆ

2) Ben Buchanan เป็นนักวิชาการชาวอเมริกันที่ศึกษาความสัมพันธ์ระหว่างเทคโนโลยีกับความมั่นคงระหว่างประเทศ ผลงานสำคัญของเขา คือ หนังสือ *The Hacker and the State* ซึ่งเสนอกรอบวิเคราะห์ที่แยกการใช้เครื่องมือไซเบอร์ออกเป็นสองประเภทใหญ่ ได้แก่ การส่งสัญญาณ (signaling) และการกำหนดทิศทางสถานการณ์ (shaping)⁵⁰ การส่งสัญญาณ คือ การใช้ปฏิบัติการไซเบอร์เพื่อสื่อความไม่พอใจหรือข่มขู่ให้อีกฝ่ายรับรู้ ส่วนการกำหนดทิศทางสถานการณ์ คือ การใช้ปฏิบัติการอย่างลับ ๆ เพื่อสร้างความได้เปรียบให้ตนเองโดยที่อีกฝ่ายอาจไม่รู้ตัว

ข้อเสนอหลักของ Buchanan คือ เครื่องมือไซเบอร์เหมาะกับการกำหนดทิศทางสถานการณ์มากกว่าการส่งสัญญาณ เหตุผลคือ ธรรมชาติของเครื่องมือไซเบอร์ต้อง

⁴⁹ Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, (New York: PublicAffairs, 2016), pp. 1-16.

⁵⁰ Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, (Cambridge, MA: Harvard University Press, 2020), pp. 2-7.

อาศัยความลับ ทั้งในส่วนของการช่องทางที่ใช้และเทคนิคที่ใช้ ดังนั้น การเปิดเผยตัวตนเพื่อเตรียมส่งสัญญาณยอมเท่ากับเปิดเผยขีดความสามารถ และทำให้อีกฝ่ายอุดช่องโหว่ได้ นอกจากนี้ การส่งสัญญาณทางไซเบอร์ ยังเสี่ยงต่อการตีความผิดพลาด เพราะผู้รับสารอาจไม่ทราบว่าใครเป็นผู้โจมตีหรือไม่อาจเชื่อมโยงการโจมตีเข้ากับข้อเรียกร้องทางการเมืองได้ทันที ซึ่งอาจนำไปสู่การยกระดับความขัดแย้งโดยไม่ได้ตั้งใจ⁵¹ นโยบายสำหรับรัฐบาลกลาง คือ การลงทุนในการเก็บรวบรวมข่าวกรอง และการสร้างความได้เปรียบเชิงข้อมูล ให้ผลตอบแทนสูงกว่าการพยายามข่มขู่ด้วยเครื่องมือไซเบอร์

3) Richard J. Harknett เป็นศาสตราจารย์ด้านวิชารัฐศาสตร์แห่งมหาวิทยาลัย Cincinnati และเคยเป็นที่ปรึกษาด้านยุทธศาสตร์ให้กองบัญชาการไซเบอร์ของสหรัฐฯ ผลงานสำคัญของเขา คือ ทฤษฎีการปะทะอย่างต่อเนื่องในพื้นที่ไซเบอร์ (Cyber Persistence Theory) ซึ่งเขียนร่วมกับ Michael P. Fischerkeller และ Emily O. Goldman ข้อเสนอหลักของทฤษฎีนี้ คือ พื้นที่ไซเบอร์เป็นปริภูมิแห่งการช่วงชิงความได้เปรียบ (sphere of exploitation) มิใช่ปริภูมิแห่งการบีบบังคับ (sphere of coercion) เหมือนปริภูมิทางทหารดั้งเดิม⁵²

Harknett เสนอว่า เมื่อพื้นที่ไซเบอร์มีลักษณะเชื่อมต่อกันตลอดเวลา และเปลี่ยนแปลงอยู่เสมอ แนวคิดการป้องปรามแบบสงครามเย็นซึ่งตั้งอยู่บนการข่มขู่ว่าจะตอบโต้ย่อมใช้ไม่ได้ผล เพราะฝ่ายตรงข้ามพยายามฝ่าด่านอย่างต่อเนื่องอยู่แล้วโดยไม่ต้องรอโอกาสพิเศษ ยุทธศาสตร์ที่เหมาะสมจึงเป็นการดำเนินปฏิบัติการอย่างต่อเนื่อง (persistent engagement) เพื่อสะสมความได้เปรียบและลดทอนขีดความสามารถของคู่แข่งตลอดเวลา แนวคิดนี้กลายเป็นรากฐานของหลักนิยม "การป้องกันเชิงรุกล่วงหน้า" (defend forward) ของสหรัฐฯ สำหรับรัฐบาลกลางอย่างไทย นโยบายสำคัญของทฤษฎีนี้มีใช้การเลียนแบบปฏิบัติการเชิงรุกของมหาอำนาจ หากคือการยอมรับว่าการแข่งขันในพื้นที่ไซเบอร์ดำเนินอยู่ตลอดเวลาแม้ในยามสงบ และการเตรียมความพร้อมจึงต้องเป็นกิจกรรมประจำวันมิใช่กิจกรรมยามวิกฤติ

4) ในฝ่ายนักวิชาการไทย ผู้ช่วยศาสตราจารย์ ดร.สุรัชณี ศรีโย เป็นนักวิจัยที่ศึกษาประเด็นความมั่นคงไซเบอร์และธรรมาภิบาลดิจิทัลของไทยและเอเชียตะวันออกเฉียงใต้อย่างต่อเนื่อง ข้อเสนอหลักของท่าน คือ กรอบกำกับดูแลและกรอบความมั่นคงไซเบอร์ของไทยยังไม่เพียงพอต่อการรับมือภัยที่ขยายตัว แม้จะมีทั้งกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

⁵¹ ภาณุทัต วัชรภรณ์, อ้าวแล้ว เจิงอรรถที่ Z, หน้า 45-46.

⁵² Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence Theory: Redefining National Security in Cyberspace, (New York: Oxford University Press, 2022), pp. 3-20.

และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้วก็ตาม เนื่องจากยังมีช่องว่างด้านการบังคับใช้การประสานงานระหว่างหน่วยงานที่อ่อนแอ และความไว้วางใจของสาธารณะที่อยู่ในระดับต่ำ⁵³

ผู้ช่วยศาสตราจารย์ ดร.สุรัชณี ยังชี้เสนอว่า ภาครัฐไทยมีแนวโน้มบังคับใช้กฎหมายอย่างเข้มงวดกับภาคเอกชนที่ทำข้อมูลรั่วไหล แต่กลับผ่อนปรนต่อหน่วยงานภาครัฐด้วยกันเองและต่อผู้กระทำผิดทางไซเบอร์ ซึ่งบั่นทอนความน่าเชื่อถือของระบบโดยรวม และอาจส่งผลกระทบต่อการพัฒนารัฐบาลอิเล็กทรอนิกส์ในระยะยาว⁵⁴ จึงมีข้อเสนอเชิงนโยบาย ประกอบด้วย การผลักดันความร่วมมือแบบพหุภาคีแทนการพึ่งพาความสัมพันธ์ทวิภาคีกับมหาอำนาจ การจัดตั้งสำนักงานข่าวกรองอาชญากรรมชายแดนแบบบูรณาการหลายหน่วยงาน และการกำหนดให้หน่วยงานภาครัฐต้องผ่านการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยมีการเปิดเผยผลการตรวจสอบต่อสาธารณะ

อนึ่ง นักวิชาการไทยกลุ่มอื่นได้ศึกษาประเด็นนี้จากมุมที่หลากหลายงาน ด้านนิติศาสตร์วิเคราะห์ความสัมพันธ์ระหว่างอำนาจรัฐกับสิทธิเสรีภาพภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และตั้งข้อสังเกตว่าความชัดเจนของขอบเขตอำนาจเป็นเงื่อนไขสำคัญของการบังคับใช้ที่ได้ผลงาน งานด้านรัฐประศาสนศาสตร์วิเคราะห์บทบาทภาครัฐ ในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ขณะทำงานด้านการทบทวนวิชาการพัฒนาแบบจำลองยุทธ์ทางไซเบอร์และบทบาทของหน่วยไซเบอร์ในกองทัพ ความหลากหลายนี้เป็นสัญญาณที่ดี แต่ยังขาดงานที่บูรณาการมุมมองทั้งหมดเข้าด้วยกันในระดับยุทธศาสตร์ชาติ

ข้อสังเกตเปรียบเทียบที่สำคัญ คือ นักวิชาการต่างประเทศทั้งสามท่านเห็นตรงกันว่า ปัญหาไซเบอร์เป็นปัญหาการเมืองระหว่างประเทศโดยแท้ ขณะที่นักวิชาการไทยส่วนใหญ่ยังเน้นการวิเคราะห์ปัญหาภายในประเทศ เช่น ประสิทธิผลของกฎหมาย ความพร้อมของหน่วยงาน และการคุ้มครองข้อมูลส่วนบุคคล ช่องว่างนี้ยืนยันความจำเป็นของการยกระดับกรอบการมองปัญหาในนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับต่อไป

2.2.1.2 องค์ความรู้ด้านไซเบอร์ในคลังความรู้ของสำนักงานสภาความมั่นคงแห่งชาติ

สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้สั่งสมองค์ความรู้ด้านไซเบอร์ไว้ในวารสารมุมมองความมั่นคงอย่างต่อเนื่อง บทความที่ขึ้นต่อไปนี้มีสำคัญเป็นพิเศษต่อรายงานฉบับนี้ เพราะทั้งสี่ชิ้นวางประเด็นไซเบอร์ไว้ในกรอบความมั่นคงแห่งชาติและการเมืองระหว่างประเทศ ซึ่งเป็นกรอบที่รายงานฉบับนี้ต้องการผลักดันให้ปรากฏในนโยบายและแผนระดับชาติฉบับต่อไป

⁵³ Surachanee "Hammerli" Sriyai, *supra* note 43, pp. 6-7.

⁵⁴ Surachanee Sriyai, *Data Leaks: Thai Government Tough on Private Firms, Soft on Public Sector and Cybercriminals*, [Online], 2024, Available from: <https://fulcrum.sg/data-leaks-thai-government-tough-on-private-firms-soft-on-public-sector-and-cybercriminals> [2026, August 12].

1) บทความเรื่อง "ความมั่นคงไซเบอร์: แนวคิด ประสบการณ์ของต่างประเทศและบทเรียนสำหรับประเทศไทย" ระบุภาพรวมของภัยคุกคามทางไซเบอร์ได้อย่างครอบคลุม บทความนี้อธิบายแนวคิดพื้นฐานด้านความมั่นคงไซเบอร์ ทบทวนประสบการณ์การจัดวางนโยบายและสถาบันของประเทศไทยต่าง ๆ และสรุปบทเรียนที่ไทยสามารถนำมาปรับใช้ได้ คุณค่าสำคัญของบทความอยู่ที่การชี้ให้เห็นว่า ประเทศที่ประสบความสำเร็จมักจัดวางความมั่นคงไซเบอร์ในระดับยุทธศาสตร์ชาติ มิใช่ในระดับหน่วยงานเทคโนโลยีสารสนเทศ⁵⁵

2) บทความเรื่อง "เทคโนโลยีสารสนเทศและการสื่อสารกับการเมืองระหว่างประเทศ" อธิบายประเด็นไซเบอร์ผ่านมุมมองความสัมพันธ์ระหว่างประเทศอย่างเป็นระบบ โดยเสนอว่า เทคโนโลยีสารสนเทศและการสื่อสารเปลี่ยนแปลงอำนาจรัฐอย่างน้อยสองระดับ ระดับแรกคือ ภายในประเทศ ซึ่งรัฐสูญเสียความสามารถในการควบคุมเสถียรภาพทางยุทธศาสตร์ภายใน เพราะประชาชนเข้าถึงข้อมูลได้มากขึ้นและอาจถูกแทรกแซงจากต่างชาติได้ง่ายขึ้น ระดับที่สองคือ ระหว่างประเทศ ซึ่งพื้นที่ไซเบอร์กลายเป็นเวทีปฏิสัมพันธ์ระหว่างรัฐทั้งในแง่การส่งสมอำนาจ การกำหนดหรือควบคุมพฤติกรรมของรัฐอื่น และการทำสงครามรูปแบบใหม่ ข้อสรุปที่สำคัญที่สุดของบทความคือ "การโจมตีทางไซเบอร์เป็นเพียงอาการของโรค" ซึ่งมีรากมาจากความขัดแย้งเชิงภูมิรัฐศาสตร์ ดังนั้น ผู้นำต้องใช้ทักษะทางการเมืองนำทักษะทางเทคนิคในการแก้ปัญหา⁵⁶

3) บทความเรื่อง "สงครามไซเบอร์กับการนิยามใหม่ของการทำสงครามในการเมืองระหว่างประเทศยุคร่วมสมัย" นำเสนอภัยไซเบอร์ผ่านมุมมองของทฤษฎีสงคราม โดยวิเคราะห์ว่า ปทัสถานว่าด้วยสงครามที่เป็นธรรม (Just War) ซึ่งประกอบด้วย หลักสิทธิในการก่อสงคราม (Jus ad Bellum) และหลักวิธีการทำสงครามที่ชอบธรรม (Jus in Bello) เผชิญความท้าทายอย่างรุนแรงในพื้นที่ไซเบอร์ เหตุผลคือ ตัวแสดงที่ก่อสงครามไซเบอร์ไม่ได้จำกัดอยู่เพียงรัฐ การระบุตัวผู้กระทำเป็นไปได้ยาก และโครงสร้างพื้นฐานทางไซเบอร์มักถูกใช้ร่วมกันระหว่างพลเรือนกับทหาร ทำให้หลักการแบ่งแยกระหว่างพลเรือนและทหารบังคับใช้ได้ยาก ข้อเสนอของบทความ คือ รัฐและองค์กรที่เกี่ยวข้องต้องปรับวิสัยทัศน์ในการจัดการด้านความมั่นคง และร่วมกันสร้างกรอบปทัสถานใหม่เพื่อให้เกิดดุลยภาพในเวทีการเมืองระหว่างประเทศ⁵⁷

4) บทความเรื่อง "ความขัดแย้งทางไซเบอร์ในมุมมองเชิงยุทธศาสตร์" นำเสนอว่า ชีตความสามารถทางไซเบอร์ถูกนำไปใช้ขับเคลื่อนผลประโยชน์เชิงยุทธศาสตร์ของรัฐอย่างไร โดยระบุปัจจัยห้าประการที่ผลักดันให้รัฐหันมาใช้เครื่องมือไซเบอร์ ได้แก่ พื้นที่และโอกาส

⁵⁵ วศิน ปั่นทอง, "ความมั่นคงไซเบอร์: แนวคิด ประสบการณ์ของต่างประเทศและบทเรียนสำหรับประเทศไทย," วารสารความมั่นคงศึกษา ฉบับที่ 1 (มิถุนายน-กันยายน 2562): 13-26.

⁵⁶ ภาณุทัต วัชรภรณ์, อ้าวแล้ว เชิงอรรถที่ 8, หน้า 23-33.

⁵⁷ รุติมาศ ศรีสุข, อ้าวแล้ว เชิงอรรถที่ 9, หน้า 52-62.

โจมตีที่กว้างขึ้น ต้นทุนที่ลดลง ความสามารถในการปกปิดตัวตน ความสามารถในการปฏิเสธความเกี่ยวข้อง และความคลุมเครือของการบังคับใช้กฎหมายระหว่างประเทศ จากนั้นจึงวิเคราะห์การใช้เครื่องมือไซเบอร์ในสี่ลักษณะ คือ การส่งสัญญาณ การป้องปรามและการบีบบังคับ การกำหนดทิศทางสถานการณ์ และการสนับสนุนปฏิบัติการทางทหาร ข้อสรุปที่สำคัญที่สุดของบทความ คือ การกำหนดนโยบาย ทางไซเบอร์ที่มีประสิทธิภาพจำเป็นต้องมองประเด็นไซเบอร์ให้กว้างกว่าการเป็นแค่ "ปัญหาเชิงเทคนิค" ที่ต้องแก้ไขเฉพาะหน้า และต้องตระหนักว่า เครื่องมือทางไซเบอร์ คือ กลไกสำคัญในการขับเคลื่อนผลประโยชน์แห่งชาติ ซึ่งต้องอาศัยทั้งมิติทางการเมืองและการทูตในการกำหนดทิศทาง⁵⁸

ข้อสังเกตที่สำคัญที่สุดจากการทบทวนบทความทั้งสี่ชิ้น คือ สมช. มีองค์ความรู้ที่จำเป็นสำหรับการยกระดับกรอบการมองปัญหาไซเบอร์อยู่แล้ว องค์ความรู้ดังกล่าวชี้ตรงกันว่า ภัยไซเบอร์เป็นปัญหาการเมืองมิใช่ปัญหาเทคนิคเพียงอย่างเดียว อย่างไรก็ตาม องค์ความรู้ยังไม่ได้ถูกแปลงเป็นถ้อยคำ เป้าหมาย และตัวชี้วัดในนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับปัจจุบันอย่างเต็มที่ ภารกิจสำคัญของนโยบายและแผนฉบับต่อไปจึงเป็นการปิดช่องว่างระหว่างองค์ความรู้กับเอกสารนโยบาย

2.2.1.3 กรอบแนวคิดที่ใช้ในการวิเคราะห์

รายงานฉบับนี้ใช้กรอบแนวคิดสี่ชุดในการวิเคราะห์การแก้ปัญหาไซเบอร์ของไทย กรอบชุดแรก คือ การจำแนกการใช้เครื่องมือไซเบอร์ตามวัตถุประสงค์เชิงยุทธศาสตร์สี่ประการ ได้แก่ การส่งสัญญาณ การป้องปรามและการบีบบังคับ การกำหนดทิศทางสถานการณ์ และการสนับสนุนปฏิบัติการทางทหาร กรอบนี้ช่วยให้วิเคราะห์ได้ว่าเหตุการณ์ที่เกิดขึ้นกับไทยแต่ละครั้ง น่าจะมีวัตถุประสงค์ใด และไทยควรตอบสนองด้วยเครื่องมือประเภทใด

กรอบชุดที่สอง คือ การแยกแยะระหว่างการป้องปรามด้วยการปฏิเสธความสำเร็จ (deterrence by denial) กับการป้องปรามด้วยการลงโทษ (deterrence by punishment) การป้องปรามแบบแรกมุ่งลดโอกาสที่การโจมตีจะสำเร็จผ่านการเสริมความแข็งแกร่งของระบบและการสร้างภูมิคุ้มกัน ส่วนการป้องปรามแบบหลังมุ่งทำให้ฝ่ายตรงข้ามเห็นว่าต้นทุนของการโจมตีสูงกว่าประโยชน์ที่จะได้รับผ่านการกล่าวโทษสาธารณะ มาตรการคว่ำบาตร และการดำเนินคดี กรอบนี้มีความสำคัญเพราะปัจจุบันไทยลงทุนกับการป้องปรามแบบแรกเป็นหลัก ขณะที่แทบไม่มีเครื่องมือสำหรับการป้องปรามแบบหลังเลย

กรอบชุดที่สาม คือ แนวคิดชุดเครื่องมือเชิงนโยบาย (policy toolbox) และการบูรณาการข้ามหน่วยงาน แนวคิดนี้เสนอว่ารัฐควรเตรียมเครื่องมือตอบสนองไว้ล่วงหน้าให้

⁵⁸ ภาณุทัต วัชรารณณ์, อั้งแล้ว เจริญรุดที่ 7, หน้า 39-51.

ครอบคลุมตั้งแต่มาตรการทางการทูต การกล่าวโทษสาธารณะ มาตรการทางเศรษฐกิจ การสนับสนุนข่าวกรองแก่อมิตรประเทศ การใช้กระบวนการยุติธรรม ไปจนถึงการใช้ขีดความสามารถทางทหาร เหตุผลสำคัญ คือ เมื่อเกิดเหตุจริงการไม่มีกรอบมาตรการที่พร้อมใช้จะทำให้รัฐตอบสนองล่าช้า หรือเสียเปรียบเชิงยุทธศาสตร์

กรอบชุดที่สี่ คือ ข้อจำกัดและโอกาสของรัฐขนาดกลาง แนวคิดนี้ยอมรับว่า ไทยไม่อาจแข่งขันสะสมขีดความสามารถไซเบอร์กับมหาอำนาจได้ และไม่ควรเลียนแบบหลักนิยมเชิงรุกของมหาอำนาจโดยไม่ไตร่ตรอง แต่ไทยสามารถสร้างอิทธิพลได้ผ่านการรวมกลุ่มกับประเทศที่มีแนวคิดใกล้เคียงกัน การมีบทบาทในการกำหนดบรรทัดฐานระหว่างประเทศ และการรักษาความเป็นกลางเชิงยุทธศาสตร์ (strategic neutrality) เพื่อมิให้ถูกบีบให้เลือกข้างระหว่างขั้วอำนาจที่กำลังแข่งขันกัน การนำกรอบทั้งสี่ชุดมาใช้ร่วมกันทำให้การวิเคราะห์ในหัวข้อถัดไปสามารถตอบคำถามได้สามข้อ คือ ไทยกำลังเผชิญกับอะไรและใคร ไทยมีเครื่องมืออะไรอยู่แล้วและขาดอะไร และไทยควรวางตำแหน่งตนเองอย่างไรในระเบียบไซเบอร์ระหว่างประเทศที่กำลังก่อตัว

2.2.2 ผลการแก้ไขปัญหาไซเบอร์ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับปัจจุบัน

นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570) กำหนดให้การป้องกันและแก้ไขปัญหามันคงทางไซเบอร์เป็นนโยบายและแผนความมั่นคงที่ 10 โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานเจ้าภาพ และกำหนดเป้าหมายไว้สามประการ ได้แก่ การเพิ่มประสิทธิภาพการป้องกันการโจมตีทางไซเบอร์ การยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ และการลดการก่ออาชญากรรมทางไซเบอร์ การประเมินผลการดำเนินงานตามเป้าหมายเหล่านี้ในห้วงที่ผ่านมาพบทั้งความสำเร็จและข้อจำกัดที่ควรนำไปพิจารณาในนโยบายและแผนฉบับต่อไป

ความสำเร็จประการแรก คือ การวางโครงสร้างสถาบันและกฎหมายได้ครบถ้วน ไทยมีคณะกรรมการระดับชาติที่มีนายกรัฐมนตรีเป็นประธาน มีหน่วยงานปฏิบัติเฉพาะทาง มีการกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) พร้อมหน้าที่ตามกฎหมาย และมีกลไกการเผชิญเหตุที่จำแนกตามระดับความรุนแรง โครงสร้างเช่นนี้เทียบเคียงได้กับประเทศที่ก้าวหน้าด้านไซเบอร์หลายประเทศ และเป็นรากฐานที่นโยบายและแผนฉบับต่อไปสามารถต่อยอดได้ทันที

ความสำเร็จประการที่สอง คือ การยกระดับมาตรฐานเชิงเทคนิคอย่างต่อเนื่อง สกมช. ได้ออกประกาศกำหนดมาตรฐานขั้นต่ำหลายฉบับ รวมถึงมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 ซึ่งเป็นมาตรฐานเฉพาะด้านฉบับแรกของไทย มาตรการเหล่านี้

ตอบสนองต่อข้อเท็จจริงที่ว่า ภัยคุกคามส่วนใหญ่ที่ไทยเผชิญมุ่งเป้าไปที่เว็บไซต์ ทั้งการเปลี่ยนหน้าเว็บ การฝังโฆษณาเว็บพแนจ และการทำเว็บปลอมเพื่อหลอกลวง⁵⁹

อย่างไรก็ตาม ข้อจำกัดประการแรกที่ปรากฏชัด คือ ตัวชี้วัดของแผนมีลักษณะเชิงปริมาณและเชิงเทคนิคเป็นด้านหลัก การวัดความสำเร็จด้วยจำนวนเหตุการณ์ที่ตรวจพบ จำนวนหน่วยงานที่ผ่านมาตรฐาน หรือจำนวนบุคลากรที่ได้รับการอบรม ไม่สามารถบอกได้ว่า ประเทศมีความมั่นคงเพิ่มขึ้นในเชิงยุทธศาสตร์หรือไม่ ยิ่งไปกว่านั้น จำนวนเหตุการณ์ที่ตรวจพบเพิ่มขึ้นอาจหมายถึงขีดความสามารถในการตรวจจับที่ดีขึ้น หรืออาจหมายถึงภัยที่รุนแรงขึ้นก็ได้ ซึ่งการตีความสองแบบนี้นำไปสู่ข้อเสนอเชิงนโยบายที่ต่างกันโดยสิ้นเชิง

ข้อจำกัดประการที่สอง คือ การทำงานแบบแยกส่วนระหว่างหน่วยงาน แม้มีนโยบายและแผนจะกำหนดให้หลายหน่วยงานมีส่วนร่วม แต่ในทางปฏิบัติ หน่วยงานด้านเทคนิค หน่วยงานข่าวกรอง หน่วยงานการทูต หน่วยงานป้องกันประเทศ และหน่วยงานบังคับใช้กฎหมาย ยังคงทำงานตามภารกิจของตนโดยมีจุดเชื่อมต่อจำกัด ผลที่ตามมาคือ ตัวบ่งชี้ภัยที่หน่วยงานหนึ่งตรวจพบมักไม่ถูกส่งต่อไปยังหน่วยงานอื่นอย่างทันท่วงที และภาพสถานการณ์ร่วม (common operational picture) ที่ครบถ้วนจึงไม่เกิดขึ้น

ข้อจำกัดประการที่สาม คือ นโยบายและแผนฉบับปัจจุบันแทบไม่ได้กล่าวถึงมิติการทูตไซเบอร์เลย ทั้งที่ไทยเข้าร่วมกระบวนการ OEWG ในกรอบสหประชาชาติมาอย่างต่อเนื่อง และเพิ่งร่วมรับรองการจัดตั้งกลไกถาวรด้านความมั่นคงไซเบอร์เมื่อ พ.ศ. 2568 การไม่มีมิตินี้ในนโยบายและแผนระดับชาติ ทำให้การดำเนินการทางการทูตขาดการเชื่อมโยงกับการดำเนินการภายในประเทศ และทำให้ท่าทีของไทยในเวทีระหว่างประเทศไม่ได้ถูกแปลงกลับมาเป็นแนวปฏิบัติของหน่วยงานภายใน

ข้อจำกัดประการที่สี่ คือ ความไม่ชัดเจนของการแบ่งบทบาทระหว่างหน่วยงาน ความมั่นคงฝ่ายทหารกับฝ่ายพลเรือน ขณะที่กองทัพกำลังยกระดับหน่วยงานไซเบอร์ของตนขึ้นเป็นกองบัญชาการ ยังไม่ปรากฏกรอบที่ชัดเจนว่า ขอบเขตภารกิจของฝ่ายทหารสิ้นสุดที่ใดและขอบเขตของ สกมช. เริ่มต้นที่ใด ความคลุมเครือนี้เสี่ยงต่อการเกิดทั้งความซ้ำซ้อนของภารกิจและช่องว่างของความรับผิดชอบไปพร้อมกัน ซึ่งเป็นปัญหาที่ประเทศอื่นแก้ไขด้วยการแยกบทบาทอย่างชัดเจนดังกรณี NCSC และ NCF ของสหราชอาณาจักร

ข้อจำกัดประการที่ห้า คือ ปัญหากำลังคนและการพึ่งพาเทคโนโลยีจากต่างชาติ ภาวะขาดแคลนบุคลากรด้านไซเบอร์เป็นปัญหาระดับโลก โดยภูมิภาคเอเชียแปซิฟิกเป็นภูมิภาคที่

⁵⁹ กรุงเทพมหานคร, ภัยไซเบอร์ป่วนไทย “ฟิชซิง-ดีดอส” ถล่มภาครัฐ-อินฟราฯ สำคัญ, [ออนไลน์], 2568, แหล่งที่มา: <https://www.bangkokbiznews.com/tech/gadget/1198511> [12 สิงหาคม 2569].

ช่องว่างกำลังขยายตัวมากที่สุด⁶⁰ สำหรับไทยปัญหานี้ทวีความรุนแรงขึ้นเมื่อประกอบกับการพึ่งพาผลิตภัณฑ์และบริการด้านความมั่นคงไซเบอร์จากต่างประเทศเกือบทั้งหมด ซึ่งสร้างความเปราะบางเชิงยุทธศาสตร์ในยามที่เกิดความตึงเครียดระหว่างประเทศหรือการหยุดชะงักของห่วงโซ่อุปทาน (supply chain)

ข้อจำกัดประการสุดท้าย คือ ความไว้วางใจของสาธารณะที่อยู่ในระดับต่ำ เหตุการณ์ข้อมูลประชาชนรั่วไหลจากระบบของหน่วยงานรัฐซ้ำแล้วซ้ำเล่า ประกอบกับการที่หน่วยงานรัฐมักปฏิเสธในขั้นต้นก่อนจะยอมรับในภายหลัง ได้บั่นทอนความเชื่อมั่นของประชาชนต่อระบบดิจิทัลภาครัฐอย่างมีนัยสำคัญ⁶¹ ความไว้วางใจที่ต่ำนี้เป็นอุปสรรคสำคัญต่อการดำเนินนโยบายเชิงรุกในอนาคต เพราะมาตรการที่เกี่ยวข้องกับการเฝ้าระวังหรือการเข้าถึงข้อมูลย่อมเผชิญการต่อต้าน หากประชาชนไม่เชื่อมั่นในความรับผิดชอบของรัฐ

ข้อจำกัดข้างต้นสอดคล้องกับความเห็นของหน่วยงานปฏิบัติ โดย สมช. ได้จัดการสัมมนาเชิงปฏิบัติการเพื่อทบทวนนโยบายด้านความมั่นคงไซเบอร์ร่วมกับหน่วยงานที่เกี่ยวข้องระหว่างวันที่ 17-20 พฤษภาคม พ.ศ. 2569⁶² และได้รับทราบปัญหาและข้อจำกัดซึ่งสอดคล้องกับข้อสังเกตของ สมช. อย่างน้อยสามประการ ประการแรก ผู้แทนเหล่าทัพระบุว่าภารกิจที่เอกสารนโยบายมิได้กำหนดเรื่องการป้องกันเชิงรุกไว้ ทำให้กองทัพไม่มีทิศทางที่ชัดเจนและไม่สามารถดำเนินการได้อย่างเต็มที่ ประการที่สอง ผู้แทนหน่วยงานบังคับใช้กฎหมายและหน่วยงานข่าวกรองเห็นตรงกันว่า การบังคับใช้กฎหมายต่อผู้กระทำความผิดที่อยู่ในประเทศอื่นเป็นเรื่องท้าทายอย่างยิ่ง โดยสิ่งสำคัญความมั่นคงแห่งชาติต่อไปควรให้ความสำคัญกับเทคโนโลยีอุบัติใหม่ (emerging technologies) อย่างมาก โดยเฉพาะปัญญาประดิษฐ์และการประมวลผลเชิงควอนตัม เนื่องจากปัจจุบันเริ่มปรากฏปัญหาด้านความมั่นคงปลอดภัยไซเบอร์อันเกิดจากเทคโนโลยีดังกล่าวแล้ว

โดยสรุป ประเด็นที่ควรนำไปดำเนินการต่อในห้วง พ.ศ. 2571-2575 ประกอบด้วย ห้าเรื่องหลัก ได้แก่ การปรับกรอบการมองปัญหาจากเชิงเทคนิคไปสู่เชิงยุทธศาสตร์ การสร้างกลไกบูรณาการข้ามหน่วยงานที่ใช้การได้จริง การเพิ่มมิติการทูตไซเบอร์เข้าไปในนโยบายและแผน

⁶⁰ ISC2, *ISC2 Cybersecurity Workforce Study (2024)*, [Online], 2024, Available from:

<https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study#KeyFindings> [2026, August 12].

⁶¹ Hfocus. สธ.-สมช. แจงข้อมูลรั่วไม่ไข สธ. เป็นไปได้ทั้งรัฐ-เอกชน ถูกอ้างหลุด 7 หน่วยงาน, [ออนไลน์], 2567, แหล่งที่มา:

<https://www.hfocus.org/content/2024/03/30032> [12 สิงหาคม 2569].

⁶² ผู้แทนหน่วยงานที่เกี่ยวข้อง ประกอบด้วย ผู้แทนสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สมช.)

กระทรวงการต่างประเทศ (กลุ่มงานความมั่นคงระหว่างประเทศ สำนักนโยบายและแผน สำนักงานปลัดกระทรวงฯ กรมอเมริกาและแปซิฟิกใต้ กรมเอเชียตะวันออก กรมเอเชียใต้ และกรมยุโรป) สำนักข่าวกรองแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงกลาโหม (สำนักงานปลัดกระทรวงฯ) กองบัญชาการกองทัพไทย (หน่วยบัญชาการไซเบอร์ทหาร) กองทัพบก กองทัพเรือ กองทัพอากาศ และสำนักงานตำรวจแห่งชาติ (กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี)

ระดับชาติด้วยความมั่นคงแห่งชาติฉบับใหม่ การแบ่งบทบาทระหว่างฝ่ายทหารกับฝ่ายพลเรือนให้ชัดเจน พร้อมกลไกกำกับดูแลและการเตรียมรับมือภัยจากปัญญาประดิษฐ์และเทคโนโลยีควอนตัมอย่างเป็นระบบ

2.2.3 ตัวอย่างประเทศที่มีแนวปฏิบัติที่ดี (best practice)

สิงคโปร์เป็นตัวอย่างที่ใกล้เคียงกับบริบทของไทยมากที่สุดในแง่ขนาดประเทศและตำแหน่งเชิงภูมิรัฐศาสตร์ หน่วยงานความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ดำเนินยุทธศาสตร์ที่ผสมผสานการกำกับดูแลโครงสร้างพื้นฐานสำคัญ (CII) เข้ากับการสร้างระบบนิเวศอุตสาหกรรมและการทูตไซเบอร์อย่างเป็นเอกภาพ ตัวอย่างที่เป็นรูปธรรมคือ แผนแม่บทความมั่นคงปลอดภัยไซเบอร์สำหรับเทคโนโลยีเชิงปฏิบัติการ (Operational Technology: OT Cybersecurity Masterplan) เริ่มใช้ครั้งแรกใน พ.ศ. 2562 และปรับปรุงใน พ.ศ. 2567 แผนนี้มุ่งยกระดับความมั่นคงของระบบควบคุมอุตสาหกรรมในภาคส่วนสำคัญผ่านสามเสาหลัก คือ คน กระบวนการ และเทคโนโลยี พร้อมผลักดันหลักการ "ปลอดภัยตั้งแต่การติดตั้ง" (secure-by-deployment)⁶³

บทเรียนสำคัญจากสิงคโปร์สำหรับไทยคือ การที่สิงคโปร์ใช้ความมั่นคงไซเบอร์เป็นเครื่องมือทางการทูตอย่างชัดเจน สิงคโปร์เป็นเจ้าภาพการประชุมรัฐมนตรีอาเซียนด้านความมั่นคงไซเบอร์ เป็นที่ตั้งของศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ และผลักดันการจัดตั้งทีมเผชิญเหตุระดับภูมิภาคของอาเซียน (ASEAN Regional CERT) ได้สำเร็จ⁶⁴ การลงทุนในบทบาทนำเชิงสถาบันเช่นนี้สร้างอิทธิพลเชิงยุทธศาสตร์ให้สิงคโปร์ได้มากกว่าที่ขนาดของประเทศจะเอื้ออำนวย

สหราชอาณาจักรเป็นตัวอย่างที่ดีที่สุดของการแบ่งบทบาทระหว่างการป้องกันกับการปฏิบัติการเชิงรุก ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติทำหน้าที่เป็นหน่วยงานฝ่ายป้องกันที่เปิดเผยและเข้าถึงได้ พร้อมดำเนินโครงการ "การป้องกันเชิงรุก" (Active Cyber Defence) โดยให้บริการอัตโนมัติแก่หน่วยงานรัฐและประชาชน เช่น การปิดกั้นเว็บไซต์ฟิชซิง (phishing) หรืออาชญากรรมคอมพิวเตอร์ที่หลอกลวงผู้ใช้งานคอมพิวเตอร์ให้กระทำการอย่างใดอย่างหนึ่ง เพื่อให้เข้าถึงข้อมูลหรือสั่งให้โปรแกรมที่ผู้หลอกลวงซ่อนไว้เริ่มทำงาน และการกรองชื่อโดเมนที่เป็น

⁶³ Cyber Security Agency of Singapore, Singapore's Operational Technology Cybersecurity Masterplan 2024, [Online], 2024, Available from: <https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/> [2026, August 12].

⁶⁴ Cyber Security Agency of Singapore, Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region, [Online], 2024, Available from: <https://www.csa.gov.sg/news-events/press-releases/singapore-and-aseanmember-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/> [2026, August 12].

อันตราย⁶⁵ ขณะที่กองกำลังไซเบอร์แห่งชาติซึ่งเป็นหน่วยงานร่วมระหว่างกระทรวงกลาโหมกับ GCHQ ทำหน้าที่ปฏิบัติการเชิงรุกภายใต้หลักการใช้อำนาจไซเบอร์อย่างมีความรับผิดชอบ

บทเรียนจากสหราชอาณาจักรมีสองประการ ประการแรก คือ การแยกหน่วยงานฝ่ายป้องกันออกจากหน่วยงานฝ่ายรุกอย่างชัดเจน ช่วยรักษาความไว้วางใจของภาคเอกชนและประชาชน เพราะภาคเอกชนจะแบ่งปันข้อมูลภัยคุกคามกับหน่วยงานรัฐได้อย่างสบายใจก็ต่อเมื่อมั่นใจว่าหน่วยงานนั้นไม่ได้มีการกีดกันสอดแนม ประการที่สอง คือ การประกาศหลักการกำกับปฏิบัติการเชิงรุกอย่างเปิดเผยช่วยสร้างความชอบธรรมทั้งในประเทศและระหว่างประเทศ ซึ่งเป็นสิ่งที่รัฐขนาดกลางจำเป็นต้องมีมากกว่ามหาอำนาจเสียอีก

ญี่ปุ่นเป็นตัวอย่างของประเทศที่เปลี่ยนผ่านจากท่าทีตั้งรับไปสู่การป้องกันเชิงรุกภายใต้ข้อจำกัดทางรัฐธรรมนูญและการเมืองภายใน กฎหมายว่าด้วยการป้องกันไซเบอร์เชิงรุกที่ผ่านรัฐสภาใน พ.ศ. 2568 กำหนดกลไกสามส่วนควบคู่กัน ได้แก่ การให้อำนาจดำเนินมาตรการเชิงรุกแก่หน่วยงานที่เกี่ยวข้อง การกำหนดหน้าที่รายงานเหตุของผู้ประกอบการโครงสร้างพื้นฐานสำคัญ (CII) และการวางกรอบการกำกับดูแลเพื่อคุ้มครองความเป็นส่วนตัวของประชาชน การออกแบบเช่นนี้แสดงว่า การเพิ่มอำนาจเชิงรุกกับการรักษาสิทธิเสรีภาพสามารถดำเนินไปพร้อมกันได้หากมีการออกแบบกลไกตรวจสอบที่รัดกุม

บทเรียนจากญี่ปุ่นที่ตรงกับบริบทของไทยมากที่สุดคือกระบวนการสร้างฉันทามติภายในประเทศ ญี่ปุ่นใช้เวลาหลายปีในการอภิปรายสาธารณะ จัดทำเอกสารประเมินภัยคุกคาม และแสดงให้เห็นว่า เหตุใดการตั้งรับเพียงลำพังจึงไม่เพียงพอ ก่อนที่จะเสนอกฎหมายเข้าสู่รัฐสภา

เนเธอร์แลนด์และออสเตรเลียเป็นตัวอย่างของประเทศขนาดกลางที่จัดทำยุทธศาสตร์ไซเบอร์ระหว่างประเทศแยกออกมาต่างหากจากยุทธศาสตร์ภายในประเทศ เนเธอร์แลนด์จัดทำยุทธศาสตร์ไซเบอร์ระหว่างประเทศ (พ.ศ. 2566-2571) โดยระบุชัดว่าประเทศต้องมีเครื่องมือเชิงนโยบายที่หลากหลายเพียงพอ เพื่อตอบสนองต่อภัยได้อย่างได้สัดส่วน⁶⁶ ส่วนออสเตรเลียกำหนดให้การพัฒนาขีดความสามารถที่เป็นเอกเทศ (sovereign capabilities) เป็นหนึ่งใน “โล่ ทาง

⁶⁵ National Cyber Security Centre, *Active Cyber Defence*, [Online], 2026, Available from:

<https://www.ncsc.gov.uk/section/advice-guidance/all-topics/active-cyber-defence> [2026, August 12].

⁶⁶ Ministry of Foreign Affairs of the Kingdom of the Netherlands, *International Cyber Strategy 2023-2028*, [Online], 2023, Available from: <https://www.government.nl/documents/2023/09/12/international-cyber-strategy-netherlands-2023-2028> [2026, August 12].

ไซเบอร์” ของชาติ พร้อมจัดสรรงบประมาณจำนวนมาก เพื่อเสริมสร้างศักยภาพให้ประเทศในภูมิภาค⁶⁷

สหรัฐฯ เป็นตัวอย่างของการบริหารงานด้านไซเบอร์ที่แบ่งบทบาทเป็นชั้น ๆ และใช้กลไกประสานงานที่อยู่ใกล้ผู้นำสูงสุด ในชั้นนโยบาย สภาความมั่นคงแห่งชาติ (National Security Council: NSC) ของทำเนียบขาวทำหน้าที่เป็นเวทีตัดสินใจและประสานนโยบายข้ามหน่วยงาน โดยมีคณะทำงานด้านไซเบอร์ภายใต้ที่ปรึกษาด้านความมั่นคงแห่งชาติเป็นผู้ร่างท่าทีและกำกับการตอบสนองเมื่อเกิดเหตุใหญ่ ควบคู่กับสำนักงานผู้อำนวยการไซเบอร์แห่งชาติ (Office of the National Cyber Director: ONCD) ซึ่งรับผิดชอบยุทธศาสตร์ไซเบอร์แห่งชาติและการจัดลำดับงบประมาณของฝ่ายบริหาร ในชั้นปฏิบัติ สหรัฐฯ แยกงานป้องกันฝ่ายพลเรือนออกจากงานปฏิบัติการทางทหารอย่างชัดเจน โดยหน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐาน (Cybersecurity and Infrastructure Security Agency: CISA) ภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิรับผิดชอบการป้องกันหน่วยงานพลเรือนและโครงสร้างพื้นฐานสำคัญ ขณะที่หน่วยงานความมั่นคงแห่งชาติ (National Security Agency: NSA) และกองบัญชาการไซเบอร์ของสหรัฐฯ (U.S. Cyber Command) รับผิดชอบงานข่าวกรองสัญญาณและปฏิบัติการทางทหาร

จุดที่เป็นเอกลักษณ์ของแบบจำลองสหรัฐฯ คือ การกำหนดให้ผู้บัญชาการ NSA ดำรงตำแหน่งผู้บัญชาการกองบัญชาการไซเบอร์ในเวลาเดียวกัน หรือที่เรียกว่า โครงสร้าง "สองหมวก" (dual-hat) ซึ่งมีขึ้นตั้งแต่การจัดตั้งกองบัญชาการไซเบอร์ใน พ.ศ. 2553 เหตุผลสนับสนุน คือ การให้สองหน่วยงานใช้โครงสร้างพื้นฐาน บุคลากร และเครื่องมือร่วมกันภายใต้ผู้บังคับบัญชาคนเดียว ช่วยย่นเวลาจากการได้ข่าวกรองไปสู่การปฏิบัติ และลดความเสี่ยงที่ปฏิบัติการของสองฝ่ายจะรบกวนกันเอง ส่วนข้อวิจารณ์ คือ การรวมอำนาจไว้ที่บุคคลเดียวอาจทำให้ภารกิจข่าวกรองถูกดึงเข้าสู่ตรรกะทางทหารและถูกทำให้เป็นเรื่องการเมืองได้ง่ายขึ้น ข้อถกเถียงเรื่องการแยกสองตำแหน่งจึงเกิดขึ้นเป็นระยะตลอดสามรัฐบาลที่ผ่านมา แต่ท้ายที่สุดสหรัฐฯ ยังคงโครงสร้างเดิมไว้ ดังปรากฏว่า วุฒิสภาสหรัฐฯ ได้ให้ความเห็นชอบให้นายทหารคนเดียวดำรงทั้งสองตำแหน่งอีกครั้งเมื่อเดือนมีนาคม พ.ศ. 2569⁶⁸ บทเรียนสำหรับไทยจึงมีสองชั้น ชั้นแรก คือ ความจำเป็นของกลไกประสานนโยบายที่อยู่ใกล้ผู้ตัดสินใจสูงสุดและมีอำนาจเรียกทุกหน่วยงานมาหารือได้ ซึ่งเป็นบทบาทที่สำนักงานสภาความมั่นคง

⁶⁷ Australian Government, Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy*, [Online], 2023, Available from: <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf> [2026, August 12].

⁶⁸ Stars and Stripes, *Senate approves Joshua Rudd as head of Cyber Command, NSA*, [Online], 2026, Available from: <https://www.stripes.com/theaters/us/2026-03-10/joshua-rudd-nsa-cyber-command-21018045.html> [2026, August 25].

แห่งชาติหรือ สมช. ของไทยดำเนินการอยู่แล้ว และควรได้รับการเสริมความชัดเจน และขั้นที่สอง คือ การเชื่อมงานข่าวกรองเข้ากับงานปฏิบัติการต้องมาพร้อมกลไกกำกับดูแลที่รัดกุม เพื่อรักษาความไว้วางใจของภาคเอกชนและประชาชนที่ต้องแบ่งปันข้อมูลกับหน่วยงานฝ่ายป้องกัน

จีนมองสหรัฐฯ ในฐานะคู่แข่งเชิงยุทธศาสตร์และรัฐฝ่ายตรงข้ามที่เป็นภัยคุกคามหลักต่อความมั่นคงไซเบอร์ของตน⁶⁹ เอกสารและถ้อยแถลงของทางการจีนกล่าวหาสหรัฐฯ ว่าอาศัยความได้เปรียบทางเทคโนโลยีดำเนินการสอดแนมและครอบงำพื้นที่ไซเบอร์ (cyber hegemony) โดยหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ของจีนได้เผยแพร่รายงานกล่าวหาหน่วยงานข่าวกรองของสหรัฐฯ ว่าเจาะระบบของสถาบันวิจัยและหน่วยงานสำคัญของจีนหลายครั้ง⁷⁰ ในเชิงหลักนิยม จีนให้น้ำหนักกับแนวคิดอธิปไตยไซเบอร์ (cyber sovereignty) การพึ่งพาตนเองด้านเทคโนโลยีหลัก และเป้าหมายการเป็นชาติมหาอำนาจทางไซเบอร์ ซึ่งสะท้อนการมองว่า การพึ่งพาเทคโนโลยีของสหรัฐฯ เป็นความเปราะบางเชิงยุทธศาสตร์

บทเรียนร่วมจากทุกประเทศข้างต้นมีสี่ประการ ประการแรก ทุกประเทศจัดวางความมั่นคงไซเบอร์ไว้ในระดับยุทธศาสตร์ชาติ และเชื่อมโยงกับนโยบายต่างประเทศอย่างชัดเจน ประการที่สอง ทุกประเทศแบ่งบทบาทระหว่างหน่วยงานอย่างชัดเจนพร้อมกลไกกำกับดูแล ประการที่สาม ทุกประเทศลงทุนในการสร้างขีดความสามารถภายในประเทศเพื่อลดการพึ่งพาต่างชาติ และประการที่สี่ ทุกประเทศใช้ความร่วมมือระหว่างประเทศเป็นเครื่องมือขยายอิทธิพลเชิงยุทธศาสตร์ มิใช่เพียงเป็นการแลกเปลี่ยนทางเทคนิค

ทั้งนี้ หลังจากที่ได้ไทยสามารถสร้างขีดความสามารถภายในประเทศให้มีฐานที่มั่นคงได้แล้ว ควรจะต่อยอดขีดความสามารถนั้นผ่านความร่วมมือระหว่างประเทศ เช่น ในกรอบอาเซียน ไทยควรเป็นศูนย์กลางการฝึกอบรมและพัฒนากำลังคนด้านไซเบอร์ของภูมิภาคผ่านศูนย์ AJCCBC และจัดให้มีการฝึกซ้อมรับมือเหตุร่วมเป็นประจำ ความร่วมมือกับญี่ปุ่นควรยกระดับจากการรับการฝึกอบรมไปสู่การพัฒนาหลักสูตรและการวิจัยร่วม โดยเฉพาะการคุ้มครองระบบเทคโนโลยีเชิงปฏิบัติการและการออกแบบกลไกกำกับดูแลปฏิบัติการเชิงรุก ความร่วมมือกับออสเตรเลียและประเทศที่มีแนวคิดใกล้เคียง เช่น สิงคโปร์ เกาหลีใต้ และสหภาพยุโรป ควรมุ่งการแลกเปลี่ยนข่าวกรองภัยคุกคามอย่างเป็นระบบ การเทียบมาตรฐานนิติวิทยาศาสตร์ดิจิทัลให้ผลการวิเคราะห์ของไทยเป็นที่ยอมรับในเวทีระหว่างประเทศ และการเรียนรู้กลไกการกล่าวโทษและมาตรการตอบสนอง

⁶⁹ CGTN, กต.จีนระบุ หลักฐานล่าสุดยืนยันอีกครั้งว่า สหรัฐฯ เป็นภัยคุกคามทางไซเบอร์อันดับแรก, [ออนไลน์], 2568, แหล่งที่มา: <https://thai.cri.cn/2025/08/02/ART11754125188502254> [25 สิงหาคม 2569].

⁷⁰ China Cybersecurity Industry Alliance: U.S., Threats and Sabotage to Global Cyberspace Security and Development, [Online], 2024, Available from: <https://china-cia.org.cn/home/WorkDetail?id=663874690200340c642b4cc4&> [2026, August 25].

และในระยะต่อไปไทยควรเปลี่ยนสถานะจากผู้รับการเสริมสร้างศักยภาพไปเป็นผู้ให้ โดยสามารถเสนอหลักสูตรผู้เชี่ยวชาญ และข้อมูลภัยคุกคามแก่ประเทศเพื่อนบ้านได้ ซึ่งจะทำให้ไทยใช้ความร่วมมือระหว่างประเทศเป็นเครื่องมือขยายอิทธิพลเชิงยุทธศาสตร์ได้เช่นเดียวกับประเทศกรณีศึกษา

2.2.4 การสร้างความร่วมมือในอาเซียน สหประชาชาติ และกับประเทศอื่น

ความร่วมมือในกรอบอาเซียนได้พัฒนาไปมากในทศวรรษที่ผ่านมา อาเซียนมีการประชุมรัฐมนตรีอาเซียนด้านความมั่นคงไซเบอร์เป็นเวทีหารือระดับนโยบาย มียุทธศาสตร์ความร่วมมือด้านความมั่นคงไซเบอร์ของอาเซียน และล่าสุดได้จัดตั้งทีมเผชิญเหตุฉุกเฉินทางคอมพิวเตอร์ระดับภูมิภาค (ASEAN Regional CERT) ซึ่งทำหน้าที่ประสานงานและแลกเปลี่ยนข้อมูลระหว่างทีมเผชิญเหตุแห่งชาติของประเทศสมาชิก จัดทำเครือข่ายจุดติดต่อของผู้เชี่ยวชาญ จัดการฝึกซ้อมระดับภูมิภาค และสนับสนุนการเสริมสร้างศักยภาพ⁷¹

ความร่วมมือด้านไซเบอร์ของอาเซียนในทางปฏิบัติดำเนินอยู่ในสี่ช่องทางคู่ขนาน ช่องทางแรก คือ กรอบภายใต้เสาเศรษฐกิจ ผ่านการประชุมรัฐมนตรีอาเซียนด้านดิจิทัล (ASEAN Digital Ministers' Meeting: ADGMIN) ซึ่งไทยเป็นประธานในวาระ พ.ศ. 2568 และเป็นเจ้าภาพการประชุมครั้งที่ 5 ณ กรุงเทพมหานคร ระหว่างวันที่ 13-17 มกราคม พ.ศ. 2568 โดยมีเอกสารผลลัพธ์ที่เกี่ยวข้องกับความมั่นคงไซเบอร์โดยตรง ได้แก่ ปฏิญญากรุงเทพฯ ว่าด้วยดิจิทัล และคู่มืออาเซียนว่าด้วยธรรมาภิบาลและจริยธรรม ปัญญาประดิษฐ์ฉบับขยายความที่ครอบคลุมปัญญาประดิษฐ์เชิงสร้าง (Generative AI) ทั้งนี้ อาเซียนได้จัดตั้งคณะกรรมการประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียน (ASEAN Cyber: CC) เพื่อประสานการทำงานขององค์กรเฉพาะสาขาที่เกี่ยวข้องเข้าด้วยกัน

ช่องทางที่สอง คือ เวทีระดับรัฐมนตรีเฉพาะด้าน ได้แก่ การประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN Ministerial Conference on Cybersecurity: AMCC) ที่สิงคโปร์เริ่มและจัดคู่ขนานกับสัปดาห์ไซเบอร์นานาชาติสิงคโปร์เป็นประจำทุกปี โดยการประชุมครั้งที่ 10 เมื่อวันที่ 22 ตุลาคม พ.ศ. 2568 ได้หารือทั้งการโจมตีทางไซเบอร์ การคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การหลอกลวงออนไลน์ และภัยรูปแบบใหม่จากปัญญาประดิษฐ์และเทคโนโลยีควอนตัม

ช่องทางที่สาม คือ กรอบกลาโหมภายใต้การประชุมรัฐมนตรีกลาโหมอาเซียน (ASEAN Defence Ministers' Meeting: ADMM) ซึ่งใน พ.ศ. 2568 ได้รับรองแนวทางและแผนดำเนินการของเครือข่ายป้องกันไซเบอร์อาเซียน (ASEAN Cyber Defence Network: ACDN) และรับรองเอกสารแนวความคิดว่าด้วยความมั่นคงปลอดภัยของโครงสร้างพื้นฐานได้ทะเลที่ไทยเสนอ

⁷¹ Cyber Security Agency of Singapore, *supra* note 64.

ร่วมกับสิงคโปร์และบรูไนในการประชุมครั้งที่ 19 เมื่อวันที่ 31 ตุลาคม พ.ศ. 2568 ทั้งยังมีศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ADMM ซึ่งจัดตั้งเมื่อ พ.ศ. 2564 ทำหน้าที่เป็นมาตรการเสริมสร้าง ความไว้วางใจ การแบ่งปันข้อมูล และการรับมือข้อมูลบิดเบือนระหว่างหน่วยงานกลาโหม

ช่องทางที่สี่ คือ กลไกเสริมสร้างขีดความสามารถ ได้แก่ ศูนย์เสริมสร้างศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-ญี่ปุ่น (ASEAN-Japan Cybersecurity Capacity Building Centre: AJCCBC) ที่กรุงเทพมหานคร ศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ (ASEAN-Singapore Cybersecurity Centre of Excellence: ASCCE) ที่สิงคโปร์ และ ASEAN Regional CERT

ประเทศไทยมีความได้เปรียบเชิงที่ตั้งในกรอบอาเซียน เนื่องจากเป็นที่ตั้งของศูนย์ AJCCBC ซึ่งฝึกอบรมบุคลากรจากประเทศสมาชิกอาเซียนอย่างต่อเนื่อง ศูนย์ดังกล่าวจัดตั้งขึ้นเมื่อ พ.ศ. 2561 ด้วยงบประมาณสนับสนุนจากกองทุนความร่วมมืออาเซียน-ญี่ปุ่น (Japan-ASEAN Integration Fund: JAIF) ปัจจุบันอยู่ระหว่างดำเนินโครงการระยะที่สอง (พ.ศ. 2566-2569) ว่าด้วยการเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์และบริการดิจิทัลที่น่าเชื่อถือ โดยได้รับการสนับสนุนจากองค์การความร่วมมือระหว่างประเทศของญี่ปุ่น (Japan International Cooperation Agency: JICA) และอยู่ระหว่างเสนอโครงการระยะที่สาม (พ.ศ. 2570-2574) ซึ่งเพิ่มมิติปัญญาประดิษฐ์เข้าไปด้วย โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบศูนย์ในฝ่ายไทย การมีศูนย์ดังกล่าวเปิดโอกาสให้ไทยแสดงบทบาทเป็นผู้ให้ในเวทีภูมิภาค และสร้างเครือข่ายความสัมพันธ์เชิงวิชาชีพที่มีคุณค่าในยามเกิดเหตุ

อย่างไรก็ตาม ไทยยังใช้ประโยชน์จากสินทรัพย์เชิงยุทธศาสตร์นี้ไม่เต็มศักยภาพเมื่อเทียบกับที่สิงคโปร์ใช้ประโยชน์จากศูนย์ ASCCE ความแตกต่างดังกล่าวอธิบายได้อย่างน้อยสามประการ ประการแรก คือ ศูนย์ AJCCBC ในไทยมุ่งการฝึกอบรมเชิงเทคนิคแก่เจ้าหน้าที่ผู้ปฏิบัติ เช่น การเผชิญเหตุและการวิเคราะห์มัลแวร์เป็นหลัก ขณะที่ศูนย์ ASCCE ออกแบบให้ครอบคลุมทั้งหลักสูตรด้านนโยบายและการทูตไซเบอร์ การพัฒนากฎหมายและบรรทัดฐานระหว่างประเทศ และการฝึกซ้อมรับมือสถานการณ์ในระดับผู้บริหาร ผลผลิตของศูนย์ ASCCE จึงเชื่อมต่อการกำหนดนโยบายได้โดยตรง ประการที่สอง คือ สิงคโปร์ลงทุนงบประมาณของตนเองในศูนย์ ASCCE และมอบหมายให้หน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นเจ้าภาพเพียงหน่วยเดียว ทำให้กำหนดทิศทางหลักสูตรให้สอดคล้องกับยุทธศาสตร์ของประเทศได้ ขณะที่ศูนย์ AJCCBC พึ่งพางบประมาณจากกองทุนความร่วมมืออาเซียน-ญี่ปุ่น และความร่วมมือของฝ่ายญี่ปุ่นเป็นหลัก ไทยจึงมีบทบาทเป็นผู้ให้สถานที่และผู้ร่วมดำเนินการมากกว่าผู้กำหนดวาระ ประการที่สาม คือ สิงคโปร์ ผูกกิจกรรมของศูนย์ ASCCE เข้ากับการประชุม AMCC และสัปดาห์ไซเบอร์นานาชาติสิงคโปร์

(Singapore International Cyber Week) ที่ตนเป็นเจ้าภาพทุกปี ทำให้ผลการฝึกอบรมและข้อเสนอเชิงบรรทัดฐานถูกยกระดับสู่การหารือระดับรัฐมนตรีอย่างต่อเนื่อง

ในกรอบภูมิภาคที่กว้างขึ้น การประชุมอาเซียนว่าด้วยการเมืองและความมั่นคงในภูมิภาคเอเชียแปซิฟิก (ASEAN Regional Forum: ARF) เป็นเวทีสำคัญสำหรับมาตรการสร้างความไว้วางใจด้านไซเบอร์ เวทีนี้มีคุณค่าเป็นพิเศษสำหรับไทยเพราะเป็นเวทีเดียวในภูมิภาคที่มีทั้งสหรัฐฯ จีน รัสเซีย ญี่ปุ่น และประเทศอาเซียนเข้าร่วมพร้อมกัน จึงเป็นพื้นที่ที่ไทยสามารถผลักดันบรรทัดฐานได้โดยไม่ต้องเลือกข้าง ความมั่นคงของและในการใช้เทคโนโลยีสารสนเทศและการสื่อสารเป็นหนึ่งในห้าสาขาหลักของความร่วมมือในกรอบ ARF โดยเน้นการสัมมนาและการประชุมเชิงปฏิบัติการที่ไม่มีผลผูกพัน เพื่อนำไปสู่การจัดทำแนวปฏิบัติหรือระเบียบปฏิบัติประจำในเรื่องที่เห็นพ้องกัน ตัวอย่างที่เป็นรูปธรรม คือ การจัดทำทำเนียบจุดติดต่อด้านความมั่นคงไซเบอร์ของ ARF ซึ่งริเริ่มโดยมาเลเซียและออสเตรเลีย และช่วยหนุนเสริมทำเนียบจุดติดต่อด้านความปลอดภัยภายใต้กรอบสหประชาชาติไปพร้อมกัน ในส่วนของไทยนั้น ไทยได้เป็นประธานร่วมจัดการประชุมเชิงปฏิบัติการว่าด้วยการต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อก่ออาชญากรรมร่วมกับรัสเซียและจีน เมื่อวันที่ 23-24 พฤษภาคม พ.ศ. 2567 ณ กรุงมอสโก และเป็นประธานร่วมจัดการประชุมเชิงปฏิบัติการว่าด้วยบทเรียนด้านธรรมาภิบาลของความมั่นคงไซเบอร์ร่วมกับแคนาดาและญี่ปุ่น เมื่อวันที่ 9-10 กุมภาพันธ์ พ.ศ. 2569 การเป็นประธานร่วมกับทั้งสองกลุ่มประเทศในระยะเวลาใกล้เคียงกันสะท้อนว่าไทยยังรักษาสถานะที่ทุกฝ่ายยอมรับได้ไว้ได้จริงในทางปฏิบัติ

ประโยชน์ที่ไทยได้รับจากกรอบภูมิภาคเหล่านี้สรุปได้สี่ประการ ประการแรก คือ ทรัพยากรและการฝึกอบรมที่ได้รับการสนับสนุนจากภายนอก ทั้งจากกองทุนความร่วมมืออาเซียน-ญี่ปุ่น และงบประมาณของสิงคโปร์ ซึ่งช่วยลดภาระงบประมาณของไทยในการพัฒนากำลังคน ประการที่สอง คือ ช่องทางประสานงานที่ใช้ได้จริงในยามเกิดเหตุ ทั้งการเชื่อมทีมเผชิญเหตุระหว่างกันผ่าน ASEAN Regional CERT และทำเนียบจุดติดต่อด้านของ ARF ซึ่งย่นเวลาในการติดต่อหน่วยงานที่รับผิดชอบของประเทศอื่นเมื่อเกิดเหตุข้ามพรมแดน ประการที่สาม คือ มาตรฐานอ้างอิงที่ช่วยลดต้นทุนการออกแบบนโยบายภายในประเทศ โดยเฉพาะรายการตรวจสอบการนำบรรทัดฐานไปปฏิบัติของอาเซียน (ASEAN Norms Implementation Checklist) ซึ่งเป็นมาตรฐานระดับภูมิภาคฉบับแรกที่แปลงหลักปฏิบัติที่ไม่ผูกมัดของรัฐที่มีความรับผิดชอบให้เป็นขั้นตอนที่ตรวจสอบได้ และคู่มือธรรมาภิบาลปัญญาประดิษฐ์ของอาเซียนที่ครอบคลุมความเสี่ยงด้านไซเบอร์ ประการที่สี่ คือ พื้นที่ทางการทูตในการวางตำแหน่งของไทย เนื่องจากการเป็นเจ้าภาพและประธานร่วมในเวทีต่าง ๆ ทำให้ไทยมีส่วนกำหนดวาระ เช่น การผลักดันประเด็นความมั่นคงของโครงสร้างพื้นฐานใต้ทะเลและภัยจากเทคโนโลยีอุบัติใหม่ แทนที่จะเป็นเพียงผู้รับกติกาที่ผู้อื่นกำหนด อย่างไรก็ตาม ข้อจำกัดสำคัญคือ กลไกเหล่านี้ส่วนใหญ่ไม่มีผลผูกพันทางกฎหมาย

ในกรอบสหประชาชาติ ไทยเข้าร่วมกระบวนการ OEWG มาอย่างต่อเนื่องและร่วมรับรองการจัดตั้งกลไกถาวรด้านความมั่นคงไซเบอร์เมื่อเดือนกรกฎาคม พ.ศ. 2568 การมีกลไกถาวรเป็นครั้งแรกหมายความว่า การหารือเรื่องบรรทัดฐาน กฎหมายระหว่างประเทศ และการเสริมสร้างศักยภาพจะดำเนินไปอย่างต่อเนื่องแทนที่จะเป็นการประชุมเฉพาะกิจเป็นรอบ ๆ ซึ่งเปิดโอกาสให้รัฐขนาดกลางที่มีทรัพยากรจำกัด สามารถวางแผนการมีส่วนร่วมได้อย่างเป็นระบบมากขึ้น

นอกจากกรอบด้านความมั่นคง ประชาคมระหว่างประเทศยังได้จัดทำอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention against Cybercrime: UNCC) ซึ่งรับรองเมื่อเดือนธันวาคม พ.ศ. 2567 อนุสัญญานี้วางกลไกความร่วมมือระหว่างประเทศในการสืบสวนสอบสวนและการส่งผู้ร้ายข้ามแดน ซึ่งมีความสำคัญอย่างยิ่งต่อไทยเนื่องจากอาชญากรรมไซเบอร์ที่กระทบไทยส่วนใหญ่มีลักษณะข้ามพรมแดน⁷²

กรอบความร่วมมือเฉพาะประเด็นเป็นอีกช่องทางที่ให้ผลเป็นรูปธรรมและรวดเร็วกว่ากรอบสากล ตัวอย่างที่สำคัญได้แก่ ความริเริ่มต่อต้านมัลแวร์เรียกค่าไถ่ (Counter Ransomware Initiative) ซึ่งเน้นการแลกเปลี่ยนข้อมูลและการปฏิบัติการร่วมของประเทศสมาชิก และกระบวนการ Pall Mall Process ซึ่งมุ่งจัดการปัญหาการแพร่ขยายของขีดความสามารถเจาะระบบเชิงพาณิชย์ รวมถึงซอฟต์แวร์สอดแนมที่อาจถูกใช้ต่อบุคคลในประเทศต่าง ๆ⁷³ กรอบเหล่านี้มีข้อดี คือ ไทยสามารถเข้าร่วมได้โดยไม่ต้องผูกมัดกับการแบ่งขั้วทางภูมิรัฐศาสตร์

ในระดับทวิภาคี ความร่วมมือที่เด่นชัดที่สุดของไทยในระยะหลัง คือ ความร่วมมือกับจีนในการปราบปรามศูนย์ฉ้อโกงตามแนวชายแดน ซึ่งนำไปสู่การจัดตั้งศูนย์ประสานงานร่วมและการปฏิบัติการช่วยเหลือเหยื่อจำนวนมาก อย่างไรก็ตาม นักวิชาการตั้งข้อสังเกตว่าการพึ่งพารูปแบบทวิภาคีกับมหาอำนาจมีความเสี่ยง เพราะในการปฏิบัติการร่วมที่ผ่านมา จีนได้อำนาจในการเก็บรวบรวมและจัดการข้อมูลที่ยึดได้ รวมถึงนำผู้ต้องสงสัยกลับไปดำเนินคดีในประเทศตน ขณะที่ไทยและประเทศอื่นมีบทบาทรองและเข้าถึงข้อมูลข่าวกรองได้จำกัด⁷⁴ ยิ่งไปกว่านั้น แรงจูงใจของจีนในการเข้าร่วมขึ้นอยู่กับแรงกดดันภายในประเทศของจีนเอง ซึ่งอาจเปลี่ยนแปลงได้ตลอดเวลา

⁷² United Nations, United Nations Convention against Cybercrime, adopted December 24, [Online], 2024, Available from: <https://www.unodc.org/unodc/en/cybercrime/convention/> [2026, August 12].

⁷³ Foreign, Commonwealth & Development Office, The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities, [Online], 2024, Available from: <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/> [2026, August 12].

⁷⁴ Surachanee "Hammerli" Sriyai, *supra* note 43, pp. 7-8.

ข้อจำกัดสำคัญของความร่วมมือในปัจจุบันจึงมีสองประการ ประการแรก คือ กลไกระดับภูมิภาคยังขาดสภาพบังคับ ทำให้การดำเนินคดีข้ามพรมแดนล่าช้า และการสืบสวนร่วมเกิดขึ้นไม่บ่อยนัก ประการที่สอง คือ การตอบสนองของรัฐในภูมิภาคมักถูกกำหนดโดยผลประโยชน์ของชนชั้นนำและความสะดวกทางการทูตมากกว่าหลักการ ซึ่งทำให้เครือข่ายอาชญากรรมสามารถปรับตัวได้เร็วกว่าการตอบสนองของรัฐเสมอ การแก้ไขปัญหานี้จึงต้องอาศัยการยกระดับความร่วมมือไปสู่กรอบพหุภาคีที่มีความต่อเนื่องและมีสภาพบังคับมากขึ้น

2.3 สรุปผลการศึกษา

การนำกรอบแนวคิดในหัวข้อ 2.2.1.3 มาวิเคราะห์ผลการดำเนินงานตามนโยบายและแผนฉบับปัจจุบัน แนวปฏิบัติที่ดีของต่างประเทศ และสภาพความร่วมมือระหว่างประเทศ นำไปสู่ข้อสรุปหลักหกประการสำหรับการจัดทำนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2571-2575) ดังนี้

ข้อสรุปประการแรก คือ ประเทศไทยยังขาดกรอบการมองปัญหาที่เชื่อมโยงเหตุการณ์ทางไซเบอร์เข้ากับวัตถุประสงค์เชิงยุทธศาสตร์ของตัวแสดง เมื่อพิจารณาผ่านกรอบการจำแนกวัตถุประสงค์วัตถุประสงค์สี่ประการ จะพบว่าระบบรายงานของไทยไม่สามารถบอกได้ว่าเหตุการณ์ใดเป็นการส่งสัญญาณ เหตุการณ์ใดเป็นการกำหนดทิศทางการดำเนินการ และเหตุการณ์ใดเป็นการวางฐานเข้าถึงระบบไว้ล่วงหน้า ผลคือไทยไม่อาจแยกแยะระหว่างเหตุการณ์ที่เป็นอาชญากรรมทั่วไปกับเหตุการณ์ที่มีนัยต่อความมั่นคงแห่งชาติได้อย่างมีระบบ

ข้อสรุปประการที่สอง คือ ไทยลงทุนกับการป้องกันภัยด้วยการปฏิเสธความสำเร็จเกือบทั้งหมด และแทบไม่มีเครื่องมือสำหรับการป้องกันภัยด้วยการลงโทษเลย ไทยไม่เคยกล่าวโทษรัฐใดต่อสาธารณะในกรณีการโจมตีทางไซเบอร์ ไม่มีกรอบมาตรการคว่ำบาตรที่พร้อมใช้ และไม่มีกระบวนการตัดสินใจที่ชัดเจนว่าใครมีอำนาจตัดสินใจกล่าวโทษและเมื่อใด การขาดเครื่องมือชุดนี้ทำให้การป้องกันภัยของไทยขาดความน่าเชื่อถือในสายตาของตัวแสดงที่มีขีดความสามารถสูง

ข้อสรุปประการที่สาม คือ ชุดเครื่องมือเชิงนโยบายของไทยยังไม่ถูกจัดวางไว้อย่างเป็นระบบ เครื่องมือที่ไทยมีอยู่กระจุกกระจายอยู่ตามหน่วยงานต่าง ๆ โดยไม่มีกลไกกลางที่ประมวลสถานการณ์และเสนอทางเลือกให้ผู้ตัดสินใจ เมื่อเปรียบเทียบกับเนเธอร์แลนด์ที่ระบุชุดเครื่องมือไว้อย่างชัดเจน ในยุทธศาสตร์ไซเบอร์ระหว่างประเทศ ช่องว่างนี้ปรากฏเด่นชัด ผลในทางปฏิบัติ คือ หากเกิดเหตุการณ์ทางไซเบอร์ที่มีนัยทางการเมืองระหว่างประเทศขึ้นในวันนี้ ไทยจะต้องใช้เวลาในการตัดสินใจนาน เกินกว่าที่สถานการณ์เอื้ออำนวย

ข้อสรุปประการที่สี่ คือ ไทยยังไม่ได้ใช้ประโยชน์จากสถานะรัฐขนาดกลางอย่างเต็มที่ ไทยมีสินทรัพย์เชิงยุทธศาสตร์ที่ประเทศอื่นในภูมิภาคไม่มี ได้แก่ ที่ตั้งของศูนย์ AICCBC ในกรุงเทพมหานคร

ความสัมพันธ์ที่สมดุลกับทั้งสหรัฐฯ และจีน และบทบาทที่ยอมรับได้ในเวทีอาเซียน แต่ไทยยังไม่ได้แปลงสินทรัพย์เหล่านี้ให้เป็นอิทธิพลในการกำหนดบรรทัดฐานระหว่างประเทศ การรวมกลุ่มกับประเทศที่มีแนวคิดใกล้เคียงกันเพื่อเพิ่มอำนาจต่อรองร่วม จึงเป็นแนวทางที่ไทยควรดำเนินการอย่างจริงจังในห้วงต่อไป

ข้อสรุปประการที่ห้า คือ แนวปฏิบัติที่ดีของต่างประเทศชี้ตรงกันว่า การแบ่งบทบาทที่ชัดเจนพร้อมกลไกกำกับดูแลเป็นเงื่อนไขของความสำเร็จ ทั้งกรณี NCSC และ NCF ของสหราชอาณาจักร และกรณีกฎหมายป้องกันไซเบอร์เชิงรุกของญี่ปุ่น ล้วนแสดงว่าการเพิ่มขีดความสามารถเชิงรุกต้อง มาพร้อมกับความโปร่งใสและความรับผิดชอบ สำหรับไทยซึ่งมีประวัติการถกเถียงเรื่องอำนาจรัฐ กับสิทธิเสรีภาพ การออกแบบกลไกกำกับดูแลจึงมิใช่เพียงเรื่องของหลักการ แต่เป็นเงื่อนไขทางการเมืองที่ขาดไม่ได้ของการดำเนินนโยบายเชิงรุก

ข้อสรุปประการที่หก คือ ความร่วมมือระหว่างประเทศที่ไทยมีอยู่ยังพึ่งพารูปแบบทวิภาคีกับมหาอำนาจมากเกินไป และยังไม่ได้ผูกโยงเข้ากับกระบวนการพหุภาคีที่ไทยเข้าร่วมอยู่แล้ว การยกระดับความร่วมมือไปสู่กรอบพหุภาคีที่มีความต่อเนื่อง ทั้งในกรอบอาเซียน กรอบสหประชาชาติ และกรอบเฉพาะประเด็น จะช่วยลดความเสี่ยงจากความไม่แน่นอนของนโยบายมหาอำนาจ และเสริมความเป็นกลางเชิงยุทธศาสตร์ของไทยไปพร้อมกัน

ตัวอย่างกลไกความร่วมมือที่ไทยควรเพิ่มบทบาทมีดังนี้ ในกรอบอาเซียน กลไกสำคัญประกอบด้วย การประชุมระดับรัฐมนตรีด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียน (ASEAN Ministerial Conference on Cybersecurity: AMCC) และคณะกรรมการประสานงานด้านไซเบอร์ของอาเซียน (ASEAN Cybersecurity Coordinating Committee) ซึ่งเป็นเวทีกำหนดทิศทางเชิงนโยบาย ศูนย์ประสานงานทีมเผชิญเหตุระดับภูมิภาค (ASEAN Regional CERT) ที่จัดตั้งขึ้นโดยมีสิงคโปร์เป็นเจ้าภาพ การฝึกซ้อมรับมือเหตุร่วมของทีมเผชิญเหตุอาเซียน (ASEAN CERT Incident Drill: ACID) คณะทำงานผู้เชี่ยวชาญด้านความมั่นคงไซเบอร์ภายใต้กรอบการประชุมรัฐมนตรีกลาโหมอาเซียนกับประเทศคู่เจรจา (ADMM-Plus) และศูนย์ AJCCBC ในกรุงเทพมหานคร แนวทางการดำเนินการโดยสังเขป คือ ไทยควรจัดตั้งคณะกรรมการหรือคณะทำงานเพื่อให้ท่าทีของไทยมีความต่อเนื่องในแต่ละกลไก เนื่องจากปัจจุบันยังมีหน่วยงานที่รับผิดชอบเข้าร่วมที่แตกต่างกัน และอาจมีแนวนโยบายหรือจุดยืนในประเด็นความมั่นคงไซเบอร์ที่แตกต่างกัน และพยายามผลักดันให้ไทยมีบทบาทนำในการเสนอหลักสูตรและวิทยากรเข้าสู่แผนเสริมสร้างศักยภาพของภูมิภาคผ่านศูนย์ AJCCBC และเสนอตัวเป็นเจ้าภาพจัดการฝึกซ้อมรับมือเหตุร่วมโดยเพิ่มโจทย์ที่ไทยมีผลประโยชน์โดยตรง

ในกรอบสหประชาชาติ กลไกสำคัญประกอบด้วยกลไกถาวรด้านความมั่นคงไซเบอร์ที่จัดตั้งขึ้น โดยไทยควรสนับสนุนการนำทะเบียนจุดติดต่อระดับโลกมาปฏิบัติใช้จริงพร้อมชักชวน การใช้ช่องทาง

ดังกล่าวเป็นประจำ รายงานความคืบหน้าการปฏิบัติตามบรรทัดฐานอย่างสม่ำเสมอเพื่อสร้างความน่าเชื่อถือของประเทศ และผลักดันให้วาระการเสริมสร้างศักยภาพของประเทศกำลังพัฒนามีงบประมาณและกลไกติดตามผลรองรับอย่างเป็นรูปธรรม

ในกรอบเฉพาะประเด็น กลไกสำคัญประกอบด้วยความร่วมมือต่อต้านมัลแวร์เรียกค่าไถ่ (Counter Ransomware Initiative: CRI) กระบวนการ Pall Mall Process ว่าด้วยการกำกับการแพร่กระจายและการใช้เครื่องมือเจาะระบบเชิงพาณิชย์ เวทีความร่วมมือของทีมเผชิญเหตุระดับโลก (Forum of Incident Response and Security Teams: FIRST) กลไกความร่วมมือของตำรวจสากลในภูมิภาคเอเชียตะวันออกเฉียงใต้ แนวทางการดำเนินการโดยสังเขป คือ ไทยควรเข้าร่วมความร่วมมือต่อต้านมัลแวร์เรียกค่าไถ่และรับหลักปฏิบัติร่วมมาปรับใช้กับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ เข้าร่วมกระบวนการ Pall Mall Process เพื่อวางกรอบการจัดหาและการใช้เครื่องมือเจาะระบบของหน่วยงานรัฐให้ตรวจสอบได้และมีความรับผิดชอบ ใช้เครือข่ายทีมเผชิญเหตุระดับโลกเป็นช่องทางแลกเปลี่ยนตัวบ่งชี้ภัยและขอความช่วยเหลือทางเทคนิคในกรณีเร่งด่วน และใช้กลไกความร่วมมือด้านการบังคับใช้กฎหมายเพื่อปฏิบัติการร่วมต่อกลุ่มอาชญากรรมไซเบอร์ ทั้งนี้ ข้อเสนอทั้งหมดประการนี้พร้อมกลไกที่กล่าวมาจะเป็นฐานของข้อเสนอในบทที่ 3 ต่อไป

บทที่ 3

ข้อเสนอ

3.1 ข้อเสนอเชิงนโยบาย

3.1.1 ประเด็นที่ควรมุ่งเน้นในห้วง พ.ศ. 2571-2575

ข้อเสนอเชิงนโยบายในรายงานฉบับนี้ตั้งอยู่บนหลักการสำคัญคือไทยต้องเพิ่มกรอบการมองภัยคุกคามทางไซเบอร์จากปัญหาเชิงเทคนิคไปสู่ปัญหาเชิงการเมืองและยุทธศาสตร์ การเพิ่มกรอบนี้มีได้หมายความว่าไทยจะลดความสำคัญของงานเชิงเทคนิคลง ตรงกันข้ามงานเชิงเทคนิคยังคงเป็นรากฐานที่ขาดไม่ได้ แต่หมายความว่าไทยต้องเพิ่มขั้นการวิเคราะห์และขั้นตอนการตัดสินใจเชิงยุทธศาสตร์เข้าไปเหนืองานเชิงเทคนิคที่มีอยู่ เพื่อให้ข้อมูลที่หน่วยงานปฏิบัติเก็บรวบรวมไว้แล้วสามารถแปลงเป็นการตัดสินใจเชิงนโยบายได้ ข้อเสนอต่อไปนี้จะเรียงลำดับจากการพัฒนาขีดความสามารถภายในประเทศซึ่งเป็นรากฐานที่ต้องมีก่อน ได้แก่ กำลังคนและอุตสาหกรรม และการคุ้มครองโครงสร้างพื้นฐานสำคัญ แล้วจึงต่อยอดไปสู่การวิเคราะห์และการตัดสินใจเชิงยุทธศาสตร์ การใช้เครื่องมือเชิงนโยบาย การสร้างความไว้วางใจของสาธารณะ และปิดท้ายด้วยการเตรียมรับมือเทคโนโลยีอุบัติใหม่ซึ่งเป็นการกิจระยะยาวที่ต้องเริ่มวางรากฐานตั้งแต่ห้วงแผนนี้ ทั้งนี้ ข้อเสนอทั้งหมดยึดเป้าหมายคือ ในห้วง พ.ศ. 2571-2575 ไทยต้องพึ่งพาตนเองในการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ให้ได้มากที่สุด

ประเด็นแรกที่ควรมุ่งเน้น คือ การพัฒนากำลังคนและอุตสาหกรรมด้านความมั่นคงทางไซเบอร์ภายในประเทศ ไทยควรเร่งผลิตและยกระดับทักษะบุคลากรวิชาชีพอย่างเป็นระบบ ตั้งแต่ระดับการศึกษา การฝึกอบรม การรับรองมาตรฐานวิชาชีพ ไปจนถึงการดึงดูดและรักษามูลค่าไว้ในภาครัฐควบคู่กันไป ไทยควรใช้กลไกการจัดซื้อจัดจ้างภาครัฐเป็นเครื่องมือสร้างอุปสงค์ให้แก่ผลิตภัณฑ์และบริการที่พัฒนาในประเทศ เพื่อลดการพึ่งพาเทคโนโลยีและผู้ให้บริการจากต่างชาติ ในภารกิจที่อ่อนไหวต่อความมั่นคง เหตุผลเชิงยุทธศาสตร์ คือ ขีดความสามารถที่ควบคุมได้ภายในประเทศย่อมเชื่อถือได้และยืดหยุ่นกว่าในยามที่เกิดความตึงเครียดระหว่างประเทศ ตัวอย่างรูปธรรม คือ ผลสำรวจกำลังคนของ ISC2 ที่ชี้ว่า ความต้องการบุคลากรวิชาชีพยังสูงกว่ากำลังคนที่มีอยู่มาก การใช้ศูนย์ AICCBC ในกรุงเทพมหานคร เป็นฐานฝึกอบรมบุคลากรทั้งของไทยและอาเซียน และการกำหนดเงื่อนไขในสัญญาจัดซื้อจัดจ้างภาครัฐให้มีการถ่ายทอดเทคโนโลยีแก่ผู้ประกอบการไทย นอกจากการผลิตบุคลากรวิชาชีพแล้ว ไทยควรกำหนดให้ความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่ง

ของหลักสูตรการศึกษาขั้นพื้นฐาน ควบคู่กับการรณรงค์สร้างความตระหนักรู้ระดับชาติอย่างต่อเนื่อง เหตุผลเชิงยุทธศาสตร์ คือ ประชาชนที่รู้เท่าทันภัยเป็นทั้งแนวป้องกันและเป็นฐานกำลังคนที่ทำให้ไทย สังคมขีดความสามารถด้านไซเบอร์ของชาติได้ด้วยตนเองในระยะยาว

ประเด็นที่สอง คือ การยกระดับการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการสร้างภูมิคุ้มกัน ไทยควรผลักดันให้หน่วยงาน CII ปฏิบัติตามหน้าที่ตามกฎหมายอย่าง ครบถ้วน ทั้งการจัดทำแผนพร้อมรับมือ การมีเจ้าหน้าที่เผชิญเหตุ และการรายงานเหตุตามกรอบเวลา ควบคู่กับการจัดตั้งทีมเผชิญเหตุรายสาขาในภาคการเงิน สาธารณสุข และพลังงาน นอกจากนี้ ไทย ควรกำหนดและทดสอบเป้าหมายระยะเวลาการฟื้นคืนบริการสำคัญ และจัดการฝึกซ้อมรับมือเหตุ ระดับชาติที่ครอบคลุมทั้งระดับนโยบายและระดับปฏิบัติการเป็นประจำ เพื่อให้ผู้เกี่ยวข้องคุ้นเคยกับ บทบาทของตนก่อนเกิดเหตุจริง ตัวอย่างรูปธรรมคือ แผนแม่บทความมั่นคงปลอดภัยไซเบอร์สำหรับ ระบบเทคโนโลยีเชิงปฏิบัติการ (OT Masterplan) ของสิงคโปร์ และบทเรียนจากการโจมตีระบบ ไฟฟ้าของยูเครนใน พ.ศ. 2558-2559 ที่ชี้ว่า ความสามารถในการสลับไปใช้การควบคุมด้วยมือและ กู้คืนบริการภายในเวลาที่กำหนด มีความสำคัญไม่น้อยกว่าการป้องกันการบุกรุก

ประเด็นที่สาม คือ การยกระดับการประเมินภัยคุกคามทางไซเบอร์ให้เป็น การประเมินเชิงยุทธศาสตร์ ไทยควรจัดทำรายงานการประเมินภัยคุกคามทางไซเบอร์ระดับชาติเป็น ประจำทุกปีโดยจำแนกภัยตามตัวแสดงและเจตนา มิใช่ตามรูปแบบทางเทคนิคเพียงอย่างเดียว รายงานดังกล่าวควรระบุว่า ไทยกำลังเผชิญกับตัวแสดงประเภทใด ตัวแสดงเหล่านั้นมุ่งหมายสิ่งใด ภาคส่วนใดของไทยตกเป็นเป้าหมายเชิงยุทธศาสตร์ และแนวโน้มในระยะห้าปีข้างหน้าเป็นอย่างไร แนวทางการเขียนควรนำมาตรฐานการวิเคราะห์ข่าวกรองมาปรับใช้ โดยแสดงระดับความน่าจะเป็น เชิงประมาณการ และระบุฐานการประเมินกำกับไว้ในแต่ละข้อ เพื่อให้ผู้กำหนดนโยบายทราบทั้ง ข้อสรุปและระดับความเชื่อมั่นของข้อสรุปนั้น ตัวอย่างรูปธรรม คือ รายงานประเมินภัยคุกคามไซเบอร์ แห่งชาติของแคนาดาและรายงานประจำปีของ NCSC สหราชอาณาจักร ซึ่งระบุรัฐที่อยู่เบื้องหลังและ เจตนาไว้อย่างเปิดเผย^{75 76} ต่างจากรายงานของไทยที่ยังนำเสนอเพียงจำนวนครั้งและประเภท เหตุการณ์

ประเด็นที่สี่ คือ การพัฒนาขีดความสามารถในการระบุตัวต้นผู้กระทำทาง ไซเบอร์ (cyber attribution) ทั้งเชิงเทคนิคและเชิงนโยบาย ในเชิงเทคนิคไทยควรลงทุนในขีด ความสามารถด้านนิติวิทยาศาสตร์ดิจิทัล และการวิเคราะห์ข่าวกรองภัยคุกคามให้อยู่ในระดับที่ผลการ วิเคราะห์เป็นที่ยอมรับในเวทีระหว่างประเทศ ในเชิงนโยบายไทยควรกำหนดกระบวนการตัดสินใจให้

⁷⁵ Canadian Centre for Cyber Security, *supra* note 41.

⁷⁶ National Cyber Security Centre, *supra* note 42.

ชัดเจนว่าหน่วยงานใดเป็นผู้เสนอ หน่วยงานใดเป็นผู้กลั่นกรอง และผู้ใดมีอำนาจตัดสินใจว่าจะกล่าวโทษหรือไม่ เมื่อใด และด้วยถ้อยคำอย่างไร การมีกระบวนการที่ชัดเจนล่วงหน้าจะทำให้ไทยตอบสนองได้ทันการณ์เมื่อเกิดเหตุจริงแทนที่จะต้องเริ่มถกเถียงกันในภาวะวิกฤต ตัวอย่างเช่น การที่ CISA และหน่วยงานพันธมิตรออกประกาศเตือนภัยร่วมกรณี Volt Typhoon โดยระบุรัฐที่หนุนหลัง และเจตนาการวางแผนเข้าถึงล่วงหน้า หรือการติดตามเส้นทางสินทรัพย์ดิจิทัลจนระบุกลุ่ม Lazarus ในเหตุโจรกรรมของ ByBit ซึ่งอาศัยทั้งนิติวิทยาศาสตร์ดิจิทัลและการตัดสินใจทางการเมืองประกอบกัน

ประเด็นที่ห้า คือ การจัดทำชุดเครื่องมือเชิงนโยบายที่พร้อมใช้ ไทยควรจัดทำกรอบมาตรการตอบสนองที่ครอบคลุมตั้งแต่มาตรการระดับต่ำ เช่น การเรียกเอกอัครราชทูตเข้าพบเพื่อชี้แจง การหยิบยกประเด็นในกรอบทวิภาคี และการออกแถลงการณ์แสดงความกังวล ไปจนถึงมาตรการระดับสูง เช่น การกล่าวโทษสาธารณะ การประสานท่าที่ร่วมกับประเทศที่มีจุดยืนใกล้เคียง การใช้กระบวนการยุติธรรม และการพิจารณามาตรการจำกัดทางเศรษฐกิจ กรอบดังกล่าวควรระบุเงื่อนไขการใช้แต่ละมาตรการและผลกระทบที่คาดว่าจะเกิดขึ้น เพื่อให้ผู้ตัดสินใจเลือกใช้ได้อย่างได้สัดส่วนโดยไม่ยกระดับความขัดแย้งเกินความจำเป็น ตัวอย่างรูปธรรมของมาตรการระดับสูง คือ การที่สหภาพยุโรปประกาศมาตรการจำกัดต่อบุคคลและหน่วยงานที่อยู่เบื้องหลังการโจมตีไซเบอร์เป็นครั้งแรกใน พ.ศ. 2563 ส่วนมาตรการระดับต่ำอาจใช้เพียงการเรียกทูตเข้าพบหรือการออกแถลงการณ์ร่วมกับประเทศที่มีจุดยืนใกล้เคียง เมื่อเกิดเหตุโจมตีโรงพยาบาลหรือระบบการเงิน ของไทย

ประเด็นที่หก คือ การสร้างกลไกบูรณาการข้ามหน่วยงานที่ใช้การได้จริง ไทยควรจัดตั้งกลไกกลางที่รวบรวมและประมวลข้อมูลภัยคุกคามจากหน่วยงานด้านเทคนิค ข่าวกกรอง การทูต การป้องกันประเทศ และการบังคับใช้กฎหมาย เพื่อสร้างภาพสถานการณ์ร่วมที่ครบถ้วน กลไกนี้ควรมีสองระดับ ระดับปฏิบัติการทำหน้าที่แลกเปลี่ยนตัวบ่งชี้ภัยแบบเกือบทันที และระดับนโยบายทำหน้าที่ประเมินภัยเชิงยุทธศาสตร์และเสนอทางเลือกต่อผู้ตัดสินใจ เหตุผลสำคัญ คือ ตัวบ่งชี้ภัยที่หน่วยงานหนึ่งตรวจพบมักเป็นสัญญาณเตือนล่วงหน้าให้หน่วยงานอื่น การส่งต่อข้อมูลที่ล่าช้าจึงเท่ากับการสูญเสียโอกาสในการป้องกัน ตัวอย่างที่ไทยศึกษาได้ คือ การแบ่งบทบาทของสหราชอาณาจักร ระหว่าง NCSC ที่ทำหน้าที่ป้องกันอย่างเปิดเผย กับ NCF ที่ปฏิบัติการเชิงรุกอย่างเป็นความลับ และแบบจำลองของสิงคโปร์ที่ให้ CSA เป็นเจ้าภาพประสานทุกภาคส่วนภายใต้กฎหมายฉบับเดียว นอกจากนี้ กลไกกลางดังกล่าวควรเปิดช่องทางรับข้อมูลและความเห็นจากผู้มีส่วนได้ส่วนเสียนอกภาครัฐอย่างเป็นระบบ ทั้งภาคเอกชน สถาบันการศึกษา ภาคประชาสังคม และประชาชน ผู้ใช้บริการ ตลอดจนเชื่อมต่อกับทีมเผชิญเหตุของประเทศเพื่อนบ้านและกลไกของอาเซียน เนื่องจากเหตุการณ์จำนวนมากถูกตรวจพบโดยผู้ใช้งานหรือผู้ให้บริการก่อนที่จะหน่วยงานของรัฐจะทราบ

ประเด็นที่เจ็ด คือ การฟื้นฟูความไว้วางใจของสาธารณะ และการเสริมสร้างธรรมาภิบาล ไทยควรกำหนดให้หน่วยงานของรัฐต้องผ่านการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์เป็น

ประจำ พร้อมเปิดเผยผลการตรวจสอบในระดับที่เหมาะสมต่อสาธารณะ และควรบังคับใช้มาตรการต่อหน่วยงานภาครัฐที่ทำข้อมูลรั่วไหลด้วยมาตรฐานเดียวกับที่ใช้กับภาคเอกชน เหตุผลสำคัญ คือ ประชาชนจะสนับสนุนการดำเนินนโยบายเชิงรุกในอนาคตก็ต่อเมื่อเชื่อมั่นว่ารัฐมีความรับผิดชอบต่อข้อมูลของตนเสียก่อน ตัวอย่างรูปธรรม คือ การกำหนดให้หน่วยงานรัฐที่ทำข้อมูลประชาชนรั่วไหลต้องเปิดเผยเหตุและรับผิดชอบตามมาตรฐานเดียวกับที่บังคับใช้กับบริษัทเอกชนภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ การฟื้นฟูความไว้วางใจต้องครอบคลุมความสัมพันธ์กับภาคเอกชนด้วย โดยรัฐควรปฏิบัติต่อบริษัทที่รายงานเหตุหรือแจ้งช่องโหว่โดยสุจริตในฐานะหุ้นส่วน มิใช่ผู้ถูกจับผิด และควรขยายเวทีแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างรัฐกับเอกชนรายสาขา เช่น ศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคาร (TB-CERT) ให้ครอบคลุมสาขาสาธารณสุข พลังงาน และโทรคมนาคม ในมิติภาคประชาชน ไทยควรลงทุนสร้างความตระหนักรู้และทักษะดิจิทัลของประชาชนอย่างต่อเนื่อง จัดให้มีช่องทางแจ้งเหตุและขอความช่วยเหลือที่เข้าถึงง่ายและตอบสนองรวดเร็ว รวมทั้งเปิดให้ภาคประชาสังคมและสื่อมวลชนมีส่วนร่วมตรวจสอบการใช้อำนาจของรัฐในพื้นที่ไซเบอร์

ประเด็นที่แปด คือ การเตรียมรับมือภัยจากปัญญาประดิษฐ์และเทคโนโลยีควอนตัม อย่างเป็นระบบ ในด้านปัญญาประดิษฐ์ ไทยควรลงทุนในระบบตรวจจับที่ใช้ปัญญาประดิษฐ์เพื่อรับมือกับการโจมตีที่มีความเร็วสูงขึ้น พร้อมกำหนดแนวปฏิบัติสำหรับการใช้ปัญญาประดิษฐ์ในหน่วยงาน ความมั่นคงอย่างมีความรับผิดชอบ ในด้านควอนตัม ไทยควรเริ่มจัดทำบัญชีระบบเข้ารหัสที่ใช้อยู่ในหน่วยงานของรัฐและหน่วยงาน CII และวางแผนการเปลี่ยนผ่านไปสู่วิทยาการรหัสที่ต้านทานควอนตัมภายในห้วงนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับใหม่ โดยจัดลำดับความสำคัญจากระบบที่เก็บข้อมูลซึ่งต้องรักษาความลับเป็นเวลานานก่อน เนื่องจากข้อมูลกลุ่มนี้มีความเสี่ยงสูงสุดจากการลักลอบเก็บไว้ถอดรหัสภายหลัง ตัวอย่างรูปธรรม คือ การเริ่มจัดทำบัญชีระบบเข้ารหัสของฐานข้อมูลทะเบียนราษฎรและข้อมูลสุขภาพ ซึ่งต้องรักษาความลับต่อเนื่องหลายสิบปีเป็นลำดับแรก ทั้งนี้ ชี้ความสามารถด้านปัญญาประดิษฐ์และวิทยาการรหัสส่วนใหญ่อยู่ในมือของภาคเอกชน ไทยจึงควรใช้และไว้วางใจหน่วยงานนอกภาครัฐที่มีความเชี่ยวชาญและให้ความร่วมมือกับภาครัฐ เช่น ผู้ให้บริการคลาวด์ ผู้ให้บริการโทรคมนาคม สถาบันการเงิน และบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ โดยจัดให้มีกลไกแลกเปลี่ยนข้อมูลภัยคุกคามและการทดสอบเทคโนโลยีร่วมกันอย่างเป็นทางการ เช่นเดียวกับที่ NCSC สหราชอาณาจักรดำเนินโครงการเพิ่มขีดความสามารถในการป้องกันเชิงรุก (Active Cyber Defence) ร่วมกับผู้ให้บริการอินเทอร์เน็ตของเอกชน

3.1.2 ประเทศและกรอบความร่วมมือที่ไทยควรร่วมมือ

หลักการเลือกคู่ความร่วมมือของไทยควรตั้งอยู่บนสี่เกณฑ์ ได้แก่ ความสอดคล้องของผลประโยชน์กับลำดับความสำคัญด้านภัยคุกคามของไทย ความเป็นไปได้ที่จะได้รับประโยชน์

ตอบแทนอย่างเป็นรูปธรรม และการรักษาความเป็นกลางเชิงยุทธศาสตร์เพื่อมิให้ไทยถูกชักนำเข้าสู่การเผชิญหน้าระหว่างขั้วอำนาจโดยไม่จำเป็น เกณฑ์ทั้งสองนี้นำไปสู่ข้อเสนอความร่วมมือในกระบวนดังต่อไปนี้

ในกรอบอาเซียน ไทยควรแสดงบทบาทนำในสองเรื่องที่ไทยมีความได้เปรียบเรื่องแรกคือ การเสริมสร้างศักยภาพโดยใช้ประโยชน์จากศูนย์ AJCCBC ในกรุงเทพมหานครให้เต็มที่ ทั้งการขยายหลักสูตร การเพิ่มจำนวนผู้เข้ารับการฝึกอบรมจากประเทศสมาชิก และการพัฒนาหลักสูตรด้านนโยบายควบคู่กับหลักสูตรด้านเทคนิค เรื่องที่สองคือ การจัดการภัยคุกคามข้ามพรมแดนร่วมกับประเทศเพื่อนบ้าน ซึ่งมีความเชื่อมโยงกับไทยทั้งทางโครงข่ายโทรคมนาคมและขบวนการหลอกลวงออนไลน์ตามแนวชายแดน ไทยควรผลักดันให้มีช่องทางประสานงานระหว่างทีมเผชิญเหตุ (CERT) ของประเทศเพื่อนบ้านที่ติดต่อได้ตลอดเวลา การฝึกซ้อมรับมือเหตุร่วมและการแลกเปลี่ยนข้อมูลภัยคุกคามผ่านกลไกระดับภูมิภาคของอาเซียน รวมถึงศูนย์ประสานงานทีมเผชิญเหตุระดับภูมิภาค เพื่อให้การป้องกันของไทยไม่ถูกจำกัดอยู่เพียงภายในพรมแดนของตน

ในกรอบสหประชาชาติ ไทยควรใช้กลไกถาวรด้านความมั่นคงไซเบอร์ที่เพิ่งจัดตั้งขึ้นเป็นเวทีหลักในการผลักดันผลประโยชน์ของประเทศขนาดกลาง ประเด็นที่ไทยควรผลักดันเป็นพิเศษได้แก่ การเสริมสร้างศักยภาพที่เป็นรูปธรรมและมีงบประมาณรองรับ การขยายมาตรการสร้างความไว้วางใจ และการพัฒนาแนวทางปฏิบัติสำหรับการคุ้มครองโครงสร้างพื้นฐานสำคัญ

ในระดับประเทศที่มีแนวคิดใกล้เคียงกัน ไทยควรกระชับความร่วมมือกับสิงคโปร์ ญี่ปุ่น เกาหลีใต้ ออสเตรเลีย และสหภาพยุโรป ความร่วมมือกับสิงคโปร์ควรเน้นการแลกเปลี่ยนแนวปฏิบัติด้านการคุ้มครองโครงสร้างพื้นฐานสำคัญ และเทคโนโลยีเชิงปฏิบัติการ ความร่วมมือกับญี่ปุ่นควรเน้นการต่อยอดศูนย์ AJCCBC และการเรียนรู้กระบวนการออกแบบกลไกกำกับดูแลปฏิบัติการเชิงรุก ความร่วมมือกับออสเตรเลียควรเน้นการพัฒนาขีดความสามารถที่เป็นเอกเทศและการเสริมสร้างศักยภาพในภูมิภาค ส่วนความร่วมมือกับสหภาพยุโรปควรเน้นการเรียนรู้กลไกการกล่าวโทษและมาตรการจำกัดที่มีอยู่แล้ว รวมถึงกรอบการรายงานเหตุตามระเบียบคำสั่งว่าด้วยข้อกำหนดด้านความปลอดภัยทางไซเบอร์ฉบับใหม่ (Network and Information Systems: NIS2) ซึ่งมาแทนฉบับแรก (NIS1) โดยมีผลบังคับใช้ตั้งแต่ปลาย พ.ศ. 2567

ในระดับมหอำนาจ ไทยควรดำเนินความร่วมมือกับทั้งสหรัฐฯ และจีนบนพื้นฐานของผลประโยชน์ร่วมและความสมดุล ความร่วมมือกับสหรัฐฯ มีคุณค่าในด้านการแลกเปลี่ยนข่าวกรองภัยคุกคามและการฝึกอบรม ขณะที่ความร่วมมือกับจีนมีคุณค่าในด้านการปราบปรามอาชญากรรมข้ามชาติในอนุภูมิภาค อย่างไรก็ตาม ไทยควรผลักดันให้ความร่วมมือกับจีนในเรื่องศูนย์ฉ้อโกง โดยเปลี่ยนรูปแบบจากทวิภาคีไปสู่พหุภาคีภายใต้กรอบอาเซียนหรือ ACMECS เพื่อลด

ความเสี่ยงจากความไม่สมมาตรของอำนาจต่อรอง และเพื่อรักษาอำนาจอธิปไตยของไทยในการจัดการข้อมูลและกระบวนการยุติธรรม

ในระดับประเทศเพื่อนบ้าน ไทยควรมีบทบาทเชิงรุกในการเสริมสร้างศักยภาพให้แก่ลาว เมียนมา และเวียดนาม (กรณีกัมพูชาควรชะลอไว้จนกว่าสถานการณ์ความขัดแย้งจะคลี่คลาย) เหตุผลเชิงยุทธศาสตร์ คือ ความมั่นคงไซเบอร์ของไทยผูกโยงกับความมั่นคงของภูมิภาคอย่างแยกไม่ออก หากประเทศเพื่อนบ้านมีจุดอ่อนภัยคุกคามย่อมแพร่มาถึงไทยได้ง่าย การเสริมสร้างศักยภาพจึงมิใช่การให้ความช่วยเหลือฝ่ายเดียวหากเป็นการลงทุนในความมั่นคงของไทยเอง ทั้งนี้ ไทยควรดำเนินการอย่างระมัดระวังในกรณีที่หน่วยงานของประเทศเพื่อนบ้านอาจมีความเชื่อมโยงกับเครือข่ายอาชญากรรม ในกรอบความร่วมมือเฉพาะประเด็น ไทยควรเข้าร่วมและใช้ประโยชน์จากความริเริ่มต่อต้านมัลแวร์เรียกค่าไถ่และกระบวนการ Pall Mall Process อย่างจริงจัง เหตุผลสำคัญ คือ กรอบเหล่านี้ให้ผลเป็นรูปธรรมและรวดเร็วกว่ากรอบสากลที่ต้องอาศัยฉันทามติของทุกฝ่าย อีกทั้งยังช่วยให้ไทยมุ่งทรัพยากรไปยังภัยที่กระทบไทยโดยตรง ทั้งมัลแวร์เรียกค่าไถ่และการฉ้อโกงออนไลน์โดยไม่จำเป็นต้องผูกมัดกับการแบ่งขั้วทางภูมิรัฐศาสตร์

3.2 ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

3.2.1 แนวทางของนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฉบับต่อไปในประเด็นไซเบอร์

นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2571-2575) ควรปรับถ้อยคำของประเด็นไซเบอร์จาก "การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์" ไปสู่ "การรักษาและขับเคลื่อนผลประโยชน์แห่งชาติในมิติไซเบอร์" การปรับถ้อยคำนี้เป็นการส่งสัญญาณเชิงนโยบายว่า ไทยมองพื้นที่ไซเบอร์เป็นปริภูมิพลที่ต้องขับเคลื่อนผลประโยชน์เชิงรุก มิใช่เพียงพื้นที่ที่ต้องตั้งรับป้องกัน ภายใต้กรอบใหม่นี้แผนควรมุ่งเน้นการรักษาผลประโยชน์แห่งชาติในสี่มิติ ที่เกื้อหนุนซึ่งกันและกัน ดังจะได้เสนอต่อไปดังนี้

มิติที่หนึ่ง ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security หรือ Cybersecurity) มิติดังนี้มุ่งสนับสนุนการพัฒนาศักยภาพในทุกภาคส่วนตั้งแต่ระดับประชาชนจนถึงระดับผู้บริหารสูงสุดในระดับประชาชน นโยบายและแผนควรกำหนดเป้าหมายการสร้างความรู้ขั้นพื้นฐานให้ประชาชนสามารถป้องกันตนเองจากภัยทางไซเบอร์ได้ โดยให้ความสำคัญเป็นพิเศษกับกลุ่มเปราะบาง ทั้งผู้สูงอายุและประชากรในพื้นที่ที่เข้าถึงการศึกษาดิจิทัลได้จำกัด ซึ่งงานศึกษาพบว่าตกเป็นเหยื่อการฉ้อโกงในสัดส่วนที่สูงกว่ากลุ่มอื่น ในระดับวิชาชีพ นโยบายและแผนควรกำหนดเป้าหมายการผลิตและยกระดับทักษะบุคลากรให้เพียงพอต่อความต้องการของประเทศ พร้อมกลไกการรับรองมาตรฐานวิชาชีพที่เป็นที่ยอมรับ

ประเด็นที่นโยบายและแผนฉบับต่อไปต้องให้ความสำคัญเป็นพิเศษ คือ การปรับเปลี่ยนทัศนคติของผู้บริหารในภาครัฐ ภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ให้ตระหนักว่าภัยไซเบอร์เป็นภัยต่อความมั่นคงแห่งชาติ มิใช่เพียงปัญหาทางเทคนิคของฝ่ายเทคโนโลยีสารสนเทศ เหตุผลที่ประเด็นนี้สำคัญเป็นพิเศษ คือ การตัดสินใจลงทุนและการกำหนดนโยบายความปลอดภัยล้วนขึ้นอยู่กับผู้บริหารระดับสูงเป็นสำคัญ หากผู้บริหารยังมองว่าความมั่นคงไซเบอร์เป็นต้นทุนมากกว่าการลงทุนเชิงยุทธศาสตร์ มาตรการทางเทคนิคที่ดีที่สุดก็ไมอาจได้รับทรัพยากรที่เพียงพอ นโยบายและแผนจึงควรกำหนดกลไกที่เป็นรูปธรรม เช่น การจัดหลักสูตรสำหรับผู้บริหารระดับสูง และการกำหนดให้ความมั่นคงไซเบอร์เป็นวาระประจำของคณะกรรมการองค์กร

มิตินี้ยังมุ่งสร้างสภาพแวดล้อมและอุตสาหกรรมด้านความมั่นคงไซเบอร์ภายในประเทศให้เติบโตได้ เพื่อลดการพึ่งพาเทคโนโลยีและผู้ให้บริการจากต่างชาติในระยะยาว นโยบายและแผนควรกำหนดมาตรการสนับสนุนผู้ประกอบการในประเทศ การส่งเสริมการวิจัยและพัฒนา และการใช้กลไกการจัดซื้อจัดจ้างภาครัฐเป็นเครื่องมือสร้างอุปสงค์ ควบคู่กับการพัฒนากลไกประเมินความเชื่อถือได้ของผู้ให้บริการและผลิตภัณฑ์ และการจัดทำข้อกำหนดด้านความโปร่งใสของห่วงโซ่อุปทานซอฟต์แวร์สำหรับหน่วยงาน CII เนื่องจากบทเรียนจากกรณี SolarWinds แสดงให้เห็นว่าการเจาะผู้ให้บริการเพียงรายเดียวสามารถทำลายความไว้วางใจในเทคโนโลยีทั้งระบบได้ในคราวเดียว

มิติที่สอง การทูตไซเบอร์ (Cyber Diplomacy) มิตินี้มุ่งใช้เครื่องมือทางการทูตเพื่อส่งเสริมบรรทัดฐานการใช้พื้นที่ทางไซเบอร์อย่างมีความรับผิดชอบของรัฐตามกรอบสหประชาชาติ การทูตไซเบอร์เป็นช่องทางสำคัญที่ช่วยให้ไทยมีส่วนร่วมกำหนดกติการะหว่างประเทศ แทนที่จะเป็นเพียงผู้รับกติกาที่ถูกกำหนดโดยมหาอำนาจ นโยบายและแผนฉบับต่อไปจึงควรกำหนดให้กระทรวงการต่างประเทศเป็นหน่วยงานร่วมรับผิดชอบในประเด็นไซเบอร์อย่างเป็นทางการ พร้อมกำหนดกลไกประสานงานระหว่างกระทรวงการต่างประเทศกับ สมช. และ สกมช. ให้ชัดเจน

เครื่องมือทางการทูตยังอาจนำมาใช้เพื่อเจรจาหรือระงับข้อพิพาทเมื่อเกิดเหตุการณ์ทางไซเบอร์ที่เชื่อมโยงกับการเมืองระหว่างประเทศ ทั้งการหารือในกรอบทวิภาคีและพหุภาคี การเข้าร่วมมาตรการสร้างความไว้วางใจ และการประสานท่าทีร่วมกับประเทศที่มีจุดยืนใกล้เคียง การดำเนินการทั้งหมดต้องคำนึงถึงความเป็นกลางเชิงยุทธศาสตร์และผลประโยชน์ของไทยในระยะยาวเป็นสำคัญ เหตุผลคือ ไทยเป็นประเทศขนาดกลางที่ตั้งอยู่ในจุดตัดของการแข่งขันระหว่าง มหาอำนาจ การเลือกข้างโดยไม่จำเป็นย่อมลดพื้นที่ทางยุทธศาสตร์ของไทยลง ขณะที่การรักษาความสัมพันธ์ที่สมดุลจะทำให้ไทยเป็นตัวกลางที่ทุกฝ่ายยอมรับได้

นโยบายและแผนควรกำหนดผลลัพธ์ที่เป็นรูปธรรมของมิตินี้ คือ การผลักดันข้อเสนอของไทยให้ปรากฏในเอกสารผลลัพธ์ของการประชุมระหว่างประเทศ ผลลัพธ์เหล่านี้วัดได้และสะท้อนอิทธิพลของไทยในเวทีระหว่างประเทศได้อย่างแท้จริง

มิติที่สาม การป้องกันประเทศทางไซเบอร์ (Cyber Defence) มิติดินี้มุ่งพัฒนาขีดความสามารถในการป้องกันเชิงรุก (Active Cyber Defence) ที่สามารถสกัดกั้นภัยคุกคามก่อนเข้าถึงเป้าหมายสำคัญ แนวทางนี้จำเป็นเพราะการตั้งรับเชิงรับเพียงลำพังไม่อาจรับมือกับตัวแสดงที่มีทรัพยากรสูงและพยายามเจาะระบบอย่างต่อเนื่องได้ ดังที่ประสบการณ์ของญี่ปุ่นและสหราชอาณาจักรแสดงให้เห็น อย่างไรก็ตาม การป้องกันเชิงรุกสำหรับไทยควรเริ่มจากรูปแบบที่มีความเสี่ยงต่ำและให้ผลตอบแทนสูงก่อน เช่น การปิดกั้นชื่อโดเมนและเว็บไซต์ที่เป็นอันตรายในระดับชาติ การถอดถอนโครงสร้างพื้นฐานที่ผู้โจมตี ใช้ซึ่งตั้งอยู่ในดินแดนไทย และการแจ้งเตือนเชิงรุกไปยังหน่วยงานที่มีความเสี่ยง มากกว่าจะเริ่มจากปฏิบัติการนอกเขตอำนาจรัฐทันที

กระบวนการทั้งหมดในยามปกติต้องตั้งอยู่บนหลักความโปร่งใสและความรับผิดชอบ นโยบายและแผนควรกำหนดให้มีกรอบกฎหมายที่ชัดเจนสำหรับปฏิบัติการเชิงรุก พร้อมกลไกกำกับดูแลที่ตรวจสอบได้ ทั้งการอนุมัติก่อนปฏิบัติการ การบันทึกและรายงานผล และการตรวจสอบโดยองค์กรอิสระ เหตุผลที่ต้องเน้นการกำกับดูแล คือ ปฏิบัติการเชิงรุกที่ปราศจากกรอบกฎหมายและการตรวจสอบอาจสร้างความเสี่ยงต่อการยกระดับความขัดแย้งและบั่นทอนความน่าเชื่อถือของไทย ยิ่งไปกว่านั้นในบริบทการเมืองไทยที่มีประวัติการถกเถียงเรื่องอำนาจรัฐกับสิทธิเสรีภาพ กลไกกำกับดูแลที่รัดกุมเป็นเงื่อนไขทางการเมืองที่ขาดไม่ได้ของการได้รับการยอมรับจากสังคม

สิ่งสำคัญที่สุดของมิตินี้ คือ การบูรณาการการทำงานระหว่างหน่วยงานความมั่นคงฝ่ายทหารและฝ่ายพลเรือนอย่างชัดเจน นโยบายและแผนฉบับต่อไปควรกำหนดขอบเขตภารกิจของแต่ละฝ่ายให้ชัด โดยอาจใช้แบบอย่างของสหราชอาณาจักรที่แยกหน่วยงานฝ่ายป้องกันที่เปิดเผยออกจากหน่วยงานฝ่ายปฏิบัติการเชิงรุกที่เป็นความลับ เพื่อมิให้เกิดความซ้ำซ้อนของภารกิจและช่องว่างของความรับผิดชอบ ขณะเดียวกันนโยบายและแผนดังกล่าวควรกำหนดให้ในห้วงความขัดแย้งขีดความสามารถทางไซเบอร์ของกองทัพต้องสามารถสนับสนุนยุทธการทางทหาร เพื่อปกป้องอธิปไตยของชาติได้อย่างเต็มประสิทธิภาพ ซึ่งต้องอาศัยการฝึกซ้อมและการวางแผนร่วมอย่างสม่ำเสมอในยามปกติ

มิติที่สี่ การปราบปรามอาชญากรรมทางไซเบอร์ (Cyber Crime หรือ Cybercrime) มิติดินี้มุ่งสนับสนุนการบังคับใช้กฎหมายต่อการกระทำผิดทางไซเบอร์อย่างมีประสิทธิภาพ นโยบายและแผนฉบับต่อไปควรกำหนดเป้าหมายการยกระดับขีดความสามารถของหน่วยงานในกระบวนการยุติธรรมให้รู้เท่าทันอาชญากรรมทางเทคโนโลยีรูปแบบใหม่ ครอบคลุมทั้งพนักงานสอบสวน พนักงานอัยการ และผู้พิพากษา เหตุผลคืออาชญากรรมไซเบอร์ที่ซับซ้อนจำเป็นต้องอาศัยความเข้าใจ

เชิงเทคนิคในทุกขั้นตอนของกระบวนการยุติธรรม หากขั้นตอนใดขั้นตอนหนึ่งขาดความเข้าใจดี ย่อมมีความเสี่ยงที่จะไม่ประสบผลแม้จะมีพยานหลักฐานเพียงพอ

การพัฒนาและบังคับใช้มาตรฐานการพิสูจน์พยานหลักฐานทางดิจิทัลให้มีความน่าเชื่อถือและเป็นที่ยอมรับในชั้นศาล ถือเป็นเงื่อนไขสำคัญที่ทำให้การดำเนินคดีประสบผลนโยบายและแผนควรกำหนดให้มีการจัดทำมาตรฐานกลางด้านนิติวิทยาศาสตร์ดิจิทัล การรับรองห้องปฏิบัติการ และการรับรองความสามารถของผู้เชี่ยวชาญ มาตรฐานเหล่านี้ยังมีประโยชน์เพิ่มเติมในมิติระหว่างประเทศ เพราะทำให้พยานหลักฐานที่ไทยรวบรวมได้เป็นที่ยอมรับในกระบวนการความร่วมมือทางอาญาระหว่างประเทศ และทำให้ผลการวิเคราะห์ของไทยมีน้ำหนักมากขึ้นหากไทยตัดสินใจกล่าวโทษผู้กระทำการในอนาคต

เนื่องจากอาชญากรรมไซเบอร์มีลักษณะข้ามพรมแดน การยกระดับกลไกความร่วมมือระหว่างประเทศเพื่อนำตัวผู้กระทำความผิดมาดำเนินคดี จึงมีความจำเป็นอย่างยิ่ง นอกจากนี้ ควรกำหนดกลไกการทำงานร่วมระหว่างหน่วยงานบังคับใช้กฎหมาย หน่วยงานกำกับดูแลภาคการเงิน และหน่วยงานข่าวกรอง เพื่อติดตามและตัดกระแสเงินที่หล่อเลี้ยงเครือข่ายอาชญากรรม ซึ่งเป็นจุดอ่อนที่สุดของเครือข่ายเหล่านี้อีกด้วย

3.2.2 ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

กลไกขับเคลื่อนและตัวชี้วัดการขับเคลื่อนข้อเสนอทั้งสี่มิติให้เกิดผลจริง ต้องอาศัยกลไกที่ชัดเจนสองระดับ ระดับแรกคือ ระดับนโยบาย ควรใช้สภาความมั่นคงแห่งชาติ (สภา มช.) มีนายกรัฐมนตรีเป็นประธาน เป็นกลไกกำกับภาพรวม โดยมี สมช. ทำหน้าที่เป็นเจ้าภาพในมิติที่มีลักษณะข้ามหน่วยงาน โดยเฉพาะมิติการทูตไซเบอร์และมิติการป้องกันประเทศทางไซเบอร์ เหตุผลคือ สองมิตินี้ต้องอาศัยการประสานระหว่างกระทรวงการต่างประเทศ กระทรวงกลาโหม หน่วยข่าวกรอง และ สมช. ซึ่งไม่มีหน่วยงานใดหน่วยงานหนึ่งมีอำนาจสั่งการข้ามกันได้

ระดับที่สองคือ ระดับอำนวยการ ควรจัดตั้งคณะกรรมการหรือคณะทำงานร่วมที่มีผู้แทนจากหน่วยงานด้านเทคนิค ข่าวกรอง การทูต การป้องกันประเทศ และการบังคับใช้กฎหมาย ทำหน้าที่ประเมินสถานการณ์ร่วม จัดทำรายงานประเมินภัยคุกคามระดับชาติประจำปี และเสนอทางเลือกเชิงนโยบายต่อผู้ตัดสินใจ กลไกนี้เป็นหัวใจของข้อเสนอทั้งหมด เพราะเป็นจุดที่ข้อมูลเชิงเทคนิคถูกแปลงเป็นสารสนเทศเชิงยุทธศาสตร์ และเป็นจุดที่การทำงานแบบแยกส่วนจะถูกแก้ไข

ตัวชี้วัดของนโยบายและแผนฉบับต่อไป ควรปรับจากตัวชี้วัดเชิงปริมาณและเชิงเทคนิคไปสู่ตัวชี้วัดเชิงขีดความสามารถและเชิงผลลัพธ์ ตัวอย่างตัวชี้วัดที่ควรเพิ่ม ได้แก่ การมีรายงานประเมินภัยคุกคามระดับชาติที่จำแนกตามตัวแสดงและเจตนาเผยแพร่เป็นประจำทุกปี สัดส่วนของเหตุการณ์สำคัญที่สามารถระบุตัวต้นผู้กระทำได้ในระดับที่น่าไปใช้เชิงนโยบายได้ ระยะเวลาเฉลี่ยจากการตรวจพบเหตุถึงการตัดสินใจเชิงนโยบาย จำนวนกรอบมาตรการเชิงนโยบาย

ที่จัดทำไว้พร้อมใช้ จำนวนหน่วยงานที่เชื่อมต่อกับกลไกแบ่งปันข้อมูลภัยคุกคามกลาง การมีกรอบกฎหมายและกลไกกำกับดูแลปฏิบัติการเชิงรุกที่ชัดเจน และความคืบหน้าของการเปลี่ยนผ่านไปสู่วิทยาการรหัสที่ต้านทานควอนตัม

การจัดลำดับห้วงเวลาดำเนินการควรแบ่งเป็นสามช่วง ช่วงแรกในปีที่หนึ่งถึงปีที่สอง ควรมุ่งวางรากฐาน ได้แก่ การจัดตั้งกลไกอำนวยการร่วม การจัดทำรายงานประเมินภัยคุกคามระดับชาติฉบับแรก การจัดทำบัญชีระบบเข้ารหัสของหน่วยงานรัฐและหน่วยงาน CII และการยกเครื่องชุดเครื่องมือ เชนนโยบาย ช่วงที่สองในปีที่สามถึงปีที่สี่ควรมุ่งขยายผล ได้แก่ การจัดทำเอกสารแสดงท่าทีด้านกฎหมายระหว่างประเทศ การจัดตั้งทีมเผชิญเหตุรายสาขา การเริ่มเปลี่ยนผ่านวิทยาการรหัสในระบบที่มีความสำคัญสูงสุด และการยกระดับความร่วมมือในกรอบอาเซียน ช่วงที่สามในปีที่ห้าควรมุ่งประเมินผลและปรับปรุง พร้อมเตรียมการสำหรับนโยบายและแผนฉบับถัดไป

ปัจจัยแห่งความสำเร็จของข้อเสนอทั้งหมดมีสามประการ ประการแรก คือ เจตจำนงทางการเมืองในระดับผู้นำ เพราะการเปลี่ยนกรอบการมองปัญหาและการจัดตั้งกลไกข้ามหน่วยงาน ล้วนต้องอาศัยอำนาจ การตัดสินใจที่เหนือกว่าระดับกระทรวง ประการที่สอง คือ การจัดสรรงบประมาณและกำลังคนที่สอดคล้องกับภารกิจ เพราะข้อเสนอที่ไม่มีทรัพยากรรองรับย่อมไม่ต่างจากการประกาศเจตนารมณ์ และประการที่สาม คือ ความไว้วางใจของสาธารณะ ซึ่งเป็นทั้งเงื่อนไขและผลลัพธ์ของนโยบายที่ดี รัฐจะดำเนินนโยบายเชิงรุกได้ก็ต่อเมื่อประชาชนเชื่อมั่นว่ารัฐใช้อำนาจอย่างมีความรับผิดชอบและตรวจสอบได้

โดยสรุป รายงานฉบับนี้เสนอว่า ไทยควรใช้โอกาสของการจัดทำนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2571-2575) ในการปรับเพิ่มกรอบการมองภัยคุกคามทางไซเบอร์จากปัญหาเชิงเทคนิคไปสู่ปัญหาเชิงการเมืองและยุทธศาสตร์ พร้อมทั้งจัดวางการทำงานร่วมกันระหว่างหน่วยงานด้านเทคนิค ข้าราชการ การทูต การป้องกันประเทศ และการบังคับใช้กฎหมายไว้ในโครงสร้างเดียวกันภายใต้สมมติที่เกี่ยวพันกัน การดำเนินการตามแนวทางนี้จะทำให้ไทยเคลื่อนจากท่าที่ตั้งรับไปสู่ท่าที่เชิงรุกที่มีความรับผิดชอบ และทำให้ไทยสามารถรักษาและขับเคลื่อนผลประโยชน์แห่งชาติในมิติไซเบอร์ได้อย่างมั่นคงและยั่งยืน ท่ามกลางการแข่งขันทางภูมิรัฐศาสตร์ที่ทวีความเข้มข้นขึ้น

บรรณานุกรม

หนังสือ

- Adam Segal. The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. New York: PublicAffairs, 2016.
- Ben Buchanan. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press, 2020.
- Michael N. Schmitt. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.
- Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett. Cyber Persistence Theory: Redefining National Security in Cyberspace. New York: Oxford University Press, 2022.

บทความ

- คณะที่ปรึกษาของสภาความมั่นคงแห่งชาติด้านการข่าวกรอง. การประเมินกำลังอำนาจของชาติ (National Power) และภัยคุกคามรูปแบบใหม่. วารสารมุมมองความมั่นคง ฉบับที่ 7 (มิถุนายน-กันยายน 2564) : 5-16.
- ฐิติมาศ ศรีสุข. สงครามไซเบอร์กับการนิยามใหม่ของการทำสงครามในการเมืองระหว่างประเทศยุคร่วมสมัย. วารสารมุมมองความมั่นคง ฉบับที่ 11 (ตุลาคม 2565-มกราคม 2566) : 52-66.
- ภาณุทัต วัชรารักษ์. ความขัดแย้งทางไซเบอร์ในมุมมองเชิงยุทธศาสตร์. วารสารมุมมองความมั่นคง ฉบับที่ 18 (กุมภาพันธ์-พฤษภาคม 2568) : 39-54.
- ภาณุทัต วัชรารักษ์. เทคโนโลยีสารสนเทศและการสื่อสารกับการเมืองระหว่างประเทศ: การเปลี่ยนแปลงอำนาจรัฐและระเบียบระหว่างประเทศในศตวรรษที่สี่สิบเอ็ด. วารสารมุมมองความมั่นคง ฉบับที่ 11 (ตุลาคม 2565-มกราคม 2566) : 23-33.
- วศิน ปั่นทอง. ความมั่นคงไซเบอร์: แนวคิด ประสพการณ์ของต่างประเทศและบทเรียนสำหรับประเทศไทย. วารสารความมั่นคงศึกษา ฉบับที่ 1 (มิถุนายน-กันยายน 2562) : 13-26.

สื่ออิเล็กทรอนิกส์

- Bangkok Bank InnoHub. ไขกุญแจความสำเร็จ ไทยครองอันดับ 7 โลกด้านความปลอดภัยทางไซเบอร์. [ออนไลน์]. 2567. แหล่งที่มา: <https://www.bangkokbankinnohub.com/th/thailand-ranks-7th-in-global-cybersecurity-index> [12 สิงหาคม 2569].
- CGTN. กต.จีนระบุ หลักฐานล่าสุดยืนยันอีกครั้งว่า สหรัฐฯเป็นภัยคุกคามทางไซเบอร์อันดับแรก. [ออนไลน์]. 2568. แหล่งที่มา: <https://thai.cri.cn/2025/08/02/ARTI1754125188502254> [25 สิงหาคม 2569].
- Hfocus. สธ.-สภมช. แจงข้อมูลรั่วไม่ใช่ สธ. เป็นไปได้ทั้งรัฐ-เอกชน ถูกอ้างหลุด 7 หน่วยงาน. [ออนไลน์]. 2567. แหล่งที่มา: <https://www.hfocus.org/content/2024/03/30032>. [12 สิงหาคม 2569].
- iLaw. ร่าง พ.ร.บ.มั่นคงไซเบอร์ฯ 62: เปิดช่องเจ้าหน้าที่รัฐ 'สอดส่อง' คนเห็นต่างได้. [ออนไลน์]. 2562. แหล่งที่มา: <https://www.ilaw.or.th/articles/3332> [12 สิงหาคม 2569].
- Techsauce Team. สรุปเหตุการณ์ ByBit โดนแฮก คดีโจรกรรมคริปโตครั้งใหญ่ที่สุดในประวัติศาสตร์ กลุ่มแฮกเกอร์คือใครและทำไมต้องแฮก?. [ออนไลน์]. 2568. แหล่งที่มา: <https://techsauce.co/news/bybit-hacked-1-5-billion-crypto-loss> [12 สิงหาคม 2569].
- ThaiPublica. พ.ร.บ. ไซเบอร์: เมื่อหลักความมั่นคงไซเบอร์แพ้ทัศนคติ “ความมั่นคง 0.4”. [ออนไลน์]. 2562. แหล่งที่มา: <https://thaipublica.org/2019/03/cybersecurity-principles-lost-national-security> [12 สิงหาคม 2569].
- THAIRATH Money. เกาหลีเหนือ ขึ้นแท่นแชมป์ถือครองบิตคอยน์อันดับ 3 ของโลกหลังทุ่มทุนปั่นแฮกเกอร์หัวกะทิไว้ปล้น. [ออนไลน์]. 2568. แหล่งที่มา: https://www.thairath.co.th/money/tech_innovation/digital_assets/2848265 [12 สิงหาคม 2569].
- กระทรวงการต่างประเทศ. ไทยร่วมรับรองการจัดตั้งกลไกถาวรด้านความมั่นคงทางไซเบอร์ภายใต้กรอบสหประชาชาติ. [ออนไลน์]. 2568. แหล่งที่มา: <https://www.mfa.go.th/th/content/th-endorses-global-mechanism-cyber-security-th> [12 สิงหาคม 2569].
- กรุงเทพธุรกิจ. O-Day ไกลกว่าที่คิด! Red Hat เนะ 4 ขั้นตอนรับมือภัยถล่มรหัส. [ออนไลน์]. 2569. แหล่งที่มา: <https://www.bangkokbiznews.com/tech/ai/1246705> [12 สิงหาคม 2569].
- กรุงเทพธุรกิจ. ภัยไซเบอร์ป่วนไทย “ฟิชซิง-ดีดอส” ถล่มภาครัฐ-อินฟราฯ สำคัญ. [ออนไลน์]. 2568. แหล่งที่มา: <https://www.bangkokbiznews.com/tech/gadget/1198511> [12 สิงหาคม 2569].

- กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร. ยุทธศาสตร์กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2560-2564. [ออนไลน์]. 2560. แหล่งที่มา: https://isoc.go.th/uploads/ITA/O4/O4_ยุทธศาสตร์_กอ_รมน.2560-2564 [12 สิงหาคม 2569].
- จตุรวิทย์ เครือวานิชกิจ. รู้จัก Lazarus แสกเกอร์มือฉกาจแห่งเกาหลีเหนือ. [ออนไลน์]. 2569. แหล่งที่มา: <https://www.beartai.com/tech/features/1355154> [12 สิงหาคม 2569].
- ไทยรัฐ. “กองทัพ” รุกตั้งหน่วยไซเบอร์ทหาร รับภัยคุกคาม เริ่มผลิตนักรบ 1 ต.ค. นี้ [ออนไลน์] 2567. แหล่งที่มา: <https://www.thairath.co.th/news/local/bangkok/2787536> [12 สิงหาคม 2569].
- รัชชัย สุขสาย และ วสันต์ เกิดสวัสดิ์. มหายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของ สกมช. [ออนไลน์]. 2566. แหล่งที่มา: https://so12.tci-thaijo.org/index.php/watmahasawat_jsc/article/view/771/640 [12 สิงหาคม 2569].
- ธัชกร ภูริธรจินดา, เกรียงชัย ปิงประวัติ, ณัฐพงศ์ บุญเหลือ และนิพนธ์ โชะเฮง. บทบาทของศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2560-2565. [ออนไลน์]. 2567. แหล่งที่มา: <https://so01.tci-thaijo.org/index.php/JDAR/article/download/275572/177933/1098471> [12 สิงหาคม 2569].
- ประชาไท. ก.กลาโหม เตรียมตั้งกองบัญชาการสงครามไซเบอร์. [ออนไลน์]. 2567. แหล่งที่มา: <https://prachatai.com/journal/2024/05/109345> [12 สิงหาคม 2569].
- ประชาไท. ข้อมูลคนไทยหลุดซ้ำ ๆ หน่วยงานไทยยังถูกโจมตีหนัก 1 ปี 3 เดือน ไทยเจอภัยกว่า 2,700 ครั้ง. [ออนไลน์]. 2568. แหล่งที่มา: <https://prachatai.com/journal/2025/04/112536> [12 สิงหาคม 2569].
- โพสต์ทูเดย์. อย่าชะล่าใจ! ข้อมูลที่ปลอดภัยวันนี้ อาจโดนเจาะในอีก 5 ปี เมื่อ 'ควอนตัม' มาถึง. [ออนไลน์]. 2569. แหล่งที่มา: <https://www.posttoday.com/smart-life/737916> [12 สิงหาคม 2569].
- มหาวิทยาลัยสุโขทัยธรรมาธิราช. ความมั่นคงปลอดภัยของระบบสารสนเทศ. เอกสารการสอนชุดวิชา 96101 หน่วยที่ 14. [ออนไลน์]. 2566. แหล่งที่มา: <https://www.stou.ac.th/Schools/sst/main/Subject96101/96101-14.pdf> [12 สิงหาคม 2569].
- สำนักเลขาธิการคณะรัฐมนตรี. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. [ออนไลน์]. 2562. แหล่งที่มา: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF [12 สิงหาคม 2569].

- สำนักเลขาธิการคณะรัฐมนตรี. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570). [ออนไลน์]. 2565. แหล่งที่มา: https://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/303/T_0003.PDF [12 สิงหาคม 2569].
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สถิติภัยคุกคามทางไซเบอร์. [ออนไลน์]. 2569. แหล่งที่มา: <https://www.ncsa.or.th/policy/threat-statistics> [12 สิงหาคม 2569].
- สำนักงานสภาความมั่นคงแห่งชาติ. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570). [ออนไลน์]. 2566. แหล่งที่มา: https://www.nsc.go.th/wp-content/uploads/2023/06/nsc_policy_66-70-2-.pdf [12 สิงหาคม 2569].
- สุธีราภรณ์ แสงจันทร์ศรี และ สติลา กลั่นเรืองแสง. มุมมองเชิงกฎหมายต่อความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน. [ออนไลน์]. 2564. แหล่งที่มา: <https://so02.tci-thaijo.org/index.php/ISSC/article/view/251833/169890> [12 สิงหาคม 2569].
- Australian Government. Department of Home Affairs. 2023-2030 Australian Cyber Security Strategy. [Online]. 2023. Available from: <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf> [2026, August 12].
- Bloomberg. Iranian Hackers Hit Sheldon Adelson's Sands Casino in Las Vegas. [Online]. 2014. Available from: <https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas> [2026, August 12].
- Canadian Centre for Cyber Security. National Cyber Threat Assessment 2025-2026. [Online]. 2024. Available from: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf> [2026, August 12].
- Center for Cybersecurity Policy and Law. Japan's New Active Cyber Defense Law: A Strategic Evolution in National Cybersecurity. [Online]. 2025. Available from: <https://www.centerforcybersecuritypolicy.org/insights-and-research/japans-new-active-cyber-defense-law-a-strategic-evolution-in-national-cybersecurity> [2026, August 12].
- China Cybersecurity Industry Alliance: U.S. Threats and Sabotage to Global Cyberspace Security and Development. [Online]. 2024. Available from:

[https://china-cia.org.cn/home/WorkDetail?id= 663874690200340c642b4cc4&](https://china-cia.org.cn/home/WorkDetail?id=663874690200340c642b4cc4&)
[2026, August 25].

Council of the European Union. EU Imposes the First Ever Sanctions against Cyber-Attacks, press release. [Online]. 2020. Available from:

<https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks> [2026, August 12].

Council on Foreign Relations. Compromise of Saudi Aramco and RasGas. [Online].

2012. Available from: <https://www.cfr.org/cyber-operations/compromise-of-saudi-aramco-and-rasgas> [2026, August 12].

Cyber Security Agency of Singapore. Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region. [Online].

2024. Available from: <https://www.csa.gov.sg/news-events/press-releases/singapore-and-aseanmember-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region/> [2026, August 12].

Cyber Security Agency of Singapore. Singapore's Operational Technology Cybersecurity Masterplan 2024. [Online]. 2024. Available from:

<https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/> [2026, August 12].

Cybersecurity and Infrastructure Security Agency. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

Cybersecurity Advisory AA24-038A. [Online]. 2024. Available from: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a> [2026, August 12].

Foreign, Commonwealth & Development Office. The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities.

[Online]. 2024. Available from: <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/> [2026, August 12].

- ISC2. ISC2 Cybersecurity Workforce Study (2024). [Online]. 2024. Available from: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study#KeyFindings> [2026, August 12].
- Microsoft Threat Intelligence. Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques. [Online]. 2023. Available from: <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/?msockid=1313e5844c506f7c33c9f2e84d0f6e88> [2026, August 12].
- Ministry of Foreign Affairs of the Kingdom of the Netherlands. International Cyber Strategy 2023-2028. [Online]. 2023. Available from: <https://www.government.nl/documents/2023/09/12/international-cyber-strategy-netherlands-2023-2028> [2026, August 12].
- National Cyber Security Centre. Active Cyber Defence. [Online]. 2026. Available from: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics/active-cyber-defence> [2026, August 12].
- National Cyber Security Centre. NCSC Annual Review 2025. [Online]. 2025. Available from: <https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-annual-review-2025.pdf> [2026, August 12].
- Sriyai, Surachanee “Hammerli”. Borderland Scam Centres and Cyber Threats: Policy Considerations for Thailand. [Online]. 2025. Available from: https://www.iseas.edu.sg/wp-content/uploads/2025/07/ISEAS_Perspective_2025_60.pdf. [2026, August 12].
- Sriyai, Surachanee. Data Leaks: Thai Government Tough on Private Firms, Soft on Public Sector and Cybercriminals. [Online]. 2024. Available from: <https://fulcrum.sg/data-leaks-thai-government-tough-on-private-firms-soft-on-public-sector-and-cybercriminals>. [2026, August 12].
- Stars and Stripes. Senate approves Joshua Rudd as head of Cyber Command, NSA. [Online]. 2026. Available from: <https://www.stripes.com/theaters/us/2026-03-10/joshua-rudd-nsa-cyber-command-21018045.html> [2026, August 25].

The Telegraph. Iran shut down British power plant in unprecedented cyber attack.

[Online]. 2026. Available from: [https://www.telegraph.co.uk/news/2026/](https://www.telegraph.co.uk/news/2026/08/22/iranian-hackers-shut-down-uk-power-plant/)

08/22/iranian-hackers-shut-down-uk-power-plant/ [2026, August 25].

United Nations General Assembly. Report of the Group of Governmental Experts on

Developments in the Field of Information and Telecommunications in the

Context of International Security, A/70/174. [Online]. 2015. Available from:

[https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-](https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf)

[of-responsible-state-behaviour-in-cyberspace.pdf](https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf) [2026, August 12].

United Nations. United Nations Convention against Cybercrime. Adopted December

24. [Online]. 2024. Available from: [https://www.unodc.org/unodc/en/](https://www.unodc.org/unodc/en/cybercrime/convention/)

[cybercrime/convention/](https://www.unodc.org/unodc/en/cybercrime/convention/) [2026, August 12].

ภาคผนวก



เล่นนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570)

https://www.nsc.go.th/wp-content/uploads/2023/06/nsc_policy_66-70-2-.pdf

ประวัติผู้เขียน

ชื่อ-สกุล	นายรพี โล่ชัยยะกุล
ประวัติการศึกษา	– รัฐศาสตรบัณฑิต (การเมืองการปกครอง) มหาวิทยาลัยธรรมศาสตร์ – วิทยาศาสตร์มหาบัณฑิต (การบริหาร) สถาบันบัณฑิตพัฒนบริหารศาสตร์
ประวัติการทำงาน	
พ.ศ. 2536	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 3 กอง 3 สำนักงานสภาพัฒนาการเศรษฐกิจ (สมช.)
พ.ศ. 2538	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 4 กอง 3 สมช.
พ.ศ. 2541	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 5 กอง 4 สมช.
พ.ศ. 2546	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 6 ว สำนักความมั่นคงกิจการ ภายในประเทศ สมช.
พ.ศ. 2551	นักวิเคราะห์นโยบายและแผนชำนาญการ สำนักความมั่นคงกิจการ ภายในประเทศ สมช.
พ.ศ. 2558	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ สำนักยุทธศาสตร์ ความมั่นคงระหว่างประเทศ สมช.
พ.ศ. 2565	ผู้เชี่ยวชาญเฉพาะด้านยุทธศาสตร์ความมั่นคง สมช.
พ.ศ. 2568	ผู้อำนวยการกองความมั่นคงภายในประเทศ สมช.
ตำแหน่งปัจจุบัน	ผู้อำนวยการกองความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ สมช.