ความมั่นคงปลอดภัยไซเบอร์ของชาติ ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติในระยะยาว และ แนวทางการกำหนดยุทธศาสตร์ชาติ

โดย

นายปริญญา หอมเอนก
ประธานกรรมการบริหารบริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๒
ประจำปีการศึกษา พุทธศักราช ๒๕๖๒ - ๒๕๖๓

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “ความมั่นคงปลอดภัยไซเบอร์ของชาติ : ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติในระยะยาว และ แนวทางการกำหนดยุทธศาสตร์ชาติ” ลักษณะวิชา ยุทธศาสตร์ ของ นายปริญญา หอมอเนก เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 62 ประจำปีการศึกษา พุทธศักราช 2562-2563

พลโท

(พิสัณห์ ปฐมเอม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง ความมั่นคงปลอดภัยไซเบอร์ของชาติ : ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติในระยะยาว และแนวทางการกำหนดยุทธศาสตร์ชาติ

ลักษณะวิชา ยุทธศาสตร์

ผู้วิจัย นายปริญญา หอมเอนก **หลักสูตร** วปอ. **รุ่นที่** 62

ไซเบอร์สเปซ (Cyberspace) เป็นช่องทางในการปฏิบัติการข่าวสาร (Information Operations : IO) โดยการกระจายข้อมูลข่าวสาร เช่น ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว การประชาสัมพันธ์ การโฆษณาชวนเชื่อ เป็นต้น ผ่านเครือข่ายสังคมออนไลน์ (Social media) ต่าง ๆ เช่น Line Facebook Twitter เป็นต้น ทำให้สามารถเข้าถึงกลุ่มเป้าหมายด้วยความรวดเร็ว ชั่วพริบตา และมีการแชร์ข้อมูลต่อ ๆ กันไปอย่างรวดเร็ว สามารถส่งผ่านข้อมูลที่มีอิทธิพลต่อทัศนคติ ความคิดเห็น พฤติกรรมและการตัดสินใจของผู้ใช้บริการได้โดยตรง โดยที่ผู้ใช้บริการอาจไม่รู้ตัว โดยเฉพาะอย่างยิ่งกลุ่มเยาวชนและคนรุ่นใหม่ ซึ่งเป็นกลุ่มที่มีการใช้งานอุปกรณ์สมาร์ทโฟน และ Social media มากกว่ากลุ่มอื่น ทำให้มีอิทธิพลต่อความรู้สึกนึกคิด ความเชื่อ อุดมการณ์ และมีผลต่อการตัดสินใจของคนเป็นจำนวนมาก จึงก่อให้เกิดปัญหาใหญ่คือ การรุกล้ำ **“อธิปไตยไซเบอร์” หรือ "ความเป็นเอกราชทางไซเบอร์" (Cyber Sovereignty)** ของประชาชนในประเทศ ตลอดจนไปถึงปัญหาความมั่นคงของชาติ (National Security) ซึ่งประชาชนส่วนใหญ่ยังไม่รู้ตัวเลยด้วยซ้ำว่ากำลังถูกละเมิดในเรื่อง “อธิปไตยไซเบอร์” เนื่องจากปัญหาดังกล่าวถูกซ่อนอยู่ในการใช้งานอินเทอร์เน็ตและการใช้งานสมาร์ทโฟนในปัจจุบันที่อยู่ในชีวิตประจำวันของคนจำนวนมาก

วัตถุประสงค์ของการวิจัยในครั้งนี้ ประกอบด้วย การศึกษาและวิเคราะห์กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รูปแบบ และลักษณะของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี มีความชัดเจน มีความเหมาะสมกับช่วงเวลา สามารถนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาอธิปไตยไซเบอร์ในระยะสั้นและระยะยาว และเสนอแนะแนวทางในการปรับปรุงกระบวนการและรูปแบบของนโยบายความมั่นคงแห่งชาติ ให้สอดคล้องกับ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และยุทธศาสตร์ชาติ 20 ปี เพื่อให้สามารถนำมาปฏิบัติจริงได้อย่างมีประสิทธิผลและประสิทธิภาพ

วิธีการวิจัยครั้งนี้จะเป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์กระบวนการ รูปแบบและลักษณะของปัญหาอธิปไตยไซเบอร์ในประเทศไทย และในต่างประเทศ รวมถึงการพิจารณายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศเฉพาะที่มีความสอดคล้อง

กับเรื่องอธิปไตยไซเบอร์ มีการศึกษาเปรียบเทียบกับต่างประเทศบางประเทศ โดยมุ่งเน้นให้เห็นถึงความแตกต่างในการแก้ปัญหาของแต่ละประเทศที่ศึกษา เพื่อนำแนวทางการกำหนดและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทย มีความเหมาะสมของเนื้อหากับกรอบเวลา รวมทั้งมีการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทยเพื่อให้สามารถนำไปปฏิบัติได้จริง

ผลการวิจัย พบว่า กฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่มีการแก้ไขเพิ่มเติม และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) และยุทธศาสตร์ด้านความมั่นคงไซเบอร์แห่งชาติ (2560 - 2564) ยังไม่ครอบคลุมทั้ง 5 มิติด้านความมั่นคงปลอดภัยไซเบอร์ ตามมิติที่ 2 ของกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model: CMM) ของ The Global Cybersecurity Capacity Centre (GCSCC) แห่ง University of Oxford ซึ่งเป็นกรอบแนวคิดมาตรฐานของสากลในเรื่อง Cyber culture and society ความรู้ความเข้าใจ ความเชื่อมั่นของผู้ใช้บริการ เกี่ยวกับการละเมิดและนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต ช่องทางการรายงานอาชญากรรมทางไซเบอร์อิทธิพลของ Social media และอธิปไตยไซเบอร์ ทั้งนี้ กฎหมายที่เกี่ยวข้องส่วนใหญ่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางกายภาพและภัยคุกคามทางไซเบอร์เป็นหลัก ไม่ครอบคลุมถึงการรุกรานทางความคิดผ่านเครือข่ายสังคมออนไลน์และอธิปไตยทางไซเบอร์

การศึกษาวิจัยครั้งนี้สรุปได้ว่า ปัญหาในเรื่องความมั่นคงปลอดภัยไซเบอร์ของประเทศแบ่งออกเป็น 2 ปัญหาใหญ่ ประกอบด้วย 1. ความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2. ความไม่พร้อมในการรับมือปรากฏการณ์ “Social media” กลายเป็น “Soft power ” และการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ

ทางผู้วิจัยจึงได้เสนอแนะกรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย 5 มิติ ตามกรอบแนวคิด CMM ประกอบด้วย มิติที่ 1 National cybersecurity framework and policy มิติที่ 2 Cyber culture and society มิติที่ 3 Cybersecurity education, training and skills มิติที่ 4 Legal and regulatory frameworks มิติที่ 5 Standards, organizations, and technologies และเสนอแนะให้จำแนกแนวทางการพัฒนายุทธศาสตร์ออกเป็น 3 บทบาท ประกอบด้วย 1. แนวทางที่ให้รัฐมีบทบาทนำ (Government-led) 2. แนวทางที่ให้ภาค

ประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3. แนวทางที่แพลตฟอร์มมีบทบาทนำ (Platform-led)

Abstract

Title : The national cybersecurity, the problem of cyber sovereignty, long-term national security impact and national strategy formulation guidelines

Field : Strategy / Science and Technology

Name : Mr. Prinya Hom-Anek **Course** NDC **Class** 62

This research paper was to study the national cybersecurity, the problem of cyber sovereignty, long-term national security impact and national strategy formulation guidelines prepared with inspiration from my experience in cybersSecurity and observed that the process of maintaining cybersecurity in Thailand in the past focus on defense of physical attacks on the Internet and networks. In addition to today's world where international platforms and social media have increasingly played a role in changing the behavior and decision-making of people of the nation. It is in line with the global awareness that these problems lead to cognitive and mental aggression of people. The so-called "cyber sovereignty" problem is emerging all over the world which directly affects the economy and society of various countries, as well as the "National Security", the researcher sees that this study will help Thailand understand the problems and impacts of aggression. "Cyber sovereignty" to be able to apply the conceptual framework developed by studying the framework for creating a strategy for solving problems. "Cyber sovereignty" is an internationally recognized concept. Let's improve the 20-year National Strategy (2018 - 2037) and the NCS's the National Cybersecurity Strategy 2017 – 2021 has finally made it more efficient.

คำนำ

เอกสารวิจัย เรื่อง ความมั่นคงปลอดภัยไซเบอร์ของชาติ ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติในระยะยาว และ แนวทางการกำหนดยุทธศาสตร์ชาติ จัดทำขึ้นโดยได้แรงบันดาลใจจากประสบการณ์ทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และได้สังเกตว่า กระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยที่ผ่านมา มุ่งเน้นแต่เพียงการป้องกันการโจมตีทางกายภาพต่อระบบอินเทอร์เน็ตและเครือข่าย ประกอบกับโลกยุคปัจจุบันที่แพลตฟอร์มต่างชาติและสื่อสังคมออนไลน์ (Social media) เข้ามามีบทบาทในการเปลี่ยนแปลงพฤติกรรมและการตัดสินใจของคนในชาติเพิ่มขึ้นเรื่อยๆ สอดคล้องกับความตื่นตัวของทั่วโลกที่เห็นว่าปัญหาดังกล่าวนำไปสู่การรุกรานทางความคิดและจิตใจของคนในชาติ หรือที่เรียกว่า ปัญหา "อธิปไตยไซเบอร์" หรือ "Cyber sovereignty " ที่กำลังเกิดขึ้นทั่วโลก ซึ่งส่งผลกระทบโดยตรงต่อเศรษฐกิจและสังคมของประเทศต่าง ๆ ตลอดจนส่งผลกระทบถึงความมั่นคงของชาติหรือ "National Security" ผู้วิจัยจึงเห็นว่า การศึกษาวิจัยในครั้งนี้จะช่วยให้ประเทศไทยเข้าใจปัญหาและผลกระทบของการรุกราน "อธิปไตยไซเบอร์" มากขึ้น เพื่อให้สามารถนำกรอบแนวคิดที่ได้จากการศึกษากรอบการจัดทำยุทธศาสตร์ในการแก้ไขปัญหา "อธิปไตยไซเบอร์" ตามแนวคิดที่เป็นที่ยอมรับในระดับสากล มาปรับปรุงยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) และยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 ได้ ให้มีประสิทธิภาพมากขึ้นในที่สุด

(นายปริญญา หอมเอนก)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 62
ผู้วิจัย

กิตติกรรมประกาศ

ในนามของผู้วิจัย ขอขอบคุณผู้ศึกษาขอขอบคุณคณะกรรมการและที่ปรึกษางานวิจัย ที่ได้กรุณาให้คำแนะนำและข้อคิดเห็นทางวิชาการที่เป็นประโยชน์อย่างยิ่งในการใช้เป็นกรอบแนวทางในการจัดทำเอกสารวิจัยส่วนบุคคลฉบับนี้ให้มีความสมบูรณ์ นอกจากนี้ผู้วิจัยขอขอบคุณท่านผู้ทรงคุณวุฒิ คณาจารย์วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ที่มีส่วนในการสนับสนุนสำคัญในระหว่างการจัดทำเอกสารวิชาการฉบับนี้ ผู้วิจัยขอขอบคุณวิทยาลัยป้องกันราชอาณาจักร และเจ้าหน้าที่ของวิทยาลัยทุกท่าน ที่ให้ความอนุเคราะห์เอื้อเฟื้อสถานที่และทรัพยากรที่จำเป็นแก่การจัดทำเอกสาร รวมทั้งการให้ความช่วยเหลือในการให้คำแนะนำรูปแบบและการตรวจทานเอกสารต้นฉบับให้มีความสมบูรณ์มาก และ หวังเป็นอย่างยิ่งว่างานวิจัยฉบับนี้ จะได้รับการนำไปปฏิบัติอย่างเป็นรูปธรรมในประเทศของเรา เพื่อให้เกิดผลสำเร็จเป็นประโยชน์ต่อประเทศชาติบ้านเมืองต่อไปในอนาคตอันใกล้นี้

(นายปริญญา หอมเอนก)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 62
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญแผนภาพ

หน้า

แผนภาพที่

สารบัญตาราง

ฌ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

จากประเด็นยุทธศาสตร์ชาติด้านความมั่นคงและประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ในเอกสารยุทธศาสตร์ชาติ ระยะ 20 ปี (พ.ศ. 2561-2580) ในด้านของความมั่นคง มีการกล่าวถึงเรื่อง ปัญหาภัยคุกคามไซเบอร์ อาชญากรรมไซเบอร์ที่ซับซ้อนขึ้น รูปแบบการก่อสงครามที่ใช้เทคโนโลยีเป็นเครื่องมือ เครื่องมือบนพื้นฐานของธรรมาภิบาลข้อมูล ซึ่งครอบคลุมความมั่นคงปลอดภัยไซเบอร์ ความมีจริยธรรม และการไม่ละเมิดสิทธิส่วนบุคคล การสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ เพื่อลดผลกระทบจากภัยคุกคามทางไซเบอร์ต่อเศรษฐกิจและสังคม และ การปกป้องอธิปไตยไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติ จากการทำธุรกิจดิจิทัล แนวโน้มเหล่านี้จะก่อให้เกิดความท้าทายต่อการพัฒนาประเทศในหลายมิติ ทั้งในส่วนของการจ้างงานและอาชีพ สาขาการผลิตและบริการใหม่ ๆ

จากกระแส “Digital disruption” และ “Digital transformation” ทั่วโลก ทำให้เราคงปฏิเสธไม่ได้ว่า การเปลี่ยนแปลงทางดิจิทัลของโลกมีผลต่อการดำเนินชีวิตประจำวันของมนุษย์ทุกคนบนโลกใบนี้อย่างหลีกเลี่ยงไม่ได้ คำว่า " Digital transformation" หรือ "Digital disruption" เป็นสิ่งที่เราได้ยินได้ฟังกันบ่อย ๆ ปัจจัยทั้ง 4 ที่มีผลต่อการเปลี่ยนแปลงทางดิจิทัลดังกล่าว ได้แก่ (The four IT mega trends in S-M-C-I Era) S หมายถึง Social media M หมายถึง Mobile computing C หมายถึง Cloud computing และ I หมายถึง Information หรือ Big data เทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ ตลอดจนการเปลี่ยนแปลงของโลกจากเทคโนโลยีปัญญาประดิษฐ์ (Artificial intelligence) และ อินเทอร์เน็ตในทุกสิ่ง (Internet of things) กำลังมีการพัฒนาและประยุกต์ใช้อย่างแพร่หลายทั่วโลก

ดังนั้น การเปลี่ยนแปลงครั้งใหญ่จากปัจจัยทั้งสี่ดังกล่าวจึงมีผลกระทบเกิดขึ้นใน 3 ระดับได้แก่ ระดับบุคคลและครอบครัว ระดับองค์กร และระดับประเทศ ไปจนถึงผลกระทบต่อความมั่นคงของชาติ (National security) ปัจจุบันประเทศไทยของเราเป็นประเทศที่มีเอกราชและอธิปไตยในดินแดนของประเทศเราในเชิงกายภาพ (Physical) แต่หลังจากระบบอินเทอร์เน็ตได้เข้ามามีบทบาทมากขึ้นในการติดต่อสื่อสารของคนไทยในหลายปีที่ผ่านมา ตลอดจนความนิยมในการใช้งานสมาร์ทโฟน และโปรแกรมเครือข่ายสังคมออนไลน์ของคนไทย ทำให้มีการเก็บข้อมูลคนไทย

ทั้งประเทศไว้ในระบบคลาวด์ โดยส่งผ่านจากทางสมาร์ทโฟนและโปรแกรมเครือข่ายสังคมออนไลน์ดังกล่าว ยกตัวอย่างเช่น Facebook, Youtube และ Line ปัจจุบันมีคนไทยใช้งานสมาร์ทโฟนมากกว่าหนึ่งร้อยล้านเครื่อง โดยเฉลี่ยใช้งานวันละกว่า 6 ชั่วโมงต่อวัน โดยโปรแกรมยอดนิยมคงหนีไม่พ้นสามโปรแกรมเครือข่ายสังคมออนไลน์ดังที่กล่าวมาแล้ว ทำให้เกิดปรากฏการณ์มหกรรมการเก็บข้อมูลของคนไทยเข้าสู่ระบบคลาวด์ของบริษัทผู้ให้บริการโปรแกรมเครือข่ายสังคมออนไลน์ดังกล่าว สืบเนื่องจากการใช้งานสมาร์ทโฟนอย่างแพร่หลายทำให้มีการจัดเก็บพฤติกรรมผู้ใช้งานสมาร์ทโฟนอย่างต่อเนื่องทั้งที่ผู้ใช้ทราบและไม่ทราบมาก่อน ไม่ว่าจะเป็นการจัดเก็บข้อมูลตำแหน่งการใช้งาน (User location) พฤติกรรมการค้นหาข้อมูล (User search behavior and search keyword) พฤติกรรมการเข้าชมภาพและวิดีโอ ตลอดจนพฤติกรรมในการเลือกซื้อสินค้าและบริการ เช่น การจองโรงแรม การจองตั๋วเครื่องบิน ทำให้ข้อมูลมหาศาลเหล่านี้ตกอยู่ในมือของผู้ให้บริการการค้นหาข้อมูลและผู้ให้บริการโปรแกรมเครือข่ายสังคมออนไลน์อย่างหลีกเลี่ยงไม่ได้

การเก็บข้อมูลในระบบคลาวด์ขนาดใหญ่ มีกลไกในการวิเคราะห์เจาะลึกข้อมูลของเราโดยใช้เทคโนโลยี “Big data” และ “Machine learning” ทำให้ผู้ให้บริการสามารถล่วงรู้พฤติกรรมการใช้อินเทอร์เน็ต การใช้สมาร์ทโฟน การค้นหาข้อมูล การใช้โปรแกรมเครือข่ายสังคมออนไลน์ การรับรู้ข้อมูลจากสื่อสังคมออนไลน์ต่าง ๆ ทำให้ผู้ให้บริการสามารถทราบถึง "Digital lifestyle" ของผู้คนอย่างไม่ยากเย็นนักจากข้อมูลที่เราเองเป็นคนใส่ข้อมูลเข้าไปในระบบทั้งรู้ตัวและไม่รู้ตัว

ปัญหาใหญ่ที่ตามมาคือปัญหา **“อธิปไตยไซเบอร์” หรือ** "ความเป็นเอกราชทางไซเบอร์" (Cyber sovereignty) ของผู้คนในประเทศตลอดจนไปถึงปัญหาความมั่นคงของชาติ (National security) ซึ่งคนไทยเองส่วนใหญ่ยังไม่รู้ตัวเลยด้วยซ้ำว่ากำลังถูกละเมิดในเรื่อง “อธิปไตยไซเบอร์” หรือ "Cyber sovereignty" เนื่องจากปัญหาดังกล่าวถูกซ่อนอยู่ในการใช้งานอินเทอร์เน็ตและการใช้งานสมาร์ทโฟนในปัจจุบันที่อยู่ในชีวิตประจำวันของคนไทย ทำให้ผู้ให้บริการที่เข้าถึงข้อมูลเชิงลึก มีความได้เปรียบในการแข่งขันทางธุรกิจ และสามารถนำข้อมูลมาใช้ในการตลาดได้อย่างมีประสิทธิผลและประสิทธิภาพ ทั้งนี้ยังไม่รวมถึงการขาดรายได้ของรัฐบาลไทยจากการจัดเก็บภาษีจากยอดเงินในระดับหมื่นล้านบาท โดยรัฐบาลไทยไม่สามารถจัดเก็บภาษีจากผู้ให้บริการได้อย่างที่ควรจะเป็น เนื่องจากผู้ให้บริการทำการ Settlement payment โดยการใช้ Payment gateway นอกประเทศไทย เป็นต้น

จึงมีผู้กล่าวเปรียบเปรยได้ว่าเรากำลังใช้ชีวิตประจำวันอยู่ใน "The Matrix" หลายท่านอาจกำลังนึกถึงนวนิยายไซไฟ แต่จริง ๆ แล้วเรากำลังอยู่ในโลกแห่งความเป็นจริงที่ชีวิตประจำวันของคนไทยทุกคนมีความเกี่ยวพันกับ S-M-C-I อย่างหลีกเลี่ยงไม่ได้ ซึ่งเปรียบเหมือนเรากำลังอยู่ใน "สภาวะไซเบอร์" ซึ่งปัจจัยทั้งสี่ S-M-C-I กำลังมีผลกับเราอย่างไม่รู้ตัว โดยปัจจุบันคนไทยมี Facebook account มากกว่า 54 ล้าน account และ LINE account มากกว่า 45 ล้าน account

โดยมีการใช้งานอย่างต่อเนื่องในแทบทุกวัน เรียกได้ว่าเป็น "New platform" ที่คนไทยกำลังใช้ในการติดต่อสื่อสารกันแทนการใช้งานเทคโนโลยีในอดีต

ประธานาธิบดีแห่งสาธารณรัฐประชาชนจีน สี จิ้นผิง ได้กล่าวเสมอในการประชุมสุดยอดผู้นำโลกเกี่ยวกับปัญหา "อธิปไตยไซเบอร์" (Cyber sovereignty) ที่กำลังเกิดขึ้นทั่วโลก ท่านกล่าวว่าทุกประเทศทั่วโลกมีสิทธิที่จะกำหนดนโยบายด้านไซเบอร์ในประเทศของตน เพื่อป้องกันการรุกรานโดยต่างชาติในรูปแบบที่ไม่ต้องใช้กำลังทางทหารหรือกระสุนแม้แต่เพียงนัดเดียว แต่เป็นการรุกรานหรือการล่าอาณานิคมในรูปแบบใหม่ ที่ประชาชนในประเทศเป้าหมายไม่ได้รับรู้ว่ากำลังถูกรุกรานอยู่ เนื่องจากการรุกรานดังกล่าวไม่ต้องใช้กำลังแต่อย่างใด เป็นการรุกรานทางความคิด ความเชื่อ ค่อย ๆ ส่งข้อมูลเข้ามาปรับเปลี่ยนพฤติกรรมของคนในชาติเหล่านี้ เราคงเคยเห็นกันจากประสบการณ์ "Arab Spring" ในตะวันออกกลางมาแล้ว มีผลต่อการเลือกตั้ง มีผลต่อการเมืองการปกครอง ภัยจากการรุกรานเข้ามาเปลี่ยนความคิดดังกล่าวนั้น น่ากลัวยิ่งกว่าภัยจากการแฮกของแฮกเกอร์เสียอีก เนื่องจากแฮกเกอร์จะเข้าระบบเพื่อดึงข้อมูล หรือทำให้ระบบล่ม ที่เราเห็นปัญหามัลแวร์กันอยู่เป็นประจำ หากแต่การเจาะเข้าไปในจิตใจของมนุษย์ ให้ปรับเปลี่ยนความคิด ความเชื่อ ความศรัทธา ทำให้ชอบหรือไม่ชอบ รักหรือเกลียดในบุคคล สินค้า หรือบริการ หรือบริษัทต่าง ๆ ตลอดจนผู้นำในแต่ละประเทศมีผลกระทบโดยตรงต่อเศรษฐกิจและสังคมของประเทศต่าง ๆ ตลอดจนส่งผลกระทบถึงความมั่นคงของชาติหรือ "National security" ในที่สุด

ปัจจุบันประเทศไทยคณะกรรมการยุทธศาสตร์ชาติได้ดำเนินการจัดทำยุทธศาสตร์ชาติ 20 ปี ประกาศในราชกิจจานุเบกษาเป็นที่เรียบร้อยแล้ว แต่ประเทศไทยยังขาดการกำหนดและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อย่างเป็นทางการ ประกอบกับยังไม่มีแนวทางการแก้ปัญหาอธิปไตยไซเบอร์กำหนดไว้ในยุทธศาสตร์ชาติ ดังนั้น จึงเป็นที่มาของงานวิจัยฉบับนี้ ที่มุ่งศึกษาค้นคว้าแนวทางการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อให้สามารถแก้ปัญหาอธิปไตยไซเบอร์และผลกระทบต่อความมั่นคงของชาติที่กำลังตามมาในระยะยาว เพื่อให้ประเทศไทยมีความพร้อมในการเข้าสู่ยุคแห่ง Data economy และ Digital transformation อีกทั้งยังสามารถปกป้องรักษาอธิปไตยไซเบอร์ของชาติเอาไว้ได้ ส่งผลต่อการรักษาความมั่นคงของชาติในที่สุด

วัตถุประสงค์ของการวิจัย

1. ศึกษาและวิเคราะห์กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รูปแบบ และ ลักษณะของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี มีความชัดเจน มีความเหมาะสมกับช่วงเวลา สามารถนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาอธิปไตยไซเบอร์ในระยะสั้นและระยะยาว

2. เสนอแนะแนวทางในการปรับปรุงกระบวนการและรูปแบบของนโยบายความมั่นคงแห่งชาติ ให้สอดคล้องกับ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และยุทธศาสตร์ชาติ 20 ปี เพื่อให้สามารถนำมาปฏิบัติจริงได้อย่างมีประสิทธิผลและประสิทธิภาพ

ขอบเขตของการวิจัย

1. เน้นการวิจัยเฉพาะเรื่องอธิปไตยไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ ไม่รวมเรื่องการโจมตีของแฮกเกอร์ในทางเทคนิค

2. วิจัยเฉพาะยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศที่เปิดเผยได้เท่านั้น

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์กระบวนการ รูปแบบ และลักษณะของปัญหาอธิปไตยไซเบอร์ในประเทศไทย และ ในต่างประเทศ รวมถึงการพิจารณายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศเฉพาะที่มีความสอดคล้องกับเรื่องอธิปไตยไซเบอร์ มีการศึกษาเปรียบเทียบกับต่างประเทศบางประเทศ โดยมุ่งเน้นให้เห็นถึงความแตกต่างในการแก้ปัญหาของแต่ละประเทศที่ศึกษา เพื่อนำแนวทางการกำหนดและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทย มีความเหมาะสมของเนื้อหากับกรอบเวลา รวมทั้งมีการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทยเพื่อให้สามารถนำไปปฏิบัติได้จริง

ประโยชน์ที่ได้รับจากการวิจัย

1. จะทำให้ได้แนวทางในการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทย และรูปแบบในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งจะช่วยให้มีทิศทางในการดำเนินการด้านการรักษาความมั่นคงของชาติ เพื่อให้บรรลุเป้าหมายในการแก้ปัญหาอธิปไตยไซเบอร์ในระยะสั้นและระยะยาว

2. ได้แนวคิดในการปรับยุทธศาสตร์ความมั่นคงแห่งชาติ นโยบายความมั่นคงแห่งชาติ บทบาท และโครงสร้างของหน่วยงานที่รับผิดชอบหลักในการกำหนดนโยบายความมั่นคงแห่งชาติ และการจัดการกับปัญหาอธิปไตยไซเบอร์ เพื่อให้สามารถปฏิบัติงานไปสู่วัตถุประสงค์หลักคือ การรักษาความมั่นคงของชาติในระยะยาวโดยสอดรับกับแผนยุทธศาสตร์ชาติ 20 ปีที่ได้ประกาศในราชกิจจานุเบกษาแล้ว

คำจำกัดความ

ความมั่นคง หมายถึง การมีความมั่นคงปลอดภัยจากภัยและการเปลี่ยนแปลงทั้งภายในประเทศและภายนอกประเทศในทุกระดับ ทั้งระดับประเทศ สังคม ชุมชน ครัวเรือน และปัจเจกบุคคล และมีความมั่นคง ในทุกมิติ ทั้งมิติทางการทหาร เศรษฐกิจ สังคม สิ่งแวดล้อม และการเมือง เช่น ประเทศมีความมั่นคงในเอกราชและอธิปไตย มีการปกครองระบบประชาธิปไตยที่มีพระมหากษัตริย์ทรงเป็นประมุขสถาบันชาติ ศาสนา พระมหากษัตริย์มีความเข้มแข็งเป็นศูนย์กลางและเป็นที่ยึดเหนี่ยวจิตใจของประชาชน มีระบบการเมืองที่มั่นคงเป็นกลไกที่นำไปสู่การบริหารประเทศที่ต่อเนื่องและโปร่งใสตามหลักธรรมาภิบาลสังคมมีความปรองดองและความสามัคคี สามารถผนึกกำลังเพื่อพัฒนาประเทศ ชุมชนมีความเข้มแข็งครอบครัวมีความอบอุ่น ประชาชน มีความมั่นคงในชีวิต มีงานและรายได้ที่มั่นคงพอเพียงกับการดำรงชีวิต มีการออมสำหรับวัยเกษียณ ความมั่นคงของอาหาร พลังงาน และน้ำ มีที่อยู่อาศัย และความปลอดภัยในชีวิตทรัพย์สิน

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคง ทางทหาร และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์

		โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์
อธิปไตยไซเบอร์	หมายถึง	แนวคิดที่รัฐบาลของแต่ละประเทศควรมีสิทธิเสรีภาพมีเอกราชและอธิปไตยในการบริหารจัดการระบบอินเทอร์เน็ตและการบริการออนไลน์ต่าง ๆ ที่อยู่บนอินเทอร์เน็ตในประเทศของตนเองแต่ในอีกความหมายหนึ่ง อาจหมายถึงเรื่องที่ประชาชนในชาติอาจถูกครอบงำทางเทคโนโลยีโดยเจ้าของแพลตฟอร์มที่ประชาชนนิยมใช้ โดยไม่รู้ตัวและรัฐบาลในประเทศนั้นไม่สามารถบริหาร จัดการได้ทำให้เกิดผลกระทบทางลบต่อเศรษฐกิจ สังคม และความมั่นคงของชาติในระยะยาว

บทที่ 2
การทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง

ทฤษฎีและแนวคิดในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศ

The Global Cybersecurity Capacity Centre (GCSCC) แห่ง University of Oxford[1] ประเทศสหราชอาณาจักร ได้จัดทำคู่มือกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cyber security capacity maturity model : CMM) ซึ่งเป็นคู่มือในการประเมินศักยภาพและขีดความสามารถในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ เพื่อช่วยเพิ่มขีดความสามารถด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศให้เป็นระบบ มีประสิทธิผล เป็นที่ยอมรับในระดับสากล ทั้งนี้ ปัจจุบัน GCSCC ได้นำ CMM มาใช้ในการประเมินความสามารถด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์มาแล้วกว่า 100 ประเทศทั่วโลก

กรอบการประเมินขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศตามแนวคิดของ CMM แบ่งหมวดหมู่ของขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ออกได้ 5 มิติ โดยมีรายละเอียด (แผนภาพที่ 2-1) ดังนี้

มิติที่ 1 National cybersecurity framework and policy เป็นขีดความสามารถในการพัฒนานโยบาย และยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ การบริหารจัดการในภาวะวิกฤต การปกป้องโครงสร้างพื้นฐานที่สำคัญ การเตือนภัยล่วงหน้า การฟื้นฟูหรือซ่อมแซมความเสียหาย รวมถึงความสามารถในการพัฒนานโยบายความมั่นคงที่มีประสิทธิภาพในการป้องป้องและทนทานต่อภัยคุกคาม

มิติที่ 2 Cyber culture and society เป็นขีดความสามารถด้านความรู้ความเข้าใจของประชาชนในเรื่องความเชื่อมั่นต่อบริการอินเทอร์เน็ต บริการอิเล็กทรอนิกส์ของภาครัฐ และพาณิชย์อิเล็กทรอนิกส์ และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนโลกออนไลน์ ความเข้าใจของประชาชนในเรื่องความเสี่ยงที่เกี่ยวข้องกับโลกไซเบอร์ต่าง ๆ กลไกการให้ผู้ใช้งาน

---

[1] Global Cyber Security Capacity Centre. Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition. University of Oxford., 2016.

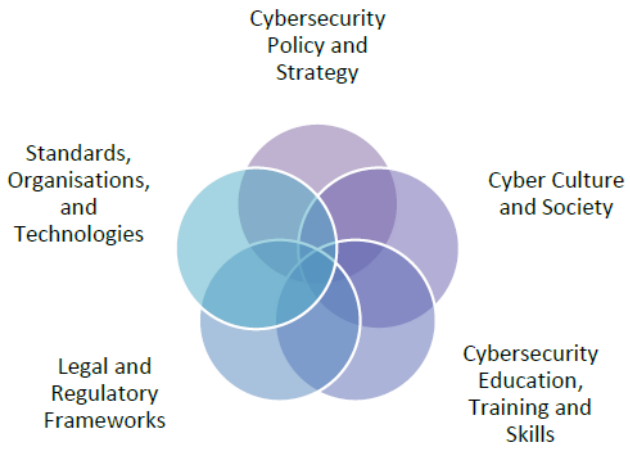
รายงานอาชญากรรมทางไซเบอร์ รวมถึงบทบาทของเครือข่ายสังคมออนไลน์ต่อการเปลี่ยนแปลงทัศนคติ และพฤติกรรมของผู้ใช้งาน

มิติที่ 3 Cybersecurity education, training and skills เป็นขีดความสามารถด้านความตระหนักรู้ (Awareness) ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ของภาครัฐ ภาคเอกชน และประชาชนทั่วไป ตลอดจนการเข้าถึงและคุณภาพของการให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชนและประชาชนทั่วไป

มิติที่ 4 Legal and regulatory frameworks เป็นขีดความสามารถในการออกแบบและบังคับใช้กฎหมาย รวมถึงการตัดสินคดีความที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ทั้งในด้านความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัว (Privacy protection) ถือว่าเป็นอีกมิติที่มีความจำเป็นต้องพัฒนาเพื่อให้เท่าทันการเปลี่ยนแปลงทางดิจิทัล (Digital transformation) ที่กำลังเกิดขึ้นและส่งผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วโลก

มิติที่ 5 Standards, organizations, and technologies เป็นขีดความสามารถด้านการใช้เทคโนโลยีที่มีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ให้กับประชาชนทั่วไป องค์กร โครงสร้างพื้นฐานของประเทศ มาตรฐานและการถอดบทเรียนจากกรณีศึกษาที่ดีด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

แผนภาพที่ 2-1 ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ 5 มิติ ตามแนวคิด CMM



ที่มา : The Global Cybersecurity Capacity Centre แห่ง University of Oxford

จากขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ทั้ง 5 มิติข้างต้น ในแต่ละมิติมีส่วนที่ทับซ้อนกัน แสดงถึงความสัมพันธ์ระหว่างขีดความสามารถแต่ละมิติ โดยในแต่ละขีดความสามารถประกอบด้วยปัจจัย (Factor) คุณลักษณะ (Aspects) ระยะของการขับเคลื่อน (Stages of maturity) และตัวชี้วัด (Indicator) โดยมีความหมายสรุปได้ (แผนภาพที่ 2-2) ดังนี้

มิติ (Dimension) แสดงถึง หมวดหมู่ของขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

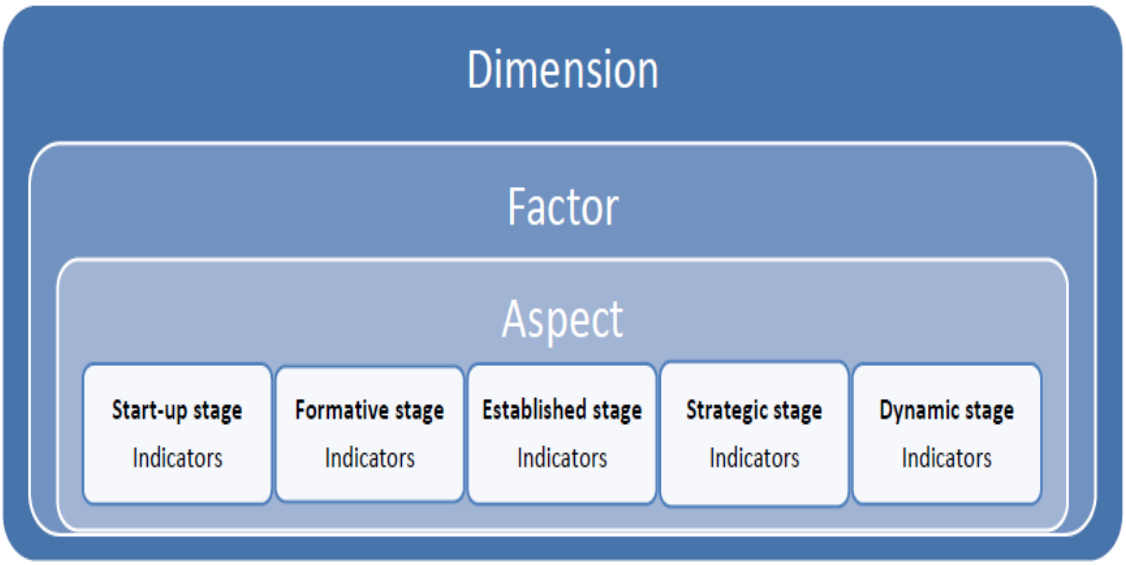
ปัจจัย (Factor) แสดงถึง คุณลักษณะของขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ เป็นองค์ประกอบที่ใช้ในการพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ รายการปัจจัยทั้งหมดสะท้อนถึงภูมิทัศน์ของขีดความสามารถความมั่นคงปลอดภัยไซเบอร์ภายใต้มิตินั้น ๆ การกำหนดรายการปัจจัยทำได้จากการทบทวนและเรียนรู้จากประสบการณ์ ภายในปัจจัยประกอบด้วยกลุ่มของคุณลักษณะ (Aspects) ซึ่งเป็นการจัดหมวดหมู่ของปัจจัย

คุณลักษณะ (Aspect) แสดงถึง การจัดกลุ่มของปัจจัยให้อยู่ในหมวดหมู่ของคุณลักษณะ จะช่วยให้สามารถจัดกลุ่มของตัวชี้วัดที่สามารถเข้าใจได้ง่ายมากขึ้น

ระยะของการขับเคลื่อน (Stages of maturity) แสดงถึง ลำดับของความก้าวหน้าในการพัฒนาขีดความสามารถในแต่ละกลุ่มปัจจัยและคุณลักษณะ โดย CMM แบ่งระยะเวลาของการขับเคลื่อนออกเป็น 5 ระยะ

ตัวชี้วัด (Indicator) แสดงถึง ขั้นตอน ปฏิบัติการ หรือองค์ประกอบ ที่บ่งชี้ถึงระยะของการขับเคลื่อนภายใต้มิติ ปัจจัย และคุณลักษณะต่าง ๆ ประเทศต้องบรรลุเป้าหมายของทุกตัวชี้วัดในมิติ ปัจจัย และคุณลักษณะนั้น ๆ เพื่อเพิ่มขีดความสามารถของประเทศ ตัวชี้วัดส่วนใหญ่มีค่าได้ 2 รูปแบบ เช่น สำเร็จ ไม่สำเร็จ เป็นต้น

แผนภาพที่ 2-2 ระยะของการขับเคลื่อน (Stages of maturity) แสดงถึงลำดับของความก้าวหน้าในการพัฒนาขีดความสามารถในแต่ละกลุ่มปัจจัยและคุณลักษณะ โดย CMM แบ่งระยะเวลาของการขับเคลื่อนออกเป็น 5 ระยะ



ที่มา : The Global Cybersecurity Capacity Centre แห่ง University of Oxford

นอกจากนี้ กรอบแนวคิดของ CMM ได้แบ่งระยะของการกำหนดยุทธศาสตร์ (Stage of Maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ ออกเป็น 5 ระยะ (แผนภาพที่ 2-3) ดังนี้

ระยะที่ 1 Start-up เป็นระดับที่เพิ่งเริ่มอภิปรายเกี่ยวกับแนวทางการสร้างขีดความสามารถ (Capacity building) ในการดูแลความมั่นคงปลอดภัยทางไซเบอร์ แต่ยังไม่เริ่มดำเนินการ ตัวอย่างเช่น การเริ่มอภิปรายเกี่ยวกับความตระหนักรู้ทางไซเบอร์ แต่ยังไม่ทราบถึงความจำเป็นของความตระหนักรู้อย่างชัดเจน เป็นต้น

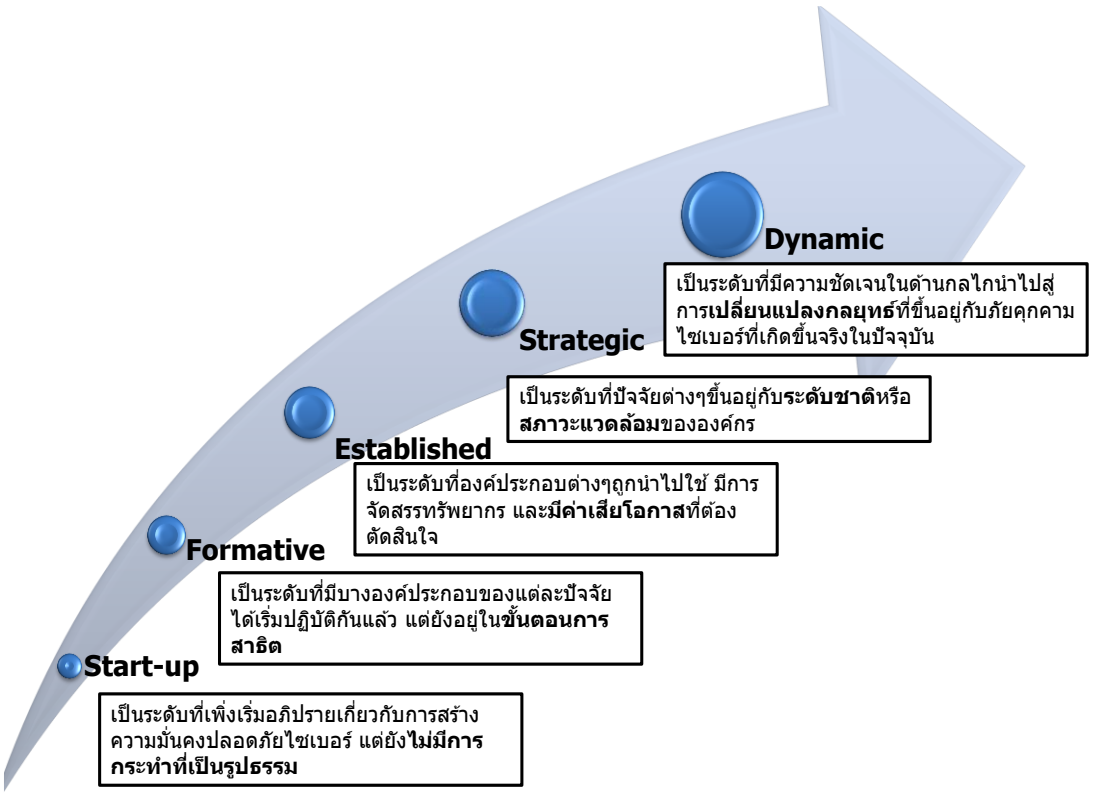
ระยะที่ 2 Formative เป็นระดับที่เริ่มปรากฏแนวทางที่ชัดเจนแล้ว แต่ยังไม่จัดเป็นระเบียบหรือไม่เป็นหมวดหมู่ ตัวอย่างเช่น การสร้างโครงการเพิ่มความตระหนักรู้ทางไซเบอร์ผ่านการอบรมพัฒนาบุคลากร โดยกำหนดกลุ่มเป้าหมายเฉพาะเจาะจง แต่โครงการยังไม่เชื่อมโยงกับยุทธศาสตร์ชาติ เป็นต้น

ระยะที่ 3 Established เป็นระดับที่เริ่มดำเนินการตามแนวทางแล้ว อยู่ในขั้นตอนของการตัดสินใจทางเลือกต่าง ๆ และจัดสรรทรัพยากร ตัวอย่างเช่น โครงการเพิ่มความตระหนักรู้ทางไซเบอร์มีหน่วยงานรับผิดชอบชัดเจนแล้ว และขยายกลุ่มเป้าหมายออกไปในวงกว้าง และเริ่มประสานขอความร่วมมือกับภาคส่วนต่าง ๆ เป็นต้น

ระยะที่ 4 Strategic เป็นระดับที่มีการจัดลำดับความสำคัญของแนวทางว่าอยู่ในระดับองค์กรหรือระดับชาติ ตัวอย่างเช่น โครงการเพิ่มความตระหนักรู้ทางไซเบอร์อยู่ในระยะที่ได้รับการบูรณาการความร่วมมือจากภาคส่วนต่าง ๆ ในประเทศ เป็นต้น

ระยะที่ 5 Dynamic เป็นระดับที่มีความชัดเจนในด้านกลไกที่จะนำไปสู่การเปลี่ยนแปลงยุทธศาสตร์ ซึ่งขึ้นอยู่กับภัยคุกคามไซเบอร์ที่เกิดขึ้นจริงในปัจจุบัน ตัวอย่างเช่น โครงการเพิ่มความตระหนักรู้ทางไซเบอร์อยู่ในระยะที่ทำให้เกิดการจัดสรรทรัพยากรและการลงทุนครั้งใหม่ สามารถเห็นผลกระทบจากการสร้างความตระหนักรู้ทางไซเบอร์อย่างชัดเจน เป็นต้น

แผนภาพที่ 2-3 ระยะของการกำหนดยุทธศาสตร์



ที่มา : The Global Cybersecurity Capacity Centre แห่ง University of Oxford

หลักการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของต่างประเทศ

1. ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศที่ต้องเผชิญกับความท้าทายทางไซเบอร์ทั้งจากผู้ก่อการร้าย และประเทศมหาอำนาจอื่น เช่น รัสเซีย จีน อิหร่าน และเกาหลีเหนือ นับตั้งแต่ปี 2546 ซึ่งสำนักงานความมั่นคงปลอดภัยและโครงสร้างพื้นฐานทางไซเบอร์ (Cybersecurity and infrastructure security agency : CISA) กระทรวงความมั่นคงแห่งมาตุภูมิ มีการจัดทำยุทธศาสตร์ชาติด้านการรักษาความมั่นคงปลอดภัยของโลกไซเบอร์สเปซ (National strategy to secure cyberspace)[2] หลังจากเกิดเหตุการณ์วินาศกรรมเมื่อวันที่ 11 กันยายน 2544 เป็นระยะเวลาถึง

[2] สำนักงานความมั่นคงปลอดภัยและโครงสร้างพื้นฐานทางไซเบอร์ (Cybersecurity and Infrastructure Security Agency : CISA) **The National Strategy to secure Cyberspace.** February 2003.

15 ปี ที่ประเทศสหรัฐอเมริกาไม่ได้ปรับปรุงยุทธศาสตร์ความมั่นคงด้านไซเบอร์ ในขณะที่ภัยคุกคามทางไซเบอร์เพิ่มขึ้นทวีคูณ จนกระทั่งในปี 2561 ทำเนียบขาว ประเทศสหรัฐอเมริกา[3] ได้เผยแพร่ยุทธศาสตร์ไซเบอร์ของประเทศ (National cyber strategy) ประกอบด้วยเสาหลัก 4 ด้าน ได้แก่ 1. เสาหลักที่ 1 การปกป้องผืนแผ่นดินและวิถีชีวิตของอเมริกันชน (Protect the American people, the homeland, and the American way of life) 2. เสาหลักที่ 2 การเสริมสร้างความมั่งคั่งของอเมริกา (Promote American prosperity) 3. เสาหลักที่ 3 การรักษาสันติภาพด้วยพลัง (Preserve peace through strength) และ 4. เสาหลักที่ 4 การขยายอิทธิพลของสหรัฐอเมริกา (Advance American influence) โดยมีสาระสำคัญ ดังนี้

1.1 เสาหลักที่ 1 การปกป้องผืนแผ่นดินและวิถีชีวิตของอเมริกันชน (Protect the American people, the homeland, and the American way of life)

1.1.1 การรักษาความมั่นคงปลอดภัยให้กับเครือข่ายกิจการโทรทัศน์ และกิจการโทรคมนาคมของสหพันธรัฐ และข้อมูลของสหพันธรัฐ (Secure federal networks and information) โดยการกำหนดมาตรฐานในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ และการรวมศูนย์การสั่งการและมอบหมายหน้าที่ความรับผิดชอบ รวมถึงกำกับดูแลภาพรวมการทำงานของหน่วยงานที่เกี่ยวข้อง

1.1.2 การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Secure critical infrastructure) โดยการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐาน การกระจายและจัดสรรความเสี่ยงระหว่างภาครัฐและภาคเอกชนในลักษณะของการร่วมลงทุนระหว่างภาครัฐและเอกชน (PPPs) การจัดลำดับความสำคัญของปฏิบัติการ (Consequence-driven) ที่ลดความรุนแรงและความยาวนานของการหยุดชะงักของโครงสร้างพื้นฐาน

1.1.3 การรับมืออาชญากรรมทางไซเบอร์และการพัฒนาการรายงานอุบัติการณ์ (Combat cybercrime and improve incident reporting) โดยอาศัยความร่วมมือระหว่างมลรัฐ ท้องถิ่น ชนเผ่า และเขตแดน ในการตรวจตรา ป้องกัน ต่อต้าน และสืบสวนสอบสวนเกี่ยวกับภัยคุกคามทางไซเบอร์ต่อประเทศสหรัฐ

1.2 เสาหลักที่ 2 การเสริมสร้างความมั่งคั่งของอเมริกา (Promote American prosperity)

---

[3] White Hourse. (2018). **National Cyber Strategy of the United States of America.**

1.2.1 พัฒนาเศรษฐกิจดิจิทัลให้มีความมั่นคั่งและมีความทนทานต่อภัยคุกคามทางไซเบอร์ (Foster a vibrant and resilient digital economy) โดยการสนับสนุนการกำหนดมาตรฐานของการรักษาความมั่นคงปลอดภัยทางเศรษฐกิจ ตลาดกลางการพาณิชย์ (Marketplace) และนวัตกรรม

1.2.2 พัฒนาและคุ้มครองทรัพย์สินทางปัญญาของประเทศสหรัฐอเมริกา (Foster and protect United States ingenuity) โดยการคุ้มครองสิ่งประดิษฐ์ เทคโนโลยี และนวัตกรรมของประเทศสหรัฐอเมริกาจากการจารกรรมทรัพย์สินทางปัญญา รวมถึงการผลักดันบทบาทผู้นำด้านเทคโนโลยี เช่น ปัญญาประดิษฐ์ (Artificial intelligence: AI) วิทยาศาสตร์ข้อมูลควอนตัม (Quantum information science) และโครงสร้างพื้นฐานโทรคมนาคมสำหรับอนาคต (Next generation telecommunication infrastructure) เป็นต้น

1.2.3 พัฒนากำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เหนือกว่า (Develop a superior cybersecurity workforce) โดยพัฒนาศูนย์รวมบุคลากรมากความสามารถ (Talent pool) และดึงดูดผู้เชี่ยวชาญจากต่างประเทศ

1.3 เสาหลักที่ 3 การรักษาสันติภาพด้วยพลัง (Preserve peace through strength)

1.3.1 สร้างเสถียรภาพทางไซเบอร์ผ่านพฤติกรรมความรับผิดชอบของรัฐที่เป็นบรรทัดฐานทางสังคม (Enhance cyber stability through norms of responsible state Behavior) ผ่านกรอบความรับผิดชอบของรัฐภายใต้กฎหมายระหว่างประเทศ การสร้างความเชื่อมั่นต่อความสามารถในการลดความเสี่ยงจากกิจกรรมไซเบอร์ที่มีความประสงค์ร้าย

1.3.2 หยุดยั้งพฤติกรรมที่ไม่เหมาะสมในโลกไซเบอร์สเปซ (Attribute and deter unacceptable behavior in cyberspace) กิจกรรมไซเบอร์ที่เป็นภัยต่อประเทศสหรัฐอเมริกาด้วยวิธีการทางการฑูต การข่าวสาร การทหาร การเงิน การข่าวกรอง และการบังคับใช้กฎหมาย

1.4 เสาหลักที่ 4 การขยายอิทธิพลของสหรัฐอเมริกา (Advance American influence)

1.4.1 สนับสนุนเสรีภาพบนระบบอินเทอร์เน็ต เชื่อมโยงกันได้ เชื่อถือได้ และมั่นคงปลอดภัย (Promote an open, interoperable, reliable, and secure internet) ซึ่งเป็นส่วนหนึ่งของหลักสิทธิมนุษยชน และเสรีภาพขั้นพื้นฐาน และป้องกันการใช้อินเทอร์เน็ตเสรีเป็นเครื่องมือทางการเมือง โดยยึดมั่นในหลักการนี้ให้เป็นมาตรฐานระดับสากล

1.4.2 สร้างขีดความสามารถไซเบอร์ระหว่างประเทศ (Build international cyber capacity) โดยส่งเสริมการพัฒนาขีดความสามารถไซเบอร์ให้ประเทศพันธมิตร เพื่อให้ประเทศพันธมิตรสามารถปกป้องตนเองได้ และสามารถสนับสนุนประเทศสหรัฐอเมริกาในการรับมือกับปัญหาภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ แลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์กับประเทศพันธมิตร

เพื่อป้องกันโครงสร้างพื้นฐานที่สำคัญยิ่งยวดและห่วงโซ่อุปทานของโลก รวมถึงขยายความร่วมมือทางด้านการฑูต การเศรษฐกิจ และความมั่นคงปลอดภัย

2. ประเทศสหราชอาณาจักร

รัฐบาลสหราชอาณาจักร[4] ได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ปี 2559 – 2564 (National cyber security strategy 2016 – 2021) ในปี 2559 โดยมีเป้าประสงค์หลัก 3 ด้าน ได้แก่ การป้องกัน (Defend) การยับยั้ง (Deter) และการพัฒนา (Develop) ในส่วนของการป้องกัน หมายถึง การป้องกันสหราชอาณาจักรจากภัยคุกคามทางไซเบอร์ การรับมือกับอุบัติการณ์ เพื่อให้ระบบเครือข่าย ระบบข้อมูล ธุรกิจ และประชาชน ได้รับความปลอดภัยและสามารถป้องกันตนเองได้ การยับยั้ง หมายถึง การตรวจสอบ ทำความเข้าใจ สืบสวนสอบสวน และหยุดยั้งกิจกรรมที่ประสงค์ร้ายต่อสหราชอาณาจักร ติดตามและลงโทษผู้กระทำความผิด และการพัฒนา หมายถึง การสร้างนวัตกรรม การวิจัย และพัฒนา เพื่อตอบสนองความต้องการของประเทศ และความพร้อมรับมือภัยคุกคามและความท้าทายในอนาคต ทั้งนี้ แผนยุทธศาสตร์จำแนกออกตามเป้าประสงค์หลัก 3 ด้าน สรุปได้ ดังนี้

2.1 การป้องกัน (Defend)

2.1.1 การพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์ (Active cyber defence : ACD) โดยสร้างความทนทานต่อการโจมตีทางไซเบอร์ ความเข้าใจต่อภัยคุกคามทางไซเบอร์ และการรับมือกับภัยคุกคามทางไซเบอร์

2.1.2 การรักษาความมั่นคงปลอดภัยของระบบอินเทอร์เน็ต (Building a more secure internet) โดยสร้างความมั่นใจว่า การพัฒนาเทคโนโลยีใหม่ต้องมีความมั่นคงปลอดภัยเป็นค่าตั้งต้น (Secure by default) และมีระบบรักษาความปลอดภัยทั้งซอฟต์แวร์และฮาร์ดแวร์

2.1.3 การคุ้มครองข้อมูลภาครัฐ (Protecting government) ในทุกหน่วยงานและทุกระดับของหน่วยงานภาครัฐ เพื่อรักษาความเชื่อมั่นของประชาชนต่อระบบและบริการของภาครัฐ

2.1.4 การคุ้มครองโครงสร้างพื้นฐานของประเทศที่สำคัญยิ่งยวดและภาคส่วนเศรษฐกิจที่มีความสำคัญยิ่งยวด (Protecting our critical national infrastructure and other priority sectors) ซึ่งมีผลกระทบต่อวิถีชีวิตของประชาชน ระบบเศรษฐกิจ ชื่อเสียงและจุดยืนของประเทศในเวทีโลก

---

[4] HM Government. **National Cyber Strategy 2016-2021.**

2.1.5 การพัฒนาพฤติกรรมของภาคธุรกิจและประชาชน (Changing public and business behaviours) ให้มีความตระหนักรู้ และความเข้าใจต่อภัยคุกคามไซเบอร์

2.1.6 การบริหารจัดการอุบัติการณ์และความเข้าใจต่อภัยคุกคามไซเบอร์ (Managing incidents and understanding the threat) โดยกำหนดกระบวนการสร้างความร่วมมือในภาวะที่เกิดภัยคุกคามไซเบอร์ระหว่างภาครัฐและเอกชน เพื่อให้มั่นใจว่า มีการจัดเก็บข้อมูล แลกเปลี่ยนข้อมูล อย่างรวดเร็วและทันการณ์

2.2 การยับยั้ง (Deter)

2.2.1 การป้องปรามในโลกไซเบอร์ (Cyber's role in deterrence) จากการรุกรานทางไซเบอร์และอธิปไตย (Sovereignty) ของประเทศ โดยสร้างความเข้มแข็งให้ประเทศจนโจมตีได้ยาก ลดผลประโยชน์ และเพิ่มต้นทุนของการโจมตีทางไซเบอร์ไม่ว่าจะเป็นการโจมตีที่มีเป้าหมายทางด้านการเมือง เป้าหมายทางการฑูต เป้าหมายทางเศรษฐกิจ หรือเป้าหมายเชิงยุทธศาสตร์

2.2.2 การลดอาชญากรรมทางไซเบอร์ (Reducing cyber crime) โดยเพิ่มต้นทุนในการโจมตีทางไซเบอร์ ลดผลประโยชน์จากการโจมตีทางไซเบอร์ ลดความเปราะบางต่อการถูกโจมตีทางไซเบอร์ และติดตามจับกุมอาชญากรที่โจมตีสหราชอาณาจักร

2.2.3 การรับมือผู้ประสงค์ร้ายจากภายนอกประเทศ (Countering hostile foreign actors) ที่พุ่งเป้าหมายโจมตีการเมือง เศรษฐกิจ และความมั่นคงทางการทหารของประเทศ

2.2.4 การป้องกันการก่อการร้าย (Preventing terrorism) โดยการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ และป้องกันการถูกโจมตีผ่านการเฝ้าระวัง ติดตามสืบสวนสอบสวน ร่วมงานกับประเทศพันธมิตรในการจับกุมผู้ก่อการร้ายทางไซเบอร์

2.2.5 การพัฒนาขีดความสามารถด้านอธิปไตยไซเบอร์เชิงรุก (Enhancing sovereign capabilities – offensive cyber) โดยการโจมตีเครือข่ายหรือระบบของผู้ประสงค์ร้าย ทำลายโอกาสในการโจมตีทางไซเบอร์ และมีการพัฒนาขีดความสามารถในการปฏิบัติการเชิงรุก

2.2.6 การพัฒนาขีดความสามารถด้านอธิปไตยการเข้ารหัสข้อมูล (Enhancing sovereign capabilities – cryptography) โดยอาศัยทักษะและเทคโนโลยีของภาคเอกชนที่มีขีดความสามารถสูง

2.3 การพัฒนา (Develop)

2.3.1 การพัฒนาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์ (Strengthening cyber security skills) โดยการพัฒนาบุคลากรและผู้เชี่ยวชาญให้มีเส้นทางการเจริญก้าวหน้าในสายอาชีพอย่างชัดเจน

2.3.2 การกระตุ้นการเจริญเติบโตในภาคส่วนการรักษาความมั่นคงปลอดภัยไซเบอร์ (Stimulating growth in the cyber security sector) โดยสนับสนุนให้ผู้ที่มีแนวคิดในการผลิตนวัตกรรม โดยเฉพาะวิสาหกิจขนาดกลางและขนาดย่อม (Small and medium enterprises : SMEs) ให้สามารถเข้าถึงเงินทุน และสามารถเพิ่มทักษะความรู้ด้านเทคโนโลยีได้

2.3.3 การสนับสนุนวิทยาการและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ (Promoting cyber security science and technology) ทั้งในด้านการวิจัยและพัฒนา และด้านวิชาการ เพื่อดึงดูดผู้มีความรู้ความสามารถให้เข้าสู่ภาคส่วนเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์

2.3.4 การเฝ้าติดตามและวิเคราะห์การเปลี่ยนแปลงของเทคโนโลยี (Effective horizon scanning) โดยการคาดการณ์ภัยคุกคามในอนาคต ในช่วงระยะ 5 – 10 ปีข้างหน้า การคาดการณ์ผลกระทบจากภัยคุกคามที่อาจจะเกิดขึ้น รวมถึงเสนอแนะเพื่อกำหนดนโยบายและแผนการรับมือภัยคุกคามที่อาจจะเกิดขึ้นในอนาคต

ทั้งนี้ สำนักงานคณะรัฐมนตรี ประเทศสหราชอาณาจักร[5] ได้เผยแพร่รายงานความก้าวหน้าของการขับเคลื่อนยุทธศาสตร์ ในปี 2561 โดยพบความก้าวหน้าของการขับเคลื่อนแผนเชิงยุทธศาสตร์ 13 เรื่อง ได้แก่ 1. ความเข้าใจในภัยคุกคามไซเบอร์ (Understanding the threat) 2. การรับมือกับอาชญากรรมไซเบอร์ (Tackling cyber crime) 3. การรับมือกับอุบัติการณ์ไซเบอร์ (Responding to cyber incidents) 4. ระบบป้องกันการโจมตีทางไซเบอร์ (Active cyber defence) 5. การสร้างความปลอดภัยทางเทคโนโลยีด้วยการออกแบบ (Making technology secure by design) 6. การพัฒนาความมั่นคงปลอดภัยไซเบอร์ของรัฐบาล (Improving the cyber security of government) 7. การบริหารจัดการความเสี่ยงไซเบอร์ในระบบเศรษฐกิจและสังคม (Managing cyber risk in the wider economy and society) 8. การบริหารจัดการความเสี่ยงไซเบอร์ในโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทศ (Managing cyber risk in critical national infrastructure) 9. การพัฒนาภาคส่วนความมั่นคงปลอดภัยไซเบอร์ (Developing the cyber security sector) 10. การพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ (Developing the cyber security skills pipeline) 11. การวางแผนการวิจัยและพัฒนา (Research, development and future planning) 12. การผลักดันประเด็นปัญหาความมั่นคงปลอดภัยไซเบอร์ในเวทีระหว่างประเทศ (International action)และ 13. การสร้างการทำงานของหน่วยงานภาครัฐให้เป็นไปในทิศทางเดียวกัน (Strengthening our whole-of-Government approach)

---

[5] Cabinet Office (2019). **National Cyber Security Strategy Progress Report 2016 – 2021.**

3. ประเทศสิงคโปร์

หน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติแห่งสิงคโปร์ (Cyber security agency of Singapore : CSA)[6] ได้เผยแพร่ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ในปี 2559 โดยกำหนดให้ยุทธศาสตร์ประกอบด้วย 4 เสาหลัก ได้แก่ 1. การสร้างโครงสร้างพื้นฐานที่มีความทนทานต่อภัยคุกคามทางไซเบอร์ (Building resilient infrastructure) 2. การสร้างโลกไซเบอร์สเปซที่ปลอดภัยยิ่งขึ้น (Creating a safer cyberspace) 3. การพัฒนาระบบนิเวศของความมั่นคงปลอดภัยไซเบอร์ (Developing a vibrant cybersecurity ecosystem) และ 4. การสร้างความร่วมมือระหว่างประเทศ (Strengthening international partnership) โดยมีสาระสำคัญ ดังนี้

3.1 การสร้างโครงสร้างพื้นฐานที่มีความทนทานต่อภัยคุกคามทางไซเบอร์ (Building resilient infrastructure)

3.1.1 การปกป้องบริการที่สำคัญยิ่งยวด (Protect our essential services) โดยการจัดทำกระบวนการบริหารจัดการความเสี่ยง การสร้างวัฒนธรรมความตระหนักรู้ถึงความเสี่ยง การเพิ่มแนวปฏิบัติความมั่นคงด้วยการออกแบบ (Secure by design) ตลอดทั้งห่วงโซ่อุปทานของการให้บริการ

3.1.2 การเพิ่มขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์อย่างเด็ดขาด (Respond decisively to cyber threats) โดยการสร้างความตระหนักรู้ต่อเหตุการณ์ การฝึกซ้อมแผนรับมือด้วยการจำลองสถานการณ์ที่ซับซ้อน และเกี่ยวโยงหลายภาคส่วน การเพิ่มทีม CIRT การเพิ่มประสิทธิภาพแผนฟื้นฟูภัยพิบัติ (Recovery plans) และแผนบริหารความต่อเนื่องทางธุรกิจ (Business continuity plans : BCP)

3.1.3 การสร้างความเข้มแข็งของโครงสร้างทางกฎหมายและการกำกับดูแลของภาครัฐ (Strengthen governance and legislative framework) โดยบัญญัติกฎหมายความมั่นคงปลอดภัยไซเบอร์ฉบับใหม่ที่กำหนดให้ผู้ให้บริการและเจ้าของโครงสร้างพื้นฐานที่สำคัญยิ่งยวดมีภาระความรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ สนับสนุนการแลกเปลี่ยนข้อมูลภัยคุกคาม ความร่วมมือของทุกภาคส่วนอย่างใกล้ชิดเพื่อแก้ไขเหตุการณ์อย่างทันการณ์

3.1.4 การรักษาความปลอดภัยให้กับเครือข่ายของรัฐบาล (Secure government networks) โดยการกำหนดสัดส่วนงบประมาณด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ที่ร้อยละ 8 ของวงเงินงบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสาร การลดการโจมตีเครือข่ายของรัฐบาล การสร้างความตระหนักรู้ต่อเหตุการณ์ในหน่วยงานภาครัฐ

---

[6] Cyber Security Agency of Singapore. (2016). **Singapore's Cybersecurity Strategy.**

3.2 การสร้างโลกไซเบอร์สเปซที่ปลอดภัยยิ่งขึ้น (Creating a safer cyberspace)

3.2.1 การต่อสู้กับอาชญากรรมทางไซเบอร์ (Combat cybercrime) โดยแผนปฏิบัติการระดับชาติ ที่เพิ่มองค์ความรู้ เพิ่มขีดความสามารถรับมือให้กับหน่วยงานภาครัฐ พัฒนากรอบกฎหมายในการตัดสินคดีอาชญากรรมทางไซเบอร์ และสร้างความร่วมมือระหว่างประเทศ

3.2.2 การพัฒนาสู่การเป็นศูนย์กลางแห่งความเชื่อมั่น (Enhance Singapore's standing as a trusted hub) โดยการสร้างระบบนิเวศของข้อมูลที่เชื่อถือได้ ทั้งต่อผู้ใช้งานข้อมูลและหน่วยงานที่ให้บริการข้อมูล การพัฒนาเจ้าหน้าที่คุ้มครองข้อมูลที่มีความเชี่ยวชาญ หมายรวมถึงการใช้งานข้อมูลข้ามประเทศด้วย (Cross border data) การสร้างความร่วมมือกับประเทศพันธมิตร รัฐบาลอื่น อุตสาหกรรมที่เป็นพันธมิตร ผู้ให้บริการอินเทอร์เน็ต องค์กรระหว่างประเทศ เพื่อสร้างอินเทอร์เน็ตที่สามารถตรวจพบภัยคุกคามได้รวดเร็ว และลดกิจกรรมที่ประสงค์ร้าย

3.2.3 การสนับสนุนความรับผิดชอบต่อส่วนรวม (Promote collective responsibility) โดยภาคธุรกิจและประชาชนต้องมีความพร้อมรับข่าวสารเพื่อป้องกันระบบคอมพิวเตอร์ และอุปกรณ์ดิจิทัลของตนเองจากผู้ประสงค์ร้ายที่อาจจารกรรมระบบหรืออุปกรณ์เพื่อใช้ในการคุกคามสังคมและภาคธุรกิจ

3.3 การพัฒนาระบบนิเวศของความมั่นคงปลอดภัยไซเบอร์ (Developing a vibrant cybersecurity ecosystem)

3.3.1 การสร้างกำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่มีความเชี่ยวชาญ (Establish a professional cybersecurity workforce) โดยสร้างเส้นทางการเจริญก้าวหน้าในสายอาชีพที่ชัดเจน สนับสนุนการให้ใบรับรองที่เป็นที่ยอมรับในระดับสากล การให้ทุนการศึกษา หลักสูตรการศึกษาเฉพาะอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ การพัฒนาทักษะที่มีอยู่เดิม (Up-skilling) และการเรียนรู้ทักษะใหม่ (Re-skilling)

3.3.2 การสร้างความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์ (Extend Singapore's cybersecurity advantage) ผ่านการสร้างความเข้มแข็งของท้องถิ่น และฐานรากโดยเฉพาะกลุ่มผู้ประกอบการหน้าใหม่ (Start-up) ด้วยการเพิ่มโอกาสทางการตลาด การสร้างแบรนด์ผลิตในประเทศสิงคโปร์ให้ติดตลาดโลก

3.3.3 การสร้างนวัตกรรมเพื่อเร่งการพัฒนา (Innovate to accelerate) โดยอาศัยความพร้อมด้านสิ่งอำนวยความสะดวกด้านการวิจัยและพัฒนาที่ได้มาตรฐานระดับโลก การพัฒนาบุคลากรผู้มีความสามารถโดดเด่น การสร้างความร่วมมือในการวิจัยและพัฒนาระหว่างภาครัฐ ภาคเอกชน ภาควิชาการ และภาคอุตสาหกรรม

3.4 การสร้างความร่วมมือระหว่างประเทศ (Strengthening international partnership)

3.4.1 การสร้างความร่วมมือระดับภูมิภาคอาเซียนและความร่วมมือระหว่างประเทศเพื่อรับมือกับภัยคุกคามไซเบอร์และอาชญากรรมทางไซเบอร์ (Forge international and ASEAN cooperation to counter cyber threats and cybercrime) โดยเพิ่มประสิทธิภาพให้กับกระบวนการรายงานและการรับมือ การอาศัยความร่วมมือกับเครือข่ายการทำงานขององค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol) และการพัฒนาขีดความสามารถในการรับมือกับอาชญากรรมทางไซเบอร์

3.4.2 การริเริ่มสร้างขีดความสามารถด้านไซเบอร์ระดับยอดเยี่ยมของภูมิภาคอาเซียนและระดับสากล (Champion international and ASEAN cyber capacity building initiatives) ในด้านปฏิบัติการ เทคนิค กฎหมาย นโยบาย และการทูต

3.4.3 การแลกเปลี่ยนเรียนรู้ประสบการณ์ในด้านการบังคับใช้กฎหมายและบรรทัดฐานไซเบอร์ของภูมิภาคและระดับสากล (Facilitate international and regional exchanges on cyber norms and legislation)

กรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

1. กรอบแนวคิดการพัฒนายุทธศาสตร์ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU)

สหภาพโทรคมนาคมระหว่างประเทศ (ITU)[7] ได้ร่วมกับธนาคารโลก (World bank) สำนักเลขาธิการประเทศเครือจักรภพ (Commonwealth secretariat : ComSec) องค์กรโทรคมนาคมประเทศเครือจักรภพ (Commonwealth telecommunication organization: CTO) องค์การนาโต (NATO) หน่วยงานความมั่นคงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของนาโต (Cooperative cyber defence centre of excellence: CCD COE) องค์กรระหว่างประเทศ และบริษัทที่ปรึกษาจากภาคเอกชนชั้นนำ ในการจัดทำและเผยแพร่คู่มือกรอบแนวคิดในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) สำหรับผู้นำประเทศและผู้กำหนดนโยบาย ในปี 2561

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) มีลักษณะสำคัญ ดังนี้

---

[7] International Telecommunication Union. (2018). **Guide to Developing a National Cybersecurity Strategy.** Strategic engagement in cybersecurity.

• การแสดงถึงวิสัยทัศน์ เป้าหมายสูงสุด หลักการ และลำดับความสำคัญของประเด็นที่จะขับเคลื่อนประเทศให้พ้นจากปัญหาความมั่นคงปลอดภัยไซเบอร์

• ภาพรวมของผู้มีส่วนเกี่ยวข้องกับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศและบทบาทหน้าที่ความรับผิดชอบของแต่ละภาคส่วน

• รายละเอียดของขั้นตอน โครงการ ความคิดริเริ่ม (Initiatives) ของประเทศในการปกป้องโครงสร้างพื้นฐานทางไซเบอร์ของประเทศ และการยกระดับความปลอดภัยและความทนทานทางไซเบอร์

ในส่วนของสาระสำคัญของคู่มือกรอบแนวคิดได้แบ่งองค์ประกอบที่สำคัญออกเป็น 3 ส่วน ได้แก่ 1) ขั้นตอนของการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ 2) ลักษณะที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 3) แนวปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเนื้อหาที่สำคัญ ดังนี้

1.1 ขั้นตอนของการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ

คู่มือกรอบแนวคิดในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) เสนอขั้นตอนของการพัฒนายุทธศาสตร์ 5 ระยะ ดังนี้

1.1.1 ระยะที่ 1 : ระยะเริ่มต้น (Initiation) ประกอบด้วย

1.1.1.1 การระบุหน่วยงานรับผิดชอบหลัก (Identifying the lead project authority)

1.1.1.2 การแต่งตั้งคณะกรรมการขับเคลื่อน (Establishing a steering committee)

1.1.1.3 การระบุหน่วยงานหรือผู้มีส่วนเกี่ยวข้องในการพัฒนายุทธศาสตร์ (Identifying stakeholders to be involved in the development of the Strategy)

1.1.1.4 การวางแผนการพัฒนายุทธศาสตร์ (Planning the development of the strategy)

1.1.2 ระยะที่ 2 : ระยะประเมินตรวจสอบและวิเคราะห์ (Stocktaking and Analysis) ประกอบด้วย

1.1.2.1 การประเมินสภาวะความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Assessing the national cybersecurity landscape)

1.1.2.2 การประเมินสภาวะความเสี่ยงทางไซเบอร์ (Assessing the cyber-risk landscape)

1.1.3 ระยะที่ 3 : กำหนดยุทธศาสตร์ความมั่นคงไซเบอร์ระดับชาติ (Production of the national cybersecurity strategy) ประกอบด้วย

1.1.3.1 การยกร่างยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Drafting the national cybersecurity strategy)

1.1.3.2 การปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องทุกภาคส่วน (Consulting with a broad range of stakeholders)

1.1.3.3 การขอความเห็นชอบยุทธศาสตร์ (Seeking formal approval)

1.1.3.4 การเผยแพร่ยุทธศาสตร์ให้มีผลใช้บังคับ (Publishing the strategy)

1.1.4 ระยะที่ 4 : การขับเคลื่อนและใช้บังคับ (Implementation) ประกอบด้วย

1.1.4.1 การพัฒนาแผนปฏิบัติงาน (Developing the action plan)

1.1.4.2 การพิจารณาโครงการนำร่องที่สามารถนำไปปฏิบัติได้จริง (Determining initiatives to be implemented)

1.1.4.3 การจัดสรรทรัพยากรบุคลากรและงบประมาณเพื่อการขับเคลื่อนแผนปฏิบัติงาน (Allocating human and financial resources for the implementation)

1.1.4.4 การกำหนดกรอบระยะเวลา และตัวชี้วัด (Setting timeframes and metrics)

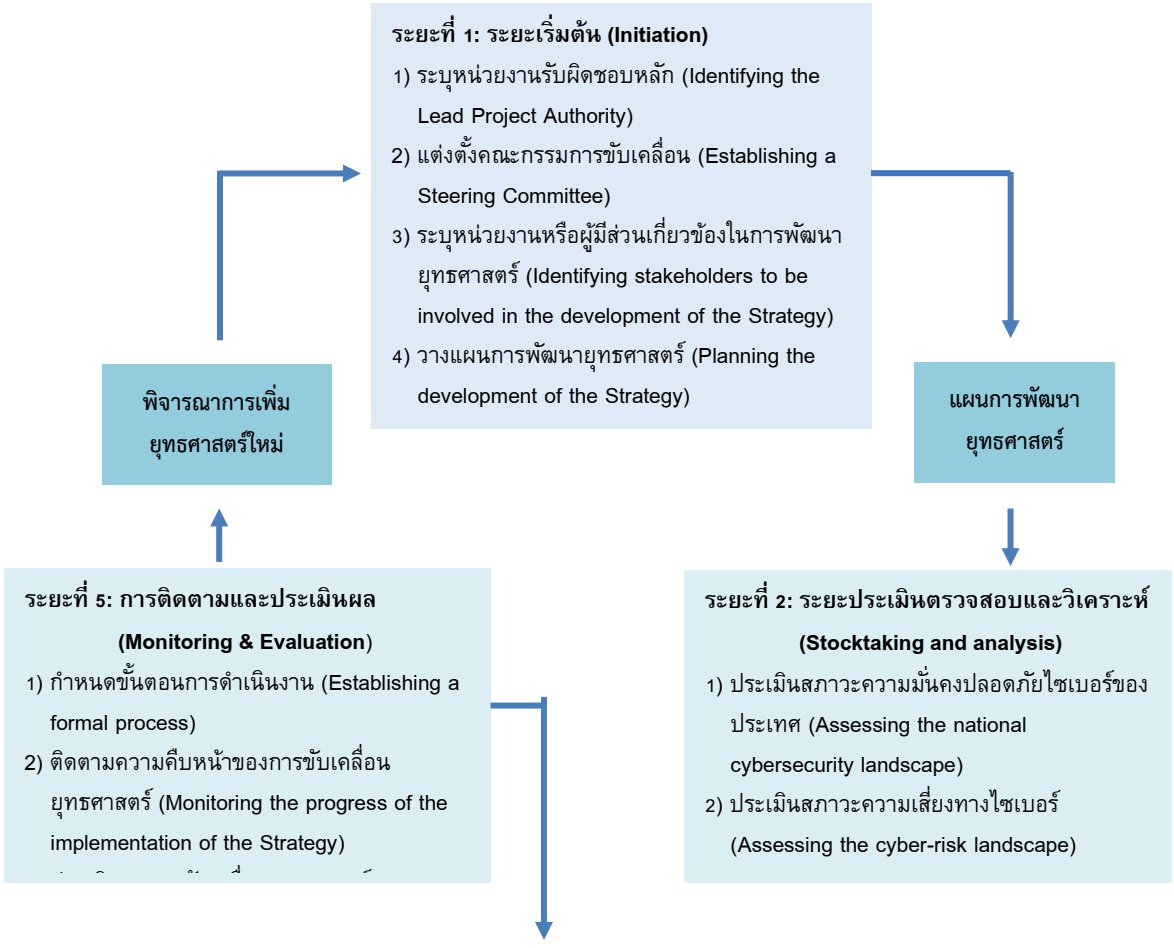
1.1.5 ระยะที่ 5 : การติดตามและประเมินผล (Monitoring and evaluation)

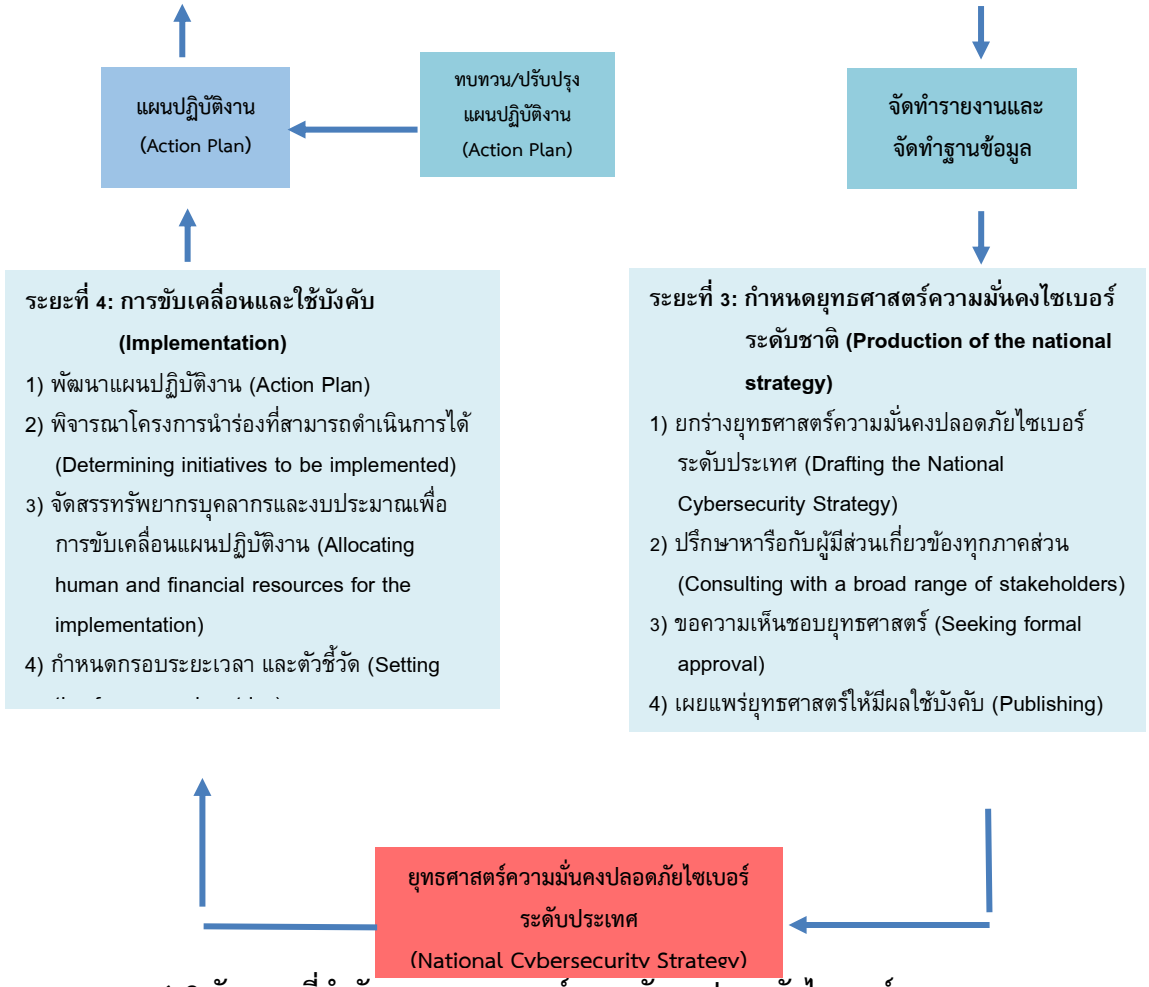
1.1.5.1 การกำหนดขั้นตอนการดำเนินงาน (Establishing a formal process)

1.1.5.2 การติดตามความคืบหน้าของการขับเคลื่อนยุทธศาสตร์ (Monitoring the progress of the implementation of the strategy)

1.1.5.3 การประเมินผลการขับเคลื่อนยุทธ์ศาสตร์ (Evaluating the outcome of the strategy)

แผนภาพที่ 2-4 ขั้นตอนของการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)





1.2 ลักษณะที่สำคัญของยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

ที่มา : International Telecommunication Union., 2018.

ปลอดภัยไซเบอร์ระดับ
ประเทศ (National Cybersecurity Strategy) โดยมีลักษณะที่สำคัญของยุทธศาสตร์ 9 ประการ ดังนี้

1.2.1 วิสัยทัศน์ของรัฐบาลและสังคมที่ชัดเจน (Clear vision)

การกำหนดจุดหมายปลายทางของวิสัยทัศน์จะประสบความสำเร็จได้ หากผู้มีส่วนเกี่ยวข้องเข้าใจถึงเหตุผลความจำเป็นของยุทธศาสตร์ เป้าหมายของยุทธศาสตร์ต้องการบรรลุ ยุทธศาสตร์เกี่ยวกับอะไร และใครได้รับผลกระทบจากการขับเคลื่อนยุทธศาสตร์ วิสัยทัศน์ที่มีความชัดเจน ทำให้ผู้นำประเทศ และผู้มีส่วนเกี่ยวข้องมีความเชื่อมั่นในกระบวนการขับเคลื่อนยุทธศาสตร์ ทำให้เกิดความร่วมมือและการร่วมดำเนินงานเพื่อขับเคลื่อนยุทธศาสตร์ การกำหนดวิสัยทัศน์ควรพิจารณาพลวัตของการเปลี่ยนแปลงสภาพแวดล้อมทางไซเบอร์ด้วย เพื่อให้การกำหนดกรอบระยะเวลาขับเคลื่อนยุทธศาสตร์สอดคล้องกับวิสัยทัศน์

1.2.2 ความเข้าใจต่อสภาพแวดล้อมทางไซเบอร์ของประเทศและการจัดลำดับประเด็นสำคัญของประเทศ (Comprehensive approach and tailored priorities)

ปัญหาความมั่นคงปลอดภัยทางไซเบอร์มิได้เป็นเพียงความท้าทายทางเทคนิค แต่เป็นประเด็นปัญหาที่มีหลายแง่มุมและมีความซับซ้อน ไม่เพียงแต่มีผลกระทบต่อการเจริญเติบโตทางเศรษฐกิจและสังคม แต่ส่งผลกระทบต่อการบังคับใช้กฎหมาย ความมั่นคงของชาติ ความมั่นระหว่างประเทศ ความสัมพันธ์ระหว่างประเทศ การเจรจาต่อรองทางการค้า และการพัฒนาอย่างยั่งยืน และส่งผลกระทบต่ออีกหลากหลายมิติ ควรมีความเข้าใจในทุกแง่มุม ทุกมิติของสภาวะไซเบอร์ที่มีความสัมพันธ์กัน ในส่วนของการจัดลำดับประเด็นสำคัญด้านไซเบอร์ของประเทศมีความเกี่ยวข้องกับเป้าหมายและกรอบระยะเวลาของยุทธศาสตร์ รวมถึงการจัดสรรทรัพยากรทั้งบุคลากรและงบประมาณเพื่อขับเคลื่อนยุทธศาสตร์ การจัดลำดับความสำคัญของแต่ละประเทศอาจมีความแตกต่างกัน ประเด็นปัญหาความมั่นคงปลอดภัยไซเบอร์บางประเด็นอาจแยกออกไปเป็นประเด็นสำคัญหนึ่งของยุทธศาสตร์ด้านความมั่นคงของประเทศ

1.2.3 การพัฒนายุทธศาสตร์จากการมีส่วนร่วมของทุกภาคส่วน (Inclusiveness)

สภาวะทางไซเบอร์กลายเป็นภัยคุกคามต่อรัฐบาล ธุรกิจ และประชาชนทุกภาคส่วนประสบปัญหาความเสี่ยงต่อความมั่นคงปลอดภัยทางไซเบอร์ และมีส่วนร่วมรับผิดชอบในการบริหารจัดการความเสี่ยงเหล่านั้น ตามบทบาทหน้าที่ความรับผิดชอบของแต่ละภาคส่วน การพัฒนายุทธศาสตร์จึงจำเป็นต้องอาศัยการมีส่วนร่วมของทุกภาคส่วนเพื่อให้การขับเคลื่อนยุทธศาสตร์ประสบความสำเร็จ การมีส่วนร่วมของทุกภาคส่วนทำให้เข้าใจถึงความต้องการของแต่ละภาคส่วน องค์ความรู้และความเชี่ยวชาญเฉพาะด้านของแต่ละภาคส่วน ย่อมช่วยในการสร้างความร่วมมือเพื่อบรรลุเป้าหมายของยุทธศาสตร์ได้

1.2.4 การสร้างความมั่งคั่งทางเศรษฐกิจและสังคม (Economic and social prosperity)

สภาพแวดล้อมทางดิจิทัลสามารถช่วยเร่งการเจริญเติบโตทางเศรษฐกิจ ความก้าวหน้าของสังคม การพัฒนาค่านิยมทางสังคม การเพิ่มขีดความสามารถในการส่งมอบบริการสาธารณะ การค้าระหว่างประเทศ การพึ่งพาสภาพแวดล้อมทางดิจิทัลมากขึ้น เพื่อขับเคลื่อนความต้องการของสังคม จึงเพิ่มความต้องการความมั่นคงปลอดภัยทางไซเบอร์ด้วย อย่างไรก็ดี ความมั่นคงปลอดภัยทางไซเบอร์อาจไม่ใช่เป้าหมายสุดท้าย แต่การขับเคลื่อนยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์จะต้องสอดคล้องไปในทิศทางเดียวกับเป้าหมายกว้างของภาวะเศรษฐกิจและสังคม และต้องนำไปสู่การสร้างความเชื่อมั่นและความมั่นใจให้กับทุกภาคส่วน รวมถึงการป้องกันประเทศจากภัยคุกคามทางไซเบอร์

1.2.5 สิทธิมนุษยชนขั้นพื้นฐาน (Fundamental human rights)

การพัฒนายุทธศาสตร์ต้องคำนึงถึงสิทธิซึ่งประชาชนมีอยู่ในภาวะออฟไลน์จะต้องได้รับการคุ้มครองในภาวะออนไลน์ด้วย สิทธิมนุษยชนเป็นที่ยอมรับทั่วโลกในฐานะที่เป็นสิทธิขั้นพื้นฐาน สิทธิมนุษยชนส่วนหนึ่งรับรองโดยองค์กรสหประชาชาติภายใต้ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal declaration of human rights) และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International covenant on civil and political rights) รวมถึงกรอบความตกลงความร่วมมือระดับภูมิภาคและพหุภาคีอื่น ๆ โดยเฉพาะประเด็นในเรื่องเสรีภาพในการแสดงออก (Freedom of expression) ความเป็นส่วนตัวในการสื่อสาร (Privacy of communications) และการคุ้มครองข้อมูลส่วนบุคคล (Personal-data protection) การกำหนดยุทธศาสตร์ควรหลีกเลี่ยงอำนาจเบ็ดเสร็จ อำนาจที่ไม่เป็นธรรม หรือการสอดส่องดูแลที่ไม่เป็นไปตามกฎหมาย (Unlawful surveillance) การแทรกแซงการสื่อสาร หรือการควบคุมข้อมูลส่วนบุคคล เพื่อให้เกิดความสมดุลระหว่างความต้องการของภาครัฐและประชาชน การกำหนดยุทธศาสตร์จะต้องสร้างความมั่นใจว่าการสอดส่องดูแล การแทรกแซงการสื่อสาร การจัดเก็บข้อมูลส่วนบุคคลต้องกระทำภายใต้กรอบกฎหมาย หรือวัตถุประสงค์ในการสืบสวนสอบสวนที่เฉพาะเจาะจงเป็นรายกรณี ภายใต้หน่วยงานของภาครัฐ ซึ่งไม่เลือกปฏิบัติ และปฏิบัติงานภายใต้หลักความถูกต้องแม่นยำและด้วยความเข้าใจ

1.2.6 การบริหารความเสี่ยงและความทนทานต่อความเสี่ยง (Risk management and resilience)

สภาพแวดล้อมทางดิจิทัลสร้างโอกาสทางเศรษฐกิจและสังคมให้กับทุกภาคส่วน ขณะเดียวกันก็สร้างความเสี่ยงต่อความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity risk) ด้วย ยกตัวอย่างเช่น กรณีที่องค์กรใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อเร่งการพัฒนานวัตกรรม สร้างผลิตภาพการผลิตและพัฒนาขีดความสามารถในการแข่งขัน หรือกรณีที่รัฐบาลเปิดการให้บริการสาธารณะทางออนไลน์ ปัญหาความมั่นคงปลอดภัยทางไซเบอร์อาจเกิดขึ้นได้ และอาจนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง การดำเนินธุรกิจหยุดชะงัก หยุดยั้งการสร้างนวัตกรรมได้

ความเสี่ยงต่อความมั่นคงปลอดภัยทางไซเบอร์ไม่อาจบริหารจัดการให้หมดสิ้นไปได้ เช่นเดียวกับความเสี่ยงประเภทอื่น แต่สามารถบริหารจัดการความเสี่ยงให้มีผลกระทบต่ำที่สุดได้ เพื่อจัดการกับความท้าทายนี้ การกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ควรสนับสนุนให้ทุกภาคส่วนให้ความสำคัญกับการลงทุนเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการบริหารความเสี่ยงเชิงรุก การรักษาสมดุลระหว่างการป้องกันและบริหารจัดการความเสี่ยง และการแสวงหาผลประโยชน์จากพลวัตของสภาพแวดล้อมทางดิจิทัล

นอกจากนี้ การกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ควรเข้าใจถึงความจำเป็นของการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง การสร้างบรรยากาศที่ดีสำหรับทุกภาคส่วนให้สามารถพึ่งพาซึ่งกันและกันได้ การบริหารจัดการความเสี่ยงของทุกภาคส่วนจะสร้างความทนทานให้กับระบบเศรษฐกิจ และกิจกรรมทางสังคมของประเทศชาติ รวมถึงจะต้องสนับสนุนให้มีการจัดทำแผนการบริหารธุรกิจอย่างต่อเนื่อง (Business continuity) ภายใต้การรับมือกับเหตุการณ์และการบริหารในสภาวะวิกฤต รวมถึงแผนการฟื้นฟูกิจการด้วย

1.2.7 กลไกขับเคลื่อนนโยบายที่เหมาะสม (Appropriate set of policy instruments)

รัฐบาลจะสามารถบรรลุเป้าหมายของการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ หากทุกภาคส่วนที่เกี่ยวข้องมีการเปลี่ยนแปลงพฤติกรรม โดยส่วนใหญ่ แต่ละรัฐบาลมักจะมีกลไกหรือเครื่องมือในการขับเคลื่อนนโยบายแตกต่างกันไป ไม่ว่าจะเป็นกฎหมาย กฎระเบียบ มาตรฐาน มาตรการจูงใจ การแลกเปลี่ยนข้อมูล การให้การศึกษา การเผยแพร่กรณีศึกษาที่ดี การกำหนดบรรทัดฐานของพฤติกรรมที่เหมาะสม การสร้างสังคมของความน่าเชื่อถือ เครื่องมือขับเคลื่อนนโยบายต่าง ๆ เหล่านี้ ล้วนมีจุดแข็ง-จุดอ่อนแตกต่างกันไป การกำหนดยุทธศาสตร์ที่เหมาะสมที่สุดควรคำนึงถึงเครื่องมือหรือกลไกการขับเคลื่อนนโยบายที่เหมาะสม

1.2.8 บทบาทความเป็นผู้นำที่เด่นชัด การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน และการจัดสรรทรัพยากรที่ชัดเจน (Clear leadership, roles, and resource allocation)

การรักษาความมั่นคงปลอดภัยไซเบอร์ ควรได้รับการส่งเสริมจากผู้บริหารสูงสุดของรัฐบาล เพื่อกำหนดภาระรับผิดชอบ (Accountability) อย่างชัดเจน ควรระบุศูนย์กลางของสายงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจน และทุกภาคส่วนที่เกี่ยวข้องควรมีความเข้าใจในบทบาทความรับผิดชอบที่เกี่ยวข้องของแต่ละภาคส่วน การกำหนดยุทธศาสตร์ควรจัดสรรบุคลากร งบประมาณ และอุปกรณ์ที่จำเป็น ทั้งนี้ ลักษณะหรือคุณสมบัติที่สำคัญในเรื่องนี้มีความจำเป็นต่อกระบวนการพัฒนายุทธศาตร์ และการกำหนดแผนปฏิบัติงานภายใต้ยุทธศาสตร์ด้วย

1.2.9 สภาพแวดล้อมของความเชื่อมั่น (Trust environment)

สิทธิของผู้ใช้งานระบบดิจิทัลควรได้รับความคุ้มครอง มีความมั่นคงปลอดภัยในข้อมูล และการใช้งานระบบ เพื่อสร้างความเชื่อมั่นต่อระบบนิเวศดิจิทัลของประเทศ เพื่อให้การใช้งานเทคโนโลยีดิจิทัล นำไปสู่การสร้างโอกาสทางสังคม เศรษฐกิจ การเมืองอย่างแท้จริง การกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ควรสนับสนุนให้เกิดนโยบาย กระบวนการ การปฏิบัติงาน ที่ส่งผลในระดับชาติ เพื่อปกป้องคุ้มครองบริการที่มีความสำคัญยิ่งยวด โดยเฉพาะการกำกับดูแลของภาครัฐทางอิเล็กทรอนิกส์ (e-governance) การพาณิชย์อิเล็กทรอนิกส์

(e-commerce) และการทำธุรกรรมการเงินทางดิจิทัล ซึ่งขับเคลื่อนได้โดยอาศัยความเชื่อมั่น (Trust) ทั้งจากประชาชนทั่วไป องค์กรภาครัฐ และภาคเอกชน ซึ่งให้บริการกับประชาชนผ่านการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร

1.3 แนวปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

ตามแนวปฏิบัติที่ดี (Good-practice) ปัจจัยสำคัญที่ทำให้ประเทศสามารถบรรลุตามเป้าหมายที่กำหนดขึ้นภายใต้ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ ประกอบด้วย 9 ปัจจัยที่สำคัญ ดังนี้

1.3.1 การกำกับดูแลของภาครัฐ (Governance)

1.3.1.1 การสนับสนุนจากผู้บริหารสูงสุดในรัฐบาล (Ensure the highest level of support)

การกำหนดยุทธศาสตร์ควรได้รับการสนับสนุนและให้ความสำคัญจากผู้บริหารสูงสุดของรัฐบาล จะช่วยสร้างความมั่นใจได้ว่า จะมีการจัดสรรทรัพยากรอย่างเพียงพอเพื่อขับเคลื่อนยุทธศาสตร์ และเป็นการส่งสัญญาณให้ระบบนิเวศทางดิจิทัลของประเทศในวงกว้างได้ทราบถึงความมุ่งมั่นของประเทศในการรักษาความมั่นคงปลอดภัยไซเบอร์

1.3.1.2 จัดตั้งหน่วยงานรับผิดชอบหลักที่มีความรู้ความเชี่ยวชาญเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Establish a competent cybersecurity authority)

ยุทธศาสตร์ควรกำหนดให้มีการจัดตั้งหน่วยงานรับผิดชอบหลักในการทำหน้าที่บริหารจัดการการขับเคลื่อนยุทธศาสตร์ กำหนดกระบวนการขับเคลื่อน กำหนดกระบวนการตัดสินใจ การแบ่งหน้าที่ความรับผิดชอบกับหน่วยงานที่เกี่ยวข้องซึ่งอาจสังกัดอยู่ต่างกรมต่างกระทรวงกัน การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การติดตามผลการปฏิบัติงานในการขับเคลื่อนยุทธศาสตร์ เพื่อให้มีความมั่นใจได้ว่า การขับเคลื่อนยุทธศาสตร์เป็นไปอย่างมีประสิทธิภาพ

1.3.1.3 การสร้างความร่วมมือของหน่วยงานภาครัฐ (Ensure intra-government cooperation)

ยุทธศาสตร์ควรกำหนดให้มีการสร้างกลไกในการระบุหน่วยงานภาครัฐที่ได้รับผลกระทบหรือหน่วยงานที่มีความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน เพื่อสร้างข้อตกลง ความร่วมมือ และการประสานงานกันระหว่างหน่วยงานภาครัฐ เพื่อให้ทุกกระทรวงตระหนักรู้ถึงหน้าที่ความรับผิดชอบ ภารกิจ และงานที่ได้รับมอบหมายโดยมีความต่อเนื่องในการขับเคลื่อนตามข้อตกลง ความร่วมมือ และการประสานงานดังกล่าว เช่น การกำหนดวาระการประชุมร่วมกันอย่างสม่ำเสมอ เพื่อติดตามการดำเนินงานตามแผนปฏิบัติงาน

และการมีความสอดคล้องกันของนโยบายการต่างประเทศและนโยบายภายในประเทศในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งทุกกระทรวงควรมีท่าทีและจุดยืนเป็นไปในทิศทางเดียวกัน ไม่ขัดแย้งกัน หรือลดความน่าเชื่อถือของกันและกัน เป็นต้น

1.3.1.4 การสร้างความร่วมมือระหว่างทุกภาคส่วน (Ensure inter-sectoral cooperation)

ยุทธศาสตร์ควรกำหนดให้มีการสร้างความร่วมมือระหว่างภาคเอกชนและผู้มีส่วนเกี่ยวข้องต่าง ๆ โดยภาครัฐควรเป็นตัวกลางในการสร้างความร่วมมือระหว่างทุกภาคส่วน เช่น การกำหนดเครือข่ายและกระบวนการติดต่อประสานสำหรับอุตสาหกรรมที่มีความสำคัญยิ่งยวด เพื่อการรับมือและฟื้นฟูบริการสาธารณะและโครงสร้างพื้นฐานที่มีความสำคัญจากการโจมตีทางไซเบอร์ เป็นต้น

1.3.1.5 การจัดสรรงบประมาณและทรัพยากรอย่างเพียงพอ (Allocate dedicated budget and resources)

ยุทธศาสตร์ควรกำหนดให้มีการจัดสรรทรัพยากรเพื่อขับเคลื่อนยุทธศาสตร์อย่างเพียงพอ สม่ำเสมอ และต่อเนื่อง จะช่วยวางรากฐานของความมั่นคงปลอดภัยไซเบอร์ โดยทรัพยากรหมายถึงบุคลากร งบประมาณ การสร้างความร่วมมือทุกภาคส่วน การแสดงเจตนารมณ์ทางการเมือง (Political commitment) และการแสดงบทบาทความเป็นผู้นำ (Leadership)

1.3.1.6 การพัฒนาแผนปฏิบัติงาน (Develop an implementation plan)

ยุทธศาสตร์ควรกำหนดให้มีแผนปฏิบัติงานที่ให้รายละเอียดเกี่ยวกับวิธีการบรรลุตามเป้าหมายของยุทธศาสตร์ หน่วยงานที่รับผิดชอบ ทรัพยากรที่จำเป็นในการขับเคลื่อน กรอบระยะเวลาในการขับเคลื่อน (ระยะสั้น กลาง และยาว) ขั้นตอนกระบวนการที่จะขับเคลื่อน และผลลัพธ์ที่คาดว่าจะเกิดขึ้น

1.3.2 การบริหารความเสี่ยง (Risk management)

1.3.2.1 กำหนดวิธีการบริหารจัดการความเสี่ยง (Define a risk-management approach)

ยุทธศาสตร์ควรกำหนดให้มีวิธีการบริหารจัดการความเสี่ยงเพื่อเป็นแนวทางให้กับหน่วยงานภาครัฐ และหน่วยงานผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญยิ่งยวด โดยระบุถึงทรัพย์สินและบริการที่สำคัญต่อเศรษฐกิจและสังคม ภัยคุกคามทางไซเบอร์ ปัจจัยความเสี่ยงและผลกระทบที่คาดว่าจะเกิดขึ้น การจัดลำดับความสำคัญตามความน่าจะเป็นของการเกิดเหตุการณ์ เพื่อให้รัฐบาลสามารถติดตามดูแลความเสี่ยงและบริหารจัดการได้อย่างทันการณ์

1.3.2.2 ระบุระเบียบวิธีการบริหารจัดการความเสี่ยงต่อความมั่นคงปลอดภัยไซเบอร์ (Identify a common methodology for managing cybersecurity risk)

ยุทธศาสตร์ควรกำหนดให้มีการระบุระเบียบวิธีการบริหารจัดการความเสี่ยงที่ได้มาตรฐานสากล (International standards) เพื่อเป็นแนวทางในการมอบหมายหน้าที่ความรับผิดชอบให้หน่วยงานที่เกี่ยวข้อง ปฏิบัติตามขั้นตอนกระบวนการบริหารจัดการความเสี่ยง เช่น การประเมินภัยคุกคาม การประเมินมูลค่าทรัพย์สินที่คาดว่าจะได้รับผลกระทบ การกำหนดมาตรการลดความเสี่ยง มาตรการรองรับผลกระทบจากความเสี่ยง โครงการรับรองหน่วยงานที่มีการบริหารจัดการความเสี่ยงที่ได้มาตรฐาน เป็นต้น นอกจากนี้ การออกแบบและพัฒนาโครงสร้างพื้นฐานและบริการสาธารณะ โดยคำนึงถึงการบริหารจัดการความเสี่ยง จะช่วยลดความเสี่ยง และสร้างความมั่นคงให้กับโครงสร้างพื้นฐานและบริการสาธารณะ

1.3.2.3 การพัฒนาบัญชีความเสี่ยงของแต่ละภาคส่วนเศรษฐกิจ (Develop sectoral cybersecurity risk profiles)

ยุทธศาสตร์ควรกำหนดให้มีการจัดทำบัญชีความเสี่ยง (Risk profile) สำหรับความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้ในการวิเคราะห์และประเมินประเภทของภัยคุกคาม ทำให้สามารถเข้าใจมูลค่าความเสี่ยงและผลกระทบของความเสี่ยงเป็นตัวเลข ควรมีการจัดทำบัญชีความเสี่ยงในภาคส่วนเศรษฐกิจที่มีความสำคัญยิ่งยวดต่อเศรษฐกิจและสังคม บัญชีความเสี่ยงจะช่วยให้สามารถบริหารจัดการความเสี่ยงอย่างเฉพาะเจาะจงเป็นรายกรณีได้มากยิ่งขึ้น

1.3.2.4 การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Establishing cybersecurity policies)

ยุทธศาสตร์ควรกำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานที่สำคัญยิ่งยวดของประเทศ ได้แก่ หน่วยงานภาครัฐ และหน่วยงานผู้ให้บริการโครงสร้างพื้นฐาน ปฏิบัติตามข้อกำหนดหลักเกณฑ์ของนโยบาย มาตรฐานขั้นต่ำและความปลอดภัยขั้นพื้นฐาน (Security baselines) ตามบทบาทหน้าที่ความรับผิดชอบของแต่ละหน่วยงาน เช่น ความมั่นคงปลอดภัยไซเบอร์บนระบบการจัดซื้อจัดจ้างภาครัฐทางอิเล็กทรอนิกส์ เป็นต้น

1.3.3 การเตรียมความพร้อมและความทนทาน (Preparedness and resilience)

1.3.3.1 การพัฒนาขีดความสามารถในการรับมือกับเหตุการณ์ (Establish cyber-incident response capabilities)

ยุทธศาสตร์ควรกำหนดให้มีการพัฒนาขีดความสามารถในการรับมือกับเหตุการณ์ โดยการจัดตั้งทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams : CERTs) ทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response teams : CSIRTs) หรือทีมรับมือกับสถานการณ์ที่เกี่ยวกับคอมพิวเตอร์ (Computer incident response teams: CIRTs) ระดับประเทศ ซึ่งจะมีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงตั้งรับ (การรับมือและการฟื้นฟู) และเชิงรุก (การป้องกัน) รวมถึงการเพิ่มขีดความสามารถในการรับมือผ่านกลไกความร่วมมือและการสื่อสารระหว่างภาคส่วนเศรษฐกิจต่าง ๆ กับทีมรับมือกับสถานการณ์ของประเทศ และองค์กรระหว่างประเทศที่เกี่ยวข้อง

1.3.3.2 การพัฒนาและจัดทำแผนรองรับสถานการณ์ฉุกเฉินสำหรับการจัดการภาวะวิกฤตด้านความมั่นคงปลอดภัยไซเบอร์ (Establish contingency plans for cybersecurity crisis management)

ยุทธศาสตร์ควรกำหนดให้มีการพัฒนาและจัดทำแผนรองรับสถานการณ์ฉุกเฉิน (Contingency plans) ระดับประเทศ เพื่อรองรับการจัดการในสถานการณ์ฉุกเฉินหรือภาวะวิกฤตของประเทศ โดยเฉพาะแผนรองรับของระบบโครงสร้างพื้นฐานที่สำคัญยิ่งยวด ทั้งนี้ ควรคำนึงถึงผลการประเมินความเสี่ยงระดับประเทศและระดับภาคส่วนเศรษฐกิจต่าง ๆ ซึ่งสามารถส่งผลกระทบเชื่อมโยงมายังโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทศได้

1.3.3.3 การสนับสนุนการแลกเปลี่ยนข้อมูล (Promote information-sharing)

ยุทธศาสตร์ควรกำหนดให้มีการสร้างกลไกการแลกเปลี่ยนข้อมูล โดยสามารถแลกเปลี่ยนข่าวกรอง และข้อมูลภัยคุกคามไซเบอร์ทั้งต่อภาคสาธารณะและภาคเอกชน การแลกเปลี่ยนข้อมูลจะช่วยให้เกิดความร่วมมือ ความแม่นยำของการสื่อสารในช่วงของการรับมือเหตุการณ์และการฟื้นฟูหลังเหตุการณ์ โดยอาจกำหนดหน่วยงานรับผิดชอบหลักในการจัดส่งและแลกเปลี่ยนข้อมูลและองค์ความรู้ที่ถูกต้อง แม่นยำ และอย่างมีประสิทธิภาพ เพื่อให้มั่นใจได้ว่าทุกภาคส่วนสามารถเตรียมพร้อมรับมือภัยคุกคามไซเบอร์ได้อย่างทันการณ์

1.3.3.4 การฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ (Conduct cybersecurity exercises)

ยุทธศาสตร์ควรกำหนดให้มีการฝึกซ้อมแผนรับมือกับเหตุการณ์ซึ่งอาจมีหลายรูปแบบ เช่น การจำลองเหตุการณ์ หรือการฝึกซ้อมเหมือนจริง โดยมุ่งเน้นกลุ่มเป้าหมายเจ้าหน้าที่ทางเทคนิคและผู้มีอำนาจตัดสินใจ การฝึกซ้อมแผนรับมือและแผนรองรับสถานการณ์ฉุกเฉินจะช่วยให้ประเทศสามารถพัฒนาขีดความสามารถในเชิงสถาบัน เพื่อให้การรับมือ

ต่อเหตุการณ์เป็นไปอย่างมีประสิทธิภาพ เป็นการทดสอบกระบวนการบริหารจัดการ และกลไกการติดต่อสื่อสาร รวมถึงพัฒนาขีดความสามารถให้ทีมรับมือสามารถบริหารจัดการในสภาวะกดดันได้ ทั้งนี้ ควรมีการฝึกซ้อมแผนรับมือร่วมกับองค์กรระหว่างประเทศเพื่อสร้างความเชื่อมั่นและความมั่นใจ และยังเป็นการพัฒนาความทนทานและความพร้อมรับมือต่อภัยคุกคามไซเบอร์ของระดับภูมิภาคด้วย

1.3.4 ระบบบริการโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical Infrastructure services and essential services)

1.3.4.1 การกำหนดวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องบริการสาธารณะและโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทศ (Establish a risk-management approach to protecting critical infrastructures and services) รวมถึงโครงสร้างพื้นฐานข้อมูลที่สำคัญยิ่งยวด (Critical information infrastructures : CIIs)

1.3.4.2 การพัฒนารูปแบบการกำกับดูแลของภาครัฐและภาระความรับผิดชอบ (Adopt a governance model with clear responsibilities) ของหน่วยงานภาครัฐและผู้มีส่วนเกี่ยวข้องในการปกป้องคุ้มครองโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical infrastructures : CIs) และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวด (CIIs)

1.3.4.3 การกำหนดความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำหรือเป้าหมายกรณีฐานของความมั่นคงปลอดภัยไซเบอร์ (Define minimum cybersecurity baselines) สำหรับผู้ให้บริการและผู้ปฏิบัติงานในโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (CIs) และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวด (CIIs) โดยควรเป็นไปตามมาตรฐานสากล หรือกรณีแนวปฏิบัติที่ดีของต่างประเทศ

1.3.4.4 การสร้างแรงจูงใจในทุกภาคส่วน (Utilise a wide range of market levers)

ยุทธศาสตร์นี้ รัฐบาลควรพิจารณากำหนดนโยบายที่มั่นใจได้ว่า ทุกภาคส่วนมีแรงจูงใจเพียงพอที่จะร่วมกันรักษาความมั่นคงปลอดภัยไซเบอร์ตามภาระหน้าที่ซึ่งตนรับผิดชอบ การประเมินช่องว่างระหว่างสิ่งที่แต่ละภาคส่วนสามารถกระทำได้กับสิ่งที่แต่ละภาคส่วนควรกระทำ ท่ามกลางสภาพแวดล้อมของความเสี่ยง จำเป็นต้องมีการประเมินสภาวะของแรงจูงใจต่าง ๆ ทั้งส่วนที่เพิ่มแรงจูงใจและลดแรงจูงใจ เพื่อให้ภาครัฐสามารถสนับสนุนให้เกิดการปฏิบัติตามสิ่งที่ควรกระทำ นั่นคือ มาตรฐานสากล และแนวปฏิบัติที่ดีของการักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (CIs) และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวด (CIIs)

1.3.4.5 การสนับสนุนการร่วมลงทุนระหว่างภาครัฐและภาคเอกชน (Establish public-private partnerships)

เพื่อสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical infrastructures: CIs) และโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวด (CIIs) ภาครัฐและภาคเอกชนควรมีโครงการร่วมลงทุน เพื่อสร้างความมั่นใจให้กับอุตสาหกรรม โดยผู้มีส่วนเกี่ยวข้องต้องมีความเข้าใจในเป้าหมายของการเป็นหุ้นส่วนที่เป็นไปเพื่อสร้างผลประโยชน์ด้านความมั่นคงปลอดภัยจากการทำงานร่วมกัน

1.3.5 ขีดความสามารถ การพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ (Capability and capacity building and awareness raising)

1.3.5.1 พัฒนาหลักสูตรการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Develop cybersecurity curricula) เพื่อเร่งการพัฒนาทักษะและความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบการศึกษา ตั้งแต่ระดับชั้นประถมศึกษา มัธยมศึกษา ไปจนถึงระดับอุดมศึกษา โดยบูรณาการหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์เข้ากับหลักสูตรที่เกี่ยวข้องกับวิทยาศาสตร์คอมพิวเตอร์ และเทคโนโลยีสารสนเทศ การสร้างคุณวุฒิปริญญาบัณฑิตด้านความมั่นคงปลอดภัยไซเบอร์ และการฝึกงานภาคปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

1.3.5.2 ส่งเสริมการพัฒนาทักษะและฝึกอบรมการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Stimulate skills development and workforce training) สำหรับตำแหน่งผู้บริหาร ผู้เชี่ยวชาญ การฝึกอบรมเพื่อการปฏิบัติงาน และนักศึกษาฝึกงาน ให้สอดคล้องตามความต้องการของอุตสาหกรรมและรัฐบาล ยุทธศาสตร์นี้ควรเร่งริเริ่มเพื่อพัฒนาเส้นทางความก้าวหน้าในสายอาชีพ และเพิ่มอุปทานด้านผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยควรสร้างความร่วมมือกับสถาบันการศึกษา ภาคเอกชน และภาคประชาสังคม

1.3.5.3 กำหนดโครงการเพิ่มความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Implement a coordinated cybersecurity awareness-raising programme) โดยมอบหมายหน่วยงานรับผิดชอบที่มีความเหมาะสม ผ่านโครงการรณรงค์ และกิจกรรม เพื่อเพิ่มความตระหนักรู้ในระดับประเทศ โดยเจาะจงกลุ่มเป้าหมาย เช่น ประชาชนทั่วไป เยาวชน ผู้บริโภค เป็นต้น

1.3.5.4 เร่งการพัฒนานวัตกรรม การวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Foster cybersecurity innovation and R&D) ทั้งองค์กรหน่วยงานวิจัยและพัฒนาภายในประเทศ และสร้างความร่วมมือหรือเป็นหุ้นส่วนกับองค์กรหรือหน่วยงานวิจัยและพัฒนาในต่างประเทศ โดยกำหนดมาตรการแรงจูงใจ เช่น เงินสนับสนุน เครดิตภาษี เป็นต้น และสร้างบรรยากาศในการแข่งขัน ทั้งนี้ สาขาของการพัฒนานวัตกรรม การวิจัยและพัฒนา อาจมุ่งเน้นสาขาวิทยาศาสตร์ เช่น วิทยาการคอมพิวเตอร์ วิศวกรรมไฟฟ้า คณิตศาสตร์

ประยุกต์ วิทยาการเข้ารหัสลับ (Cryptography) เป็นต้น แต่อาจมุ่งเน้นสาขาที่ไม่ใช่ทางเทคนิคด้วย เช่น สังคมศาสตร์ รัฐศาสตร์ บริหารศาสตร์ เป็นต้น

1.3.6 กฎหมายและระเบียบกฎเกณฑ์ (Legislation and regulation)

1.3.6.1 การบัญญัติกฎหมายว่าด้วยการป้องกันอาชญกรรมทางไซเบอร์ (Establish cybercrime legislation) โดยอาจเป็นการปรับปรุงแก้ไขกฎหมายที่มีอยู่แล้ว ในปัจจุบัน ให้มีบทลงโทษเกี่ยวกับการกระทำความผิดทางไซเบอร์

1.3.6.2 ให้ความสำคัญกับการคุ้มครองสิทธิของประชาชน ข้อมูลส่วนบุคคล และเสรีภาพในการแสดงออกของประชาชน (Recognise and safeguard individual rights and liberties) ตามหลักการของสิทธิมนุษยชนขั้นพื้นฐาน

1.3.6.3 สร้างกลไกในการปฏิบัติตาม (Create compliance mechanisms) เช่น การบังคับใช้กฎหมาย และมาตรการจูงใจ เป็นต้น รวมถึงการสืบสวนสอบสวนคดีไซเบอร์ การสกัดกั้นการสื่อสาร (Interception of communications) และการใช้หลักฐานทางดิจิทัล

1.3.6.4 สนับสนุนการเพิ่มขีดความสามารถในการบังคับใช้กฎหมาย (Promote capacity-building for law enforcement) ผ่านการจัดฝึกอบรม การสร้างความรู้ความเข้าใจ ให้แก่บุคลากรภาครัฐที่เกี่ยวข้อง เช่น ตุลาการ อัยการ ทนายความ ตำรวจผู้บังคับใช้กฎหมาย พนักงานสืบสวน ผู้เชี่ยวชาญด้านกฎหมาย เป็นต้น เพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ เช่น องค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol) และหน่วยงานตำรวจของสหภาพยุโรป (Europol) เป็นต้น

1.3.6.5 สร้างกระบวนการความร่วมมือระหว่างหน่วยงานภายในประเทศ (Establish inter-organisational processes) โดยมีหน่วยงานหลักที่บูรณาการอำนาจหน้าที่ความรับผิดชอบของแต่ละหน่วยงานให้ปฏิบัติตามกฎหมายว่าด้วยการป้องกันอาชญากรรมทางไซเบอร์ และปกป้องโครงสร้างพื้นฐานที่สำคัญยิ่งยวด และอาจตั้งหน่วยงานที่เกี่ยวข้องโดยตรง เช่น ทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams: CERTs) เป็นต้น

1.3.6.6 สนับสนุนการเข้าร่วมความตกลงและร่วมมือระหว่างประเทศในการต่อต้านอาชญากรรมทางไซเบอร์ (Support international cooperation to combat cybercrime) โดยกฎหมายในประเทศควรเปิดโอกาสในการจัดทำความตกลงและความร่วมมือระหว่างประเทศ

1.3.7 ความร่วมมือระหว่างประเทศ (International cooperation)

1.3.7.1 จัดลำดับให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญในการกำหนดนโยบายการต่างประเทศ (Recognise the importance of cybersecurity as a priority of foreign policy)

1.3.7.2 มีส่วนร่วมกับการประชุมระหว่างประเทศที่สำคัญ ทั้งระดับโลกและภูมิภาค ในประเด็นไซเบอร์ (Engage in international discussions)

1.3.7.3 ส่งเสริมการสร้างความร่วมมือระหว่างประเทศในด้านต่าง ๆ เช่น การพัฒากฎหมาย การบังคับใช้กฎหมาย การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ เป็นต้น ทั้งในรูปแบบที่เป็นทางการและไม่เป็นทางการ ที่เกี่ยวข้องกับโลกของไซเบอร์สเปซ (Promote formal and informal cooperation in cyberspace)

1.3.7.4 พัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติที่ดีและแนวปฏิบัติสากลต่าง ๆ ที่เริ่มขับเคลื่อนแล้ว ทั้งในระดับภูมิภาคและทั่วโลก (Align domestic and international cybersecurity efforts)

2. กรอบแนวคิดของหน่วยงานด้านความมั่นคงปลอดภัยของเครือข่ายและข้อมูลของสหภาพยุโรป (European union agency for network and information security agency : ENISA)

หน่วยงานด้านความมั่นคงปลอดภัยของเครือข่ายและข้อมูลของสหภาพยุโรป (ENISA)[8] ได้จัดทำคู่มือแนวปฏิบัติที่ดีในการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับประเทศ (National Cybersecurity Strategy: NCSS) ในปี 2559 ซึ่งปรับปรุงจากคู่มือแนวปฏิบัติที่ดีฉบับปี 2555 เพื่อเป็นแนวทางให้กับประเทศสมาชิกของกลุ่มสหภาพยุโรปในการกำหนดยุทธศาสตร์ และการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 1. วัฏจักรของยุทธศาสตร์ 2. หลักการในการออกแบบและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 6 หลักการ และ 3. เป้าหมายที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 15 ประการ โดยมีสาระสำคัญสรุปได้ ดังนี้

2.1 วัฏจักรของยุทธศาสตร์

ENISA ได้พัฒนาวัฏจักรของยุทธศาสตร์เพื่อให้มีการตรวจสอบและทบทวนยุทธศาสตร์และนโยบายที่เกี่ยวข้องอย่างต่อเนื่อง โดยกำหนดให้วัฏจักรของยุทธศาสตร์ประกอบด้วย 4 ระยะ ดังนี้

---

[8] European Union Agency for Network and Information Security Agency. (2016). **NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies.**

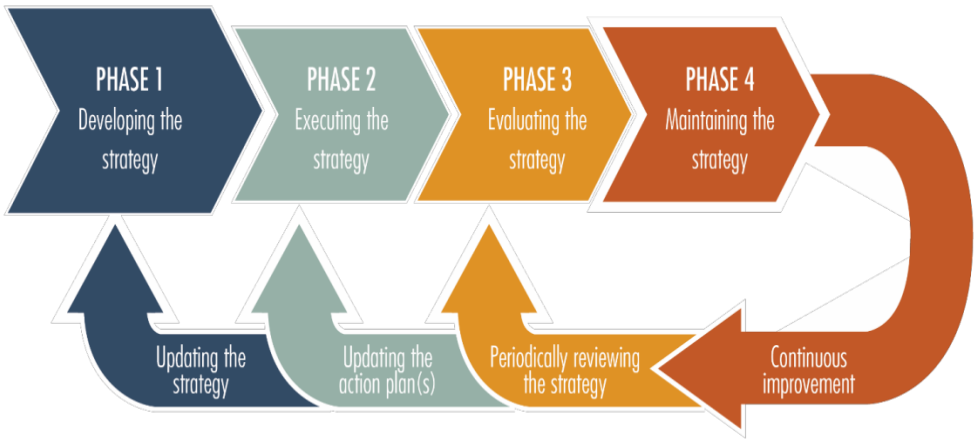
2.1.1 ระยะที่ 1 พัฒนายุทธศาสตร์ โดยมีการปรับปรุงยุทธศาสตร์ให้สอดคล้องกับสภาพและสถานการณ์ปัจจุบัน

2.1.2 ระยะที่ 2 ขับเคลื่อนยุทธศาสตร์ไปสู่การปฏิบัติ โดยมีการปรับแผนปฏิบัติงานให้สอดคล้องกับสภาพและสถานการณ์ปัจจุบัน

2.1.3 ระยะที่ 3 ประเมินผลการปฏิบัติตามยุทธศาสตร์ โดยมีการทบทวนยุทธศาสตร์เป็นระยะ

2.1.4 ระยะที่ 4 การรักษาไว้ซึ่งยุทธศาสตร์ โดยมีการพัฒนายุทธศาสตร์

แผนภาพที่ 2-5 วัฏจักรของยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศของหน่วยงานด้านความมั่นคงปลอดภัยของเครือข่ายและข้อมูลของสหภาพยุโรป (ENISA)



ที่มา : European Union Agency for Network and Information Security Agency, 2016

2.2 หลักการในการออกแบบและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์หมายถึงแผนในการปฏิบัติเพื่อให้บรรลุเป้าหมายในระยะยาวหรือเป้าหมายในภาพรวม การออกแบบและพัฒนายุทธศาสตร์จะต้องคำนึงถึงหลักการที่สำคัญ 6 ประการ ดังต่อไปนี้

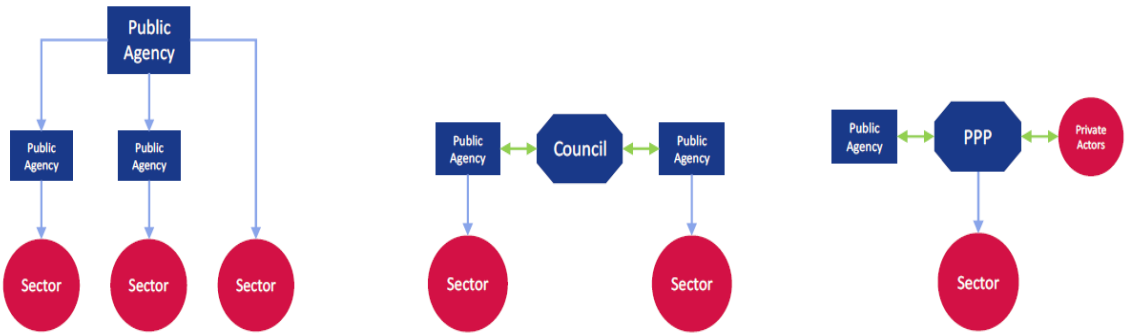
2.2.1 การกำหนดวิสัยทัศน์ ขอบเขตของภาคธุรกิจและบริการที่สำคัญ เป้าประสงค์ และจัดลำดับความสำคัญของเป้าหมายและผลกระทบต่อสังคม เศรษฐกิจ และประชาชน (Set the vision, scope, objectives and priorities)

2.2.2 ความสอดคล้องกับผลการประเมินความเสี่ยงของประเทศ (Follow a risk assessment approach) โดยมีขั้นตอนสำคัญ 3 ขั้นตอน ได้แก่ การระบุถึงความเสี่ยง (Risk identification) การวิเคราะห์ความเสี่ยง (Risk analysis) และการประเมินระดับความรุนแรงของความเสี่ยง (Risk evaluation)

2.2.3 การสำรวจนโยบาย กฎหมาย และขีดความสามารถที่มีอยู่ในปัจจุบัน (Take stock of existing policies, regulations and capabilities) เพื่อพัฒนาให้ครอบคลุมถึงประเด็นการรักษาความมั่นคงปลอดภัยไซเบอร์

2.2.4 การกำหนดโครงสร้างการกำกับดูแลหน่วยงานภาครัฐที่ชัดเจน (Set a clear governance structure) โดยกำหนดหน่วยงานรับผิดชอบ บทบาทหน้าที่ ความรับผิดชอบ รวมถึงคณะกรรมการที่ทำหน้าที่สร้างความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐ การร่วมมือระหว่างภาครัฐและภาคเอกชน (Public Private Partnership : PPP)

แผนภาพที่ 2-6 โครงสร้างหน่วยงานรับผิดชอบการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์



ที่มา: European Union Agency for Network and Information Security Agency, 2016

2.2.5 การระบุถึงและการมีส่วนร่วมจากผู้มีส่วนเกี่ยวข้อง (Identify and engage stakeholders) เพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน โดยหน่วยงานภาครัฐต้องปฏิบัติตามนโยบาย กฎระเบียบ และอำนาจหน้าที่ ส่วนภาคเอกชนเป็นเจ้าของบริการและโครงสร้างพื้นฐานที่สำคัญของประเทศโดยส่วนใหญ่

2.2.6 การสร้างกลไกการแลกเปลี่ยนข้อมูลที่เชื่อถือได้ (Establish trusted information-sharing mechanisms) รวมถึงข้อมูลข่าวกรองที่สำคัญและข้อมูลจากทีมสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ เพื่อช่วยให้เข้าใจถึงสภาพแวดล้อมไซเบอร์ที่เปลี่ยนแปลงไปและสามารถลดความเสี่ยงและความเปราะบางที่มีอยู่ได้

2.3 เป้าหมายที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

2.3.1 การพัฒนาแผนรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์ของประเทศ (Develop national cyber contingency plans) เพื่อใช้ในการรับมือและฟื้นฟูโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวดของประเทศ ซึ่งควรสอดคล้องกับแผนรองรับสถานการณ์ฉุกเฉินในภาพรวมของประเทศด้วย โดยกำหนดหลักเกณฑ์ในการบังคับใช้แผน แนวทางการปฏิบัติเพื่อรับมือ และกำหนดบทบาทหน่วยงานที่มีส่วนเกี่ยวข้องอย่างชัดเจน

2.3.2 การคุ้มครองโครงสร้างพื้นฐานข้อมูลที่สำคัญยิ่งยวด (Protect critical information infrastructure) โดยระบุถึงประเภทของโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวดและกำหนดมาตรการลดความเสี่ยง

2.3.3 การจัดการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ (Organise Cybersecurity exercises) โดยระบุถึงกระบวนการขั้นตอนและขีดความสามารถที่ต้องได้รับการทดสอบก่อนเกิดเหตุการณ์ และจัดตั้งทีมรับมือที่กำหนดอำนาจหน้าที่ความรับผิดชอบไว้อย่างชัดเจน

2.3.4 การกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน (Establish baseline security measures) หรือหลักเกณฑ์ระดับความปลอดภัยขั้นต่ำที่ทุกภาคส่วนต้องปฏิบัติตาม เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถตรวจสอบและบ่งชี้ถึงขีดความสามารถของตนเองได้ และทำให้สามารถจัดลำดับความสำคัญของการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ได้

2.3.5 การสร้างกลไกการรายงานเหตุการณ์ (Establish incident reporting mechanisms) เพื่อสร้างความเข้าใจต่อภาพรวมสถานการณ์ภัยคุกคามไซเบอร์ ช่วยให้สามารถประเมินผลกระทบได้ ได้ทราบถึงความเปราะบางและรูปแบบของการโจมตีทางไซเบอร์ ทำให้สามารถปรับปรุงแผนการรับมือให้เป็นปัจจุบันได้

2.3.6 การสร้างความตระหนักรู้ให้กับประชาชน เยาวชน และผู้บริโภค (Raise user awareness) โดยระบุถึงช่องว่างของความรู้ความเข้าใจหรือความตระหนักรู้จากปัญหาจากการใช้งานระบบอินเทอร์เน็ต และเติมเต็มช่องว่างนั้นด้วยการให้ความรู้และการสร้างความตระหนักรู้ผ่านการรณรงค์ การจัดกิจกรรม การจัดการประชุม และปรับปรุงเว็บไซต์ของหน่วยงานภาครัฐ ให้ครอบคลุมเนื้อหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การอภิปราย การบรรยาย และการสัมมนาผ่านเว็บไซต์ เป็นต้น

2.3.7 การจัดทำโครงการฝึกอบรมและหลักสูตรการศึกษา (Strengthen training and educational programmes) ซึ่งเป็นส่วนหนึ่งของสาขาวิทยาการคอมพิวเตอร์ โดยปรับปรุงเนื้อหาให้ทันต่อสถานการณ์อย่างต่อเนื่อง เพิ่มขีดความสามารถให้กำลังแรงงานการรักษาความมั่นคงปลอดภัยทางข้อมูล ส่งเสริมให้นักศึกษาเข้าร่วมในสาขาวิชาว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ สนับสนุนให้เกิดความเชื่อมโยงกันระหว่างการรักษาความปลอดภัยทางข้อมูลในแวดวงวิชาการ และอุตสาหกรรมความมั่นคงปลอดภัยในการรักษาความมั่นคงปลอดภัยทางข้อมูล

2.3.8 การเพิ่มขีดความสามารถในการรับมือกับเหตุการณ์ (Establish an incident response capability) โดยจัดตั้งทีมสำหรับรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (CSIRT) ของประเทศ ซึ่งจะมีบทบาทสำคัญในการประสานความร่วมมือกับผู้มีส่วนเกี่ยวข้อง รวมถึงการร่วมมือกับทีม CSIRT ของประเทศอื่น

2.3.9 การแก้ไขปัญหาอาชญากรรมไซเบอร์ (Address cyber crime) โดยอาศัยความร่วมมือของทุกภาคส่วนและสังคม การบัญญัติกฎหมาย และการเพิ่มประสิทธิภาพของหน่วยงานด้านการบังคับใช้กฎหมาย

2.3.10 การสร้างความร่วมมือกับองค์กรระหว่างประเทศ (Engage in international cooperation) เพื่อสร้างองค์ความรู้พื้นฐานร่วมกัน และช่วยส่งเสริมผลประโยชน์ร่วมกันในการรับมือกับภัยคุกคามไซเบอร์และอาชญากรรมทางไซเบอร์ โดยระบุประเทศพันธมิตรและแง่มิติที่ต้องการสร้างความร่วมมือ และกำหนดหน่วยงานภายในประเทศให้มีหน้าที่ความรับผิดชอบในการสร้างความร่วมมือระหว่างประเทศ

2.3.11 การสร้างการร่วมมือระหว่างภาครัฐและเอกชน (Establish a public-private partnership) ซึ่งมักจะเป็นผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยการประสานงานและร่วมมือระหว่างภาครัฐและเอกชนช่วยทำให้รัฐบาลเข้าใจถึงความต้องการของภาคเอกชน และความท้าทายที่ภาคเอกชนต้องเผชิญ การรร่วมมือระหว่างภาครัฐและเอกชนจะช่วยให้เกิดการรวมกลุ่มของผู้เชี่ยวชาญและทรัยากรที่จำเป็นในการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์และการสร้างความทนทานต่อภัยคุกคามทางไซเบอร์

2.3.12 การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและความเป็นส่วนตัว (Balance security with privacy) โดยพิจารณาหลักเกณฑ์ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ควบคู่กับการบัญญัติกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปรึกษาหารือกับหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในประเด็นข้อกฎหมาย การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลควรเป็นไปตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์

2.3.13 การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ (Institutionalise cooperation between public agencies) เช่น คณะกรรมการที่ปรึกษา คณะกรรมการกำกับดูแล สภา ศูนย์ปฏิบัติการ การประชุมกลุ่มผู้เชี่ยวชาญ เป็นต้น เพื่อให้เกิดการแลกเปลี่ยนข้อมูล การปรึกษาหารือ และการร่วมมือกัน จะช่วยให้การขับเคลื่อนยุทธศาสตร์ประสบผลสำเร็จได้

2.3.14 การเร่งการศึกษาวิจัยและพัฒนา (Foster R&D) เครื่องมือในการตรวจสอบและป้องกันการโจมตีทางไซเบอร์รูปแบบใหม่ ๆ รวมถึงการระบุถึงสาเหตุของความเปราะบางต่อการโจมตีทางไซเบอร์

2.3.15 การสร้างแรงจูงใจให้ภาคเอกชนในการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Provide incentives for the private sector to invest in security measures) วิธีที่ง่ายที่สุดในการกระตุ้นให้ภาคเอกชนลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การใช้บังคับตามกฎหมาย อย่างไรก็ดี รัฐบาลมักจะใช้วิธีการสร้างแรงจูงใจให้ภาคเอกชนมากกว่า เช่น สิทธิประโยชน์ทางภาษี การให้เงินช่วยเหลือ และการสนับสนุนเงินทุนวิจัยและพัฒนา เป็นต้น

3. กรอบโครงสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (National institute of standards and technology : NIST) ประเทศสหรัฐอเมริกา

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (NIST)[9] เป็นหนึ่งในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบัน ไม่เพียงแค่องค์กรในประเทศสหรัฐอเมริกา เท่านั้น framework ดังกล่าวยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลก รวมไปถึงประเทศไทย หลายองค์กรเริ่มนำ Framework นี้ประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์ Framework นี้รวบรวมเอาแนวปฏิบัติที่ดีที่สุดอันหลากหลายเข้าไว้ด้วยกัน เพื่อช่วยให้ธุรกิจองค์กรสามารถกำหนดแนวทางบังคับใช้งาน และปรับปรุงแนวทางการรักษาความมั่นคงปลอดภัย รวมถึงมีภาษากลางสำหรับใช้ในการสื่อสารประเด็นปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างผู้ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

Framework นี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจ

---

[9] National Institute of Standards and Technology. (2018). **Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.**

ยังคงดำเนินต่อไปได้อย่างเนื่อง โดยหัวใจสำคัญของ Framework แบ่งออกเป็น 5 ขั้นตอนที่สำคัญ ได้แก่ Identity Protect Detect Respond และ Recovery โดยสรุปได้ ดังนี้

3.1 Identify – การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง

3.2 Protect – การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

3.3 Detect – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

3.4 Respond – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

3.5 Recovery – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

ทั้งนี้ แต่ละขั้นตอนหลักจะแบ่งออกเป็นขั้นตอนย่อยๆ พร้อมระบุเอกสารอ้างอิง เช่น ISO/IEC 27001:2013 , COBIT 5, NIST SP800-53 เพื่อให้ผู้อ่านนำกระบวนหรือแนวทางปฏิบัติจากเอกสารเหล่านั้นมาใช้เพื่อดำเนินการตามขั้นตอนย่อยๆ เหล่านี้ได้ทันที

แผนภาพที่ 2-7 กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (NIST) สหรัฐอเมริกา

ที่มา : National Institute of Standards and Technology., 2018

การศึกษาวิจัยที่เกี่ยวกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. การศึกษาวิจัยภายในประเทศ

พลเรือตรี อุดม ประตาทะยัง (2560)[10] ได้ศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษา แนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต โดยผลการศึกษาพบว่า การมีหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อการป้องกันภัยคุกคามทางไซเบอร์ และประสานงานทั้งภายในและระหว่างประเทศในการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์มีความสำคัญอีกทั้งต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐและเอกชนเพื่อยกระดับความพร้อมรับมือภัยคุกคามทางไซเบอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ถึงแม้ว่าในปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์มากขึ้น แต่องค์กรต่าง ๆ มีการรักษาความปลอดภัยแบบแยกส่วนและบางครั้งมีความขัดแย้งกัน ประกอบกับการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์ และการพัฒนาบุคลากรด้านนี้ยังไม่ทันต่อความต้องการของประเทศ องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์ เนื่องจากกลัวการเสียชื่อเสียง นอกจากนี้ ร่างพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันนั้นอาจยังขาดองค์ประกอบที่สำคัญหลายประการ

พลเรือตรี อุดม ประตาทะยัง (2560) ได้เสนอแนะแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ใน 3 ประเด็น ประกอบด้วย 1) การกำหนดให้มีเป้าหมาย (Ends) ที่ชัดเจน คือ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์

---

[10] พลเรือตรี อุดม ประตาทะยัง. (2560). **แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์.** นักศึกษาวิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561. ลักษณะวิชายุทธศาสตร์.

อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ 2) การกำหนด แผนงาน/โครงการ (Projects/Plans) ประกอบยุทธศาสตร์ไว้อย่างเหมาะสม และ 3) การมีแนวทางในการนำยุทธศาสตร์ไปสู่การปฏิบัติ (Implementation) ไว้อย่างเหมาะสม นอกจากนี้ ยังได้เสนอให้มีการจัดตั้งศูนย์ไซเบอร์แห่งชาติ เพื่อบูรณาการการดำเนินการในส่วนที่เกี่ยวข้อง การกำหนดกรอบแนวคิดนโยบายและแผนระดับชาติ การยกระดับแผนการทำงานร่วมกัน เช่นแผนการซ้อมรับมือภัยคุกคามทางไซเบอร์ เป็นต้น การวางรากฐานการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ การศึกษากระบวนการการรักษาความปลอดภัยสารสนเทศ และการสร้างความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ

ยุทธนา เจียมตระการ (2560)[11] ได้ศึกษาแนวทางการจัดการความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมขนาดใหญ่ให้มีประสิทธิผลและประสิทธิภาพ และสอดรับกับนโยบายของประเทศในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ และข้อเสนอแนะการดำเนินการสำคัญสำหรับภาครัฐและอุตสาหกรรมขนาดใหญ่ในภาคธุรกิจเพื่อช่วยให้การสร้างความมั่นคงปลอดภัยไซเบอร์บรรลุความสำเร็จอย่างมีประสิทธิภาพยิ่งขึ้น เช่น การกำหนดเป้าหมายในยุทธศาสตร์ชาติ การจัดทำแผนแม่บทของประเทศ การสร้างความตระหนักกับผู้บริหารระดับสูงขององค์กร การใช้หลักการบริหารจัดการความเสี่ยงเพื่อการดำเนินการ การสร้างเครือข่ายความร่วมมือ เป็นต้น

ผลการศึกษาพบว่า ยุทธศาสตร์ที่ 1 และยุทธศาสตร์ที่ 2 ของร่างยุทธศาสตร์ชาติ 20 ปี ไม่มีการกำหนดเป้าหมายในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ และขาดความเชื่อมโยงในส่วนของเป้าหมายกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2560-2564) ขาดการเตรียมการของหน่วยงานภาครัฐที่เกี่ยวข้องซึ่งไม่ได้อยู่ในเป้าหมายระยะ 5 ปีแรก แต่ต้องรองรับในเฟสถัดไป (ปีที่ 6 ถึงปีที่ 20) ขาดการแสดงสมดุลและบูรณาการในระยะยาวของแผนพัฒนาด้านความมั่นคง และด้านเศรษฐกิจ ทำให้แผนพัฒนา 5 ปี ของหน่วยงานด้านความมั่นคง และหน่วยงานด้านเศรษฐกิจที่รองรับอาจมีความขัดแย้งกัน จึงเสนอแนะให้ภาครัฐกำหนดเป้าหมายเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ในยุทธศาสตร์ชาติ จัดทำแผนแม่บทของประเทศในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์ กำหนดกลไกในการขับเคลื่อนภาคธุรกิจให้เกิดการปฏิบัติตามแผนแม่บทของประเทศ สนับสนุนให้เกิดหน่วยงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในส่วนของภาครัฐเอง และของภาคธุรกิจในลักษณะกลุ่มอุตสาหกรรม เพื่อให้เกิดการจัดตั้งเครือข่ายความร่วมมือในการเฝ้าระวังภัย การแบ่งปันข้อมูลทั้งเรื่องภัยคุกคามไซเบอร์ และแนวปฏิบัติที่ดี

---

[11] ยุทธนา เจียมตระการ. (2560). **การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่.** นักศึกษาวิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561. ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยี.

(Good practices) การพัฒนาความรู้และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากร การจัดตั้งกลุ่มผู้เชี่ยวชาญร่วม (Pool specialist) เพื่อให้ความช่วยเหลือหรือเป็นที่ปรึกษาด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ จัดตั้งศูนย์พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งระดับผู้เชี่ยวชาญในการทำสงครามไซเบอร์ ระดับตรวจสอบหรือประเมินช่องโหว่ของระบบ และระดับประกาศนียบัตรด้านมาตรฐานการจัดการ จัดตั้งศูนย์วิจัยและพัฒนาเครื่องมือ และ/หรือโปรแกรมการป้องกันหรือตรวจสอบภัยคุกคามไซเบอร์ จัดตั้งศูนย์กลางรวบรวมข่าวสาร หรือแหล่งความรู้ด้านภัยคุกคามไซเบอร์ทั้งของประเทศไทยและทั่วโลกที่ภาคธุรกิจหรือประชาชนทั่วไปสามารถเข้าถึงได้ตลอดเวลา

นาวาอากาศเอก ชนินทร เฉลิมทรัพย์ (2560)[12] ได้ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กรการบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการศึกษาค้นคว้า นโยบาย ยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม โดยผลการศึกษาพบว่า การศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กรการบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีองค์กร ที่นำเทคนิคการบริหารจัดการมาใช้ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้น การบูรณาการการบริหารจัดการ ต้องมีเจ้าภาพที่ชัดเจน ทำงานแบบมุ่งเน้นผลงานตามยุทธศาสตร์ โดยใช้ทรัพยากรร่วมกันเพื่อให้บรรลุเป้าหมาย สำหรับภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามที่มีการเปลี่ยนแปลงไปจากเดิม มีรูปแบบการโจมตีที่หลากหลาย การวางแผนป้องกัน คือ การปรับกลยุทธ์ในการรับมือและใช้ระบบมาตรฐานทางไซเบอร์ (ISO/IEC 27001 : 2013) หรือมาตรฐานที่จะถูกพัฒนาขึ้นต่อไป มาช่วยดำเนินการบริหารจัดการ แต่ปัจจัยในการดำเนินงานที่สำคัญที่สุดคือมนุษย์ การศึกษาแนวนโยบายและยุทธศาสตร์ ตลอดจนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่า กระทรวงกลาโหมใช้แนวความคิดในการป้องกันทางไซเบอร์ เช่นเดียวกับการศึกษามั่นคงของประเทศ โดยเน้นการป้องกันเชิงรุก การผนึกกำลังป้องกันประเทศ และการร่วมมือด้านความมั่นคงทางไซเบอร์ โดยได้จัดตั้งส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity operation center : CSDC) เชิงรับและส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer security incident response team : CSIRT)

---

[12] นาวาอากาศเอก ชนินทร เฉลิมทรัพย์. (2560). **แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ.** นักศึกษาวิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561. ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยี.

สำหรับกระทรวงดิจิทัลฯ ได้กำหนด กรอบแนวคิดและนโยบายในระดับชาติกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure : CII) ของประเทศ กำหนดแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard operating procedure : SOP) รวมทั้งเสนอแนวความคิดในการจัดตั้ง Cybersecurity agency (CSA) หน้าที่เป็นหน่วยงานกลาง ในการประสานงานและเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์

ข้อเสนอแนะสำหรับแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีดังนี้ คือ การจัดการความรู้และบริหารความเสี่ยง (Knowledge management & risk) เพื่อให้ผู้นำองค์กร ผู้กำหนดนโยบายและผู้ปฏิบัติ ได้ตระหนักรู้และเก็บสะสมองค์ความรู้ และประสบการณ์ เพื่อเป็นประโยชน์ต่อไป มีการทำงานแบบเครือข่าย (Network) เชื่อมโยงตามประเด็นยุทธศาสตร์ร่วม (Common agenda) ปฏิบัติงานตามมาตรฐานการปฏิบัติทางเทคโนโลยีและจัดตั้งศูนย์การศึกษาและการวิจัย พัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์

พลตรี ปรัชญา เฉลิมวัฒน์ (2560)[13] ได้ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในระดับชาติ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ทั้งปัจจัยด้านเวลาการพัฒนาและด้านการเสริมสร้างกำลังพลไซเบอร์ในรูปแบบกองกำลังผสมพลเรือน ตำรวจ ทหาร และการพิจารณาใช้ข้อกฎหมายที่เกี่ยวข้องกับการเตรียมกำลังพลสำรองในระดับชาติ โดยผลการศึกษาพบว่า แนวทางในการพัฒนากำลังพลด้านไซเบอร์จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งของบุคลากรด้านไซเบอร์ให้กับประเทศชาติ ซึ่งหากนำไปใช้ปฏิบัติได้อย่างจริงจังจะทำให้สามารถลดปัญหาการขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความ “ยั่งยืน” ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี นอกจากนั้นกำลังพลสำรองไซเบอร์ยังเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมซอฟท์แวร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศในอนาคต

ข้อเสนอแนะสำหรับการพัฒนากำลังพลด้านไซเบอร์ ประกอบด้วย 1) การกำหนดแนวทางในการจัดการกำลังพลสำรองที่ปลดประจำการ (ผ่านการเกณฑ์ทหารไปแล้ว) แต่ทำงานในสาขาที่เกี่ยวข้องอยู่แล้ว พิจารณาการเรียกเข้ามาเพื่อเป็นผู้ฝึกให้กับ “ทหารใหม่ไซเบอร์” ได้เป็นอย่างดี โดยที่เขาเหล่านั้นก็ถือได้ว่ามารับใช้ประเทศชาติในอีกทางหนึ่งในมิติของไซเบอร์ 2) การกำหนดนโยบายกำลังพลสำรองไซเบอร์ เพื่อนำทหารกองหนุน/กองเกินที่มีประสบการณ์ด้าน

---

[13] พลตรี ปรัชญา เฉลิมวัฒน์. **แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ.** นักศึกษาวิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561. ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยี.

ไซเบอร์มาประกอบกำลังในสถานการณ์ฉุกเฉิน และการทำให้บุคลกรไซเบอร์สามารถทำงานได้ทั้งภาครัฐและเอกชน อาศัยหลักการ “แบ่งเวลา” ตามความเหมาะสมหรือความต้องการของบุคคลนั้น ๆ 3) การจัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างหน่วยที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารจัดการกำลังพลสำรองไซเบอร์ 4) การยื่นข้อเสนอพิเศษให้บุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์อยู่แล้ว เป็นการสร้างทางเลือกให้แก่ผู้ที่คิดจะหลีกเลี่ยงการเกณฑ์ทหารด้วยมีภาพลักษณ์ของการฝึกทหารใหม่ที่มีการใช้ความรุนแรง แต่สามารถเข้ารับการเกณฑ์ทหารด้วยการฝึกแบบพิเศษเพื่อให้สามารถเข้าทำการในลักษณะปฏิบัติการไซเบอร์ได้ทั้งในหน่วยทหารและองค์กรที่มีความต้องการบุคลากรด้านไซเบอร์

2. การศึกษาวิจัยต่างประเทศ

Darius และคณะ (2560)[14] ได้ศึกษารูปแบบของการกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของประเทศลิทัวเนีย ซึ่งเป็นประเทศสมาชิกกลุ่มสหภาพยุโรป ที่มีการนำระบบ FTTP (Fiber to the premise) ซึ่งเป็นโครงข่ายโทรคมนาคมที่ใช้ optical fiber ตั้งแต่อุปกรณ์ส่งสัญญาณของผู้ให้บริการไปจนถึงพื้นที่บริเวณจุดใช้งานของผู้ใช้ เช่น ห้องนั่งเล่นภายในบ้านหรือ สำนักงานของผู้ใช้ เป็นต้น มาใช้งานสูงที่สุดในกลุ่มสหภาพยุโรป โดยศึกษาจากงานวิจัยที่ผ่านมา บทสัมภาษณ์ผู้เชี่ยวชาญ และกรณีศึกษาที่ดี โดยผลการศึกษาได้เสนอยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 7 ด้าน ประกอบด้วย 1) การคุ้มครองโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Protection of critical infrastructure) 2) การคุ้มครองทรัพยากรข้อมูลภาครัฐ (Protection of state information resources) 3) การสร้างความร่วมมือระหว่างภาครัฐและเอกชน (Cooperation of the private and public sectors) 4) การมอบหมายอำนาจหน้าที่ของหน่วยงานภาครัฐอย่าง

[14] Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Malinauskaitė-van de Castel (2560). **A Model for the National Cyber Security Strategy.** Lithuanian Case. Journal of Security and Sustainability Issues. 2017 March Volume 6 Number 3.

เป็นระบบ (Formation of the institutional system) 5) การพัฒนาวัฒนธรรมไซเบอร์ที่ดี (Development of the cyber culture) 6) การสร้างความร่วมมือกับองค์กรระหว่างประเทศ (International cooperation) และ 7) การพัฒนาสภาพแวดล้อมของการบังคับใช้กฎหมาย (Development of the legal environment)

นอกจากนี้ Darius และคณะ (2560) ได้สรุปว่า ความมั่นคงปลอดภัยไซเบอร์สามารถเชื่อมโยงกับภาคส่วนเศรษฐกิจต่าง ๆ ผ่านการให้บริการทางอิเล็กทรอนิกส์ (e-service) และการติดต่อสื่อสารบนเครือข่ายอิเล็กทรอนิกส์ ปัญหาความมั่นคงปลอดภัยไซเบอร์ของประเทศลิทัวเนียส่วนใหญ่เกิดจากประเทศเพื่อนบ้าน ซึ่งหากประเทศเพื่อนบ้านมียุทธศาสตร์ที่แตกต่างออกไป การสร้างความร่วมมือในการค้นหากลไกวิธีจัดการกับภัยคุกคามไซเบอร์อาจทำได้ยากขึ้น จึงมีความจำเป็นต้องจัดทำยุทธศาสตร์ให้มีความง่ายต่อการเข้าใจ และมีค่าบ่งชี้ที่เป็นสากล เพื่อให้สามารถสื่อสารกับประเทศอื่น ๆ ด้วยความเข้าใจที่ตรงกัน อย่างไรก็ดี ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ยังจำเป็นต้องเน้นการรับมือกับสถานการณ์และอุบัติการณ์ทางไซเบอร์ที่เกิดขึ้นภายในประเทศ เนื่องจากภัยคุกคามไซเบอร์ที่เกิดขึ้นทั่วโลกย่อมมีความแตกต่างกัน

Kaushik และคณะ (2562)[15] ได้ศึกษาเปรียบเทียบยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศบังคลาเทศกับต่างประเทศ เพื่อให้ประเทศบังคลาเทศ มียุทธศาสตร์ที่ทันสมัย โดยศึกษาและจัดหมวดหมู่ของยุทธศาตร์ความมั่นคงปลอดภัยไซเบอร์ของ 5 ประเทศ ได้แก่ สหรัฐอเมริกา ญี่ปุ่น สิงคโปร์ อินเดีย และมาเลเซีย และกำหนดสถานะของแต่ละยุทธศาสตร์ออกเป็น 3 สถานะ ได้แก่ 1) มี 2) มีบางส่วน และ 3) ไม่มี โดยพบว่า ยุทธศาสตร์ที่ทุกประเทศมีเหมือนกันมีทั้งสิ้น 11 ยุทธศาสตร์ ได้แก่ 1) การสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ (Promote cybersecurity R& D) 2) การสนับสนุนการศึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Promote cybersecurity education) 3) การบริหารจัดการความเสี่ยง (Ensuring ongoing risk assessment) 4) การสนับสนุนนโยบายรับมืออาชญากรรมไซเบอร์ (Promote counter cybercrime policy) 5) การบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ในกฎหมายระหว่างประเทศ (Promote cybersecurity in international law) 6) การมีกฎระเบียบและการกำหนดอำนาจหน้าที่ขององค์กร (Forms of regulation and institutional aspects) 7) การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและ

---

[15] Kaushik Sarker, Hasibur Rahman, Khandaker Farzana Rahman, Md. Shohel Arman, Saikat Biswas, Touhid Bhuiyan. (2562). **A Comparative Analysis of the Cyber Security Strategy of Bangladesh.** International Journal on Cybernetics & Informatics (IJCI) Vol. 8, No.2, April 2019.

เสรีภาพของประชาชน (Balancing Cybersecurity with civil liberties) 8) การสร้างความร่วมมือระหว่างภาครัฐและเอกชน (Public private platform) 9) การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ (Inter-governmental cooperation) 10) การสร้างความร่วมมือระหว่างภูมิภาค (Regional cooperation) และ 11) การสร้างความร่วมมือระหว่างรัฐบาล (Intra-governmental cooperation) ดังปรากฏในตารางที่ 2-1

ตารางที่ 2-1 เปรียบเทียบยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศบังคลาเทศและประเทศอื่น ๆ

ยุทธศาสตร์	สถานะ	สหรัฐอเมริกา	ญี่ปุ่น	สิงคโปร์	อินเดีย	มาเลเซีย	บังคลาเทศ
1. การสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ (Promote cybersecurity R& D)	มี	√	√	√	√		
	มีบางส่วน					√	√
	ไม่มี						

ยุทธศาสตร์		สถานะ	สหรัฐอเมริกา	ญี่ปุ่น	สิงคโปร์	อินเดีย	มาเลเซีย	บังคลาเทศ
2. การสนับสนุนการศึกษา (Promote cybersecurity education)		มี	√	√	√	√	√	√
		มีบางส่วน						
		ไม่มี						
3. การบริหารจัดการความเสี่ยง (Ensuring ongoing risk assessment)		มี	√		√			√
		มีบางส่วน		√		√	√	
		ไม่มี						
4. การสนับสนุนนโยบายรับมืออาชญากรรมไซเบอร์ (Promote counter cybercrime policy)		มี	√					
		มีบางส่วน		√	√	√		√
		ไม่มี					√	
5. การบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ในกฎหมายระหว่างประเทศ (Promote cybersecurity in international law)		มี	√					
		มีบางส่วน		√				√
		ไม่มี			√	√	√	
6. การมีกฎระเบียบและการกำหนดอำนาจหน้าที่ขององค์กร (Forms of regulation and institutional aspects)		มี	√	√	√	√	√	√
		มีบางส่วน						
		ไม่มี						
7. การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและเสรีภาพของประชาชน (Balancing cybersecurity with civil liberties)		มี	√	√	√			
		มีบางส่วน						√
		ไม่มี				√	√	
8. รูปแบบของความร่วมมือ (Types of cooperation)	i. ความร่วมมือภาครัฐและเอกชน (Public private platform)	มี	√		√			√
		มีบางส่วน		√		√	√	
		ไม่มี						
	ii. ความร่วมมือระหว่างหน่วยงานภาครัฐ (Inter-governmental cooperation)	มี				√		√
		มีบางส่วน	√	√	√			
		ไม่มี					√	
	iii. ความร่วมมือระหว่างภูมิภาค (Regional cooperation)	มี						
		มีบางส่วน	√	√	√	√		
		ไม่มี					√	√
	iv. ความร่วมมือระหว่างรัฐบาล (Intra-governmental cooperation)	มี	√	√	√	√	√	√
		มีบางส่วน						
		ไม่มี						

ที่มา : Kaushik และคณะ, 2562

Narmeen และ Ashraf (2559)[16] ได้ศึกษาเปรียบเทียบยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของ 20 ประเทศ โดยพิจารณาจากกฎหมาย การดำเนินงาน นโยบายที่เกี่ยวข้อง โดยยุทธศาสตร์ส่วนใหญ่เน้นการมอบหมายหน่วยงานรับผิดชอบในการรับมือกับภัยคุกคามไซเบอร์ เช่น ทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams : CERTs) และทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response teams: CSIRTs) เป็นต้น การให้ความสำคัญกับการสร้างความตระหนักรู้ทางไซเบอร์ (Cyber awareness) และขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ด้วย ทั้งนี้ หากพิจารณาความมั่นคงปลอดภัยไซเบอร์ของประเทศพัฒนาแล้วตามการจัดลำดับของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ในปี 2558 จะเห็นได้ว่า ประเทศสหรัฐอเมริกาเป็นประเทศที่อยู่อันดับที่ 1 เนื่องจากมีการปรับปรุงยุทธศาสตร์ให้ทันสมัยอย่างสม่ำเสมอ และเป็นประเทศที่มียุทธศาสตร์และแผนปฏิบัติการที่ชัดเจนทั้งเชิงรับและเชิงรุก รองลงมาคือกลุ่มประเทศแคนาดา สเปน ญี่ปุ่น และออสเตรเลีย ซึ่งมีอัตราการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร และอัตราการเกิดอาชญากรรมไซเบอร์อยู่ในระดับสูง แสดงได้ดังตารางที่ 2-2

ตารางที่ 2-2 การจัดลำดับความมั่นคงปลอดภัยไซเบอร์ของประเทศพัฒนาแล้ว

ลำดับของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Ranking)	**ประเทศ**
1	สหรัฐอเมริกา
2	แคนาดา
3	ออสเตรเลีย
4	นิวซีแลนด์
5	เอสโตเนีย ญี่ปุ่น สหราชอาณาจักร เยอรมัน
6	ออสเตรเลีย อิสราเอล เนเธอร์แลนด์
8	ฟินแลนด์
9	ฝรั่งเศส สเปน
12	สาธารณรัฐเช็ก

[16] Narmeen Shafqat และAshraf Masood. (2559). **Comparative Analysis of Various National Cyber Security Strategies**. International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016.

ที่มา : Narmeen และ Ashraf, 2559

การจัดลำดับความมั่นคงปลอดภัยไซเบอร์ของประเทศกำลังพัฒนาตามแนวคิดของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) จะเห็นได้ว่า ประเทศมาเลเซียเป็นประเทศที่มีความก้าวหน้าด้านความมั่นคงปลอดภัยไซเบอร์มากที่สุด ส่วนประเทศอินเดียและอิหร่านเป็นกลุ่มประเทศที่ประสบปัญหาการโจมตีทางไซเบอร์ในระดับสูง แสดงได้ดังตารางที่ 2-3

ตารางที่ 2-3 การจัดลำดับความมั่นคงปลอดภัยไซเบอร์ของประเทศกำลังพัฒนา

ลำดับของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Ranking)	**ประเทศ**
3	มาเลเซีย
5	อินเดีย
7	ตุรกี
19	อิหร่าน

ที่มา : Narmeen และ Ashraf, 2559

หากพิจารณาหน่วยงานรับผิดชอบหลักของแต่ละประเทศ เพื่อพิจารณากลไกการสั่งการเพื่อรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ จะเห็นได้ว่า หลายประเทศกำหนดหน่วยงานหลักที่แตกต่างกัน รายละเอียดปรากฏตามตารางที่ 2-4

ตารางที่ 2-4 หน่วยงานรับผิดชอบหลักการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

กลุ่ม	**หน่วยงานรับผิดชอบหลัก**	**ประเทศ**
1	ผู้ว่าการรัฐ	สหรัฐอเมริกา
2	สำนักงานคณะรัฐมนตรี	ออสเตรเลีย ญี่ปุ่น สหราชอาณาจักร
3	กระทรวง (เทคโนโลยีสารสนเทศ มหาดไทย	แคนาดา เยอรมัน อินเดีย สาธารณรัฐเช็ก เนเธอร์แลนด์ นิวซีแลนด์ ซาอุดีอาระเบีย

	กฎหมาย กลาโหม)	มาเลเซีย ตุรกี อิหร่าน ออสเตรีย สเปน
4	หน่วยงานใหม่	ฝรั่งเศส เอสโตเนีย

ที่มา : Narmeen และ Ashraf, 2559

การจัดตั้งทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (CERTs) และทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (CSIRTs) ระดับประเทศ ถือได้ว่าเป็นวิธีการรับมือภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ โดยมีลักษณะของการเตือนภัยล่วงหน้า โดยแต่ละประเทศได้มีเวลาที่ริเริ่มการจัดตั้ง CERTs แตกต่างกันไป รายละเอียดปรากฏตามตารางที่ 2-5

ตารางที่ 2-5 การจัดตั้งทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (CERTs) ในแต่ละประเทศ

ประเทศ	**ปี ค.ศ. ที่มีการจัดตั้ง CERT**
ออสเตรเลีย	2010
ออสเตรีย	2008
แคนาดา	2003
สาธารณรัฐเช็ก	2011
เอสโตเนีย	2006
ฟินแลนด์	2014
ฝรั่งเศส	2008
เยอรมัน	2012
อินเดีย	2004
อิสราเอล	2014
ญี่ปุ่น	1996
มาเลเซีย	1997
เนเธอร์แลนด์	2012

ประเทศ	ปี ค.ศ. ที่มีการจัดตั้ง CERT
นิวซีแลนด์	2011
ซาอุดีอาระเบีย	2006
สเปน	2008
ตุรกี	2007
สหราชอาณาจักร	2014
สหรัฐอเมริกา	2003

ที่มา : Narmeen และ Ashraf, 2559

แนวคิดของผู้ทรงคุณวุฒิ

ในการศึกษาวิจัยครั้งนี้ ได้สัมภาษณ์ผู้ทรงคุณวุฒิ ซึ่งเป็นกรรมการในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[17] ซึ่งแต่งตั้งขึ้นภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จำนวน 3 ท่าน ประกอบด้วย 1) พันตำรวจเอก ญาณพล ยั่งยืน (กรรมการผู้ทรงคุณวุฒิ ด้านวิศวกรรมศาสตร์) 2) นายไพบูลย์ อมรภิญโญเกียรติ (กรรมการผู้ทรงคุณวุฒิด้านกฎหมาย) และ 3) รองศาสตราจารย์ปณิธาน วัฒนายากร (กรรมการผู้ทรงคุณวุฒิด้านความสัมพันธ์ระหว่างประเทศ) โดยผู้ทรงคุณวุฒิได้ให้ข้อเสนอแนะ โดยมีรายละเอียดดังต่อไปนี้

1. พันตำรวจเอกญาณพล ยั่งยืน กรรมการผู้ทรงคุณวุฒิ ด้านวิศวกรรมศาสตร์ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ปัจจุบันมีการใช้สื่อสังคมออนไลน์ (Social network) และระบบแอปพลิเคชันต่าง ๆ ในชีวิตประจำวันของผู้คนในโลกเป็นอย่างมากมาย แน่นอนว่า เพื่อเสริมสร้างประสิทธิภาพในการทำงาน ในชีวิตประจำวัน เสริมความรู้ ความบันเทิง ฯลฯ ซึ่งระบบส่วนใหญ่นั้น ก็ต้องมาจาก

[17] ประกาศสำนักนายกรัฐมนตรี เรื่อง แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (วันที่ 3 มกราคม 2563) ราชกิจจานุเบกษา. เล่ม 137 ตอนที่ 2 ง.

ต่างประเทศ ทั้งนี้ เพราะระบบต่าง ๆ จำเป็นจะต้องใช้ระบบฐานข้อมูลขนาดใหญ่ (Big data) เป็นข้อมูลปัจจุบันสมัย (Real time) ต้องมีผู้ใช้งานมหาศาลจึงจะเพิ่มประสิทธิภาพได้ ต้องมีเทคโนโลยีที่ล้ำหน้าทันสมัย ซึ่งจำเป็นจะต้องใช้ทุนมหาศาล ยากที่ผู้ประกอบการรายเล็กในประเทศจะสามารถกระทำได้ ข้อดีอีกอย่างคือ ระบบส่วนใหญ่มักจะเป็นของฟรี (ดูเหมือนจะฟรี) จึงทำให้มีผู้ใช้งานกันอย่างกว้างขวางทั่วโลกด้วยความเชื่ออย่างสนิทใจ “ว่าฟรี” ทำให้ผู้ประกอบการมีข้อมูลของผู้ใช้บริการอย่างมากมาย แต่แน่นอนว่า ของฟรีย่อมไม่มีในโลก เบื้องต้น เมื่อมีผู้ใช้งานมากขึ้นก็ย่อมมีเพียงโฆษณาเข้ามาบ้าง ต่อมาเมื่อมีเทคโนโลยี AI เข้ามาจึงทำให้ มีการแสวงหาประโยชน์จากข้อมูลของผู้มาใช้บริการได้ง่ายและมากขึ้น ผู้ประกอบการจึงสามารถนำข้อมูลเหล่านั้นมาวิเคราะห์หาความสัมพันธ์ รสนิยมความชอบไม่ชอบ ทัศนคติ ชีวิตประจำวัน และสามารถส่งข้อมูลบางประการเพื่อมาโน้มน้าวผู้คนตามเป้าหมายให้เป็นไปตามประสงค์ได้ ซึ่งนับเป็นภัยอย่างมหันต์ จนมีบางท่านกล่าวว่า การที่บริษัทยักษ์ใหญ่ต่างชาติ ยินยอมให้เราใช้แอปพลิเคชันต่าง ๆ ฟรีนั้น เปรียบเสมือนกัน พวกเราผู้ใช้บริการเป็นสัตว์ที่ถูกเลี้ยงในฟาร์มปศุสัตว์ต่าง ๆ ซึ่งจะได้การเลี้ยงดูเป็นอย่างดี กินฟรี อยู่ฟรี ไม่ต้องทำอะไร กินอาหารที่เขาป้อนให้ไปเรื่อยๆ ขุนจนอ้วนพี เมื่อถึงเวลาเจ้าของคอกปศุสัตว์ ก็จะนำไปเชือดได้อย่างดีมีราคา

ตัวอย่างที่มีให้เห็นแล้วได้แก่ กรณี อาหรับสปริง (Arab Spring) ที่ทำให้รัฐบาลในหลายประเทศมีการล่มสลายและถูกเปลี่ยนแปลง การโน้มน้าวให้ผู้มีสิทธิออกเสียงเลือกตั้งผู้นำประเทศ มีความชื่นชอบฝ่ายใดเพิ่มขึ้น และไม่ชอบหรือเกลียดชังฝ่ายใดที่เขากำหนดได้ง่ายขึ้น นอกจากนั้นเจ้าของแอปพลิชันต่าง ๆ เหล่านี้ นอกจากจะมักหลีกเลี่ยงไม่ชำระภาษีให้แต่ประเทศนั้น ๆ แล้ว ยังไม่ให้ความร่วมมือใด ๆ กับการปฏิบัติตามกฎหมายอื่น ๆ ของประเทศนั้น ๆ อีกด้วย โดยไม่สนใจเรื่องของความมั่นคงของประเทศนั้น ๆ จนทำตัวเหมือนเป็น ผู้อยู่เหนือกฎหมาย โดยอ้างว่าไม่มีบริษัทหรือสาขาในประเทศนั้น ๆ

สิ่งต่าง ๆ เหล่านี้ สมควรแล้วที่ประเทศเราจำเป็นจะต้องมีการศึกษาถึงความเหมาะสมเรื่อง ปัญหาอธิปไตยทางไซเบอร์ กันอย่างจริงจังให้ครอบคลุมในทุกมิติ เพื่อให้มีการเตรียมการแก้ไขไว้ก่อนที่เราจะสูญเสียอธิปไตยทางไซเบอร์ในอันดับแรกไปมากกว่านี้ และตามไปด้วยอธิปไตยของชาติอันเป็นที่รักของเรา เป็นอันดับต่อไป

2. นายไพบูลย์ อมรภิญโญเกียรติ กรรมการผู้ทรงคุณวุฒิด้านกฎหมาย ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เมื่อพิจารณาถึงรายละเอียดของงานวิจัยดังกล่าวแล้ว ผู้ทรงคุณวุฒิด้านกฎหมายเห็นด้วยกับงานวิจัยดังกล่าว แต่เห็นควรเพิ่มเติมรายละเอียดเกี่ยวกับการป้องกันหรือยุทธศาสตร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของประเทศ ในหัวข้อ “Quick win project” (กรณีที่มีการแก้ไขแผนยุทธศาสตร์แห่งชาติ) ดังนี้

ในส่วนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ พ.ศ. 2560 – 2564 ระบุให้ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามทางความมั่นคงแห่งชาติ ซึ่งกำหนดแนวทางไว้ในประเด็นที่ 3.7.15 ในเรื่องการป้องกันความมั่นคงทางไซเบอร์ โดยระบุให้ต้องมีกลยุทธ์ 6 ด้าน คือ

2.1 การพัฒนาขีดความสามารถขององค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือน และตำรวจ

2.2 การพัฒนากรอบความร่วมมือของประเทศและอาเซียน

2.3 การพัฒนามนุษย์ องค์ความรู้ ให้ตระหนักรู้ถึงความสำคัญของภัยคุกคามทางไซเบอร์

2.4 การปกป้อง ป้องกันภัยคุกคามทางไซเบอร์ โดยสร้างเครือข่ายทุกภาคส่วนทั้งในประเทศ และนอกประเทศ

2.5 *** การพัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อรักษาความมั่นคงทางไซเบอร์ ***

2.6 การส่งเสริมพัฒนาขีดความสามารถขององค์กรทุกภาคส่วนให้มีความรู้ความเชี่ยวชาญทางไซเบอร์

ในส่วนประเด็นข้อที่ 2.5 ในเรื่องการป้องกันรักษาความมั่นคงของชาติ และการมั่นคงทางไซเบอร์ รวมถึงอธิปไตยทางไซเบอร์ เดิมระบุกฎหมาย (Legal framework) ไว้เพียงเรื่อง คือ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 รวมถึงหมวดกฎหมายความมั่นคงปลอดภัยที่เป็นกฎหมายพิเศษ

ผู้ทรงคุณวุฒิ มีความเห็นว่า ควรเพิ่มเติมกฎหมายอีก 1 ฉบับที่เกี่ยวข้องกับการดูแลความมั่นคงและการดูแลอธิปไตยทางไซเบอร์ (ในกรณีที่มีการแก้ไขแผนยุทธศาสตร์แห่งชาติ หรือแผนยุทธศาสตร์แห่งชาติในปี พ.ศ. 2565 - 2567 คือ “พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” เนื่องจากในการดูแลเรื่องการรักษาความปลอดภัยมั่นคงทางไซเบอร์ ซึ่งตามรายงานการวิจัยของอาจารย์ปริญญาฯ ผู้ศึกษา ระบุว่า ควรจะพัฒนากฎหมายลูก มีกองบัญชาการ และพัฒนาตำรวจไซเบอร์ หรือดูแลหน่วยงานที่ดูแลความปลอดภัยทางไซเบอร์โดยเฉพาะ ในกรณีดังกล่าว ผู้ทรงคุณวุฒิเห็นว่า กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมควรทำงานร่วมมือกับสภาความมั่นคงแห่งชาติ (สมช.) และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยร่วมกันบูรณาการให้กฎหมายลูกที่ออกตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความสอดคล้องกับแผนความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ และสอดคล้องกับนโยบายและสอดคล้องกับนโยบายแผนแม่บทและการปรับใช้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เพื่อหาจุดถ่วงดุลระหว่างความมั่นคงปลอดภัยทางไซเบอร์ และสร้างการให้ความคุ้มครอง

ข้อมูลส่วนบุคคล เนื่องจากองค์ประกอบและมาตรการหลักของการปกป้องอธิปไตยไซเบอร์ และการป้องกันความปลอดภัยไซเบอร์ ที่ประกอบด้วย 3 ส่วนคือ บุคลากร (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) เป็นมาตรการที่ใช้แก้ไขปัญหาเพื่อใช้รักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity solution) ในส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งสิ้น กล่าวคือ การดำเนินการเพื่อดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ไม่ว่าจะเป็นการป้องกัน (Prevention) การลดความเสี่ยง (Reduction) การตรวจสอบ (Detection) การป้องปราม (Repression) การแก้ไข (Correction) และการประเมินความเสี่ยง (Evaluation) เป็นกระบวนการที่ต้องใช้ข้อมูลส่วนบุคคลของประชาชนและภาคส่วนต่าง ๆ เพื่อบูรณาการให้เกิดความมั่นคงปลอดภัยและรักษาอธิปไตยไซเบอร์ได้

โดยผู้ทรงคุณวุฒิขอเสนอเพิ่มเติมให้หน่วยงานความมั่นคงควรออกหรือบังคับใช้กฎหมายลำดับรองข้างต้น กล่าวคือ นโยบาย แผน กฎกระทรวง ข้อบังคับ และแนวทางต่าง ๆ หน่วยงานที่เกี่ยวข้องจำเป็นต้องใช้ “ข้อมูลส่วนบุคคล” ของประชาชน และ “ข้อมูลส่วนบุคคล” ที่อยู่ในหน่วยงานต่าง ๆ ทั้ง ภาครัฐและเอกชน เพื่อวัตถุประสงค์ตามแผนความมั่นคงปลอดภัยแห่งชาติ และความมั่นคงปลอดภัยทางไซเบอร์ ตามแผนแม่บทยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดังต่อไปนี้

ก) ป้องกันภัยคุกคามต่อความมั่นคงแห่งชาติ และภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นจากการโจมตีด้วยวิธีการทางอาชญากรรมทางคอมพิวเตอร์

ข) เฝ้าระวังความเสี่ยง ติดตาม วิเคราะห์ ประมวลผล ภัยคุกคามเกี่ยวกับเรื่องความมั่นคงทั้งทางกายภาพและไซเบอร์ที่อาจเกิดขึ้น รวมถึงการกระทำที่อาจเป็นภัยต่อความมั่นคงของรัฐ หรือเพื่อรักษาไว้ซึ่งระบอบประชาธิปไตยอันมีพระมหากษัตริย์อันเป็นประมุข ความปลอดภัยของประชาชน ความสงบเรียบร้อยของส่วนรวม หรือภัยพิบัติสาธารณะ

ค) การดำเนินการสืบสวนสอบสวนข้อเท็จจริง รวบรวมพยานหลักฐานเพื่อดำเนินคดีกับบุคคลที่กระทำความผิดหรืออาชญากรรมคอมพิวเตอร์ ซึ่งก่อให้เกิดภัยคุกคามทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

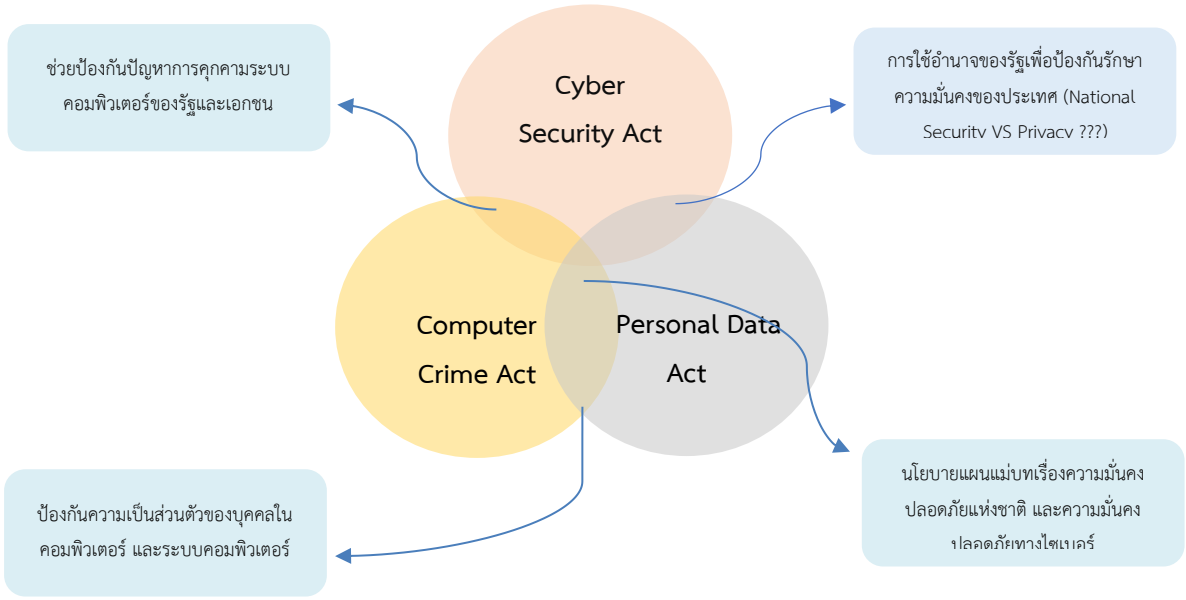
ง) การประเมินสถานการณ์ภัยคุกคามทางไซเบอร์ ตรวจสอบแหล่งที่มาของการกระทำความผิดทางไซเบอร์

จ) การดำเนินการรวบรวมพยานหลักฐาน เพื่อดำเนินคดีกับผู้กระทำความผิดที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

ฉ) การดำเนินการกู้ข้อมูลคอมพิวเตอร์ที่ถูกทำลาย การตรวจสอบข้อมูลหรือรักษาสถานะของข้อมูลคอมพิวเตอร์เพื่อหาข้อบกพร่องในทางเทคนิค

ช) การกำหนดมาตรการการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ที่ต้องมีมาตรการการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐาน

แผนภาพที่ 2-8 ความเกี่ยวข้องของกฎหมาย 3 ฉบับ



ที่มา : นายไพบูลย์ อมรภิญโญเกียรติ กรรมการผู้ทรงคุณวุฒิด้านกฎหมาย

3. รองศาสตราจารย์ปณิธาน วัฒนายากร กรรมการผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ผู้ทรงคุณวุฒิด้านความสัมพันธ์ระหว่างประเทศ เห็นว่า แนวทางการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ (ยุทธศาสตร์ฯ) ควรจำแนกออกตามองค์กรที่มีบทบาทเป็นผู้นำของการขับเคลื่อนยุทธศาสตร์ในแต่ละประเด็นยุทธศาสตร์ โดยควรจำแนกแนวทางการขับเคลื่อนการพัฒนายุทธศาสตร์ฯ ออกเป็น 3 แนวทาง ได้แก่ 1) แนวทางขับเคลื่อนยุทธศาสตร์ที่ให้รัฐมีบทบาทนำ (Government-led) 2) แนวทางขับเคลื่อนยุทธศาสตร์ฯ ที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางการขับเคลื่อนยุทธศาสตร์ฯ ที่แพลตฟอร์มมีบทบาทนำ (Platform-led) โดยสรุปได้ ดังนี้

3.1 แนวทางการขับเคลื่อนยุทธศาสตร์ฯ ที่ให้รัฐมีบทบาทนำ (Government-led) โดยรัฐบาลควรอาศัยกลไกหน่วยงานภาครัฐ เช่น สกมช. กมช. ดศ. สมช. เป็นต้น เพื่อขับเคลื่อน

แผนปฏิบัติงานที่หน่วยงานรัฐต้องเป็นผู้นำ เช่น การสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ การตั้งหน่วยงานรับมือภัยคุกคามไซเบอร์ เป็นต้น กำหนดหน่วยงานกลางที่บทบาทในการบูรณาการและประสานการทำงานของหน่วยงานภาครัฐต่าง ๆ รัฐบาลต้องเป็นผู้นำในการสร้างความร่วมมือระหว่างรัฐและผู้เชี่ยวชาญในภาคเอกชน ทั้งภายในประเทศและภายนอกประเทศในการขับเคลื่อนแผนปฏิบัติการ (Action Plan) และโครงการที่เกี่ยวข้อง เช่น การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน การระบุและบริหารความเสี่ยง การเตือนภัยล่วงหน้า การรณรงค์สร้างความตระหนักรู้ให้กับประชาชน การพัฒนาบุคลากรภาครัฐให้มีขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

3.2 แนวทางการขับเคลื่อนยุทธศาสตร์ฯ ที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian led) โดยภาครัฐควรเสริมสร้างขีดความสามารถด้าน Cybersecurity ให้กับภาคประชาชนอย่างต่อเนื่อง ควรอาศัยกลไกของกระทรวงศึกษาธิการ หน่วยงานภาครัฐ รัฐวิสาหกิจ ภาคเอกชน ในการพัฒนาความรู้และความตระหนักรู้ให้แก่ประชาชน เช่น การปรับปรุงหลักสูตรการเรียนการสอนตั้งแต่ระดับชั้นประถมศึกษา และมัธยมศึกษา รวมถึงสาขาวิชาด้าน Cybersecurity ในระดับอุดมศึกษา การให้รัฐวิสาหกิจและภาคเอกชนมีส่วนร่วมในการสร้างความรับผิดชอบต่อสังคมผ่านการจัดทำโครงการถ่ายทอดความรู้และสร้างความตระหนักรู้ด้าน Cybersecurity ให้แก่เยาวชน เพื่อให้ประชาชนมีภูมิคุ้มกันทางไซเบอร์ มีความรู้ทางดิจิทัล และรู้เท่าทันภัยคุกคามไซเบอร์ทุกรูปแบบ

3.3 แนวทางการขับเคลื่อนยุทธศาสตร์ฯ ที่ให้แพลตฟอร์มมีบทบาทนำ (Platform Led) โดยภาครัฐควรส่งเสริมและสนับสนุนการวิจัยและพัฒนาการสร้างแพลตฟอร์มของประเทศไทย ที่เป็นนวัตกรรมทางเทคโนโลยีดิจิทัล ตอบสนองความต้องการของประชาชนได้อย่างมีประสิทธิภาพสูงกว่าแพลตฟอร์มต่างประเทศ และสามารถดูแลข้อมูลส่วนบุคคลของประชาชนด้วย ซึ่งแพลตฟอร์มต่างประเทศไม่สามารถกระทำได้ รวมถึงสามารถป้องกันประชาชนจากการรุกล้ำทางเศรษฐกิจ สังคม วัฒนธรรม ความคิด ความเชื่อ อุดมการณ์ ทัศนคติ ค่านิยมผ่านสื่อสังคมออนไลน์ (Social media) ของแพลตฟอร์มต่างประเทศ เช่น ข่าวปลอม ปฏิบัติการข่าวสารที่หวังผลทางการเมือง การยุยงปลุกปั่นที่ส่งผลกระทบต่อสถาบันหลักของชาติ เป็นต้น โดยอาจระดมผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัลทั้งจากภายในประเทศและต่างประเทศมาช่วยวิจัยและพัฒนา ซึ่งอาจให้แรงจูงใจต่าง ๆ เช่น สิทธิประโยชน์ทางภาษี เป็นต้น

ทั้งนี้ ควรจัดให้มีหน่วยงานฝ่ายความมั่นคงทำหน้าที่ประสานงานทั้ง 3 ภาคส่วนในแนวทาง co-ordination mechanism เพื่อให้เกิดการบูรณาการในการทำงานร่วมกัน เช่น จัดให้มีหน่วยงานภายใต้สำนักงานสภาความมั่นคงแห่งชาติ ทำหน้าที่เป็น co-ordination body

กรอบความคิดของงานวิจัย

1. ในการศึกษาวิจัยนี้ จะนำกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model : CMM) ของ GCSCC แห่ง University of Oxford มาประยุกต์ใช้ในการประเมินศักยภาพและขีดความสามารถของประเทศไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นการวิเคราะห์และระบุประเด็นปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เพื่อเสนอแนะแนวทางการแก้ไขปัญหาใหญ่ด้านความมั่นคงของประเทศ

2. ในการศึกษาวิจัยนี้ จะนำข้อเสนอแนะของผู้ทรงคุณวุฒิมาสังเคราะห์เป็นแนวทางการแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยเสนอแนะโครงการและแผนปฏิบัติการภายใต้แนวทางการขับเคลื่อนการแก้ไขปัญหา หน่วยงานรับผิดชอบ รวมถึงเพื่อให้ข้อเสนอแนะเชิงนโยบายต่อรัฐบาลเพื่อเป็นแนวทางในการปรับปรุงยุทศาสตร์ชาติ 20 ปี ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยรอบระยะเวลาของการทบทวนปรับปรุงแก้ไขยุทธศาสตร์ชาติครั้งแรกคือ ปี 2565 (เนื่องจากกรอบระยะเวลาของการทบทวนยุทธศาสตร์ชาติคือ 5 ปี หลังจากยุทธศาสตร์ชาติมีผลใช้บังคับในปี 2560)

สรุป

จากการการทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง ในการศึกษานี้พบว่าการพัฒนาและจัดทำยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ควรมีเครื่องมือที่เหมาะสมในการวิเคราะห์ปัญหาของประเทศ ซึ่งเป็นการประเมินสภาพแวดล้อมทางไซเบอร์ของประเทศ การประเมินขีดความสามารถของประเทศในการรับมือกับภัยคุกคามทางไซเบอร์ โดยที่ปัจจุบัน เครื่องมือที่เหมาะสมดังกล่าวคือ กรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model : CMM) ของ GCSCC แห่ง University of Oxford ซึ่งแบ่งมิติของการประเมินขีดความสามารถของประเทศออกเป็น 5 มิติ ได้แก่ มิติที่ 1 National cybersecurity framework and policy มิติที่ 2 Cyber culture and society มิติที่ 3 Cybersecurity education, training and skills มิติที่ 4 legal and regulatory frameworks และมิติที่ 5 Standards, organizations, and technologies ดังนั้น การศึกษานี้ใช้ CMM ในการวิเคราะห์ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

นอกจากนี้ จากการศึกษาแนวคิดในการพัฒนายุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี (Good practice) ของต่างประเทศ พบว่า โครงสร้างยุทธศาสตร์

ของประเทศให้ความสำคัญกับวิสัยทัศน์และบทบาทผู้นำ ซึ่งเป็นปัจจัยแห่งความสำเร็จที่จะจุดประกายให้ทุกภาคส่วนมีการบูรณาการ ประสานความร่วมมือ (Inclusiveness) ความเข้าใจต่อปัญหา ประเภท แหล่งที่มาของภัยคุกคาม การปกป้องโครงสร้างพื้นฐานและบริการที่สำคัญยิ่งยวดของประเทศ การบริหารจัดการความเสี่ยงและการเตือนภัยล่วงหน้า การเพิ่มขีดความสามารถและความตระหนักรู้ (Awareness) ให้กับประชาชนและบุคลากรภาครัฐ การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ทั้งภายในและภายนอกประเทศ การบัญญัติกฎหมายและการบังคับใช้กฎหมาย การฝึกซ้อมแผนรับมือ การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและเสรีภาพของประชาชน รวมถึงการวิจัยและพัฒนานวัตกรรมด้านเทคโนโลยีดิจิทัลเพื่อรับมือกับภัยคุกคามทางไซเบอร์

บทที่ 3
การพิจารณายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเฉพาะที่มีความสอดคล้องกับอธิปไตยไซเบอร์

วิเคราะห์กระบวนการ รูปแบบ และลักษณะของปัญหาอธิปไตยไซเบอร์ในระดับสากล

ปรากฏการณ์ “Digital transformation” และการเข้าสู่ยุค S-M-I-C (Social–Mobile–Information–Cloud) นำไปสู่การเจริญเติบโตของธุรกิจแพลตฟอร์ม (Platform) ซึ่งธุรกิจไม่จำเป็นต้องผลิตสินค้าและบริการเอง แต่เป็นการให้บริการอำนวยความสะดวกและเป็นตัวกลางในการทำธุรกิจระหว่างลูกค้ามากกว่าหนึ่งประเภท ตัวอย่าง Platform ประเภทเครือข่ายสังคม เช่น Facebook Twitter Line Instagram เป็นต้น ประเภทค้าปลีก เช่น eBay Alibaba Amazon เป็นต้น ประเภทสื่อ เช่น YouTube เป็นต้น ประเภทการชำระเงิน เช่น PayPal Alipay เป็นต้น ประเภทระบบปฏิบัติการบนสมาร์ทโฟน เช่น ios Android เป็นต้น ประเภทการท่องเที่ยว เช่น Airbnb เป็นต้น ประเภทบริการรถสาธารณะ เช่น Uber Grab เป็นต้น

นอกจากจากรูปแบบกระบวนการดำเนินธุรกิจที่เปลี่ยนแปลงไปตามการพัฒนาเทคโนโลยีแล้ว การวิเคราะห์ทางการตลาดยังเปลี่ยนแปลงไปด้วย จากเดิมที่วิเคราะห์กลุ่มเป้าหมายด้วยหลักประชากรศาสตร์ (Demographic) เช่น อายุ เพศ การศึกษา รายได้ สถานภาพ เป็นต้น เป็นการวิเคราะห์กลุ่มเป้าหมายด้วยหลักจิตนิสัย (Psychographic) เช่น รูปแบบการดำเนินชีวิต (Lifestyles) ความชื่นชอบ ความเชื่อ ค่านิยม เป็นต้น โดยอาศัยข้อมูลที่อยู่ในความครอบครองของแพลตฟอร์ม (Platform) บนสมาร์ทโฟน หรือเครือข่ายสังคมออนไลน์ (Social media) ซึ่งทำให้ธุรกิจ Platform มีความได้เปรียบในการประกอบธุรกิจ

แม้ว่าเครือข่ายสังคมออนไลน์ (Social media) และสมาร์ทโฟนจะเป็นประโยชน์ต่อการใช้ชีวิตประจำวันของทุกคนอย่างมหาศาล ด้วยเจตนารมณ์ที่หวังจะส่งมอบสิ่งที่ดีที่สุดให้ผู้ใช้บริการ แต่ผู้ให้บริการย่อมถูกกดดันด้วยภาวะการแข่งขันของธุรกิจ เพื่อเข้าถึงผู้ใช้บริการให้มากที่สุด จึงสร้างผลเสียต่อประชาชนโดยไม่รู้ตัว อาทิ การเสพติดดิจิทัล (Digital addiction) จากอุปกรณ์ดิจิทัลที่เข้ามาครอบงำชีวิตเราในทุกเรื่อง สุขภาพทางจิตใจ (Mental health) จากความทุกข์ที่เกิดจากการเปรียบเทียบตัวเองกับคนอื่น หรือเรื่องเล่าบนเครือข่ายสังคมโซเชียล และถูกกลั่นแกล้งในเครือข่ายสังคมโซเชียล (Cyber bullying) การแยกแยะความจริงจากความไม่จริง (Breakdown

of truth) ทำได้ยากขึ้นเรื่อย ๆ การแบ่งขั้วแยกข้าง (Polarization) ทางอุดมการณ์ ทำให้การสร้างความปรองดองและความร่วมมือในสังคมกระทำได้ยากยิ่งขึ้น และสุดท้ายการชักใยทางการเมือง (Political manipulation) เพื่อสร้างความขัดแย้งและการทำสงครามไซเบอร์ ผลเสียเหล่านี้ล้วนเกิดมาจากขีดความสามารถของเทคโนโลยีที่ก้าวข้ามขีดความสามารถของมนุษย์ ซึ่งเข้าใจง่ายกว่าหากพิจารณาจากเทคโนโลยีที่ก้าวข้ามข้อด้อยของมนุษย์ (Human vulnerabilities) ในขณะเดียวกันความไม่สอดคล้องกันระหว่างความก้าวหน้าทางเทคโนโลยีอย่างก้าวกระโดดและความสามารถในการตระหนักรู้ของมนุษย์ (Human sensitivities) ส่งผลกระทบต่อความคิด ความรู้สึก และการกระทำของมนุษย์ ซึ่งล้วนสร้างผลเสีย เช่น ช่วงความสนใจที่สั้นลง (Attention span) อ่านแค่พาดหัวโดยไม่สนใจรายละเอียด แข่งขันกันที่ยอดไลค์และยอดแชร์บน Social media เป็นต้น

นอกจากนี้ ข้อมูลส่วนบุคคลจำนวนมหาศาลที่อยู่ในอำนาจการควบคุมของแพลตฟอร์ม (Platform) หรือผู้ให้บริการ Social media ต่างประเทศ ทำให้ผู้ให้บริการสามารถล่วงรู้ถึงรูปแบบการดำเนินชีวิตทางดิจิทัล หรือ "Digital lifestyle" ของผู้ใช้งาน ในด้านหนึ่งย่อมมีประโยชน์ต่อระบบเศรษฐกิจ โดยทำให้ผู้ใช้บริการสามารถได้รับบริการที่มีประสิทธิภาพ และตรงตามความคาดหวัง ในอีกด้านหนึ่ง การใช้ประโยชน์จากข้อมูลส่วนบุคคลจำนวนมหาศาลผ่าน Google Facebook และ Social media เช่น ตำแหน่งการใช้งาน พฤติกรรมการค้นหาข้อมูล (Search behavior) พฤติกรรมการเข้าชมภาพ/วีดีโอ พฤติกรรมการเลือกซื้อสินค้าและบริการ เป็นต้น อาจนำไปสู่การส่งผ่านข้อมูลที่มีอิทธิพลต่อทัศนคติ ความคิดเห็น พฤติกรรมและการตัดสินใจของผู้ใช้บริการได้โดยตรง โดยที่ผู้ใช้บริการอาจไม่รู้ตัว โดยเฉพาะอย่างยิ่งกลุ่มเยาวชนและคนรุ่นใหม่ ซึ่งเป็นกลุ่มที่มีการใช้งานอุปกรณ์สมาร์ทโฟน และ Social media มากกว่ากลุ่มอื่น อิทธิพลจากการเข้าถึงข้อมูลส่วนบุคคลและ Social media อาจทำให้เกิดการเปลี่ยนแปลงความเข้าใจ ความเชื่อ แนวคิด อุดมการณ์ และอาจทำให้เกิดการรับรู้ข้อมูลที่ไม่ตรงกับความเป็นจริงได้ เนื่องจากผู้ใช้บริการอาจไม่ได้ตรวจสอบความถูกต้องของข้อมูลก่อน รวมถึงสามารถส่งผ่านข้อมูลที่ชักจูงและสร้างกระแสสังคมที่ส่งผลกระทบในวงกว้าง และอาจส่งผลกระทบต่อความมั่นคงของสถาบันหลักของชาติได้โดยง่าย จึงถือเป็นการรุกรานทางความคิดต่อประชาชนรูปแบบใหม่ที่สามารถส่งผลกระทบต่อเศรษฐกิจ สังคม และประเทศชาติได้

ปัจจุบัน การปฏิบัติการข่าวสาร (Information operations : IO) ทั้งภาวะปกติ และภาวะสงคราม รวมไปถึงความขัดแย้งทางการเมืองและทางสังคม มักนิยมใช้ ไซเบอร์สเปซเป็นช่องทางในการดำเนินการ โดยการกระจายข้อมูลข่าวสาร เช่น ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว การประชาสัมพันธ์ การโฆษณาชวนเชื่อ เป็นต้น ผ่านเครือข่ายสังคมออนไลน์ (Social media) ต่าง ๆ เช่น Line Facebook Twitter เป็นต้น ทำให้สามารถเข้าถึงกลุ่มเป้าหมายด้วยความรวดเร็วชั่วพริบตา และมีการแชร์ข้อมูลต่อ ๆ กันไปอย่างรวดเร็ว ซึ่งมีอิทธิพลต่อความรู้สึกนึกคิด ความเชื่อ

ทัศนคติ อุดมการณ์ และมีผลต่อการตัดสินใจของคนเป็นจำนวนมาก จึงก่อให้เกิดปัญหาใหญ่คือการรุกล้ำ **“อธิปไตยไซเบอร์” หรือ "ความเป็นเอกราชทางไซเบอร์" (Cyber sovereignty)** ของประชาชนในประเทศ ตลอดจนปัญหาความมั่นคงของชาติ (National security) ซึ่งประชาชนส่วนใหญ่ยังไม่รู้ตัวเลยด้วยซ้ำว่ากำลังถูกละเมิดในเรื่อง “อธิปไตยไซเบอร์” เนื่องจากปัญหาดังกล่าวถูกซ่อนอยู่ในการใช้งานอินเทอร์เน็ตและการใช้งานสมาร์ทโฟนในปัจจุบันที่อยู่ในชีวิตประจำวันของคนจำนวนมาก

ประธานาธิบดีแห่งสาธารณรัฐประชาชนจีน สี จิ้นผิง ได้กล่าวเสมอในการประชุมสุดยอดผู้นำโลกเกี่ยวกับปัญหา "อธิปไตยไซเบอร์" (Cyber sovereignty) ที่กำลังเกิดขึ้นทั่วโลก ท่านกล่าวว่าทุกประเทศทั่วโลกมีสิทธิที่จะกำหนดนโยบายด้านไซเบอร์ในประเทศของตน เพื่อป้องกันการรุกรานโดยต่างชาติในรูปแบบที่ไม่ต้องใช้กำลังทางทหารหรือกระสุนแม้แต่เพียงนัดเดียว แต่เป็นการรุกรานหรือการล่าอาณานิคมในรูปแบบใหม่ ที่ประชาชนในประเทศเป้าหมายไม่ได้รับรู้ว่ากำลังถูกรุกรานอยู่ เนื่องจากการรุกรานดังกล่าวไม่ต้องใช้กำลังแต่อย่างใด เป็นการรุกรานทางความคิด ความเชื่อ ค่อย ๆ ส่งข้อมูลเข้ามาปรับเปลี่ยนพฤติกรรมของคนในชาติเหล่านี้

เราคงเคยเห็นกันจากประสบการณ์การปฏิวัติประชาธิปไตยในหลายประเทศในตะวันออกกลางและอาฟริกาเหนือ หรือการลุกฮือขึ้นโค่นล้มรัฐบาลในหลายประเทศของชาวอาหรับ (Arab Spring) มาแล้ว การใช้สื่อสังคมออนไลน์ที่สะดวก รวดเร็วนี้ เป็นมีดสองคม อาจเริ่มจากสร้างเพจ Facebook เพื่อหาแนวร่วม ไปจนถึงการออกมาแสดงพลังเงียบในโลกจริง มีผลต่อการเลือกตั้ง มีผลต่อการเมืองการปกครอง ภัยจากการรุกรานเข้ามาเปลี่ยนความคิดดังกล่าวนั้น น่ากลัวยิ่งกว่าภัยจากการแฮกของแฮกเกอร์เสียอีก เนื่องจากแฮกเกอร์จะเข้าระบบเพื่อดึงข้อมูลหรือทำให้ระบบล่ม ที่เราเห็นปัญหามัลแวร์ (Malware) กันอยู่เป็นประจำ หากแต่การเจาะเข้าไปในจิตใจของมนุษย์ ให้ปรับเปลี่ยนความคิด ความเชื่อ ความศรัทธา ทำให้ชอบหรือไม่ชอบ รักหรือเกลียดในตัวบุคคล สินค้า หรือบริการ หรือบริษัทต่าง ๆ ตลอดจนผู้นำในแต่ละประเทศมีผลกระทบโดยตรงต่อเศรษฐกิจและสังคมของประเทศต่าง ๆ ตลอดจนส่งผลกระทบถึงความมั่นคงของชาติหรือ "National security" ในที่สุด

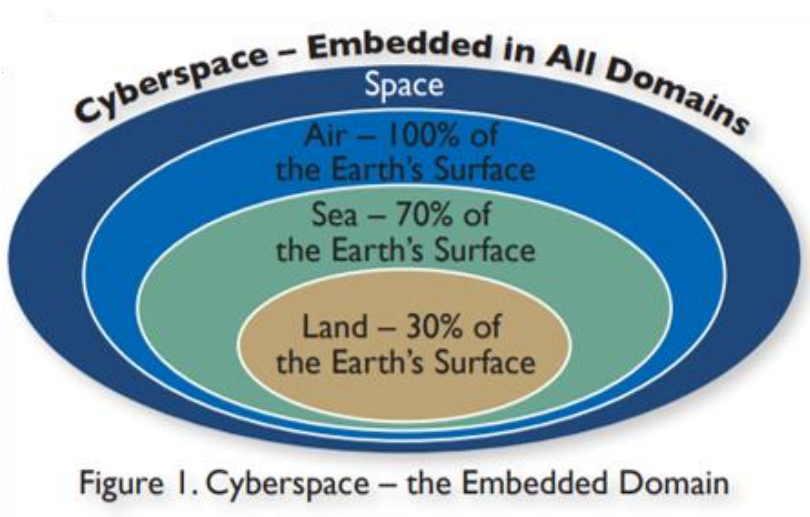
จากผลการศึกษาของ Hao Yeli (2560)[1] ได้กล่าวว่า ปัญหาการรุกล้ำอธิปไตยทางไซเบอร์ (Cyber sovereignty) เป็นภัยคุกคามทางไซเบอร์อันดับหนึ่ง (Tier one) ของปัญหาความมั่นคงปลอดภัยไซเบอร์ของประเทศ และถือเป็นโดเมนที่ห้าแห่งการทำสงครามทางการทหาร

---

[1] Hao Yeli. (2560). **A Three-Perspective Theory of Cyber Sovereignty.** The Fifth Domain. PRISM vol. 7 No. 2 2017. A Journal of the Center for Complex Operation.

(The fifth domain of warfare) นอกเหนือจาก พื้นดิน ผืนฟ้า อากาศ และอวกาศ โดยปัจจุบันประเทศสหรัฐอเมริกาและองค์การสนธิสัญญาแอตแลนติกเหนือหรือนาโต (NATO) ได้กำหนดให้โลกไซเบอร์สเปซ (Cyberspace) เป็นโดเมนแห่งสงคราม และจัดตั้งกองกำลังทางทหารด้วยแล้ว ในขณะที่ในยุคโบราณพื้นดินถูกห้อมล้อมไปด้วยผืนน้ำ ผืนน้ำถูกห้อมล้อมไปด้วยอากาศ อากาศถูกห้อมล้อมไปด้วยอวกาศ ในขณะที่ไซเบอร์สเปซนั้นไร้ขอบเขตจำกัด ถือว่าเป็นโดเมนหนึ่งที่มีความสำคัญในการสู้รบเอาชนะฝ่ายตรงข้าม (แผนภาพที่ 3-1) ประเทศสหรัฐอเมริกาและประเทศจีนได้ให้ความสำคัญกับเรื่อง สงครามไซเบอร์ (Cyber warfare) ถึงขนาดให้การสนับสนุนให้มีการผลิตนักรบไซเบอร์ (Cyber warriors) ขึ้นมาประจำการในกองกำลังทหาร เพื่อเสริมสร้างกำลังอำนาจทางทหาร ซึ่งเป็นกำลังอำนาจแห่งชาติ (National power) ที่สำคัญด้านหนึ่ง

แผนภาพที่ 3-1 ไซเบอร์สเปซ หรือ ปริภูมิไซเบอร์ เป็นสมรภูมิที่ 5



ที่มา : Institute for Defense Analyses

อย่างไรก็ตาม หลายประเทศยังคงให้ความสำคัญกับการคุ้มครองโลกไซเบอร์สเปซของตนเองจากการคุกคามและการโจมตีทางไซเบอร์ทางกายภาพจากภายนอกประเทศ โดยไม่คำนึงถึงการคุกคามในระดับผู้ใช้งาน (Practical level)

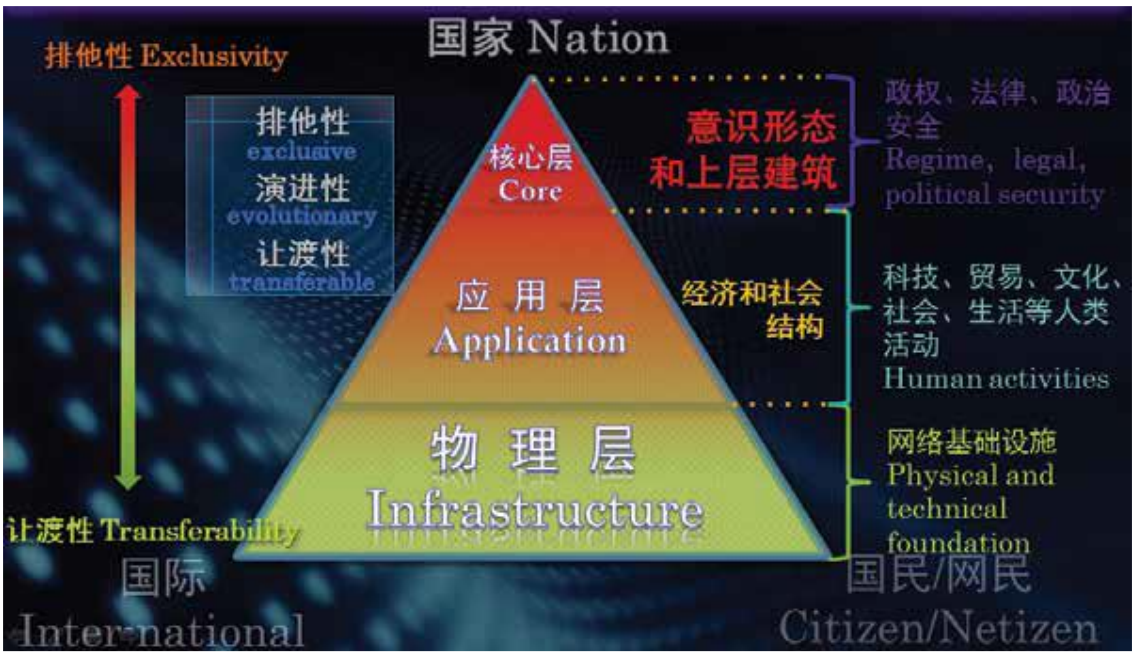
Hao Yeli (2560) ได้เสนอทฤษฎีสามมุมมอง (Three perspective theory) เพื่ออภิปรายถึงปัญหาของการรุกล้ำอธิปไตยทางไซเบอร์ (Cyber sovereignty) โดยสามารถแบ่งชั้นของการรุกล้ำออกเป็น 3 ระดับ ในลักษณะของพีระมิด ดังปรากฏในแผนภาพที่ 3-2

1. ระดับล่างสุดของพีระมิด หรือฐานพีระมิดคือ ระดับการรุกล้ำทางกายภาพ (Physical level) หมายถึงโครงสร้างพื้นฐานทางไซเบอร์สเปซและโครงสร้างพื้นฐานทางเทคนิค (Technical foundation) การป้องกันคือ การพัฒนามาตรฐานระบบป้องกันภัยคุกคามทัดเทียมมาตรฐานระดับโลกการสร้างความเชื่อมโยงกันของระบบเทคโนโลยีสารสนเทศ และการพัฒนาขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์

2. ระดับกลางพีระมิดคือ ระดับแอพพลิเคชั่น (Application level) หมายถึง แพลตฟอร์มและตัวกลางที่เชื่อมโยงภาคส่วนต่าง ๆ เข้าด้วยกัน อาทิ เทคโนโลยี วัฒนธรรม เศรษฐกิจ การค้า และการใช้ชีวิตประจำวันของประชาชน การป้องกันคือ การสร้างดุลยภาพและความร่วมมือระหว่างหน่วยงานรัฐและเอกชนเพื่อรักษาสมดุลระหว่างความเป็นอิสระเสรีและความมั่นคง

3. ระดับยอดของพีระมิด (Top or core level) ประกอบด้วยรากฐานความมั่นคงของรัฐ ได้แก่ นโยบายรัฐ กฎหมาย เสถียรภาพทางเมือง และอุดมการณ์ทางการเมือง และโครงสร้างของความหลากหลาย เช่น ศาสนา และวัฒนธรรม เป็นต้น การป้องกันคือ การสร้างความร่วมมือระหว่างภาครัฐและภาคส่วนอื่นๆ (Multi-stakeholder) การกำหนดนโยบายและกติกาการใช้งานระบบอินเทอร์เน็ตร่วมกัน ทั้งนี้ บางรัฐอาจมีอำนาจตามกฎหมายในการควบคุมโครงสร้างพื้นฐานด้านข้อมูลสารสนเทศของประเทศ

แผนภาพที่ 3-2 แนวคิดของประเทศจีนในการรับมือกับการรุกล้ำอธิปไตยทางไซเบอร์



ที่มา : PRIMS. (2017). The Fifth Domain. A Journal of the Center for Complex Operations

ตัวอย่างประเทศที่ป้องกันการรุกล้ำอธิปไตยทางไซเบอร์ได้สำเร็จ คือ ประเทศจีน ขอบเขตของความปลอดภัยทางไซเบอร์ของจีนกว้างขวางกว่าของชาติตะวันตก ในขณะที่ชาติตะวันตกเน้นเรื่องความปลอดภัยของระบบและโครงสร้างพื้นฐานเป็นสำคัญ ในประเทศจีน ความปลอดภัยทางไซเบอร์มีความหมายกว้าง โดยรวมถึงการรักษาเสถียรภาพทางการเมืองและสังคมด้วย โดยประเทศจีนสามารถควบคุมการใช้อินเทอร์เน็ตของพลเมืองภายในประเทศตนเองได้ การคุ้มครองข้อมูลส่วนบุคคลให้อำนาจรัฐบาลในการเข้าถึงข้อมูลเหล่านั้น ผู้ให้บริการทางโครงข่ายระบบโครงสร้างพื้นฐานที่สำคัญมีความรับผิดชอบในการปกป้องความมั่นคงของรัฐด้วย มีการเร่งพัฒนาศักยภาพด้านไซเบอร์ให้มีเทคโนโลยีและนวัตกรรมเป็นของตนเอง โดยได้ดำเนินโครงการ National public security work informational project ตั้งแต่ปี 2541 ซึ่งมีโครงการย่อยภายใต้ชื่อกำแพงเมืองจีนบนโลกออนไลน์ “The great firewall” หรือ “GFW” ใช้ทางผ่านอินเทอร์เน็ต 3 ช่องทาง อยู่ที่ปักกิ่ง เซี่ยงไฮ้ และกว่างโจว ในด้านเทคนิคถือว่ามี 3 ช่องทางแต่ในด้านการควบคุมเป็น “National gateway" ซึ่งพัฒนามาเป็นลำดับตลอดระยะเวลา 20 ปี ที่ผ่านมา และมีการออกกฎหมายควบคุม Virtual private networks (VPN) หรือ “เครือข่ายส่วนตัวเสมือน” ที่ไม่ได้รับอนุญาต ซึ่งเป็นบริการที่ช่วยให้ชาวจีนสามารถเชื่อมต่อกับอินเทอร์เน็ตได้โดยไม่ต้องการผ่าน National gateway ทำให้เครือข่าย VPN บางเครือข่ายไม่สามารถใช้งานได้ และบางรายถูกปิดอย่างถาวร

ด้วยเหตุนี้เว็บไซต์ที่คนใช้กันอย่างแพร่หลายทั่วโลก เช่น Facebook Youtube Twitter Google Instagram LINE dropbox ไม่สามารถใช้งานในประเทศจีนได้ โดยประเทศจีนได้สร้างสังคมออนไลน์ใช้ภายในประเทศขึ้นมามากมาย เช่น เว็บไซต์ค้นหา (Search engine) อย่างไป่ตู้ (Baidu) ซึ่งมีฟังก์ชั่นการใช้งานที่คล้ายกับ Google แอพพลิเคชั่นไป่ตู้แมพ (Baidu map) ซึ่งเป็นบริการค้นหาสถานที่คล้ายกับ Google map เครือข่ายสังคมออนไลน์เวย์ปั๋ว (Weibo) ซึ่งคล้ายกับ Twitter วีแชท (WeChat) ซึ่งมีลักษณะคล้ายกับ LINE ในขณะที่ประเทศเวียดนาม กัมพูชา และเมียนมา กำลังพัฒนาศักยภาพด้านไซเบอร์เชิงรุกเช่นกัน โดยที่รัฐบาลของมาเลเซีย อินโดนีเซีย สิงคโปร์ และเวียดนาม สนับสนุนให้ภาคเอกชนพัฒนาและเริ่มใช้ Platform เป็นของตนเอง

ตัวอย่างประเทศที่อยู่ระหว่างริเริ่มการป้องกันการรุกล้ำอธิปไตยทางไซเบอร์ คือ ประเทศออสเตรเลีย ซึ่งมีการบัญญัติกฎหมายการเข้ารหัสข้อมูล (Assistance and access act - AAA) เมื่อเดือนธันวาคมปี 2561 ซึ่งกำหนดให้บริษัทผู้ให้บริการเทคโนโลยีคอมพิวเตอร์ และเว็บไซต์ที่ปฏิบัติการในออสเตรเลีย ต้องให้ความร่วมมือกับรัฐ ตำรวจ หรือข้าราชการในองค์การเกี่ยวกับความปลอดภัย เข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งาน โดยเจ้าหน้าที่อาจแฮกเข้าอุปกรณ์ไอที ผังมัลแวร์เพื่อทำลายการเข้ารหัส อัยการสูงสุดของออสเตรเลียมีอำนาจออกคำสั่งให้บริษัทเทคชั้นนำอย่าง Apple, Facebook และ Whatsapp สร้างโค้ดซอฟต์แวร์หรืออื่นๆ หากบริษัทปฏิเสธไม่ยอมทำตามจะเจอโทษปรับ 10 ล้านดอลลาร์ และ 5 หมื่นดอลลาร์ นอกจากนี้ บริษัทเหล่านี้อาจต้องมอบข้อมูลเกี่ยวกับสเป็คการออกแบบทางเทคโนโลยีให้กับตำรวจ เพื่ออำนวยความสะดวกในการเข้าถึงอุปกรณ์และบริการเฉพาะได้ อีกทั้งช่วยเหลือทางการออสเตรเลียในการพัฒนาขีดความสามารถของตนเอง และช่วยปกปิดข้อเท็จจริงเกี่ยวกับปฏิบัติการของทางการด้วย เพื่อประโยชน์ต่อการสืบสวนคดี และรับมือกับเครือข่ายการก่ออาชญากรรม การก่อการร้าย และดูแลความมั่นคงของประเทศออสเตรเลีย

นอกจากนี้ ประเทศสิงคโปร์เป็นอีกประเทศที่ริเริ่มการป้องกันการรุกล้ำอธิปไตยทางไซเบอร์ โดยองค์กรด้านการพัฒนาและกำกับดูแลสื่อสารสนเทศภาครัฐของสิงคโปร์ (Infocomm media development authority: IMDA) ได้ออกแนวปฏิบัติทางอินเทอร์เน็ต (Internet code of practice)[2] ภายใต้ Broadcasting act เพื่อควบคุมเนื้อหาต้องห้ามทางออนไลน์ (Prohibited online material) ตั้งแต่ปี 2539 จนกระทั่งเมื่อปลายเดือนพฤษภาคม พ.ศ. 2556 รัฐบาลได้ประกาศให้ผู้ที่จะเปิดเว็บไซต์ข่าวจะต้องมาขึ้นทะเบียนขออนุญาตจากหน่วยงานของรัฐ ทั้งนี้ เพื่อให้สอดคล้องกับสื่อกระจายเสียงที่ต้องปฏิบัติตามแนวปฏิบัติในเรื่องการนำเสนอเนื้อหาข้อมูลข่าวสาร และหากเจ้าหน้าที่รัฐพบว่า มี “เนื้อหาต้องห้าม” จะต้องลบข้อมูลดังกล่าวภายใน 24 ชั่วโมง เนื้อหา

[2] Infocomm Media Development Authority. **Internet Code of Practice.**

ต้องห้าม ดังกล่าว ประกอบด้วย เรื่องลามกอนาจาร ความรุนแรงแบบสุดขั้ว และเนื้อหาที่เกี่ยวข้องกับการเมือง และศาสนา องค์กรที่กำกับเรื่องสื่อของสิงคโปร์ได้แก่ The media development authority (MDA) อยู่ภายใต้กระทรวงข้อมูลและการสื่อสาร หน่วยงานแห่งนี้ก่อตั้งขึ้นในปี พ.ศ. 2546 โดยผู้บริหารองค์กรได้รับการแต่งตั้งจากรัฐบาล และมีการบัญญัติกฎหมาย Protection from online falsehoods and manipulation act 2019 (POFMA) หรือที่เรียกง่าย ๆ ว่า Fake news law เมื่อวันที่ 3 ตุลาคม 2562 เพื่อจัดการกับการเผยแพร่ข่าวปลอม และการปลุกปั่นในโลกออนไลน์ กฎหมายฉบับนี้ กำหนดโทษแก่ผู้ที่ถูกตัดสินว่าเผยแพร่ข่าวปลอมผ่านบัญชีออนไลน์ โดยผู้กระทำผิดประเภทรายบุคคลจะต้องเสียค่าปรับ 1 แสนดอลลาร์สิงคโปร์ หรือ 72,108 ดอลลาร์สหรัฐฯ หรือจำคุกเป็นเวลาถึง 10 ปี (ขั้นสูงสุด) หรือทั้งจำคุกและปรับ ขณะที่ผู้กระทำผิดที่เป็นองค์กร จะต้องจ่ายค่าปรับขั้นสูงสุดถึง 1 ล้านดอลลาร์สิงคโปร์ กฎหมายให้อำนาจแก่รัฐบาลในการกำหนดทิศทางการแก้ไข เพื่อบังคับให้ผู้โพสต์ข่าวปลอมบนช่องทางออนไลน์ต้องแก้ไขและหยุดเผยแพร่ข้อมูลข่าวปลอมนั้น ๆ นอกจากนี้ รัฐบาลยังสามารถสั่งให้ผู้ให้บริการอินเทอร์เน็ตหรือตัวกลางผู้ให้บริการอินเทอร์เน็ตระงับการเข้าถึงเว็บไซต์ที่ฝ่าฝืน หรือปรับสูงถึงวันละ 20,000 ดอลลาร์สหรัฐฯ รวมสูงสุดไม่เกิน 500,000 ดอลลาร์สหรัฐฯ

กองทัพแห่งประเทศสหรัฐอเมริกาได้จัดการประชุมเชิงปฏิบัติการเกี่ยวกับปัญหาการรุกรานอธิปไตยไซเบอร์ในโลกของไซเบอร์สเปซ ในปี 2560 Cynthia (2559)[3] ได้สรุปผลการประชุมเชิงสัมมนาว่า สหรัฐอเมริกายังขาดยุทธศาสตร์แบบองค์รวมในการป้องกันการรุกรานอธิปไตยทางไซเบอร์ การแก้ไขปัญหาด้วยการสร้างการทำงานของหน่วยงานภาครัฐให้เป็นไปในทิศทางเดียวกัน (Whole-of-government approach) ไม่เพียงพอที่จะแก้ไขปัญหาได้ จำเป็นต้องขยายการแก้ไขปัญหาเป็นการทำงานของสังคมในทิศทางเดียวกัน (Whole-of-community) และการทำงานของชาติในทิศทางเดียวกัน (Whole-of-nation) หมายความถึงการดึงให้ภาคเอกชน รัฐบาล และกองทัพของประเทศพันธมิตรเข้ามามีส่วนร่วมด้วย

ในขณะที่ประเทศรัสเซียมีแนวคิดว่า รูปแบบการรุกรานอธิปไตยทางไซเบอร์มีอยู่ 3 รูปแบบ ได้แก่ 1) การรุกรานรัฐ (State) ด้วยนโยบายการต่างประเทศ 2) การรุกรานประเทศ (National) ผ่านการเมือง วัฒนธรรม และเอกลักษณ์ของชาติ และ 3) ความชื่นชอบ (Popular) ผ่านกระบวนการรู้คิด (Cognitive processes) ของประชาชน โดยประเทศรัสเซียเริ่มมีมาตรการป้องกันการรุกรานอธิปไตยทางไซเบอร์ เช่น การห้ามนักลงทุนต่างชาติถือครองหุ้นของสื่อในรัสเซีย

---

[3] Cynthia E. Ayers. (2559). **Rethinking Sovereignty in the Context of Cyberspace : The Cyber Sovereignty Workshop Series.** Center for Strategic Leadership, United States Army.

มากกว่าร้อยละ 20 การทดลองเครือข่ายอินเทอร์เน็ตภายในประเทศ (Runet) หรืออินเทอร์เน็ตทางเลือก เพื่อควบคุมการเชื่อมต่ออินเทอร์เน็ตของประชาชนกับเครือข่ายในต่างประเทศ ซึ่งมีลักษณะเดียวกับกำแพงเมืองจีนบนโลกออนไลน์ “The great firewall” ของประเทศจีน รวมถึงมีเป้าหมายให้บริษัทเทคโนโลยีในประเทศสามารถผลิตเทคโนโลยี แอปพลิเคชัน (Application) และบริการต่าง ๆ ที่เป็นที่นิยมในกลุ่มผู้ใช้งานในประเทศขึ้นมาด้วยตัวเองเหมือนที่ประเทศจีนประสบความสำเร็จ เป็นต้น อย่างไรก็ดี รัสเซียยังประสบความล้มเหลวในการสกัดกั้นไม่ให้ประชาชนเข้าถึงแอพพลิเคชั่นสนทนา “เทเลแกรม (Telegram)” ที่บทสนทนาของผู้ใช้งานจะถูกเข้ารหัสเพื่อรักษาความเป็นส่วนตัว และการทดสอบเครือข่ายอินเทอร์เน็ตภายในประเทศ (Runet) ของรัสเซียไม่มีข้อมูลที่ชัดเจนว่าประสบความสำเร็จเพียงใดในการตัดการเชื่อมต่อจากโลกภายนอก

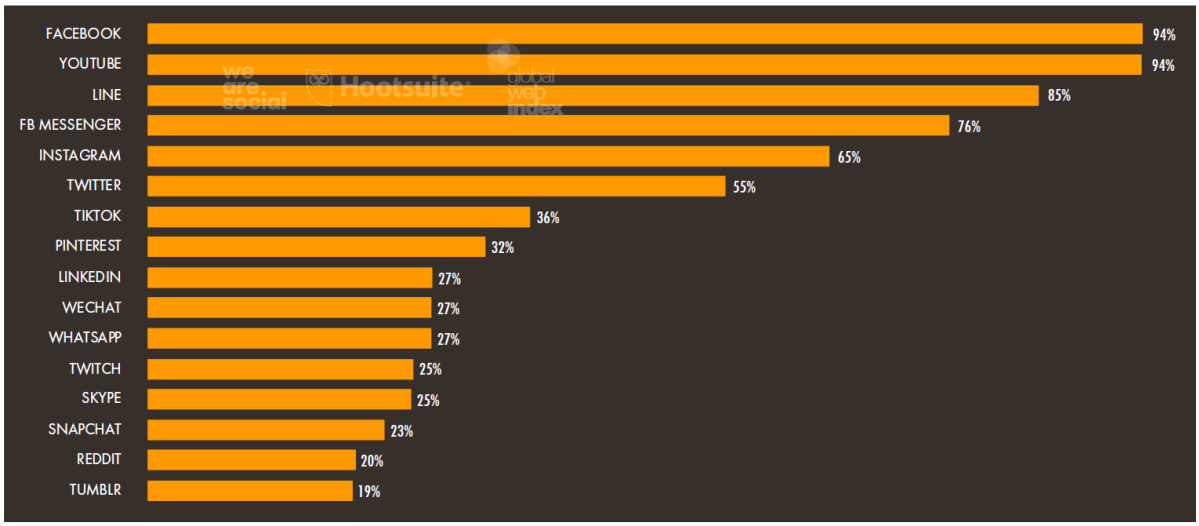
ดังนั้น เมื่อพิจารณาสถานะของการป้องกันการรุกรานทางอธิปไตยไซเบอร์ สามารถกล่าวได้ว่า ประเทศจีนเป็นประเทศที่ประสบความสำเร็จประเทศเดียว จากการมี “National gateway" หรือ “The great firewall” และการมีแพลตฟอร์มของประเทศตนเอง เช่น เว็บไซต์ค้นหา (Search engine) อย่างไป่ตู้ (Baidu) ซึ่งมีฟังก์ชั่นการใช้งานที่คล้ายกับ Google เครือข่ายสังคมออนไลน์เว่ย์ปั๋ว (Weibo) วีแชท (WeChat) ซึ่งมีลักษณะคล้ายกับ LINE ในขณะที่ประเทศที่กำลังตามหลังประเทศจีน และริเริ่มมาตรการการป้องกันอธิปไตยไซเบอร์ ได้แก่ ประเทศออสเตรเลีย และประเทศสิงคโปร์ โดยกรณีประเทศออสเตรเลีย มีกฎหมายการเข้ารหัสข้อมูล (Assistance and access act - AAA) ที่ช่วยให้เจ้าหน้าที่รัฐหรือตำรวจเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งาน เพื่อประโยชน์ต่อการสืบสวนคดี และรับมือกับเครือข่ายการก่ออาชญากรรมทางไซเบอร์ และกรณีประเทศสิงคโปร์ที่มีแนวปฏิบัติควบคุม “เนื้อหาต้องห้าม” บนอินเทอร์เน็ต และกฎหมาย Protection from online falsehoods and manipulation act 2019 (POFMA) เพื่อจัดการกับการเผยแพร่ข่าวปลอม และการปลุกปั่นในโลกออนไลน์ ในขณะที่ เมื่อพิจารณาขีดความสามารถด้านเทคโนโลยีของประเทศในภูมิภาคอาเซียน จะเห็นได้ว่า ประเทศในภูมิภาคอาเซียนไม่มีหรือไม่ได้ครอบครองเทคโนโลยีดิจิทัลเป็นของตนเอง ไม่มี Platform หรือโปรแกรม Social media เป็นของตนเอง เช่นเดียวกับกรณีของประเทศไทย จึงมีแนวโน้มที่จะถูกประเทศ/องค์กรที่มีศักยภาพด้านไซเบอร์ ใช้เครื่องมือ Cyber ผ่าน Platform และ Social media เป็นเครื่องมือ Soft power รุกรานอธิปไตยไซเบอร์ได้ หากไม่มีการวางระบบป้องกันด้านไซเบอร์ของประเทศที่เพียงพอ

วิเคราะห์กระบวนการ รูปแบบ และลักษณะของปัญหาอธิปไตยไซเบอร์ในประเทศไทย

1. วิเคราะห์กระบวนการ รูปแบบ และลักษณะของปัญหาอธิปไตยไซเบอร์ในประเทศไทย

1.1 ประเทศไทยไม่มีการพัฒนาเทคโนโลยีและนวัตกรรมให้เป็นของตนเองต้องพึ่งพาแพลตฟอร์มจากต่างประเทศ ไม่มี Platform ที่ทำธุรกิจหารายได้เข้าประเทศลดการสูญเสียเงินตราให้กับ Platform ต่างประเทศ ทั้งนี้ จากการสำรวจสัดส่วนการใช้งานแพลตฟอร์มสื่อสังคมออนไลน์ในประเทศไทยต่อการใช้งานอินเทอร์เน็ตทั้งหมด ของ We Are Social และ Hootsuite[4] เมื่อเดือนมกราคมปี 2563 พบว่า กว่าร้อยละ 94 ของผู้ใช้งานอินเทอร์เน็ตใช้งาน Facebook และ Youtube และแพลตฟอร์มใหม่ ๆ อย่าง Tiktok เริ่มมีสัดส่วนเพิ่มขึ้นอย่างรวดเร็ว แพลตฟอร์มทั้งหลายเหล่านี้ล้วนเป็นแพลตฟอร์มของต่างประเทศทั้งสิ้น (แผนภาพที่ 3-3)

แผนภาพที่ 3-3 สัดส่วนการใช้งานสื่อสังคมออนไลน์ในประเทศไทยต่อการใช้งานอินเทอร์เน็ตทั้งหมด



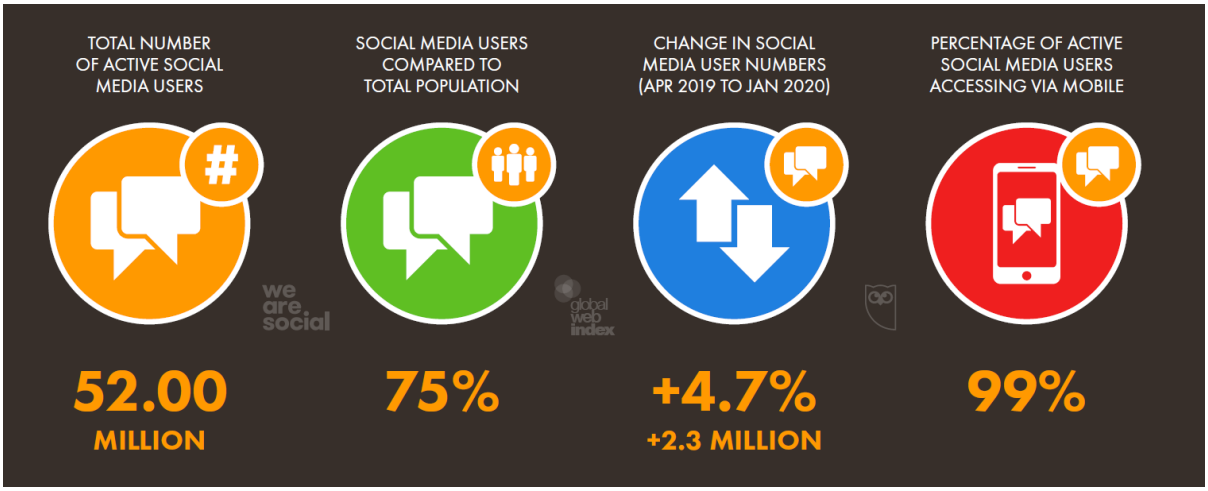
ที่มา : Globalwebindex.com (ข้อมูล ณ ไตรมาสที่ 3 ของปี 2562)

1.2 อัตราการใช้สื่อสังคมออนไลน์และการใช้โทรศัพท์เคลื่อนที่ของประชาชนในประเทศไทยอยู่ในระดับต้น ๆ ของโลกเมื่อเทียบกับจำนวนประชากร และในห้วงการแพร่ระบาดของโรคโควิด-19 ปรากฏชัดว่าประชาชนใช้บริการอินเทอร์เน็ตสูงขึ้นในการทำกิจกรรมที่เกี่ยวกับ

[4] We Are Social และ Hootsuite. (2019). **DIGITAL 2020 THAILAND.**

การค้า การเงิน การใช้ชีวิตประจำวัน ฯลฯ ทั้งระดับองค์กร และประชาชนรายบุคคล ทั้งนี้ จากการสำรวจของ We Are Social และ Hootsuite เมื่อเดือนมกราคมปี 2563 พบว่า จำนวนผู้ใช้งานสื่อสังคมออนไลน์ในประเทศไทยมีจำนวน 52 ล้านคน คิดเป็นร้อยละ 75 ของประชากร มีอัตราเพิ่มของจำนวนผู้ใช้งาน Social media ร้อยละ 4.7 หรือเพิ่มขึ้น 2.3 ล้านคนจากปีก่อน และผู้ใช้งานสมาร์ทโฟนร้อยละ 99 ใช้งาน Social media ด้วย (แผนภาพที่ 3-4) และจากข้อมูลงานวิจัยของ Kantar GREYnJ United และ Mindshare (Thailand)[5] พบว่า คนไทยมีความตื่นตัวกับการใช้ Social media อย่างมาก ทั้งเพื่อติดตามสถานการณ์ และข้อมูล COVID-19 และเพื่อคลายเหงา ซึ่งเกิดจากการมี Emotional engagement กับสถานการณ์การแพร่ระบาดของโรค COVID-19 โดยพฤติกรรมและไลฟ์สไตล์ของคนไทยร้อยละ 63 ลดการเข้าสังคม /พบปะผู้คน และหันไปกระทำกิจกรรมบน Social media มากขึ้น

แผนภาพที่ 3-4 ภาพรวมการใช้งานสื่อสังคมออนไลน์ของประเทศไทย ปี 2563



ที่มา : Globalwebindex.com (ข้อมูล ณ เดือนมกราคม ปี 2563)

[5] Kantar GREYnJ United และ Mindshare (Thailand). (2563). **Thailand COVID-19 Situation.**

1.3 ไซเบอร์มีแนวโน้มที่จะถูกนำมาใช้ทั้งเชิงรุกและเชิงรับในการปฏิบัติการทางทหารมากขึ้น ซึ่งอาจสามารถเอาชนะกันได้ตั้งแต่ต้นโดยไม่ต้องใช้อาวุธหรือการรบเกิดขึ้นจริง และในสงครามผสมผสาน (Hybrid war) ซึ่งเป็นสงครามที่มีการผสมผสานกำลังตามแบบและกำลังนอกแบบปฏิบัติการทางทหารร่วมกันอย่างแยกไม่ออก โดยอยู่ในรูปแบบ **“สงครามข่าวสาร” (Information warfare)** ที่เข้าถึงประชาชนได้ง่ายผ่านสื่อสังคมออนไลน์ เช่น การใช้เพจ Facebook หรือ Twitter สร้างมวลชนที่ต่อต้านอำนาจรัฐและสถาบันหลักของชาติ ข่าวสารที่บิดเบือนความจริงที่นำไปสู่การขาดความเชื่อมั่นต่อรัฐและสถาบันหลักของชาติ หรือการสื่อสารกันโดยตรงที่ยากที่จะตรวจจับ เป็นต้น

1.4 ภัยคุกคามจากตัวแสดงที่ไม่ใช่รัฐ (Non-state actor) เช่น อาชญากร กลุ่มผู้ก่อการร้าย กลุ่มค้ายาเสพติด กลุ่มการพนันออนไลน์ เป็นต้น มีแนวโน้มจะใช้/แสวงประโยชน์ ใช้ไซเบอร์ในการปฏิบัติการมากขึ้น รวมถึงกลุ่มตรงข้าม/ศัตรูทางการเมืองจะใช้ประโยชน์ในกิจกรรมทางการเมืองมากขึ้นเช่นกัน โดยเฉพาะการใช้ Social media ที่มีการใช้อย่างแพร่หลายในการเลือกตั้งสำคัญต่าง ๆ เนื่องจากเครื่องมือในการสื่อสารที่มีพลังอำนาจสูงในการสร้างความเปลี่ยนแปลงให้เกิดขึ้นได้ในสังคม เป็นช่องทางการสื่อสารระหว่างพรรคการเมือง แกนนำทางการเมืองและแกนนำทางการเคลื่อนไหว และใช้ในการติดต่อสื่อสารกับผู้สนับสนุน ระดมบุคลากรและทรัพยากรในการเคลื่อนไหวทางการเมือง ส่งผลให้นักการเมืองและพรรคการเมืองสามารถใช้ Social media ในการหาเสียง โจมตีให้ร้ายคู่แข่ง สร้างความเกลียดชัง และสร้างความรู้สึกแตกแยกให้เกิดขึ้นในสังคมได้ ผู้ติดตามใน Social media เป็นผู้ช่วยแชร์ (Share) และกระจายข้อมูลไปยังกลุ่มเพื่อนและเครือข่ายของตนได้อย่างรวดเร็ว

1.5 มีบุคคล/กลุ่มบุคคลใช้ไซเบอร์ เป็นเครื่องมือบ่อนทำลายสถาบันหลักของชาติโดยการปฏิบัติการข่าวสาร (Information Operation: IO) การโฆษณาชวนเชื่อการบิดเบือนข้อมูลที่กระทำซ้ำ ๆ และการปลูกฝังแนวความคิดที่กระทบต่อความมั่นคง (ในรูปแบบการแอบแฝง/ทำซ้ำ/จิตวิทยาหมู่) รวมถึงมีแนวโน้มที่จะมีการใช้เพื่อประโยชน์ทางการเมืองมากขึ้น ทั้งด้วยเครื่องมือ เทคนิค/วิธีการ และเทคโนโลยี ตลอดจนการระดมกลุ่มที่มีแนวคิดเดียวกันด้วยสื่อออนไลน์ (วิธีการทางไซเบอร์) เช่น เว็บไซต์หมิ่นสถาบันพระมหากษัตริย์ เพจ Facebook จาบจ้วงสถาบันพระมหากษัตริย์ ข้อความหมิ่นสถาบันพระมหากษัตริย์ทาง Facebook และ Youtube channel ที่บิดเบือนบ่อนทำลายสถาบันหลักของชาติ เป็นต้น

1.6 บริษัทต่างชาติที่ครอบครองเทคโนโลยีและนวัตกรรมใช้ประโยชน์ดูดซับความมั่งคั่งออกไปนอกประเทศ โดยอำนาจการจัดเก็บเสียภาษีตามกฎหมายของประเทศไทยยังไม่ครอบคลุม โดยประมวลรัษฎากรและอนุสัญญาภาษีซ้อน (Double tax agreement : DTA)

ที่ประเทศไทยลงนามกับประเทศคู่สัญญา 60 ประเทศ กำหนดให้บริษัทต่างชาติที่มีกิจการในประเทศไทย หรือมีตัวแทนที่ขายในประเทศไทย มีหน้าที่เสียภาษีเงินได้นิติบุคคล เฉพาะกรณีมีสถานประกอบการถาวรอยู่ในไทย (Permanent establishment: PE) เช่น สำนักงาน สาขา โรงงาน เป็นต้น เฉพาะเงินได้ในส่วนที่เป็นของ PE ซึ่งบริษัทต่างชาติที่ใช้แพลตฟอร์มในการประกอบธุรกิจให้บริการในประเทศไทย เช่น Facebook Youtube Google Twitter เป็นต้น มักจะหลีกเลี่ยง การจัดตั้ง PE ในประเทศไทย ทำให้ประเทศไทยไม่สามารถจัดเก็บภาษีเงินได้จากบริษัทต่างชาติได้ นอกจากนี้ กรณีที่มีการจ่ายเงินได้ให้บริษัทต่างชาติ ประมวลรัษฎากรได้ยกเว้นภาษี หัก ณ ที่จ่าย สำหรับเงินได้ตามมาตรา 40 (8) (เงินได้จากการธุรกิจ การพาณิชย์ การเกษตร การอุตสาหกรรม การขนส่ง หรือการอื่น เช่น ค่าจ้างโฆษณา ค่าเบี้ยประกันภัย ค่าธรรมเนียมที่เกี่ยวกับการพาณิชย์ เป็นต้น) ด้วยเหตุนี้ กรณี Youtube และ Facebook มีเงินได้ค่าโฆษณา จากประเทศไทย ซึ่งเป็นเงินได้ประเภท 40 (8) ผู้จ่ายเงินได้ค่าโฆษณาไปให้แพลตฟอร์มต่างประเทศ ซึ่งส่วนใหญ่เป็นผู้ประกอบการไทย จึงไม่มีหน้าที่หักภาษีเงินได้ ณ ที่จ่าย นำส่งกรมสรรพากร ตามมาตรา 70 แห่งประมวลรัษฎากร

1.7 หน่วยงานที่เป็นกลไกตามกฎหมาย (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒) ยังอยู่ระหว่างการจัดตั้งและขับเคลื่อน แม้ว่าหน่วยงานด้านความมั่นคง โดยเฉพาะกองทัพมีการจัดตั้งหน่วยงานด้านไซเบอร์ขึ้นมารับผิดชอบแล้ว เช่น การจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army cyber center) ในปี 2559 การจัดตั้งศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ในปี 2560 เป็นต้น ทั้งนี้ ปัจจุบัน ณ เดือนมิถุนายน 2563 สำนักงานตำรวจแห่งชาติ อยู่ระหว่างการจัดตั้งกองบัญชาการ “ตำรวจไซเบอร์” เพื่อแยกหน้าที่กับหน่วยปฏิบัติให้มีความชัดเจน เนื่องจากปัจจุบัน สำนักงานตำรวจแห่งชาติมีเพียงหน่วยงานกองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี หรือ บก.ปอท. ซึ่งเป็นระดับกองบังคับการ เท่านั้น นอกจากนี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ยังอยู่ระหว่างการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ภายใต้อำนาจตามมาตรา 22 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ตารางที่ 3-1 หน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน่วยงาน	ชื่อย่อ	อำนาจหน้าที่หลัก

หน่วยงาน	ชื่อย่อ	อำนาจหน้าที่หลัก
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	กมช.	1) เสนอนโยบายและแผนต่อคณะรัฐมนตรี 2) กำหนดนโยบายการบริหารจัดการสำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 3) จัดทำแผนปฏิบัติการเสนอต่อคณะรัฐมนตรี 4) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ 5) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญให้พนักงานเจ้าหน้าที่ 6) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่น
คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์	กกม.	1) ติดตามการดำเนินการตามนโยบายและแผน 2) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง 3) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ 4) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานขั้นต่ำ 5) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล 6) กำหนดระดับของภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับ 7) วิเคราะห์สถานการณ์ และประเมินผลกระทบ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	สกมช.	รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กมช. และ กกม.
คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์	กบส.	ดูแลงานด้านกิจการบริหารงานทั่วไปของ สกมช.

ที่มา : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.8 กฎหมายที่เกี่ยวข้อง (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) และยุทธศาสตร์ด้านความมั่นคงไซเบอร์แห่งชาติ (2560-2564) ยังไม่ครอบคลุมทั้ง 5 มิติด้านความมั่นคงปลอดภัยไซเบอร์ ตามมิติที่ 2 ของกรอบแนวคิด CMM ในเรื่อง Cyber culture and society ความรู้ความเข้าใจ ความเชื่อมั่นของผู้ใช้บริการ เกี่ยวกับการละเมิดและนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต ช่องทางการรายงานอาชญากรรมทางไซเบอร์อิทธิพลของ Social media และอธิปไตยไซเบอร์ ทั้งนี้ กฎหมายที่เกี่ยวข้องส่วนใหญ่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางกายภาพและภัยคุกคามทางไซเบอร์เป็นหลักไม่ครอบคลุมถึงการรุกรานทางความคิดผ่านเครือข่ายสังคมออนไลน์และอธิปไตยทางไซเบอร์

2. วิเคราะห์การขับเคลื่อนทางยุทธศาสตร์ในช่วงที่ผ่านมา

2.1 การป้องกันการรุกล้ำอธิปไตยไซเบอร์ภายใต้ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)

รัฐบาลพลเอก ประยุทธ์ จันทร์โอชา ได้ให้ความสำคัญกับความมั่นคงปลอดภัยทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และรักษาความมั่นคงปลอดภัยทางไซเบอร์ของชาติ โดยกำหนดให้ความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นส่วนหนึ่งของยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) ในด้านความมั่นคง โดยแผนแม่บทย่อยจะมุ่งเน้นที่ความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ เป็นหลัก ประกอบด้วย 9 แผนงาน 15 โครงการที่สำคัญ (ตารางที่ 3-2) ดังนี้

ตารางที่ 3-2 โครงการสำคัญภายใต้แผนย่อยในการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

แผนงาน	โครงการที่สำคัญ	หน่วยงานดำเนินงาน
1. การพัฒนาแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์	1) โครงการจัดทำนโยบายและแนวทางปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระดับชาติ 2) โครงการทบทวนนโยบายและแนวทางปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระดับชาติ	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) สภาความมั่นคงแห่งชาติ (สมช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
2. การจัดตั้งองค์กร และพัฒนาขีดความสามารถใน	โครงการจัดตั้งองค์กรกำกับดูแลการรักษาความมั่นคงปลอดภัยทางไซเบอร์	ดศ./สมช.

แผนงาน	โครงการที่สำคัญ	หน่วยงานดำเนินงาน
งานมั่นคงปลอดภัยทางไซเบอร์	แห่งชาติ (***โครงการเร่งด่วน***)	
3. การพัฒนาศักยภาพระบบบริหารจัดการด้าน ไซเบอร์	1) โครงการพัฒนาระบบบริหารจัดการด้านไซเบอร์ (Cybersecurity Management System: CSMS) (***โครงการเร่งด่วน***) 2) โครงการยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์	ดศ. สมช. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
4. การพัฒนาศักยภาพระบบตอบโต้สถานการณ์ฉุกเฉิน (Cybersecurity management system: CSMS)	โครงการจัดทำแผนฉุกเฉินด้านภัยคุกคามทางไซเบอร์ (***โครงการเร่งด่วน***)	ดศ. สมช. หน่วยงานภาครัฐ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
5. การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	โครงการซ้อมรับมือสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (***โครงการเร่งด่วน***)	ดศ. สมช. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
6. การป้องกัน แก้ไขปัญหาการเผยแพร่ข้อมูลที่ส่งผลกระทบต่อความมั่นคง	1) โครงการพัฒนาระบบป้องกันและแก้ไขปัญหาการเผยแพร่ข้อมูลที่ส่งผลกระทบต่อความมั่นคง (***โครงการเร่งด่วน***) 2) โครงการทบทวนระบบป้องกันและแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง	ดศ. และหน่วยงานด้านความมั่นคง
7. การสร้างความตระหนักรู้ประชาชนและหน่วยงาน	1) โครงการสร้างความตระหนักและรอบรู้การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์ภาคประชาชนและหน่วยงานทั่วไป (***โครงการเร่งด่วน***) 2) โครงการสร้างกลไกการกำกับดูแลตนเอง (Self-regulation) และสร้างศูนย์รับเรื่องร้องเรียนด้านภัยคุกคามทางด้านไซเบอร์	ดศ. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แผนงาน	โครงการที่สำคัญ	หน่วยงานดำเนินงาน
8. การพัฒนากฎหมาย	1) โครงการพิจารณากฎหมาย กฎ ระเบียบ แนวทางและมาตรการการป้องกันปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ (***โครงการเร่งด่วน***) 2) โครงการติดตามผลภายหลังการบังคับใช้กฎหมาย Cybersecurity	ดศ. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
9. การพัฒนาศักยภาพบุคลากรของหน่วยงาน และทุกภาคส่วน	1) โครงการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ (***โครงการเร่งด่วนโดยใช้เงินกองทุน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม***) 2) โครงการวิจัย และพัฒนาศักยภาพทางเทคโนโลยีในการแจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟู ปราบปราม/ตอบโต้	ดศ. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี (วท.) หน่วยงานที่เกี่ยวข้อง

ในส่วนของการให้ความสำคัญกับ **“ปัญหาอธิปไตยทางไซเบอร์ (Cyber sovereignty)”** ถูกบรรจุอยู่ในยุทธศาสตร์ชาติ 20 ปี ในประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ประเด็นที่ 4.2 อุตสาหกรรมและบริการแห่งอนาคต ประเด็นย่อยที่ 4.2.5 อุตสาหกรรมความมั่นคงของประเทศ เพื่อสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ และเพื่อปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล โดยแผนแม่บทยุทธศาสตร์ของอุตสาหกรรมความมั่นคงของประเทศได้กำหนดโครงการที่สำคัญเอาไว้ 3 โครงการ ดังปรากฏในตารางที่ 3-3

ตารางที่ 3-3 โครงการสำคัญภายใต้แผนย่อยการสร้างอุตสาหกรรมความมั่นคงของประเทศ

โครงการ	สาระสำคัญ	งบประมาณ (ล้านบาท)	ระยะเวลาดำเนินการ	หน่วยงานดำเนินงานหลัก
1. เทคโนโลยีสองทางเพื่อความมั่นคงและปลอดภัย	ส่งเสริมให้เกิดอุตสาหกรรมเทคโนโลยีป้องกันประเทศ โดยส่งเสริมการพัฒนาเทคโนโลยีสองทาง ที่สามารถใช้ได้ทั้งทางทหารและเชิงพาณิชย์ และใช้แพลตฟอร์มด้านความมั่นคงของประเทศ	1,500	20 ปี (2561-2580)	กระทรวงวิทยาศาสตร์และเทคโนโลยี

โครงการ	สาระสำคัญ	งบประมาณ (ล้านบาท)	ระยะเวลาดำเนินการ	หน่วยงานดำเนินงานหลัก
2. เทคโนโลยีระบบกักเก็บพลังงาน	วิจัยและพัฒนาองค์ประกอบของเทคโนโลยีระบบกักเก็บพลังงานด้านวัสดุ ด้าน system package การใช้เซลล์เชื้อเพลิงสำหรับการใช้งานระบบกักเก็บพลังงานขนาดใหญ่ การพัฒนา power electronics controls และ system integration รวมถึงการต่อยอดงานวิจัยเพื่อประยุกต์ใช้งานจริงผ่านโครงการสาธิต รวมถึงกระตุ้นการลงทุนของอุตสาหกรรมการผลิต เพื่อประยุกต์ใช้เทคโนโลยีระบบกักเก็บพลังงานในด้านความมั่นคง นิคมอุตสาหกรรม พลังงานทดแทน และพื้นที่ห่างไกล	1,500	20 ปี (2561-2580))	กระทรวงวิทยาศาสตร์และเทคโนโลยี
3. โครงการจัดทำระบบฐานข้อมูลอุตสาหกรรมความมั่นคงของประเทศ	จัดทำฐานข้อมูลอุตสาหกรรมความมั่นคงของประเทศ โดยกำหนดนิยาม ขอบเขตและรหัสสินค้า บูรณาการและเชื่อมโยงข้อมูลร่วมระหว่างหน่วยงาน และพัฒนาข้อมูลอย่างเป็นระบบและต่อเนื่อง	600	3 ปี (2563-2565)	กระทรวงกลาโหม สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงสาธารณสุข กระทรวงมหาดไทย กระทรวงการคลัง กระทรวงพาณิชย์

จะเห็นได้ว่า การให้ความสำคัญของ**ปัญหาการรุกรานอธิปไตยทางไซเบอร์**ในยุทธศาสตร์ชาติ 20 ปี มีมีความหมายในเชิงการป้องกันการรุกรานระบบฐานข้อมูล โครงสร้างพื้นฐาน และการโจมตีเทคนิค ซึ่งยังไม่มีความชัดเจนในการสร้างความตระหนักรู้แก่ภาคประชาชนเพื่อป้องกันการรุกรานทางความคิด ความเชื่อ และอุดมการณ์ และการสร้างความรู้ความเข้าใจให้ประชาชนรู้เท่าทันปฏิบัติการข่าวสารผ่านสื่อสังคมออนไลน์ (Social media) การโฆษณาชวนเชื่อและข่าวปลอม (Fake news) โดยเฉพาะอย่างยิ่งกลุ่มเป้าหมายที่เป็นเยาวชนและคนรุ่นใหม่ ซึ่งมีการใช้งานอุปกรณ์สมาร์ทโฟน และ Social media มากกว่ากลุ่มอื่น

2.2 การป้องกันการรุกล้ำอธิปไตยไซเบอร์ภายใต้ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564) (National cybersecurity strategy) โดยสำนักงานสภาความมั่นคงแห่งชาติ

สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้จัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ (2560 - 2564) (National cybersecurity strategy) ซึ่งเป็นแนวนโยบายระดับชาติฉบับแรกของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่กำหนดยุทธศาสตร์ที่สำคัญ 6 ด้าน (ตารางที่ 3-4) พร้อมทั้งมีการแต่งตั้งคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในปี 2560 และมีการแต่งตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National cybersecurity committee: NCSC) (กมช.) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ซึ่งมีรัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ตารางที่ 3-4 ประเด็นยุทธศาสตร์ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564)

ประเด็นยุทธศาสตร์	เป้าหมาย
1. เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ	1) รัฐบาลให้ความสำคัญและสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 2) ภาคธุรกิจและประชาชนมั่นใจในการใช้เทคโนโลยีดิจิทัลอินเทอร์เน็ตและไซเบอร์สเปซที่ได้มาตรฐาน ทั้งจากการใช้บริการภาครัฐภาคธุรกิจและส่วนบุคคล
. ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้าน การรับมือภัยคุกคามทางไซเบอร์	1) ประเทศไทยมีการบูรณาการการทำงานด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 2) ประเทศไทยมีหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ และมีการกำหนดบทบาทและหน้าที่หน่วยงานต่าง ๆ ของรัฐอย่างชัดเจน เพื่อดูแลการปกป้องโครงสร้างพื้นฐานสำคัญ ที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน 3) มีการทำงานขององค์กรต่าง ๆ ในรูปแบบที่

ประเด็นยุทธศาสตร์	เป้าหมาย
	สามารถทำงานที่พร้อมรับมือกับภัยคุกคามทางไซเบอร์ในแบบ Computer emergency response team (CERT) มากขึ้น
3. ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่	1) มีการวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ ที่ทันสมัย ครอบคลุมรอบด้าน ต่อเนื่อง และถูกต้องแม่นยำเพื่อประโยชน์ในการตัดสินใจทางนโยบายและปฏิบัติที่เหมาะสม 2) กองทัพและหน่วยงานความมั่นคงที่เกี่ยวข้องมีความพร้อมรับมือภัยคุกคามทางไซเบอร์ทั้งในรูปแบบเดิมและภัยคุกคามในรูปแบบใหม่ ๆ 3) มีแผนเผชิญภัยคุกคามทางไซเบอร์เมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์
4. เสริมสร้างระบบเศรษฐกิจดิจิทัล	1) ประเทศไทยเปลี่ยนผ่านเข้าสู่เศรษฐกิจดิจิทัลอย่างราบรื่นและมีความยั่งยืน 2) มีการใช้เทคโนโลยีดิจิทัลในวงกว้างมากขึ้นในภาคเอกชน 3) มียุทธศาสตร์/แผนงาน กฎระเบียบที่มีประสิทธิภาพ เหมาะสมต่อระบบเศรษฐกิจดิจิทัล ได้มาตรฐาน และเอกชนมีส่วนร่วม
5. สร้างความตระหนักและส่งเสริมความร่วมมือ ภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	1) ประชาชนทั่วไปทุกระดับ ทุกเพศและวัยที่เป็นผู้ใช้อินเทอร์เน็ตมีความตระหนักถึงภัยคุกคามทางไซเบอร์ และมีความรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์ 2) รัฐ ภาคเอกชน และประชาสังคมร่วมมือกันในการรักษาความมั่นคงปลอดภัยไซเบอร์ 3) ช่องทาง/กลไกการสื่อสารแนวนโยบายสู่การปฏิบัติในภาคเอกชนและภาคประชาสังคม

ประเด็นยุทธศาสตร์	เป้าหมาย
6. เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม	1) ให้มีกลไกที่มีการปลูกฝังจิตสำนึกที่ดีในการใช้ไซเบอร์สเปซไปในทางที่เหมาะสม และเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์ 2) ส่งเสริมให้เกิดเครือข่ายผู้ใช้อินเทอร์เน็ตที่ช่วยกันดูแล การใช้ไซเบอร์สเปซไปในทางที่เหมาะสม 3) ส่งเสริมการเรียนรู้ โดยเฉพาะอย่างยิ่งในกลุ่มเด็กและเยาวชนให้รู้เท่าทันและมีความตระหนักเกี่ยวกับภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยของ ไซเบอร์สเปซ

ที่มา : สำนักงานสภาความมั่นคงแห่งชาติ

จะเห็นได้ว่า ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564) ของ สมช. ส่วนใหญ่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางกายภาพ และภัยคุกคามทางไซเบอร์เป็นหลัก มีเพียงยุทธศาสตร์เดียวที่กล่าวถึงการสร้างความรู้ทางดิจิทัลให้แก่ประชาชน แต่เป็นการสร้างความรู้เฉพาะในด้านการเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์ และตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เป็นการคุมทางกายภาพ มิใช่การรุกรานทางความคิดและอธิปไตยทางไซเบอร์

วิเคราะห์ความสอดคล้องยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับการแก้ปัญหาอธิปไตยไซเบอร์ในระดับสากล

เมื่อพิจารณาเปรียบเทียบยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) และยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5 ปี (พ.ศ. 2560 - 2564) กับกรอบแนวคิด National cybersecurity capacity maturity model (CMM) ซึ่งจัดทำโดย The Global Cybersecurity capacity centre แห่ง University of Oxford (ตารางที่ 3-5) จะเห็นได้ว่า ประเด็นยุทธศาสตร์ของยุทธศาสตร์ชาติครอบคลุมทุกมิติของแนวคิด CMM แล้ว แต่หากพิจารณาในรายละเอียดจะพบว่าแผนงานที่ 7 การสร้างความตระหนักรู้ประชาชนและหน่วยงาน เน้นเฉพาะในการโจมตีทางไซเบอร์ยังไม่ครอบคลุมเรื่องการรักษาอธิปไตยทางไซเบอร์ตามมิติที่ 2 ของ CMM ส่วนแผนงานที่ 5

การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ซึ่งมีเรื่องของการพัฒนาบุคลากรและแลกเปลี่ยนความรู้ แต่ยังไม่ครอบคลุมการพัฒนาบุคลากรให้รู้เท่าทันการละเมิดข้อมูลส่วนบุคคลและนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต และการรักษา “อธิปไตยทางไซเบอร์” ตามมิติที่ 2 ของ CMM เช่นกัน

สำหรับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564) ของ สมช. มีเพียงยุทธศาสตร์เดียวที่กล่าวถึงการสร้างความรู้ทางดิจิทัลให้แก่ประชาชน แต่เป็นการสร้างความรู้เฉพาะในด้านการเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์ และตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เป็นการคุมทางกายภาพ มิใช่การรุกรานทางความคิด และ **“อธิปไตยทางไซเบอร์ (Cyber sovereignty)”** ตามมิติที่ 2 ของ CMM นอกจากนี้ ถึงแม้ว่ายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564) ของ สมช. ครอบคลุมทุกมิติของแนวคิด CMM แล้ว แต่ในมิติที่ 3 ของ CMM ในเรื่อง Cybersecurity education, training and skills แต่กลับไม่มียุทธศาสตร์รองรับ มีเพียงแนวทางการดำเนินการที่ 2.8 ภายใต้ประเด็นยุทธศาสตร์ที่ 2 การปกป้องโครงสร้างพื้นฐานสำคัญ ที่พูดถึงเฉพาะเรื่องการพัฒนาศักยภาพของบุคลากรในภาครัฐ แต่ไม่ครอบคลุมถึงกลุ่มเยาวชนและประชาชนทั่วไป ซึ่งจำเป็นต้องมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับแต่ละช่วงวัยแต่ตั้งระดับประถมศึกษา และใน มิติที่ 4 ของ CMM ในเรื่อง Legal and regulatory frameworks ก็ไม่มียุทธศาสตร์รองรับ มีเพียงแนวทางการดำเนินการที่ 2.7 ภายใต้ประเด็นยุทธศาสตร์ที่ 2 การปกป้องโครงสร้างพื้นฐานสำคัญ ที่พูดถึงการร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติ และข้อกำหนด เพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ดังนั้น จึงควรนำ Cybersecurity capacity maturity model (CMM) มาใช้เป็นกรอบแนวคิดในการพัฒนาและขับเคลื่อนยุทธศาสตร์ชาติ และยุทธศาสตร์การดูแลความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 3-5 เปรียบเทียบยุทธศาตร์ชาติ 20 ปี และยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทยกับกรอบแนวคิด CMM

กรอบแนวคิด Cybersecurity capacity maturity model (CMM)	**ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)**	**ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5 ปี (พ.ศ. 2560 - 2564)**

กรอบแนวคิด Cybersecurity capacity maturity model (CMM)	**ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)**	**ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5 ปี (พ.ศ. 2560 - 2564)**
มิติที่ 1 National Cybersecurity framework and policy กรอบยุทธศาสตร์และนโยบาย การรับมือภัยคุกคาม การป้องกันโครงสร้างพื้นฐานที่สำคัญ การบริหารความเสี่ยง การรับมือภาวะวิกฤต ระบบป้องกัน การประสานงาน	**ประเด็นยุทธศาสตร์ความมั่นคง** แผนงานที่ 3 การพัฒนาศักยภาพระบบบริหารจัดการด้านไซเบอร์ แผนงานที่ 4 การพัฒนาศักยภาพระบบตอบโต้สถานการณ์ฉุกเฉิน แผนงานที่ 9 การพัฒนาศักยภาพบุคลากรของหน่วยงาน และทุกภาคส่วน	ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์
มิติที่ 2 Cyber culture and society ความรู้ความเข้าใจความเชื่อมั่นของผู้ใช้บริการเกี่ยวกับการละเมิดและนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต ช่องทางการรายงานอาชญากรรมทางไซเบอร์ อิทธิพลของ Social media และอธิปไตยไซเบอร์	**ประเด็นยุทธศาสตร์ความมั่นคง** แผนงานที่ 7 การสร้างความตระหนักรู้ประชาชนและหน่วยงาน	ประเด็นยุทธศาสตร์ที่ 5 สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประเด็นยุทธศาสตร์ที่ 6 เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม
มิติที่ 3 Cybersecurity education, training and skills การสร้างความตระหนักรู้ถึงความเสี่ยงและภัยคุกคาม	**ประเด็นยุทธศาสตร์ความมั่นคง** แผนงานที่ 5 การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ	ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซ

กรอบแนวคิด Cybersecurity capacity maturity model (CMM)	**ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)**	**ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5 ปี (พ.ศ. 2560 - 2564)**
การสร้างระบบการศึกษา ระบบการอบรม ระบบการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์		เบอร์ (แนวทางการดำเนินการที่ 2.8 การพัฒนาศักยภาพของบุคลากรในภาครัฐภาค การศึกษาฝึกอบรมรูปแบบต่าง ๆ และส่งเสริม การถ่ายทอดความรู้ภายในภาครัฐ หรือระหว่างภาครัฐกับเอกชน การพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม)
มิติที่ 4 Legal and regulatory frameworks กรอบของกฎหมาย การบังคับใช้กฎหมาย ความสามารถในการสืบสวนอาชญากรรมทางไซเบอร์ ความสามารถของศาลในการตัดสินคดีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ ความร่วมมือระหว่างประเทศ	**ประเด็นยุทธศาสตร์ความมั่นคง** แผนงานที่ 2 การจัดตั้งองค์กรและพัฒนาขีดความสามารถในงานมั่นคงปลอดภัยทางไซเบอร์ แผนงานที่ 8 การพัฒนากฎหมาย	ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์ (แนวทางการดำเนินการที่ 2.7 การร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติ และข้อกำหนดเพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณากำหนดบท

กรอบแนวคิด Cybersecurity capacity maturity model (CMM)	ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)	ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 5 ปี (พ.ศ. 2560 - 2564)
		คุ้มครองและบทลงโทษที่เหมาะสม)
มิติที่ 5 Standards, organizations, and technologies มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ การสร้างความเชื่อมั่นให้ประชาชน การส่งเสริมภาคเอกชนในการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การพัฒนาหน่วยงานจัดเก็บข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์	**ประเด็นยุทธศาสตร์ความมั่นคง** แผนงานที่ 1 การพัฒนาแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ แผนงานที่ 6 การป้องกัน แก้ไขปัญหา การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง **ประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน** แผนงานเสริมสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์	ประเด็นยุทธศาสตร์ที่ 1 เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ ประเด็นยุทธศาสตร์ที่ 3 ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคาม รูปแบบเดิมและรูปแบบใหม่ ประเด็นยุทธศาสตร์ที่ 4 เสริมสร้างระบบเศรษฐกิจดิจิทัล

สรุป

จากการศึกษายุทธศาสตร์ในการป้องกันการรุกรานทางอธิปไตยไซเบอร์ของต่างประเทศ พบว่า ประเทศจีนเป็นประเทศที่ประสบความสำเร็จเพียงประเทศเดียว จากการมี “National gateway" หรือ “The great firewall” และการมีแพลตฟอร์มของประเทศตนเอง เช่น เว็บไซต์ค้นหา (Search engine) อย่างไป่ตู้ (Baidu) ซึ่งมีฟังก์ชั่นการใช้งานที่คล้ายกับ Google เครือข่ายสังคมออนไลน์เวย์ปั๋ว (Weibo) วีแชท (WeChat) ซึ่งมีลักษณะคล้ายกับ LINE ในขณะที่ประเทศออสเตรเลีย และศสิงคโปร์ กำลังตามหลังประเทศจีน โดยริเริ่มมาตรการการป้องกัน

การรุกรานอธิปไตยทางไซเบอร์แล้ว ได้แก่ โดยกรณีประเทศออสเตรเลีย มีกฎหมายการเข้ารหัสข้อมูล (Assistance and access act: AAA) ที่ช่วยให้เจ้าหน้าที่รัฐหรือตำรวจเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งาน เพื่อประโยชน์ต่อการสืบสวนคดี และรับมือกับเครือข่ายการก่ออาชญากรรมทางไซเบอร์ และกรณีประเทศสิงคโปร์ที่มีแนวปฏิบัติควบคุม “เนื้อหาต้องห้าม” บนอินเทอร์เน็ต และกฎหมาย Protection from online falsehoods and manipulation act 2019 (POFMA) เพื่อจัดการกับการเผยแพร่ข่าวปลอม และการปลุกปั่นในโลกออนไลน์ ในขณะที่ เมื่อพิจารณาขีดความสามารถด้านเทคโนโลยีของประเทศในภูมิภาคอาเซียน จะเห็นได้ว่า ประเทศในภูมิภาคอาเซียนไม่มีหรือไม่ได้ครอบครองเทคโนโลยีดิจิทัลเป็นของตนเอง ไม่มี Platform หรือโปรแกรม Social media เป็นของตนเอง เช่นเดียวกับกรณีของประเทศไทย จึงมีแนวโน้มที่จะถูกประเทศ/องค์กรที่มีศักยภาพด้านไซเบอร์ ใช้เครื่องมือ Cyber ผ่าน Platform และ Social media เป็นเครื่องมือพลังอำนาจอ่อน (Soft power) รุกรานอธิปไตยไซเบอร์ได้

กรณีของประเทศไทย ความไม่พร้อมในการรับมือปรากฏการณ์ Social media และการสูญเสียอธิปไตยทางไซเบอร์ (Cyber sovereignty) รัฐบาลยังไม่มีวิธีจัดการทั้งตามยุทธศาสตร์ชาติและยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประเด็นยุทธศาสตร์ของยุทธศาสตร์ชาติ 20 ปี (2561 - 2580) มีแผนงานการสร้างความตระหนักรู้ประชาชนและหน่วยงานที่เน้นเฉพาะในการการโจมตีทางไซเบอร์ ยังไม่ครอบคลุมเรื่องการรักษาอธิปไตยทางไซเบอร์และแผนงานการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ซึ่งมีเรื่องของการพัฒนาบุคลากรและแลกเปลี่ยนความรู้ แต่ยังไม่ครอบคลุมการพัฒนาบุคลากรให้รู้เท่าทันการละเมิดข้อมูลส่วนบุคคลและนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต และการรักษา “อธิปไตยทางไซเบอร์”

บทที่ 4
การกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทย และกรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ใน 5 มิติ

แนวคิดในการปรับยุทธศาสตร์ความมั่นคงแห่งชาติ นโยบายความมั่นคงแห่งชาติ

จากการวิเคราะห์สภาพแวดล้อมทางไซเบอร์ในภาพรวมของประเทศไทย ในเรื่องความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ สามารถสรุปปัญหาที่สำคัญของประเทศออกเป็น 2 ปัญหาใหญ่ ดังนี้

1. ความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ (Lack of national cybersecurity incident response capability and national cybersecurity defense capability)

2. ความไม่พร้อมในการรับมือปรากฏการณ์ “Social Media as a new source of soft power” และการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ (Lack of defensive/offensive capability in cyber warfare/hybrid warfare, cybersecurity strategy for protecting cyber sovereignty at the national level)

ปัญหาใหญ่ที่ 1 เปรียบเสมือนยอดภูเขาน้ำแข็ง (Tip of the iceberg) ที่ส่วนใหญ่เป็นภัยคุกคามไซเบอร์ทางกายภาพ ซึ่งสามารถรับรู้ได้ชัดเจน และรัฐได้ดำเนินการไปบ้างแล้วผ่านยุทธศาสตร์ชาติ 20 และการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2560 - 2564) (National cybersecurity strategy) โดยสำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

ปัญหาใหญ่ ที่ 2 ความไม่พร้อมในการรับมือปรากฏการณ์ “Social Media as a new source of soft power” และการสูญเสียอธิปไตยทางไซเบอร์ (Cyber sovereignty) นั้น เปรียบเสมือนส่วนของภูเขาน้ำแข็งที่จมอยู่ใต้น้ำ (Submerged part of the iceberg) ซึ่งเป็นส่วนที่ใหญ่กว่ามาก เราควบคุมไม่ได้ และรัฐยังไม่มีวิธีจัดการทั้งตามยุทธศาสตร์ชาติและยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (แผนภาพที่ 4-1)

แผนภาพที่ 4-1 ปัญหาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมของประเทศไทย

เมื่อทำการวิเคราะห์เจาะลึกลงไปในรายละเอียดของปัญหาพบว่า เราสามารถจัดกลุ่มของปัญหาใหญ่ทั้ง 2 ออกเป็น 10 ปัญหาย่อย ดังนี้

ปัญหาย่อยที่ 1 การโจมตีโครงสร้างพื้นฐานที่สำคัญยิ่งยวดในระดับประเทศ (National level critical infrastructure attack) การขาดยุทธศาสตร์ แผนงานที่มีประสิทธิภาพในการบริหารจัดการความเสี่ยงทางไซเบอร์ในระดับประเทศ โดยในปัจจุบันจำนวนเหตุการณ์การหยุดให้บริการของหน่วยงานโครงสร้างพื้นฐานมีอัตราการเกิดเหตุเพิ่มขึ้นอย่างต่อเนื่องและยาวนานขึ้น เช่น “พลเมืองต่อต้าน Single gateway #opsinglegateway” รณรงค์ให้มีการโจมตี DDoS กับเว็บไซต์ของหน่วยงานของรัฐ ทำให้หลายระบบสำคัญของรัฐขัดข้อง ในปี 2559 ATM 21 ตู้ของธนาคารออมสินถูกโจมตีด้วยมัลแวร์และลอบขโมยเงิน 12 ล้านบาทมัลแวร์ที่พบคล้ายกับที่ใช้โจมตี ATM ในประเทศไต้หวันในปีเดียวกัน ในปี 2559 ระบบคอมพิวเตอร์ของ มหาวิทยาลัยธรรมศาสตร์ถูกกลุ่ม GOP (Guardians of peace) ใช้เป็นฐานการโจรกรรมข้อมูลจากบริษัท Sony Pictures สหรัฐอเมริกา ในปี 2557 เป็นต้น ส่งผลกระทบต่อประชาชน คงปฏิเสธไม่ได้ว่าประเทศไทยกำลังเผชิญกับความเสี่ยงทางไซเบอร์รายวันทั้งในระดับประชาชน องค์กร และระดับประเทศ

ปัญหาย่อยที่ 2 ปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ในระดับประเทศ การขาดการพัฒนาทักษะความรู้ในระดับต้น ระดับกลาง ระดับสูง ของผู้ปฏิบัติและควบคุมในการปฏิบัติงานด้านไซเบอร์ทั้งในระดับองค์กรและระดับประเทศ โดยในปัจจุบัน องค์กรทั้งภาครัฐและเอกชนในประเทศไทย ขาดแคลนผู้เชี่ยวชาญทางไซเบอร์ ส่งผลกระทบต่อความเชื่อมั่นและความมั่นคงในระดับชาติในระยะยาว จากการประมาณการของบริษัทไซเบอร์ซีเคียวริตี้เวนเจอร์ส[1] คาดว่า ในปี พ.ศ. 2564 โลกจะขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ถึง 3,500,000 คน และจากการประมาณการของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์[2] ประเทศไทยจะขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์สูงถึง 12,000 คน โดยกลุ่มที่ขาดแคลนมากที่สุดคือกลุ่มผู้พัฒนาและออกแบบระบบ (Securely provision : SP)

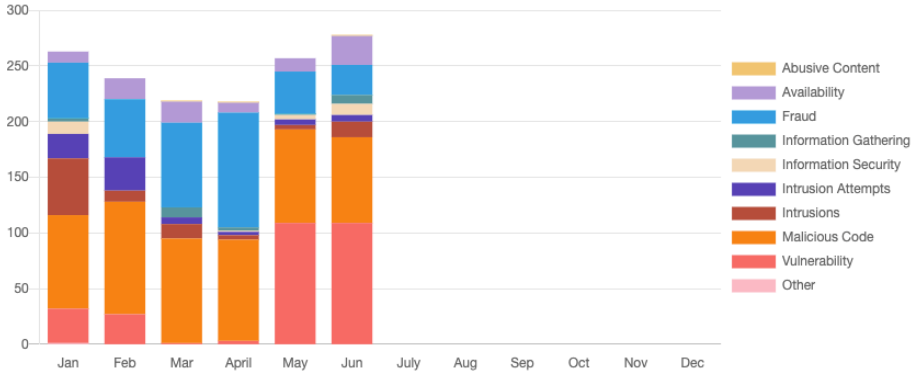
ปัญหาย่อยที่ 3 ปัญหาอาชญากรรมไซเบอร์ ภัยคุกคามไซเบอร์ การโจมตีทางไซเบอร์ต่อภาครัฐ ภาคเอกชน และประชาชนทั่วไป (Rising of cyber crime at national level) โดยประชาชนส่วนใหญ่ และองค์กรทั้งภาครัฐและเอกชน ถูกโจมตีทางไซเบอร์รายวัน ขณะที่ประเทศไทยยังขาดหน่วยงานรับผิดชอบโดยตรง ส่งผลต่อเศรษฐกิจและสังคม และ ส่งผลกระทบต่อความเชื่อมั่นในระดับชาติ ทั้งนี้ ในช่วงครึ่งปีแรกของปี 2563 จำนวนภัยคุกคามไซเบอร์ที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้รับแจ้งและดำเนินการทั้งสิ้น 1,474 กรณี โดยภัยคุกคามที่ได้รับแจ้งมากที่สุด คือ การโจมตีด้วยโปรแกรมไม่พึงประสงค์หรือโค้ดอันตราย (Malicious code) และการฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) โดยมีอัตราส่วนถึงร้อยละ 36 และ 24 ตามลำดับ

แผนภาพที่ 4-2 สถิติภัยคุกคามไซเบอร์ ปี 2563 จำแนกรายเดือน

---

[1] สมาคมโทรคมนาคมแห่งประเทศไทย. แนวทางการสร้างกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์.

[2] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (2560). การพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐเพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล “รู้ทัน Cyber”.



ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ปัญหาย่อยที่ 4 ปัญหาขาดยุทธศาสตร์และแผนงานที่มีประสิทธิภาพในการบังคับใช้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ โดยในปัจจุบันจำนวนเหตุการณ์การหยุดให้บริการของหน่วยงานโครงสร้างพื้นฐานมีอัตราการเกิดเหตุเพิ่มขึ้นอย่างต่อเนื่องและยาวนานขึ้น ส่งผลกระทบต่อประชาชน คงปฏิเสธไม่ได้ว่าประเทศไทยกำลังเผชิญกับความเสี่ยงทางไซเบอร์รายวันทั้งในระดับประชาชน องค์กร และ ระดับประเทศ

ปัญหาย่อยที่ 5 ปัญหาการขาดการถ่ายทอดความรู้ให้กับหน่วยงานยุติธรรมในการปฏิบัติและควบคุมการปฏิบัติตามกฎหมาย โดยหลายปีที่ผ่านมา ประเทศไทยมีกฎหมายด้านเทคโนโลยีสารสนเทศหลายฉบับ แต่ยังไม่สามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพเท่าใดนัก ในปัจจุบัน ตำรวจ ผู้พิพากษา อัยการ ศาล หลายท่านยังขาดองค์ความรู้ทางด้านไซเบอร์ในการพิจารณาคดี ทำให้มีผลต่อการบังคับใช้กฎหมาย

ปัญหาย่อยที่ 6 ปัญหาอธิปไตยทางไซเบอร์ (Cyber sovereignty) การขาดความเข้าใจในผลกระทบจากกระบวนการปฏิบัติการข่าวสารในรูปแบบใหม่ผ่านสื่อสังคมออนไลน์ (Social media) โดยปัจจุบันประชาชนชาวไทยกำลังถูกละเมิดข้อมูลส่วนบุคคลทางไซเบอร์ และถูกทำให้หลงเชื่อในการโฆษณาชวนเชื่อรายวัน อย่างต่อเนื่อง จากปรากฏการณ์ดังกล่าว ทำให้มีผลต่อเศรษฐกิจ สังคม การเมือง การปกครอง ทั้งในระยะสั้นและระยะยาว มีผลกระทบต่อความมั่นคงของชาติในระยะยาว

ปัญหาย่อยที่ 7 ปัญหาการใช้ประโยชน์จากการเข้าถึงข้อมูลส่วนบุคคล และการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์โดยไม่ได้รับอนุญาต เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ

เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น

ปัญหาย่อยที่ 8 ปัญหาขาดทักษะและความเข้าใจและความรู้ในการใช้เทคโนโลยีดิจิทัล หรือ Digital literacy โดยเฉพาะการทิ้งรอยเท้าดิจิทัล (Digital footprint) เช่น หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประชาชน ส่งผลให้ข้อมูลอยู่ในมือผู้ไม่หวังดี มีโอกาสโดนทำสำเนาไปนับไม่ถ้วน เป็นต้น เทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล (Phishing) เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น การหลอกลวงออนไลน์ (Fraud) เช่น ส่งสินค้าปลอมให้เหยื่อ หรือในกรณีที่แย่ที่สุด คือไม่ส่งสินค้าใด ๆ ให้เลย เป็นต้น ความเข้าใจสื่อดิจิทัล เช่น กับดักโซเชียลจากข่าวปลอม เป็นต้น

ปัญหาย่อยที่ 9 ปัญหาขาดการบูรณาการทั้งองค์กรภาครัฐ ฝ่ายตำรวจ ทหาร พลเรือน และภาคส่วนต่าง ๆ ภายในประเทศเพื่อป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ ขาดการพัฒนากรอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ จากปัญหาที่ประเทศไทยยังไม่สามารถบริหารจัดการปัญหาความมั่นคงปลอดภัยไซเบอร์ให้เกิดการบูรณาการได้ ทำให้เกิดความซ้ำซ้อน สิ้นเปลืองงบประมาณ ไม่ส่งผลเป็นรูปธรรม ไม่เกิดประสิทธิผลและประสิทธิภาพในการรับมือต่อการโจมตีทางไซเบอร์ รวมถึงขาดการถ่ายทอดความรู้และการประสานงานความร่วมมืออย่างเป็นทางการในระดับชาติกับประชาคมอาเซียน

ปัญหาย่อยที่ 10 ปัญหาขาดการพัฒนาแพลตฟอร์มของประเทศ เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์และอธิปไตยไซเบอร์ในระดับชาติ โดยแพลตฟอร์ม Social media ไทยมีอยู่แพลตฟอร์มเดียวคือ Pantip แต่ Pantip นั้นถูกแพลตฟอร์มต่างชาติแย่งเวลาของคนไปเป็นส่วนใหญ่ โดยปัจจุบัน คนไทยใช้ Facebook มากกว่า 50 ล้านคนแล้ว และใช้ Twitter มากกว่า 20 ล้านคนแล้ว แม้แต่ในยามที่เกิดวิกฤตการระบาดของโรค COVID-19 ธุรกิจแพลตฟอร์มดิลิเวอร์รี่ไทยยังมีขนาดเล็ก ประเทศไทยจึงยังต้องพึ่งพาแพลตฟอร์มดิลิเวอรี่ขนาดใหญ่ของต่างชาติ การทำงานที่บ้านหรือ Work from home ที่ผู้ประกอบการเล็กใหญ่ทุกราย ต้องปรับตัวประชุมทางไกล (Video-conference) ซึ่งก็อยู่บนแพลตฟอร์มของต่างชาติเช่นกัน

ทั้งนี้ สามารถนำเสนอแนวคิดในการปรับยุทธศาสตร์ชาติ 20 ปี เพื่อแก้ไขปัญหาย่อยทั้ง 10 ปัญหาได้ (ตารางที่ 4-1) ดังนี้

ตารางที่ 4-1 ปัญหาย่อย และแนวคิดในการปรับปรุงยุทธศาสตร์

ที่	ปัญหาย่อย	แนวคิดในการปรับปรุงยุทธศาสตร์
ปัญหาใหญ่ที่ 1 ความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และ		

ที่	ปัญหาย่อย	แนวคิดในการปรับปรุงยุทธศาสตร์
ความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ		
1.	1.1 การโจมตีโครงสร้างพื้นฐานที่สำคัญยิ่งยวดในระดับประเทศ (National level critical infrastructure attack) 1.2 การขาดยุทธศาสตร์ แผนงานที่มีประสิทธิภาพในการบริหารจัดการความเสี่ยงทางไซเบอร์ในระดับประเทศ	1) บริหารความเสี่ยงและสร้างกลไกรับมือจากภัยคุกคามทางไซเบอร์ในหน่วยงานโครงสร้างพื้นฐานที่สำคัญ
2.	2.1 การขาดแคลนบุคลากรด้านไซเบอร์ในระดับประเทศ 2.2 การขาดการพัฒนาทักษะความรู้ในระดับต้น ระดับกลาง ระดับสูง ของผู้ปฏิบัติและควบคุมในการปฏิบัติงานด้านไซเบอร์ทั้งในระดับองค์กรและระดับประเทศ	2) พัฒนาระบบการศึกษา และบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์
3.	ปัญหาอาชญากรรมไซเบอร์ ภัยคุกคามไซเบอร์ การโจมตีทางไซเบอร์ต่อภาครัฐ ภาคเอกชน และประชาชนทั่วไป (Rising of cyber crime at national level)	3) สร้างความตระหนักรู้เรื่องความปลอดภัยไซเบอร์ (Cybersecurity awareness) และจัดการกับอาชญากรรมทางไซเบอร์อย่างเด็ดขาด
4.	ขาดยุทธศาสตร์และแผนงานที่มีประสิทธิภาพในการบังคับใช้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์	4) พัฒนานโยบาย กฎหมายลูก และมาตรฐานความปลอดภัยทางไซเบอร์
5.	ขาดการถ่ายทอดความรู้ให้กับหน่วยงานยุติธรรมในการปฏิบัติและควบคุมการปฏิบัติตามกฎหมาย	5) พัฒนาบุคลากรด้านการบังคับใช้กฎหมาย การสืบสวน และการตัดสินคดีทางไซเบอร์
ปัญหาใหญ่ที่ 2 ความไม่พร้อมในการรับมือการรุกรานทางความคิดผ่านเครือข่ายสังคมออนไลน์ (Social media) และการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ		
6.	ปัญหาอธิปไตยทางไซเบอร์ (Cyber	6) สร้างความรู้ความเข้าใจประชาชน

ที่	ปัญหาย่อย	แนวคิดในการปรับปรุงยุทธศาสตร์
	sovereignty) การขาดความเข้าใจในผลกระทบจากกระบวนการปฏิบัติการข่าวสารในรูปแบบใหม่ผ่านสื่อสังคมออนไลน์ (Social media)	ให้รู้เท่าทันปฏิบัติการข่าวสารทางสื่อสังคมออนไลน์ (Social media)
7.	ปัญหาการใช้ประโยชน์จากการเข้าถึงข้อมูลส่วนบุคคล และการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์โดยไม่ได้รับอนุญาต	7) สร้างความตระหนักรู้ถึงการใช้ประโยชน์จากข้อมูลส่วนบุคคลในการโฆษณาชวนเชื่อ รวมถึงสิทธิและวิธีการปกป้องและคุ้มครองข้อมูลส่วนบุคคล
8.	ปัญหาขาดทักษะและความเข้าใจและความรู้ในการใช้เทคโนโลยีดิจิทัลหรือ Digital literacy	8) สร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy ให้มี "ภูมิคุ้มกันทางดิจิทัล" และ “ภูมิคุ้มกันทางไซเบอร์” (Digital immunity/Cyber immunity) ที่ดี
9.	9.1 ขาดการบูรณาการทั้งองค์กรภาครัฐ ฝ่ายตำรวจ ทหาร พลเรือน และภาคส่วนต่าง ๆ ภายในประเทศเพื่อป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ 9.2 ขาดการพัฒนากรอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์	9) บูรณาการหน่วยงานภาครัฐ (Joint-force) มีเจ้าภาพชัดเจน และสร้างความร่วมมือองค์กรระหว่างประเทศ และจัดการอย่างเป็นระบบ
10.	ขาดการพัฒนาแพลตฟอร์มภายในประเทศเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์และอธิปไตยไซเบอร์ในระดับชาติ	10) ส่งเสริมและสนับสนุนการสร้าง Digital platform ของประเทศไทย

แนวทางในการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติของประเทศไทย และรูปแบบในการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เมื่อพิจารณาแนวทางขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับชาติเพื่อค้นหาแนวทางในการปรับปรุงแก้ไขยุทธศาสตร์ชาติ โดยจำแนกออกตามองค์กรที่มีบทบาทเป็นผู้นำของการขับเคลื่อนยุทธศาสตร์ในแต่ละประเด็นยุทธศาสตร์ ตามแนวคิดของผู้ทรงคุณวุฒิ (รองศาสตราจารย์ปณิธาน วัฒนายากร กรรมการผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ) ซึ่งได้เสนอแนะให้จำแนกแนวทางการพัฒนายุทธศาสตร์ออกเป็น 3 บทบาท ได้แก่ 1) แนวทางที่ให้รัฐมีบทบาทนำ (Government-led) 2) แนวทางที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางที่แพลตฟอร์มมีบทบาทนำ (Platform-led) สามารถจัดหมวดหมู่ของ 10 แนวคิดในการปรับปรุงยุทธศาสตร์ที่ได้จากการวิเคราะห์ปัญหาย่อยทั้ง 10 ปัญหา ออกตามผู้มีบทบาทนำในการขับเคลื่อนยุทธศาสตร์ได้ ดังนี้

1. แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led)

โดยรัฐบาลควรอาศัยกลไกหน่วยงานภาครัฐ เช่น สกมช. กมช. ดศ. สมช. เป็นต้น ร่วมกับผู้เชี่ยวชาญในภาคเอกชนในการขับเคลื่อนแผนปฏิบัติการและโครงการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

1.1 บริหารความเสี่ยงและสร้างกลไกตอบสนองต่อความเสี่ยงในหน่วยงานโครงสร้างพื้นฐานที่สำคัญ

1.2 พัฒนานโยบาย กฎหมายลูก และมาตรฐานด้านความมั่นคงปลอยภัยทางไซเบอร์

1.3 พัฒนาบุคลากรจากหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น การบังคับใช้กฎหมาย การสืบสวน และการตัดสินคดีทางไซเบอร์ เป็นต้น

1.4 บูรณาการหน่วยงานภาครัฐ ในลักษณะของปฏิบัติการร่วม (Joint-force) โดยมีหน่วยงานหลักที่เป็นเจ้าภาพชัดเจน และสร้างความร่วมมือกับภาคเอกชน ภาคประชาสังคม และองค์กรระหว่างประเทศ เพื่อรักษาสมดุลระหว่างเสรีภาพในโลกไซเบอร์สเปซและความมั่นคงปลอดภัยทางไซเบอร์

2. แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian-led)

โดยรัฐบาลควรสร้างความร่วมมือและอาศัยกลไกของกระทรวงศึกษาธิการ หน่วยงานภาครัฐ รัฐวิสาหกิจ ภาคเอกชน ในการพัฒนาความรู้และความตระหนักรู้ให้แก่ประชาชน เพื่อให้ประชาชนและภาคเอกชนมีบทบาทนำในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

2.1 พัฒนาระบบการศึกษา โดยปฏิรูปหลักสูตรการเรียนการสอน โดยสอดแทรกเนื้อหาความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในแต่ละระดับการเรียนการสอน และพัฒนาบุคลากรภาครัฐโดยเฉพาะหน่วยงานด้านโครงสร้างพื้นฐานที่สำคัญให้มีความรู้ด้านความมั่นคงปลอดภัยด้านไซเบอร์

2.2 สร้างความตระหนักรู้ (Awareness) ด้านความมั่นคงปลอดภัยด้านไซเบอร์ให้แก่ประชาชนเพื่อให้รู้เท่าทันภัยจากการใช้งานสื่อสังคมออนไลน์ (Social media) และการเปิดเผยข้อมูลส่วนบุคคลให้แก่แพลตฟอร์ม (Platform) ต่างประเทศ เพื่อป้องกันการรุกล้ำทางไซเบอร์ในระดับประเทศ

2.3 สร้างความรู้ความเข้าใจให้ประชาชนรู้เท่าทันปฏิบัติการข่าวสาร (IO) ทางสื่อสังคมออนไลน์ (Social Media) ทั้งจากภายในประเทศและต่างประเทศ

2.4 สร้างความตระหนักรู้ถึงการใช้ประโยชน์จากข้อมูลส่วนบุคคลในการโฆษณาชวนเชื่อ รวมถึงสิทธิและวิธีการปกป้องและคุ้มครองข้อมูลส่วนบุคคล

2.5 สร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy ให้มี "ภูมิคุ้มกันทางดิจิทัล" และ“ภูมิคุ้มกันทางไซเบอร์” (Digital immunity/Cyber immunity) ที่ดี

3. แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform-led)

โดยรัฐบาลควรส่งเสริมและสนับสนุนการวิจัยและพัฒนาเพื่อสร้างแพลตฟอร์มที่เป็นนวัตกรรมทางดิจิทัลที่ล้ำหน้าทันสมัย (Leapfrog digital innovation platform) ของประเทศไทย ที่สามารถตอบสนองความต้องการของประชาชนเหนือกว่าแพลตฟอร์มต่างประเทศ เพื่อให้ประเทศไทยมีแพลตฟอร์มของตนเองที่สามารถดูแลข้อมูลส่วนบุคคลของประชาชนได้ด้วย และสามารถป้องกันการรุกรานอธิปไตยทางไซเบอร์ผ่านทางสื่อสังคมออนไลน์ (Social media) เพื่อป้องกันประชาชนจากการรุกล้ำทางเศรษฐกิจ สังคม วัฒนธรรม ความคิด ความเชื่อ อุดมการณ์ ทัศนคติ ค่านิยมผ่านสื่อสังคมออนไลน์ (Social media) และแพลตฟอร์ม (Platform) ต่างประเทศ

ทั้งนี้ การสร้างแพลตฟอร์มของประเทศไทย ในลักษณะที่เป็นการเลียนแบบหรือเพื่อแข่งขันกับแพตฟอร์มต่างประเทศ เช่น Twitter และ Netflix เป็นต้น ในระยะสั้นอาจไม่สามารถเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานได้ อาจไม่ตรงตามความต้องการของประชาชน และอาจด้อยกว่าแพลตฟอร์มต่างประเทศที่มีลูกเล่น (Feature) ใหม่เพิ่มอยู่ตลอดเวลาได้ รวมถึงอาจด้อยกว่าในเชิงโครงสร้างพื้นฐานและเครือข่ายสนับสนุนการใช้งาน หรือพันธมิตร (Partner) จึงควรกำหนดแผนระยะปานกลางถึงระยะยาวในการวิจัยและพัฒนาแพลตฟอร์มที่มีความใหม่ แตกต่าง และล้ำหน้าด้วยการใช้นวัตกรรมทางดิจิทัล ซึ่งต้องอาศัยผู้เชี่ยวชาญทางเทคโนโลยีดิจิทัลทั้งจากภายในประเทศไทยและต่างประเทศ เพื่อสร้างสิ่งใหม่ที่สามารถเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานได้ และตอบโจทย์ความต้องการของประชาชนอย่างแท้จริง

จากการเปรียบเทียบปัญหาใหญ่ที่ 1 ความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ ซึ่งเปรียบเสมือนเป็นยอดภูเขาน้ำแข็งที่ลอยอยู่เหนือน้ำ (Tip of the iceberg) และปัญหาใหญ่ที่ 2 ความไม่พร้อมในการรับมือปรากฏการณ์การใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรุกรานความคิด และการสูญเสียอธิปไตยไซเบอร์ของชาติ ซึ่งเปรียบเสมือนเป็นส่วนของภูเขาน้ำแข็งที่จมอยู่ใต้น้ำ (Submerged part of the iceberg) ประเทศไทยเปรียบเหมือนเป็นเรือไทยทานิค (แผนภาพที่ 4-3) ซึ่งหากไม่มีการปรับปรุงแก้ไขยุทธศาสตร์ชาติ ทุก 5 ปี โดยรอบระยะเวลาของการทบทวนปรับปรุงแก้ไขครั้งแรกคือ ปี 2565 ซึ่งหากไม่มีการปรับปรุงแก้ไขยุทธศาสตร์ชาติในด้านความมั่นคงปลอดภัยไซเบอร์และอธิปไตยไซเบอร์ของชาติ ภายในปี 2568 หรืออีก 5 ปีข้างหน้า ปัญหาใหญ่ที่ 1 และปัญหาใหญ่ที่ 2 จะส่งผลกระทบต่อความมั่นคงของสถาบันหลักของชาติระบบเศรษฐกิจ อันดับความมั่นคงปลอดภัยไซเบอร์ของประเทศ การสูญเสียอธิปไตยทางไซเบอร์ และการขาดรายได้ภาษีจากแพลตฟอร์มต่างชาติ ซึ่งเปรียบเหมือนเรือไทยทานิคชนกับภูเขาน้ำแข็งจนต้องอับปางลงนั่นเอง

แผนภาพที่ 4-3 ปัญหาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมของประเทศไทย

กรณีที่ประเทศไทยมีการทบทวนและปรับปรุงแก้ไขยุทธศาสตร์ชาติ โดยยึดหลักการขับเคลื่อนตามแนวทางที่รัฐมีบทบาทนำ (Government-led) ภาคประชาชนมีบทบาทนำ (Civilian-led) และแพลตฟอร์มมีบทบาทนำ (Platform-led) ตามที่อภิปรายไว้ข้างต้น ย่อมเปรียบเหมือนเรือดำน้ำที่พุ่งชนภูเขาน้ำแข็งให้เปลี่ยนทิศทางออกไปจนเรือไทยทานิคสามารถหลุดพ้นปัญหาใหญ่ที่ 1 และปัญหาใหญ่ที่ 2 ได้

แผนภาพที่ 4-4 ตัวอย่างโครงการกรณีที่มีปรับปรุงแก้ไขยุทธศาสตร์ชาติ

การปรับปรุงยุทธศาสตร์ชาติตามแนวคิดในการกำหนดบทบาทผู้ขับเคลื่อนแนวทางการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ 3 บทบาท ได้แก่ 1) แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led) 2) แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform-led) สามารถกำหนดโครงการภายในแนวทางการขับเคลื่อน หน่วยงานรับผิดชอบหลัก/หน่วยงานรับผิดชอบรอง เป้าหมาย วิธีดำเนินการ และกรอบระยะเวลาดำเนินการได้ ดังนี้

ตารางที่ 4-2 หน่วยงานรับผิดชอบการขับเคลื่อนการปรับปรุงยุทธศาสตร์ชาติด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
1. แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led)				
1.1 โครงการเร่งรัดการพัฒนากฎหมายลูก และประกาศมาตรฐานความมั่นคงปลอดภัยไซเบอร์ภายใต้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.	หน่วยงานหลัก: สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ) สำนักงานสภาความมั่นคง	หน่วยงานภาครัฐสามารถบังคับใช้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้อย่างมีประสิทธิภาพ	สกมช. ศึกษาและออกประกาศกำหนดหลักเกณฑ์การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ และศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสากล เสนอมาตรฐานและแนวทาง	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
2562	แห่งชาติ (สมช.) หน่วยงานรอง: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ)		ส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์โปรแกรมคอมพิวเตอร์ ต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ตามลำดับ	
1.2 โครงการการจัดตั้ง “ส.ส.ส. ไซเบอร์”	หน่วยงานหลัก: สกมช. หน่วยงานรอง: สพธอ.	ประชาชนมีความตระหนักรู้ถึงความมั่นคงปลอดภัยทางไซเบอร์	รณรงค์ประชาสัมพันธ์ให้ความรู้แก่ประชาชนผ่านสื่อรูปแบบต่าง ๆ เกี่ยวกับการตระหนักรู้ถึงภัยไซเบอร์ และการใช้เครื่องมืออุปกรณ์นวัตกรรม อินเทอร์เน็ต และโทรศัพท์มือถือให้รู้วิธีป้องกัน/รักษาความปลอดภัยไซเบอร์เบื้องต้นด้วยตนเอง	พ.ศ. 2563-2565
1.3 โครงการการจัดตั้ง	หน่วยงานหลัก: สำนักงานตำรวจ	หน่วยงานภาครัฐสามารถป้องกัน	สตช. ยกร่างพระราชกฤษฎีกาแบ่งส่วน	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
กองบัญชาการตำรวจไซเบอร์และพัฒนาตำรวจไซเบอร์	แห่งชาติ (สตช.)	และรับมือกับอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพ	ราชการสำนักงานตำรวจแห่งชาติ และร่างกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ เสนอต่อคณะรัฐมนตรี เพื่อจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางไซเบอร์	
1.4 โครงการบูรณาการการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ในรูปแบบ Joint-Force หน่วยงานภาครัฐและเอกชน	หน่วยงานหลัก: สกมช. หน่วยงานรอง: ภาคเอกชน	บูรณาการการแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างหน่วยงานภาครัฐและภาคเอกชน	สกมช. เป็นหน่วยงานเจ้าภาพในการบูรณาการภาครัฐ และสร้างความร่วมมือกับภาคเอกชน และสร้างความร่วมมือกับองค์กรระหว่างประเทศ	พ.ศ. 2563-2565
1.5 โครงการพัฒนาบุคลากรในหน่วยงานด้านยุติธรรม	หน่วยงานหลัก: สำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.) สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) หน่วยงานรอง: สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม	พัฒนาบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมาย การสืบสวน และการตัดสินคดีทางไซเบอร์	กำหนดให้มีการพัฒนาบุคลากรภาครัฐโดยเฉพาะบุคลากรในหน่วยงานด้านยุติธรรมให้มีความเข้าใจในเรื่องความมั่นคงปลอดภัยไซเบอร์ และการบังคับใช้พ.ร.บ. ความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
			2562.	
2. แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian-led)				
โครงการสร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy "ภูมิคุ้มกันทางดิจิทัล" และ “ภูมิคุ้มกันทางไซเบอร์” ให้กับประชาชน	หน่วยงานหลัก: กระทรวงศึกษาธิการ (ศธ.) หน่วยงานรับผิดชอบรอง: กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) สมช. และภาคเอกชน	สร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy "ภูมิคุ้มกันทางดิจิทัล" และ “ภูมิคุ้มกันทางไซเบอร์” ให้กับประชาชน	1) ปรับปรุงและพัฒนาตำราเรียน แบบเรียน โดยสร้างทักษะความรู้ความเข้าใจ และความตระหนักรู้ทางด้านไซเบอร์ การใช้เทคโนโลยีดิจิทัล และความมั่นคงปลอดภัยทางไซเบอร์ให้แก่เยาวชนอย่างเหมาะสมกับแต่ละช่วงวัย 2) พัฒนาและกำหนดหลักสูตร วิชา กระบวนการเรียนรู้ที่เกี่ยวข้องในสถาบันการศึกษาทั้งภาครัฐและเอกชน	พ.ศ. 2563-2568
3. แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform Led)				
ส่งเสริมและสนับสนุนการสร้าง Leapfrog digital innovation platform ของประเทศไทย	หน่วยงานหลัก: ดศ. หน่วยงานรอง: สพธอ. สมช. และภาคเอกชน	ส่งเสริมและสนับสนุนการสร้างแพลตฟอร์มที่เป็นนวัตกรรมทางดิจิทัลที่ล้ำหน้าทันสมัย (Leapfrog digital innovation platform) ของประเทศไทย เพื่อป้องกันประชาชน	การวิจัยและพัฒนาแพลตฟอร์มที่มีความใหม่ แตกต่าง และล้ำหน้าด้วยการใช้นวัตกรรมทางดิจิทัล โดยอาศัยผู้เชี่ยวชาญทางเทคโนโลยีดิจิทัลทั้งจากภายในประเทศไทยและต่างประเทศ เพื่อสร้างสิ่งใหม่ที่สามารถเปลี่ยนแปลงพฤติกรรมของผู้ใช้งาน	พ.ศ. 2563-2568

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
		จากการรุกล้ำทางเศรษฐกิจ สังคม วัฒนธรรม ความคิด ความเชื่อ อุดมการณ์ ทัศนคติ ค่านิยม ผ่านสื่อสังคมออนไลน์ (Social media) และแพลตฟอร์ม (Platform) ต่างประเทศ	ได้ และตอบโจทย์ความต้องการของประชาชน อย่างแท้จริง	

กรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยใน 5 มิติ

การพัฒนา “กรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย” ได้นำกรอบแนวคิด National cybersecurity capacity maturity model (CMM) ซึ่งจัดทำโดย The Global Cybersecurity Capacity Centre แห่ง University of Oxford มาประยุกต์ให้เหมาะสมกับสถานการณ์ปัจจุบันและสภาวะแวดล้อมของประเทศไทย เพื่อช่วยเพิ่มขีดความสามารถด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้เป็นระบบ มีประสิทธิผล และได้มาตรฐานสากลได้

ทั้งนี้ Global Cybersecurity Capacity Centre ได้นำ CMM มาใช้ในการประเมินความสามารถด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์มาแล้วกว่า 100 ประเทศทั่วโลก โดยสามารถแบ่งมิติในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยออกเป็น 5 มิติ (แผนภาพที่ 4-5) ดังนี้

มิติที่ 1 National cybersecurity framework and policy การพัฒนานโยบายและกรอบแนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ`เป็นเรื่องสำคัญในลำดับต้น ๆ ของการพัฒนายุทธศาสตร์ไซเบอร์ในระดับประเทศ

มิติที่ 2 Cyber culture and society การปรับมุมมองและทัศนคติของประชาชนในเรื่องความเชื่อมั่นในการใช้ชีวิตในโลกไซเบอร์ เป็นการสร้างความเชื่อมั่นของประชาชนในการใช้

บริการอินเทอร์เน็ต หรือ Online service ต่าง ๆ รวมทั้งความเข้าใจของประชาชนในเรื่องความเสี่ยงในการใช้อินเทอร์เน็ต

มิติที่ 3 Cybersecurity education, training and skills การบริหารจัดการเรื่องการสร้างความตระหนักรู้ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ ของภาครัฐภาคเอกชนและประชาชนทั่วไป ตลอดจน การอบรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐภาคเอกชนและประชาชนทั่วไป

มิติที่ 4 Legal and regulatory frameworks การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ถือว่าเป็นอีกมิติที่มีความจำเป็นต้องพัฒนาเพื่อให้เท่าทันการเปลี่ยนแปลงทางดิจิทัล (Digital transformation) ที่กำลังเกิดขึ้นและส่งผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วโลก

มิติที่ 5 Standards, organizations, and technologies การพัฒนามาตรฐานและการปฏิบัติตามมาตรฐานที่เกี่ยวกับการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การควบคุมความมั่นคงปลอดภัยไซเบอร์ การใช้เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยไซเบอร์ในระดับบุคคล ระดับองค์กร และ โครงสร้างพื้นฐานของประเทศ ตลอดจนการพัฒนาเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

แผนภาพที่ 4-5 ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามแนวคิด CMM

1.1 การพัฒนากรอบแนวคิดเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (National cybersecurity framework)
1.2 การพัฒนานโยบายด้านความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (National cybersecurity policy)
1.3 การระบุและกระบวนการในการตอบสนองต่อภัยคุกคามด้านไซเบอร์ระดับประเทศ (Incident response)
1.4 การระบุโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทซ และการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (Criticali (CI) Protection and national cybersecurity risk management)
1.5 การวางแผนบริหารจัดการกับวิกฤตการณ์ฉุกเฉิน การฝึกฝนเตรียมรับวิกฤตการณ์ฉุกเฉิน และ การสร้างสถานการณ์จำลองให้พนักงานในองค์กรเตรียมพร้อมรับมือกับวิกฤตการณ์ทางไซเบอร์ต่าง ๆ (Crisis management)
1.6 การออกแบบระบบป้องกันภัยไซเบอร์ระดับประเทศและการนำกลยุทธ์การป้องกันทางไซเบอร์ของภาครัฐไปปฏิบัติจริง(Cyber defense consideration)
1.7 การวางแผนให้ระบบสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องเมื่อเกิดภัยคุกคามทางไซเบอร์ยังสามารถติดต่อกันได้ยาม

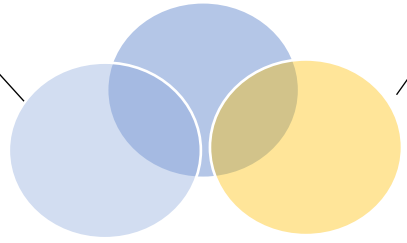
5.1 การพัฒนาและการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ และ การนำมาตรฐานความมั่นคงปลอดภัยไซเบอร์มาปฏิบัติจริงในประเทศ (Adherence to standards)
5.2 การสร้างความเชื่อมั่นให้ประชาชนในส่วนของการประเมินและควบคุมผู้ให้บริการอินเทอร์เน็ตและโครงสร้างพื้นฐานสำคัญของประเทศ (Internet infrastructure resilience)
5.3 การตรวจสอบคุณภาพการใช้งานของโปรแกรมคุณสมบัติต่าง ๆ ในโปรแกรมด้านความมั่นคงปลอดภัยไซเบอร์ (Software quality)
5.4 การควบคุมความมั่นคงปลอดภัยไซเบอร์ในทางเทคนิค ภาครัฐ ภาคเอกชน และบุคคลทั่วไป (Technical security controls)
5.5 การควบคุมการเข้ารหัสของทุกภาคส่วนในอุตสาหกรรมและบุคคลทั่วไป เพื่อป้องกันไม่ให้ข้อมูลสำคัญถูกเผยแพร่โดยไม่ได้รับอนุญาต (Cryptographic controls)
5.6 การส่งเสริมตลาดให้มีการแข่งขันในการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity marketplace)
5.7 การพัฒนาหน่วยงานที่มีหน้าที่ในการเก็บข้อมูลและเผยแพร่ข้อมูลด้านความ

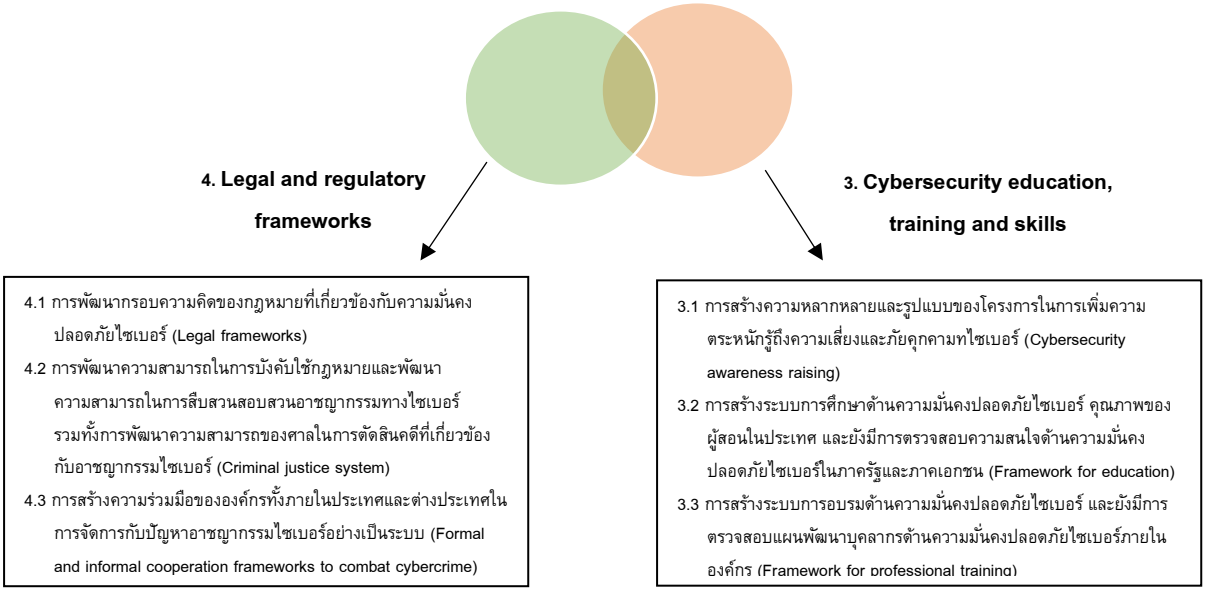
2.1 การให้ความสำคัญอย่างต่อเนื่องในเรื่อง ทัศนคติต่อความมั่นคงปลอดภัยด้านไซเบอร์ ของภาครัฐ ภาคเอกชนรวมทั้งผู้ใช้บริการ Online service ต่าง ๆ (Cybersecurity mind-set)
2.2 การสร้างความเชื่อมั่นด้านความปลอดภัยด้านไซเบอร์ของผู้ใช้บริการ Online service, e-government และ e-commerce (Trust and confidence on the internet)
2.3 การสร้างความเข้าใจถึงผลกระทบจากปัญหาข้อมูลส่วนบุคคลถูกละเมิดและนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาตให้กับภาครัฐและภาคเอกชน ตลอดจนผู้ใช้บริการ Online service, e-government และ e-commerce ทั่วไป (User understanding of personal information protection online)
2.4 การสร้างช่องทางการส่งรายงานที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์อย่างเป็นระบบในระดับประเทศ (Reporting mechanisms)
2.5 การให้ความรู้อย่างต่อเนื่องเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในการใช้งาน Social media และ อธิปไตยไซเบอร์แก่ประชาชน (Media and social media and Cyber sovereignty)

1. Cybersecurity framework and policy

5. Standards, organizations, and technologies

2. Cyber culture and society





สรุป

ปัญหาความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และ ความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ เปรียบเสมือนยอดภูเขาน้ำแข็ง (Tip of the iceberg) ที่ส่วนใหญ่เป็นภัยคุกคามไซเบอร์ทางกายภาพ ซึ่งสามารถรับรู้ได้ชัดเจน ปัญหาความไม่พร้อมในการรับมือปรากฏการณ์ “Social media as a new source of soft power” ที่ใช้ในการรุกรานอธิปไตยทางไซเบอร์ (Cyber sovereignty) นั้นเปรียบเสมือนส่วนของภูเขาน้ำแข็งที่จมอยู่ใต้น้ำ (Submerged part of the iceberg) ซึ่งเป็นส่วนที่ใหญ่กว่าการโจมตีทางกายภาพมาก กฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงยุทธศาสตร์ชาติ 20 ปี ด้านความมั่นคงและยุทธศาสตร์ด้านความมั่นคงไซเบอร์แห่งชาติ (2560-2564) ยังไม่ครอบคลุมทั้ง 5 มิติด้านความมั่นคงปลอดภัยไซเบอร์ ตามมิติที่ 2 ของกรอบแนวคิด CMM ในเรื่อง Cyber culture and society ความรู้ความเข้าใจ ความเชื่อมั่นของผู้ใช้บริการ เกี่ยวกับการละเมิดและนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตช่องทางการรายงานอาชญากรรมทางไซเบอร์อิทธิพลของ Social media และอธิปไตยไซเบอร์

ผู้วิจัยจึงได้เสนอแนะแนวทางขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ โดยนำแนวคิดของผู้ทรงคุณวุฒิ (รองศาสตราจารย์ปณิธาน วัฒนายากร กรรมการผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) มาประยุกต์ใช้ โดยแบ่งแนวทางออกเป็น 3 บทบาท ประกอบด้วย 1) แนวทาง

ที่ให้รัฐมีบทบาทนำ (Government-led) 2) แนวทางที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางที่แพลตฟอร์มมีบทบาทนำ (Platform-led) และได้นำกรอบแนวคิดในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ 5 มิติ CMM มาประยุกต์ใช้กับประเทศไทย ประกอบด้วย มิติที่ 1 National cybersecurity framework and policy มิติที่ 2 Cyber culture and society มิติที่ 3 Cybersecurity education, training and skills มิติที่ 4 legal and regulatory frameworks มิติที่ 5 Standards, organizations, and technologies เพื่อเสนอแนะแนวทางการทบทวนและปรับปรุงยุทธศาสตร์ชาติ 20 ปี ด้านความมั่นคง และยุทธศาสตร์ด้านความมั่นคงไซเบอร์แห่งชาติ (2560-2564) ให้ครอบคลุมการป้องกันและรับมือกับปัญหาปรากฏการณ์ Social media เป็นเครื่องมือ Soft power รุกรานอธิปไตยทางไซเบอร์ (Cyber sovereignty)

บทที่ 5
สรุปและข้อเสนอแนะ

สรุปผลการวิจัย

ในการวิจัยครั้งนี้ เป็นการทำการวิจัยเรื่อง ความมั่นคงปลอดภัยไซเบอร์ของชาติ : ปัญหาอธิปไตยไซเบอร์ ผลกระทบต่อความมั่นคงของชาติ ในระยะยาว และแนวทางการกำหนดยุทธศาสตร์ชาติ โดยผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ 2 ข้อ คือ

วัตถุประสงค์การวิจัยข้อที่ 1 ศึกษาและวิเคราะห์กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รูปแบบ และลักษณะของยุทธศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี มีความชัดเจน มีความเหมาะสมกับช่วงเวลา สามารถนำไปสู่การปฏิบัติจริงทั้งในการแก้ปัญหาอธิปไตยไซเบอร์ในระยะสั้นและระยะยาว

วัตถุประสงค์การวิจัยข้อที่ 2 เสนอแนะแนวทางในการปรับปรุงกระบวนการและรูปแบบของนโยบายความมั่นคงแห่งชาติ ให้สอดคล้องกับ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ ยุทธศาสตร์ชาติ 20 ปี เพื่อให้สามารถนำมาปฏิบัติจริงได้อย่างมีประสิทธิผลและประสิทธิภาพ

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ 1 สรุปได้ดังนี้ จากการศึกษายุทธศาสตร์ในการป้องกันการรุกรานทางอธิปไตยไซเบอร์ของต่างประเทศ พบว่า ประเทศจีนเป็นประเทศที่ประสบความสำเร็จเพียงประเทศเดียว จากการมี “National gateway" หรือ “The great firewall” และการมีแพลตฟอร์มของประเทศตนเอง เช่น เว็บไซต์ค้นหา (Search engine) อย่างไป่ตู้ (Baidu) ซึ่งมีฟังก์ชั่นการใช้งานที่คล้ายกับ Google เครือข่ายสังคมออนไลน์เวย์ปั๋ว (Weibo) วีแชท (WeChat) ซึ่งมีลักษณะคล้ายกับ LINE ในขณะที่ประเทศที่กำลังตามหลังประเทศจีน และริเริ่มมาตรการการป้องกันการรุกรานอธิปไตยทางไซเบอร์แล้ว ได้แก่ ประเทศออสเตรเลีย และประเทศสิงคโปร์ โดยกรณีประเทศออสเตรเลีย มีกฎหมายการเข้ารหัสข้อมูล (Assistance and access act - AAA) ที่ช่วยให้เจ้าหน้าที่รัฐหรือตำรวจเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งาน เพื่อประโยชน์ต่อการสืบสวนคดี และรับมือกับเครือข่ายการก่ออาชญากรรมทางไซเบอร์ และกรณีประเทศสิงคโปร์ที่มีแนวปฏิบัติควบคุม “เนื้อหาต้องห้าม” บนอินเทอร์เน็ต และ

กฎหมาย Protection from online falsehoods and manipulation act 2019 (POFMA) เพื่อจัดการกับการเผยแพร่ข่าวปลอม และการปลุกปั่นในโลกออนไลน์

ในขณะที่ เมื่อพิจารณาขีดความสามารถด้านเทคโนโลยีของประเทศในภูมิภาคอาเซียน จะเห็นได้ว่า ประเทศในภูมิภาคอาเซียนไม่มีหรือไม่ได้ครอบครองเทคโนโลยีดิจิทัลเป็นของตนเอง ไม่มี Platform หรือโปรแกรม Social media เป็นของตนเอง เช่นเดียวกับกรณีของประเทศไทย จึงมีแนวโน้มที่จะถูกประเทศ/องค์กรที่มีศักยภาพด้านไซเบอร์ ใช้เครื่องมือ Cyber ผ่าน Platform และ Social media เป็นเครื่องมือ Soft power รุกรานอธิปไตยไซเบอร์ได้

กรณีของประเทศไทย ความไม่พร้อมในการรับมือปรากฏการณ์ Social media และการสูญเสียอธิปไตยทางไซเบอร์ (Cyber sovereignty) นั้นเปรียบเสมือนส่วนของภูเขาน้ำแข็งที่จมอยู่ใต้น้ำ (Submerged part of the iceberg) ซึ่งเป็นส่วนที่ใหญ่กว่าการโจมตีทางกายภาพมาก รัฐบาลยังไม่สามารถควบคุมได้ และรัฐบาลยังไม่มีวิธีจัดการทั้งตามยุทธศาสตร์ชาติและยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประเด็นยุทธศาสตร์ของยุทธศาสตร์ชาติ 20 ปี (2561 - 2580) มีแผนงานการสร้างความตระหนักรู้ประชาชนและหน่วยงาน ที่เน้นเฉพาะในการการโจมตีทางไซเบอร์ ยังไม่ครอบคลุมเรื่องการรักษาอธิปไตยทางไซเบอร์ และแผนงานการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ซึ่งมีเรื่องของการพัฒนบุคลากรและแลกเปลี่ยนความรู้ แต่ยังไม่ครอบคลุมการพัฒนาบุคลากรให้รู้เท่าทันการละเมิดข้อมูลส่วนบุคคลและนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาต และการรักษา “อธิปไตยทางไซเบอร์”

กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีการวิเคราะห์ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ของประเทศ และกำหนดระยะของการกำหนดยุทธศาสตร์ (Stage of maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ โดยตามกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model : CMM) ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ประกอบด้วย มิติที่ 1 National Cybersecurity framework and policy มิติที่ 2 Cyber culture and society มิติที่ 3 Cybersecurity education, training and skills มิติที่ 4 Legal and regulatory frameworks มิติที่ 5 Standards, organizations, and technologies ส่วนระยะของการกำหนดยุทธศาสตร์ ประกอบด้วย 5 ระยะ ได้แก่ ระยะที่ 1 Start-up เป็นระดับที่เพิ่งเริ่มอภิปรายเกี่ยวกับแนวทางการสร้างขีดความสามารถ แต่ยังไม่เริ่มดำเนินการ ระยะที่ 2 Formative เป็นระดับที่เริ่มปรากฏแนวทางที่ชัดเจนแล้ว แต่ยังไม่จัดเป็นระเบียบหรือไม่เป็นหมวดหมู่ ระยะที่ 3 Established เป็นระดับที่เริ่มดำเนินการตามแนวทางแล้ว อยู่ในขั้นตอนของการตัดสินใจทางเลือกต่าง ๆ และจัดสรรทรัพยากร ระยะที่ 4 Strategic เป็นระดับที่มีการจัดลำดับความสำคัญของแนวทางว่า

อยู่ในระดับองค์กรหรือในระดับชาติ และระยะที่ 5 Dynamic เป็นระดับที่มีความชัดเจนในด้านกลไกนำไปสู่การเปลี่ยนแปลงยุทธศาสตร์ที่ขึ้นอยู่กับภัยคุกคามไซเบอร์ที่เกิดขึ้นจริงในปัจจุบัน

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ 2 สรุปได้ดังนี้ การวิเคราะห์ปัญหาในเรื่องความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย สามารถแบ่งออกเป็น 2 ปัญหาใหญ่ ประกอบด้วย 1) ความไม่พร้อมในการปกป้อง ป้องกัน รับมือและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2) ความไม่พร้อมในการรับมือปรากฏการณ์ “Social media” กลายเป็น “Soft power ” และการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ การปรับปรุงกระบวนการและรูปแบบของนโยบายความมั่นคงแห่งชาติ ควรนำกรอบแนวคิดแบบจำลองวุฒิภาวะความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity capacity maturity model: CMM) 5 มิติ มาใช้ในการพัฒนายุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ประกอบด้วย มิติที่ 1 National cybersecurity framework and policy มิติที่ 2 Cyber culture and society มิติที่ 3 Cybersecurity education, training and skills มิติที่ 4 Legal and regulatory frameworks มิติที่ 5 Standards, organizations, and technologies โดยมีรายละเอียดดังนี้

ตารางที่ 5-1 ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ตามแนวคิดของ CMM

ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	การพัฒนายุทธศาสตร์
มิติที่ 1 National cybersecurity framework and policy	1.1 การพัฒนากรอบแนวคิดเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (National cybersecurity framework) 1.2 การพัฒนานโยบายด้านความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (National cybersecurity policy) 1.3 การระบุและกระบวนการในการตอบสนองต่อภัยคุกคามด้านไซเบอร์ระดับประเทศ (Incident response) 1.4 การระบุโครงสร้างพื้นฐานที่สำคัญยิ่งยวดของประเทศ และการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยด้านไซเบอร์ระดับประเทศ (Critical infrastructure (CI) protection and national cybersecurity risk management) 1.5 การวางแผนบริหารจัดการกับวิกฤตการณ์ฉุกเฉิน การฝึกฝนเตรียมรับวิกฤตการณ์ฉุกเฉิน และ การสร้างสถานการณ์

ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	การพัฒนายุทธศาสตร์
	จำลองให้พนักงานในองค์กรเตรียมพร้อมรับมือกับวิกฤตการณ์ทางไซเบอร์ต่าง ๆ (Crisis management) 1.6 การออกแบบระบบป้องกันภัยไซเบอร์ระดับประเทศและการนำกลยุทธ์การป้องกันทางไซเบอร์ของภาครัฐไปปฏิบัติจริง (Cyber defense consideration) 1.7 การวางแผนให้ระบบสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องเมื่อเกิดภัยคุกคามทางไซเบอร์ยังสามารถติดต่อกันได้ยามระบบสื่อสารหลักใช้งานไม่ได้ มีการระบุหน้าที่ของบุคลากรที่เกี่ยวข้องอย่างชัดเจน รวมไปถึงการมีแผนสำรอง เมื่อระบบการสื่อสารหลักล้มเหลว (Communications redundancy)
มิติที่ 2 Cyber culture and society	2.1 การให้ความสำคัญอย่างต่อเนื่องในเรื่องทัศนคติต่อความมั่นคงปลอดภัยด้านไซเบอร์ ของภาครัฐ ภาคเอกชนรวมทั้งผู้ใช้บริการ Online service ต่าง ๆ (Cybersecurity mind-set) 2.2 การสร้างความเชื่อมั่นด้านความปลอดภัยด้านไซเบอร์ของผู้ใช้บริการ Online service, e-government และ e-commerce (Trust and confidence on the internet) 2.3 การสร้างความเข้าใจถึงผลกระทบจากปัญหาข้อมูลส่วนบุคคลถูกละเมิดและนำไปใช้ประโยชน์โดยไม่ได้รับอนุญาตให้กับภาครัฐและภาคเอกชน ตลอดจนผู้ใช้บริการ Online service, e-government และ e-commerce ทั่วไป (User understanding of personal information protection online) 2.4 การสร้างช่องทางการส่งรายงานที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์อย่างเป็นระบบในระดับประเทศ (Reporting mechanisms) 2.5 การให้ความรู้อย่างต่อเนื่องเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในการใช้งาน Social media และอธิปไตยไซเบอร์แก่

ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	การพัฒนายุทธศาสตร์
	ประชาชน (Cyber sovereignty)
มิติที่ 3 Cybersecurity education, training and skills	3.1 การสร้างความหลากหลายและรูปแบบของโครงการในการเพิ่มความตระหนักรู้ถึงความเสี่ยงและภัยคุกคามไซเบอร์ (Cybersecurity awareness raising) 3.2 การสร้างระบบการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ คุณภาพของผู้สอนในประเทศ และยังมีการตรวจสอบความสนใจด้านความมั่นคงปลอดภัยไซเบอร์ในภาครัฐและภาคเอกชน (Framework for education) 3.3 การสร้างระบบการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ และยังมีการตรวจสอบแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร
มิติที่ 4 Legal and regulatory frameworks	4.1 การพัฒนากรอบความคิดของกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Legal frameworks) 4.2 การพัฒนาความสามารถในการบังคับใช้กฎหมายและพัฒนาความสามารถในการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ รวมทั้งการพัฒนาความสามารถของศาลในการตัดสินคดีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ (Criminal justice system) 4.3 การสร้างความร่วมมือขององค์กรทั้งภายในประเทศและต่างประเทศในการจัดการกับปัญหาอาชญากรรมไซเบอร์อย่างเป็นระบบ (Formal and informal cooperation frameworks to combat cybercrime)
มิติที่ 5 Standards, organizations, and technologies	5.1 การพัฒนาและการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ และ การนำมาตรฐานความมั่นคงปลอดภัยไซเบอร์มาปฏิบัติจริงในประเทศ (Adherence to standards) 5.2 การสร้างความเชื่อมั่นให้ประชาชนในส่วนของการประเมินและควบคุมผู้ให้บริการอินเทอร์เน็ตและโครงสร้างพื้นฐาน

ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์	การพัฒนายุทธศาสตร์
	สำคัญของประเทศ (Internet infrastructure resilience) 5.3 การตรวจสอบคุณภาพการใช้งานของโปรแกรมคุณสมบัติต่าง ๆ ในโปรแกรมด้านความมั่นคงปลอดภัยไซเบอร์ (Software quality) 5.4 การควบคุมความมั่นคงปลอดภัยไซเบอร์ในทางเทคนิคภาครัฐ ภาคเอกชน และ บุคคลทั่วไป (Technical security controls) 5.5 การควบคุมการเข้ารหัสของทุกภาคส่วนในอุตสาหกรรมและบุคคลทั่วไป เพื่อป้องกันไม่ให้ข้อมูลสำคัญถูกเผยแพร่โดยไม่ได้รับอนุญาต (Cryptographic controls) 5.6 การส่งเสริมภาคเอกชนให้มีการแข่งขันในการพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity marketplace) 5.7 การพัฒนาหน่วยงานที่มีหน้าที่ในการเก็บข้อมูลและเผยแพร่ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีความเกี่ยวข้องกับทุกภาคส่วนในอุตสาหกรรม (Responsible disclosure cybercrime)

นอกจากนี้ ควรจำแนกแนวทางการพัฒนายุทธศาสตร์ออกเป็น 3 บทบาท ประกอบด้วย 1) แนวทางที่ให้รัฐมีบทบาทนำ (Government-led) 2) แนวทางที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางที่แพลตฟอร์มมีบทบาทนำ (Platform-led)

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

การกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติควรทบทวนและปรับปรุงโดยจำแนกออกตามองค์กรที่มีบทบาทเป็นผู้นำของการขับเคลื่อนยุทธศาสตร์ในแต่ละประเด็นยุทธศาสตร์ ตามแนวคิดของผู้ทรงคุณวุฒิ (รองศาสตราจารย์ปณิธาน วัฒนายากร กรรมการผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ)

ซึ่งได้เสนอแนะให้จำแนกแนวทางการพัฒนายุทธศาสตร์ออกเป็นสามภาคส่วน ได้แก่ 1) แนวทางที่ให้รัฐมีบทบาทนำ (Government-led) 2) แนวทางที่ให้ภาคประชาชนและภาคเอกชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางที่แพลตฟอร์มมีบทบาทนำ (Platform-led) สามารถจัดหมวดหมู่ของ 10 แนวคิดในการปรับปรุงยุทธศาสตร์ที่ได้จากการวิเคราะห์ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

1.1 แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led)

รัฐบาลควรใช้กลไกหน่วยงานภาครัฐ เช่น สกมช. กมช. ดศ. สมช. เป็นต้น ร่วมกับผู้เชี่ยวชาญในภาคเอกชนในการขับเคลื่อนแผนปฏิบัติการและโครงการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

1.1.1 บริหารความเสี่ยงและสร้างกลไกตอบสนองต่อความเสี่ยงในหน่วยงานโครงสร้างพื้นฐานที่สำคัญ

1.1.2 พัฒนานโยบาย กฎหมายลูก และมาตรฐานด้านความมั่นคงปลอยภัยทางไซเบอร์

1.1.3 พัฒนาบุคลากรจากหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น การบังคับใช้กฎหมาย การสืบสวน และการตัดสินคดีทางไซเบอร์ เป็นต้น

1.1.4 บูรณาการหน่วยงานภาครัฐ ในลักษณะของปฏิบัติการร่วม (Joint-force) โดยมีหน่วยงานหลักที่เป็นเจ้าภาพชัดเจน และสร้างความร่วมมือกับภาคเอกชน ภาคประชาสังคม และองค์กรระหว่างประเทศ เพื่อรักษาสมดุลระหว่างเสรีภาพในโลกไซเบอร์สเปซและความมั่นคงปลอดภัยทางไซเบอร์

1.2 แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian-led)

รัฐบาลควรสร้างการบูรณาการร่วมกันของกระทรวงศึกษาธิการ หน่วยงานภาครัฐ รัฐวิสาหกิจ ภาคเอกชน ในการพัฒนาความรู้และความตระหนักรู้ให้แก่ประชาชน ดังต่อไปนี้

1.2.1 พัฒนาระบบการศึกษา โดยปฏิรูปหลักสูตรการเรียนการสอนโดยสอดแทรกเนื้อหาความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในแต่ละระดับการ

เรียนการสอน และพัฒนาบุคลากรภาครัฐโดยเฉพาะหน่วยงานด้านโครงสร้างพื้นฐานที่สำคัญให้มีความรู้ด้านความมั่นคงปลอดภัยด้านไซเบอร์

1.2.2 สร้างความตระหนักรู้ (Awareness) ด้านความมั่นคงปลอดภัยด้านไซเบอร์ ให้แก่ประชาชนเพื่อให้รู้เท่าทันภัยจากการใช้งานสื่อสังคมออนไลน์ (Social media) และการเปิดเผยข้อมูลส่วนบุคคลให้แก่แพลตฟอร์ม (Platform) ต่างประเทศ เพื่อป้องกันการรุกล้ำทางไซเบอร์ในระดับประเทศ

1.2.3 สร้างความรู้ความเข้าใจให้ประชาชนรู้เท่าทันปฏิบัติการข่าวสาร (IO) ทางสื่อสังคมออนไลน์ (Social media) ทั้งจากภายในประเทศและต่างประเทศ

1.2.4 สร้างความตระหนักรู้ถึงการใช้ประโยชน์จากข้อมูลส่วนบุคคลในการโฆษณาชวนเชื่อ รวมถึงสิทธิและวิธีการปกป้องและคุ้มครองข้อมูลส่วนบุคคล

1.2.5 สร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy ให้มี "ภูมิคุ้มกันทางดิจิทัล" และ“ภูมิคุ้มกันทางไซเบอร์” (Digital immunity/Cyber immunity) ที่ดี

1.3 แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform-led)

รัฐบาลควรส่งเสริมและสนับสนุนการวิจัยและพัฒนาเพื่อสร้างแพลตฟอร์มที่เป็นนวัตกรรมทางดิจิทัลที่ล้ำหน้าทันสมัย (Leapfrog digital innovation platform) ของประเทศไทยที่สามารถตอบสนองความต้องการของประชาชนเหนือกว่าแพลตฟอร์มต่างประเทศ สามารถดูแลข้อมูลส่วนบุคคลของประชาชนได้ด้วย และสามารถป้องกันการรุกรานอธิปไตยทางไซเบอร์ผ่านทางสื่อสังคมออนไลน์ (Social media) เพื่อป้องกันประชาชนจากการรุกล้ำทางเศรษฐกิจ สังคม วัฒนธรรม ความคิด ความเชื่อ อุดมการณ์ ทัศนคติ ค่านิยมผ่านสื่อสังคมออนไลน์ (Social media) และแพลตฟอร์ม (Platform) ต่างประเทศ

2. ข้อเสนอแนะเชิงยุทธศาสตร์

2.1 กรอบแบบจำลองธุรกิจเพื่อความมั่นคงปลอดภัยสารสนเทศ (Business Model for Information Security : BMIS)

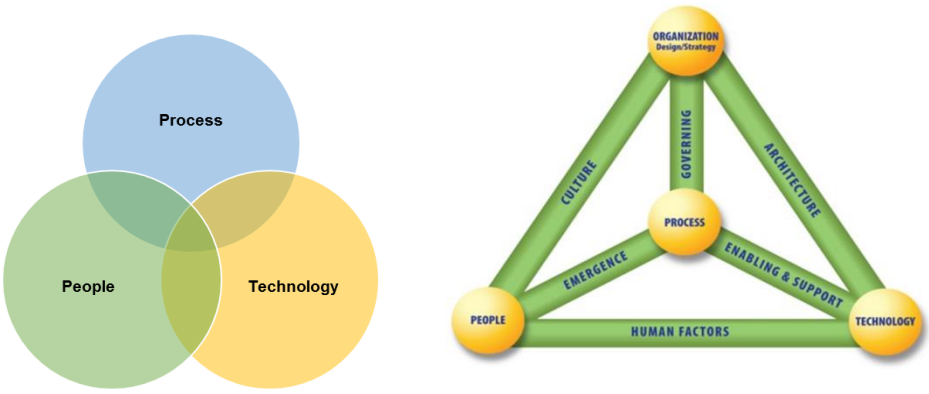
การกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศควรประยุกต์ใช้กรอบแบบจำลองธุรกิจเพื่อความมั่นคงปลอดภัยสารสนเทศ (BMIS) ตามแนวคิดของสมาคม Information security audit and control association (ISACA)[1] โดยแบ่งองค์ประกอบออกเป็น 4 ด้าน ได้แก่ 1) องค์กร (Organisation) หมายถึงเครือข่ายของบุคลากร

[1] Information Security Audit and Control. (2552). **An Introduction to the Business Model for Information Security.** United States of America.

สินทรัพย์ และขั้นตอนการปฏิบัติงานที่สัมพันธ์กันเพื่อไปสู่เป้าหมาย 2) บุคลากร (People) หมายถึง ทรัพยากรมนุษย์และประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรมนุษย์ 3) ขั้นตอนการปฏิบัติงาน (Process) หมายถึง ขั้นตอนหรือกลไกการปฏิบัติงานเพื่อบรรลุผลสำเร็จ เช่น มาตรการ การบริหารจัดการ และการความคุมความเสี่ยง เป็นต้น ซึ่งได้จากการกำหนดยุทธศาสตร์ขององค์กร และ 4) เทคโนโลยี (Technology) หมายถึง เครื่องมือ แอพพลิเคชั่นหรือ โครงสร้างพื้นฐานที่ทำให้ขั้นตอนการปฏิบัติงานมีประสิทธิภาพมากขึ้น

องค์ประกอบ 4 ด้าน ตามกรอบแบบจำลอง BMIS มีความสัมพันธ์ซึ่งกันและกัน ทำให้เกิดแรงดึงและแรงผลัก เมื่อมีองค์ประกอบใดองค์ประกอบหนึ่งเปลี่ยนแปลง โดยแต่ละองค์ประกอบมีพลวัตของความเชื่อมโยง 6 ด้าน ประกอบด้วย 1) การกำกับดูแล (Governing) 2) วัฒนธรรม หรือรูปแบบของพฤติกรรม (Culture) 3) การพัฒนาและสนับสนุน (Enabling and support) 4) ความฉุกเฉินเร่งด่วน (Emergence) 5) ปัจจัยมนุษย์ (Human factor) และ 6) โครงสร้างความมั่นคงปลอดภัย (Architecture)

แผนภาพที่ 5-1 แบบจำลองธุรกิจเพื่อความมั่นคงปลอดภัยด้านข้อมูล



ที่มา : People-process-technology model และ Business model of information security (BMIS)

เมื่อประยุกต์องค์ประกอบ 4 ด้าน ตามกรอบแบบจำลอง BMIS เข้ากับการรักษา ความมั่นคงปลอดภัยไซเบอร์ โดยแต่ละองค์ประกอบ

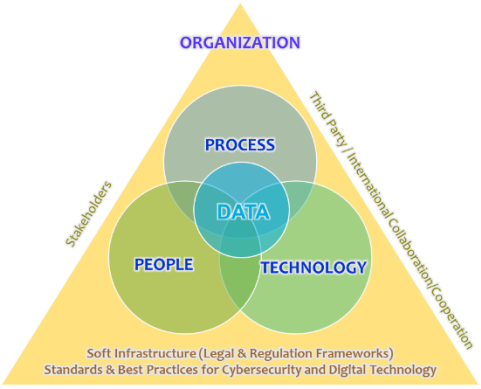
1. องค์กร (Organisation) หมายถึง รัฐบาล และเครือข่ายหน่วยงานภาครัฐที่ทำหน้าที่เกี่ยวข้องกับการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศ แต่ละหน่วยงานได้รับมอบหมายหน้าที่ความรับผิดชอบและเป้าหมาย

2. บุคลากร (People) หมายถึง ประชาชน บุคลากรภาครัฐ และภาคเอกชน ซึ่งมีบทบาทในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ในส่วนที่เกี่ยวข้องกับแต่ละกลุ่มบุคลากร

3. ขั้นตอนการปฏิบัติงาน (Process) หมายถึง ยุทธศาสตร์ ซึ่งกำหนดกลไกการขับเคลื่อนยุทธศาสตร์ โครงการ แผนปฏิบัติงาน และขั้นตอนการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4. เทคโนโลยี (Technology) หมายถึง แพลตฟอร์มของประเทศไทย และเทคโนโลยีดิจิทัลที่ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ และการปกป้องอธิปไตยทางไซเบอร์ของประเทศ

แผนภาพที่ 5-2 องค์ประกอบของการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามแนวคิดของ ISACA



ที่มา : ACIS Research, www.acisonline.net

2.2 ยุทธศาสตร์เชิงรุก (Offensive strategy)

การกำหนดกลยุทธ์เพื่อให้บรรลุเป้าหมายในการป้องกันภัยคุกคามไซเบอร์และการรุกรานอธิปไตยทางไซเบอร์ จำเป็นต้องดำเนินการทั้งเชิงรับและเชิงรุก ด้านเชิงรับ เน้นการติดตามเฝ้าระวัง การเตือนภัยล่วงหน้า การรับมือกับเหตุการณ์ และการฟื้นฟูจากความเสียหาย ด้านเชิงรุกควรสร้างและพัฒนาขีดความสามารถของทีมรับมือกับเหตุการณ์ให้สามารถโจมตีเครือข่ายหรือระบบของผู้ประสงค์ร้าย เพื่อทำลายโอกาสของการโจมตีทางไซเบอร์ ควรพัฒนาและสร้างแพลตฟอร์มของประเทศขึ้นเองให้สามารถตอบสนองความต้องการของผู้ใช้งานและสามารถคุ้มครองความมั่นคง

ปลอดภัยของข้อมูลได้ด้วย ควรส่งผู้ดูแลรักษาผลประโยชน์ของชาติ (Custodian) ทั้งหน่วยงานด้านความมั่นคงและหน่วยงานด้านพัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ไปเข้าร่วมในเวทีความร่วมมือระหว่างประเทศต่าง ๆ ทั้งในระดับโลกและภูมิภาคอาเซียน เพื่อสร้างพันธมิตรในการต่อต้าน ติดตาม และลงโทษผู้ประสงค์ร้ายทางไซเบอร์ เช่น องค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol) และหน่วยงานตำรวจของสหภาพยุโรป (Europol) เป็นต้น รวมถึงเพื่อแลกเปลี่ยนประสบการณ์และร่วมเรียนรู้ไปพร้อมกับประเทศที่เริ่มตระหนักถึงปัญหาอธิปไตยทางไซเบอร์ และอยู่ระหว่างวางรากฐานของการป้องกันการรุกรานอธิปไตยทางไซเบอร์ เช่น มาเลเซีย อินโดนีเซีย สิงคโปร์ และเวียดนาม เป็นต้น

3. ข้อเสนอแนะระดับปฏิบัติ

3.1 แนวทางการพัฒนายุทธศาสตร์ออกเป็นสามภาคส่วน

การปรับปรุงกระบวนการและรูปแบบของนโยบายความมั่นคงแห่งชาติ ควรมีการทบทวนและปรับปรุงยุทธศาสตร์ชาติตามแนวคิดในการกำหนดบทบาทผู้ขับเคลื่อนแนวทางการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ 3 บทบาท ได้แก่ 1) แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led) 2) แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian-led) และ 3) แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform-led) โดยสามารถกำหนดแผนปฏิบัติการ/โครงการภายในแนวทางการขับเคลื่อน หน่วยงานรับผิดชอบหลัก/หน่วยงานรับผิดชอบรอง เป้าหมาย วิธีดำเนินการ และกรอบระยะเวลาดำเนินการได้ ดังนี้

ตารางที่ 5-2 หน่วยงานรับผิดชอบการขับเคลื่อนการปรับปรุงยุทธศาสตร์ชาติด้านความมั่นคงปลอดภัยไซเบอร์

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
1. แนวทางขับเคลื่อนที่รัฐมีบทบาทนำ (Government-led)				
1.1 โครงการเร่งรัดการพัฒนากฎหมายลูกและประกาศมาตรฐานความมั่นคงปลอดภัยไซเบอร์ภายใต้	หน่วยงานหลัก: สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	หน่วยงานภาครัฐสามารถบังคับใช้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้อย่างมีประสิทธิภาพ	สกมช. ศึกษาและออกประกาศกำหนดหลักเกณฑ์การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์และศึกษามาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	(ดศ.) สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) หน่วยงานรอง: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)		ของสากล เสนอมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ ต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ตามลำดับ	
1.2 โครงการการจัดตั้ง “ส.ส.ส. ไซเบอร์”	หน่วยงานหลัก: สกมช. หน่วยงานรอง: สพธอ.	ประชาชนมีความตระหนักรู้ถึงความมั่นคงปลอดภัยทางไซเบอร์	รณรงค์ประชาสัมพันธ์ให้ความรู้แก่ประชาชนผ่านสื่อรูปแบบต่าง ๆ เกี่ยวกับการตระหนักรู้ถึงภัยไซเบอร์ และ	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
			การใช้เครื่องมือ อุปกรณ์ นวัตกรรม อินเทอร์เน็ต และโทรศัพท์มือถือให้รู้วิธีป้องกัน/รักษาความปลอดภัยไซเบอร์เบื้องต้นด้วยตนเอง	
1.3 โครงการการจัดตั้งกองบัญชาการตำรวจไซเบอร์และพัฒนาตำรวจไซเบอร์	หน่วยงานหลัก: สำนักงานตำรวจแห่งชาติ (สตช.)	หน่วยงานภาครัฐสามารถป้องกันและรับมือกับอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพ	สตช. ยกร่างพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ และร่างกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ เสนอต่อคณะรัฐมนตรี เพื่อจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางไซเบอร์	พ.ศ. 2563-2565
1.4 โครงการบูรณาการการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ในรูปแบบ Joint-Force	หน่วยงานหลัก: สกมช. หน่วยงานรอง: ภาคเอกชน	บูรณาการการแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างหน่วยงานภาครัฐและภาคเอกชน	สกมช. เป็นหน่วยงานเจ้าภาพในการบูรณาการภาครัฐ และสร้างความร่วมมือกับภาคเอกชน และสร้างความร่วมมือกับองค์กรระหว่างประเทศ	พ.ศ. 2563-2565

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
หน่วยงานภาครัฐและเอกชน				
1.5 โครงการพัฒนาบุคลากรในหน่วยงานด้านยุติธรรม	หน่วยงานหลัก: สำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.) สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) หน่วยงานรอง: สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม	พัฒนาบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมาย การสืบสวน และการตัดสินคดีทางไซเบอร์	กำหนดให้มีการพัฒนาบุคลากรภาครัฐ โดยเฉพาะบุคลากรในหน่วยงานด้านยุติธรรม ให้มีความเข้าใจในเรื่องความมั่นคงปลอดภัยไซเบอร์ และการบังคับใช้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.	พ.ศ. 2563-2565
2. แนวทางขับเคลื่อนที่ภาคประชาชนมีบทบาทนำ (Civilian Led)				
โครงการสร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy "ภูมิคุ้มกันทางดิจิทัล" และ “ภูมิคุ้มกันทางไซเบอร์” ให้กับประชาชน	หน่วยงานหลัก: ศธ. หน่วยงานรับผิดชอบ รอง: อว. สมช. ภาคเอกชน	สร้างทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy "ภูมิคุ้มกันทางดิจิทัล" และ “ภูมิคุ้มกันทางไซเบอร์” ให้กับประชาชน	1) ปรับปรุงและพัฒนาตำราเรียนแบบเรียน โดยสร้างทักษะความรู้ ความเข้าใจ และความตระหนักรู้ทางด้านไซเบอร์ การใช้เทคโนโลยีดิจิทัล และความมั่นคงปลอดภัยทางไซเบอร์ให้แก่เยาวชนอย่างเหมาะสมกับแต่ละช่วงวัย	พ.ศ. 2563-2568

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
			2) พัฒนาและกำหนดหลักสูตร วิชา กระบวนการเรียนรู้ที่เกี่ยวข้องใสถาบันการศึกษาทั้งภาครัฐและเอกชน	
3. แนวทางการขับเคลื่อนที่แพลตฟอร์มมีบทบาทนำ (Platform-led)				
ส่งเสริมและสนับสนุนการสร้าง Leapfrog digital innovation platform ของประเทศไทย	หน่วยงานหลัก: ดศ. หน่วยงานรอง: สพธอ. สมช. และภาคเอกชน	ส่งเสริมและสนับสนุนการสร้างแพลตฟอร์มที่เป็นนวัตกรรมทางดิจิทัลที่ล้ำหน้าทันสมัย (Leapfrog digital innovation platform) ของประเทศไทย เพื่อป้องกันประชาชนจากการรุกล้ำทางเศรษฐกิจ สังคม วัฒนธรรม ความคิด ความเชื่อ อุดมการณ์ ทัศนคติ ค่านิยม ผ่านสื่อสังคมออนไลน์ (Social media)	การวิจัยและพัฒนาแพลตฟอร์มที่มีความใหม่ แตกต่าง และล้ำหน้าด้วยการใช้นวัตกรรมทางดิจิทัล โดยอาศัยผู้เชี่ยวชาญทางเทคโนโลยีดิจิทัลทั้งจากภายในประเทศไทยและต่างประเทศ เพื่อสร้างสิ่งใหม่ที่สามารถเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานได้ และตอบโจทย์ความต้องการของประชาชนอย่างแท้จริง	พ.ศ. 2563-2568

โครงการ	หน่วยงานรับผิดชอบ	เป้าหมาย	วิธีดำเนินการ	กรอบระยะเวลาดำเนินการ
		และแพลตฟอร์ม (Platform) ต่างประเทศ		

3.2 การจัดตั้งองค์กรภายใต้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ที่มีบทบาทสำคัญ ประกอบด้วย 3 หน่วยงาน ได้แก่ ทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response team: CSIRT) ทีมรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams: CERTs) และศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (Security Operations Center: SOC) เมื่อพิจารณาวัตถุประสงค์หลักและความสำคัญของ CSIRT และ CERT แล้ว จะเห็นได้ว่า CERT มีหน้าที่หลักในการจัดเก็บ รวบรวม และเผยแพร่ข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ ไม่มีความจำเป็นต้องมีปฏิบัติการเพื่อรับมือ หรือโต้ตอบกับเหตุการณ์ภัยคุกคามทางไซเบอร์ ในขณะที่ CSIRT มีหน้าที่หลักในการรับมือและโต้ตอบเหตุการณ์ภัยคุกคามทางไซเบอร์ และกำจัดภัยคุกคามทางไซเบอร์ รวมถึงการฟื้นฟูจากความเสียหาย อย่างไรก็ดี การทำหน้าที่ของ CSIRT และ CERT อาจมีหน้าที่บางส่วนที่เหมือนกันได้ เช่น การทำความเข้าใจกับเหตุการณ์ และการให้คำแนะนำ เป็นต้น นอกจากนี้ ในส่วนของศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (SOC) มีหน้าที่ติดตามเหตุการณ์ ลงทุนในระบบป้องกันโครงสร้างพื้นฐานด้านสารสนเทศขององค์กร และพัฒนาขีดความสามารถของบุคลากรด้านการป้องกันเครือข่ายและระบบระดับองค์กร

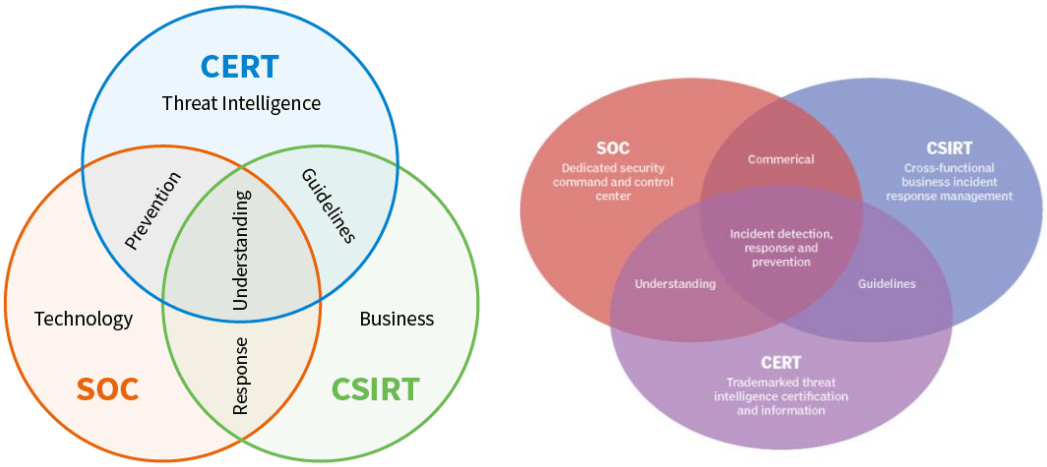
ตารางที่ 5-3 วัตถุประสงค์หลักและบทบาทที่สำคัญของหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงาน	วัตถุประสงค์หลัก	ความสำคัญ
CSIRT (Computer security incident response team)	โต้ตอบกับเหตุการณ์เผชิญเหตุ (Incident Respond)	โต้ตอบเหตุการณ์ กำจัดภัยคุกคาม และฟื้นฟูจากความเสียหาย

หน่วยงาน	วัตถุประสงค์หลัก	ความสำคัญ
CERT (Computer emergency response team)	จัดเก็บและเผยแพร่ข้อมูลเหตุการณ์	จัดเก็บ รวบรวมข้อมูลเหตุการณ์จากแหล่งข้อมูลต่าง ๆ แต่ไม่จำเป็นต้องป้องกันเครือข่ายหรือโต้ตอบเหตุการณ์
SOC (Security operations center)	ติดตามสถานการณ์และป้องกันโครงสร้างพื้นฐานและระบบเทคโนโลยีสารสนเทศขององค์กร	ลงทุนด้านเทคโนโลยีและบุคลากรด้านการติดตามสถานการณ์และป้องกันเครือข่าย เซิร์ฟเวอร์ และโครงสร้างพื้นฐานอื่น

ที่มา : Exabeam expert

แผนภาพที่ 5-3 หน้าที่หลักของ CERT CSIRT และ SOC



ที่มา : Exabeam expert และ TechTarget

กรณีของประเทศไทย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ควรจัดตั้งทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (CSIRT) ระดับประเทศ ตามมาตรฐานของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) เพิ่มเติมจากศูนย์ประสานการรักษาความมั่นคง

ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ซึ่งอยู่ระหว่างจัดตั้ง ภายใต้อำนาจตามมาตรา 22 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยปัจจุบันศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand computer emergency response team: ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปฏิบัติหน้าที่แทน National CERT ดังกล่าวอยู่ ซึ่งครอบคลุมเฉพาะการติดตาม แนะนำ ประสานงาน และเผยแพร่ข่าวสารและเหตุการณ์ด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน แต่ไม่ครอบคลุมถึงภารกิจของ CSIRT ตามแนวคิดของ ITU ซึ่งปฏิบัติการโต้ตอบเหตุการณ์ความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ภายในประเทศ รวมถึงร่วมมือกับ CSIRT ในต่างประเทศด้วย

นอกจากนี้ CSIRT ควรจัดทำโครงการนำร่องในการพัฒนาขีดความสามารถของบุคลากร (Human capacity building) ในหน่วยงานภาครัฐต่าง ๆ ให้สามารถพัฒนาระบบเตือนภัยล่วงหน้า ระบบป้องกัน และปฏิบัติการโต้ตอบเหตุการณ์ความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ในระดับองค์กร ในลักษณะเดียวกับศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (SOC) ด้วย และสร้างความตระหนักให้ผู้นำหน่วยงานภาครัฐในเรื่องความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ เพื่อให้ทุกหน่วยงานภาครัฐสามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ สามารถป้องกันผลประโยชน์ของชาติจากการโจมตีโครงสร้างพื้นฐานและฐานข้อมูลสารสนเทศที่สำคัญของประเทศ และสามารถโต้ตอบผู้ประสงค์ร้ายต่อรัฐได้อย่างรวดเร็ว ทันการณ์และมีประสิทธิภาพ

3.3 การจัดเก็บภาษีดิจิทัล (Digital tax)

ความท้าทายและประเด็นปัญหาในการจัดเก็บภาษีธุรกิจดิจิทัล แบ่งออกตามประเภทภาษี 2 ประเภท ได้แก่ ภาษีการบริโภค (Consumption tax) และภาษีเงินได้ (Income tax) โดยสรุปสาระสำคัญได้ ดังนี้

3.3.1 ภาษีการบริโภค (Consumption tax)

ปัญหาอุปสรรคในการจัดเก็บภาษีการบริโภคธุรกิจดิจิทัล แบ่งออกตามประเภทสินค้าและบริการ 2 ประเภท ได้แก่ (1) สินค้าที่มีตัวตนทางกายภาพ (Physical goods) ที่สั่งซื้อทางออนไลน์จากต่างประเทศแล้วจัดส่งเข้าประเทศทางไปรษณีย์ (2) บริการอิเล็กทรอนิกส์ (e-service) ที่สั่งซื้อและจัดส่งทางอิเล็กทรอนิกส์ถึงผู้ใช้บริการโดยตรง

3.3.1.1 กรณี Physical goods

หลักปฏิบัติของหลายประเทศทั่วโลก กำหนดให้มีการยกเว้นภาษี การบริโภคให้สินค้าที่มีราคาต่ำ (Low value) เนื่องจากกรมศุลกากร ซึ่งเป็นหน่วยงานประเมิน

และจัดเก็บภาษี มักจะมีข้อจำกัดหลายประการ เช่น ไม่มีระบบอิเล็กทรอนิกส์ที่การเชื่อมโยงข้อมูลกับผู้ให้บริการไปรษณีย์หรือผู้ให้บริการขนส่งสินค้า (Express Carrier) อื่น ๆ ทำให้ขาดข้อมูลที่จะใช้ประเมินภาษี จำนวนเจ้าหน้าที่ไม่เพียงพอในการตรวจสอบและประเมินภาษีทั้งอากรขาเข้าและภาษีมูลค่าเพิ่ม และอาจไม่คุ้มค่ากับจำนวนภาษีที่จะได้รับจากสินค้าที่มีราคาต่ำ ไม่มีระบบคัดแยกพัสดุว่า พัสดุใดเป็นสินค้านำเข้า พัสดุใดเป็นของฝาก/ของขวัญ และจุดบริการรับชำระค่าภาษียังไม่ครอบคลุมทั่วประเทศ เป็นต้น ดังนั้น ผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์พยายามแสวงหาโอกาสจากประเทศที่ยกเว้นการจัดเก็บภาษีการบริโภคสำหรับสินค้านำเข้าที่มีราคาต่ำ ส่งผลให้รัฐสูญเสียรายได้ภาษีการบริโภคอันพึงได้ และไม่เป็นธรรมกับผู้เสียภาษีสินค้าประเภทเดียวกันที่อยู่ในประเทศ

3.3.1.2 กรณี e-service

กฎหมายแม่บทด้านภาษีของหลายประเทศส่วนใหญ่ยังไม่ครอบคลุมถึงธุรกิจประเภท e-service ที่มีการสั่งซื้อและใช้บริการทางอิเล็กทรอนิกส์ กรณีของประเทศไทยการจัดเก็บภาษีมูลค่าเพิ่มจาก e-Service กำหนดหน้าที่ในการเสียภาษีไว้อยู่แล้วในประมวลรัษฎากร โดยกำหนดให้ผู้ซื้อมีหน้าที่นำส่งภาษีมูลค่าเพิ่ม (ยื่นแบบ ภ.พ. 36) ถึงแม้ว่าในกรณีของผู้จ่ายเงินค่าบริการ e-service ที่เป็นนิติบุคคล ไม่มีประเด็นปัญหาในการนำส่งภาษีมูลค่าเพิ่มให้กรมสรรพากร อย่างไรก็ดี กรณีผู้จ่ายเงินค่าบริการที่เป็นบุคคลธรรมดา มีการนำส่งภาษีมูลค่าเพิ่มจากการใช้บริการ e-service อย่างจำกัด

3.3.2 ภาษีเงินได้ (Income tax)

ปัญหาอุปสรรคในการจัดเก็บภาษีเงินได้จากแพลตฟอร์มต่างประเทศเกิดขึ้นจากกรณีที่ประมวลรัษฎากรมาตรา 66 วรรคสอง มาตรา 76 ทวิ และอนุสัญญาภาษีซ้อน (Double tax agreement: DTA) ที่ประเทศไทยลงนามไว้กว่า 60 ฉบับ กำหนดให้ธุรกิจต่างประเทศที่มีกิจการในไทย หรือมีตัวแทนที่ขาย ในไทย มีหน้าที่เสียภาษีเงินได้นิติบุคคล หากมีสถานประกอบการถาวร (Permanent establishment: PE) ในประเทศไทย เช่น สำนักงาน สาขา โรงงาน เป็นต้น เฉพาะเงินได้ในส่วนที่เป็นของ PE ซึ่งแพลตฟอร์มต่างประเทศมักจะหลีกเลี่ยงการมี PE ในประเทศไทย เพื่อเลี่ยงภาระภาษีดังกล่าว นอกจากนี้ ยังมีปัญหาในการตีความหมายของค่าตอบแทนจากการใช้บริการ ซึ่งมีผลกระทบต่อการประเมินภาระภาษีอีกด้วย กล่าวคือ ค่าตอบแทนนั้นเป็นค่าบริการหรือค่าสิทธิ หากเป็นค่าบริการ กรณีที่ไม่มี PE ในประเทศไทย ไม่มีหน้าที่ต้องเสียภาษีเงินได้ ตามมาตรา 70 แห่งประมวลรัษฎากร หากเป็นค่าสิทธิ กรณีที่ไม่มี PE ในประเทศไทย ค่าสิทธิดังกล่าวต้องเสียภาษีหัก ณ ที่จ่ายจากค่าสิทธิตามอัตราที่ตกลงไว้ในอนุสัญญาภาษีซ้อน (DTA) ด้วย

แนวทางการแก้ไขปัญหาอุปสรรคในการจัดเก็บภาษีและสถานะปัจจุบันของการดำเนินการในส่วนที่เกี่ยวข้อง แบ่งออกตามประเภทภาษี 2 ประเภท ได้แก่ 1) ภาษีการบริโภค (Consumption tax) และ 2) ภาษีเงินได้ (Income tax) สามารถสรุปได้ ดังนี้

1. ภาษีการบริโภค (Consumption tax)

องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for economic co-operation and development: OECD) ได้เผยแพร่รายงานและเสนอแนะแนวทางการจัดเก็บภาษีมูลค่าเพิ่มจากแพลตฟอร์มดิจิทัลในปี 2558 และ 2562[2] โดยพบว่า หลายประเทศได้เริ่มนำแนวทาง The vendor collection model ในการกำหนดให้แพลตฟอร์มดิจิทัลมีการจดทะเบียนภาษีมูลค่าเพิ่มอย่างง่าย (Simplified VAT registration) ต่อกรมสรรพากรในประเทศที่มีการใช้บริการ เช่น ออสเตรเลีย นิวซีแลนด์ กลุ่มสหภาพยุโรป สิงคโปร์ มาเลเซีย เป็นต้น

กรณีของประเทศไทย กระทรวงการคลังอยู่ระหว่างการตราร่างพระราชบัญญัติแก้ไขเพิ่มประมวลรัษฎากร (ฉบับที่ ..) พ.ศ. .... (ร่าง พ.ร.บ. การจัดเก็บภาษีมูลค่าเพิ่มจากผู้ประกอบการที่ได้ให้บริการทางอิเล็กทรอนิกส์จากต่างประเทศและได้มีการใช้บริการนั้นในราชอาณาจักรโดยผู้ใช้ซึ่งมิใช่ผู้ประกอบการจดทะเบียน) โดยกำหนดให้ผู้ประกอบการที่ได้ให้บริการทางอิเล็กทรอนิกส์ในต่างประเทศแก่ผู้ที่ไม่ได้เป็นผู้ประกอบการจดทะเบียนภาษีมูลค่าเพิ่มในประเทศไทย และได้มีการใช้บริการนั้นในประเทศไทย หากมีรายรับจากการให้บริการดังกล่าวเกินกว่า 1.8 ล้านบาทต่อปี ให้ยื่นคำขอจดทะเบียนภาษีมูลค่าเพิ่ม และให้มีหน้าที่เสียภาษีมูลค่าเพิ่ม ทั้งนี้ สถานะปัจจุบันของร่าง พ.ร.บ. คณะรัฐมนตรีเห็นชอบหลักการเมื่อวันที่ 17 กรกฎาคม 2561 สภาผู้แทนราษฎรเห็นชอบหลักการ วาระที่ 1 เมื่อวันที่ 29 กรกฎาคม 2563 จากนั้นจะนำเข้าสู่วาระที่ 2 วาระที่ 3 และการพิจารณาของวุฒิสภา

2. ภาษีเงินได้ (Income tax)

ปัจจุบัน OECD อยู่ระหว่างการพิจารณาแนวทางการจัดเก็บภาษีเงินได้จากธุรกิจดิจิทัลภายใต้ OECD/G 20 Inclusive framework on base erosion and profit shifting (BEPS) เพื่อเป็นแนวทางการปฏิบัติมาตรฐานสำหรับทุกประเทศ ซึ่งปัจจุบัน OECD อยู่ระหว่างพิจารณาประเด็นที่สำคัญ 2 ประเด็น ดังนี้

---

[2] OECD. (2019). **The Role of Digital Platforms in the Collection of VAT/GST on Online Sales.** (Published on June 20, 2019) As presented for consideration at the fifth meeting of the Global Forum on VAT March 2019.

2.1 การจัดสรรกำไรเพื่อชำระภาษี (Profit allocation) โดยอยู่ระหว่างเสนอวิธีการแบ่งกำไร (Profit Split) และวิธีการกำหนดอัตราภาษี ซึ่งมีความสัมพันธ์กับปัจจัยที่สำคัญ 3 ปัจจัย ดังนี้

2.1.1 จำนวนผู้ใช้บริการ (User participation)

2.1.2 ทรัพย์สินไม่มีรูปร่างประเภทการตลาด (Marketing intangibles) เช่น เครื่องหมายการค้า รายชื่อและข้อมูลลูกค้า ช่องทางการจำหน่าย เป็นต้น

2.1.3 การมีนัยสำคัญทางเศรษฐกิจ (Significant economic presence) ซึ่งเป็นจุดเชื่อมโยงการชำระภาษี (Nexus/Tax presence) จุดใหม่ เช่น การกำหนดหลักเกณฑ์เกี่ยวกับการมีตัวตนทางดิจิทัล (Digital presence) จากเดิมที่มีเพียงสถานประกอบการถาวร (Permanent establishment: PE) การกำหนดรายรับขั้นต่ำ (Revenue threshold) เป็นต้น

2.2 การกำหนดภาษีเงินได้ขั้นต่ำ (Minimum taxation) เพื่อแก้ไขปัญหาการโอนย้ายกำไร (Profit shifting) ไปประเทศที่เสียภาษีต่ำกว่า โดยอยู่ระหว่างเสนอขอบเขตของประเภทรายจ่าย และอัตราภาษี

อย่างไรก็ดี ประเทศสหรัฐอเมริกาได้ประเทศถอนตัวจากการเจรจากับกลุ่มสหภาพยุโรปในเรื่องภาษีดิจิทัล (Digital tax) เมื่อเดือนมิถุนายน 2563 ซึ่งส่งผลกระทบต่อการประชุมหารือของ OECD เพื่อหาข้อยุติร่วมกัน ทั้งนี้ หลายประเทศทั่วโลกได้ทำเดินมาตรการภาษีฝ่ายเดียว (Unilateral tax measure) โดยจัดเก็บภาษีบริการดิจิทัล (Digital service tax: DST) แล้ว เช่น ฝรั่งเศส อิตาลี เป็นต้น

ดังนั้น กรณีของประเทศไทยควรรอให้ได้ข้อยุติเกี่ยวกับแนวทางการจัดเก็บภาษีเงินได้จากแพลตฟอร์มต่างประเทศในเวทีการเจรจาระดับโลกและภูมิภาค โดยเฉพาะ OECD ก่อน เนื่องจากการจัดเก็บภาษี โดยไม่รอให้ได้ข้อยุติร่วมกัน แม้ว่าจะจัดเก็บภาษีได้ แต่อาจเกิดข้อพิพาททางการค้า และถูกกีดกันทางการค้าสำหรับสินค้าและบริการอื่น ๆ ของประเทศไทยได้ ทั้งนี้ ควรศึกษาและประเมินผลดีและผลเสียของการดำเนินมาตรการจัดเก็บภาษีฝ่ายเดียว (Unilateral tax measure) ซึ่งบางประเทศเริ่มจัดเก็บภาษีโดยไม่รอข้อยุติจากองค์กรระหว่างประเทศ

3.4 การใช้ประโยชน์จากสมาร์ทโฟนและระบบอินเทอร์เน็ต

การใช้งานสมาร์ทโฟนและระบบอินเทอร์เน็ตช่วยให้โลกของเราเปิดกว้างและเชื่อมโยงถึงกันได้ ทำให้การติดต่อสื่อสารกันทำได้ง่าย สามารถค้นหาข้อมูลสถานที่ การสั่งซื้อของ รวมไปถึงการใช้เพื่อส่งเสริมการศึกษา เช่น ค้นหาคำศัพท์ ค้นหาข้อมูล และศึกษาผ่านวิดีโอ เป็นต้น นอกจากผลประโยชน์แล้ว การใช้งานสมาร์ทโฟนและระบบอินเทอร์เน็ตอย่างไม่เหมาะสมส่งผลเสียต่อผู้ใช้งานหลายประการ เช่น การเสพติดการใช้สมาร์ทโฟนตลอดเวลาจนไม่ทันได้สังเกตสิ่งกีดขวาง

ขณะเดินหรือขับรถยนต์ การเสพติดการใช้งานสื่อสังคมออนไลน์ และการเสพติดเกมส์ออนไลน์ จนไม่สามารถพักผ่อนได้อย่างเพียงพอ หรือเสียโอกาสในการทำกิจกรรมอื่น ๆ เช่น การออกกำลังกาย พูดคุยกับพ่อแม่ การทำการบ้าน หรือการพัฒนาตนเอง เป็นต้น

กรณีของประเทศไทย จึงควรมีการปรับปรุงหลักสูตรการเรียนการสอนตั้งแต่ระดับประถมศึกษา เพื่อให้ประชาชนเข้าใจถึงวิธีที่ถูกต้องในการใช้สมาร์ทโฟนและระบบอินเทอร์เน็ต เพื่อการเรียนรู้อย่างเหมาะสมและมีขอบเขตความรับผิดชอบต่อการใช้งาน โดยสามารถรู้จักการจำกัดเวลาอย่างเหมาะสมด้วยตนเองในการใช้งานเครือข่ายสังคมออนไลน์ และเกมออนไลน์เพื่อความบันเทิง

3.5 การพัฒนาขีดความสามารถและความตระหนักรู้ในการหวงแหนข้อมูลส่วนบุคคล

การเข้าสู่ยุค S-M-C-I (Social–Mobile–Information–Cloud) ทำให้ข้อมูลส่วนบุคคลจำนวนมหาศาลอยู่ในความควบคุมของแพลตฟอร์มต่างประเทศ ซึ่งเป็นผลของการพัฒนาเทคโนโลยีดิจิทัล ที่แซงหน้าการพัฒนาขีดความสามารถและความตระหนักรู้ของมนุษย์ ทำให้เกิดปัญหาหลายประการ เช่น ความทุกข์ที่เกิดจากการเปรียบเทียบตัวเองกับคนอื่น หรือเรื่องเล่าบนเครือข่ายสังคมโซเชียล การไม่สามารถแยกแยะเรื่องจริงและเรื่องไม่จริงในเครือข่ายสังคมออนไลน์ได้ ความอ่อนไหวต่อเรื่องราวในเครือข่ายสังคมออนไลน์ที่มีเป้าประสงค์ในการเปลี่ยนแปลงความคิด ความเชื่อ และอุดมการณ์ได้ นอกจากนี้ ข้อมูลที่ไหลเวียนอยู่ในแพลตฟอร์มต่างประเทศสุ่มเสี่ยงต่อการถูกนำไปใช้ประโยชน์ โดยที่เจ้าของข้อมูลไม่รู้ตัว ซึ่งเท่ากับการถูกรุกรานอธิปไตยด้านข้อมูล หรือ “Data Sovereignty”

ดังนั้น รัฐบาลควรเพิ่มบทบาทในการพัฒนาขีดความสามารถและสร้างความตระหนักรู้ให้กับประชาชน เช่น การเพิ่มพื้นที่ของการให้ความรู้ ความเข้าใจ และการสร้างความตระหนักรู้ในเรื่องการคุ้มครองและหวงแหนข้อมูลส่วนบุคคลบนเว็บไซต์ของหน่วยงานภาครัฐ การประชาสัมพันธ์อย่างแพร่หลายให้ประชาชนทั่วไปรู้เท่าทันวิธีการที่ผู้ประสงค์ร้ายมักจะใช้ล้วงข้อมูลส่วนบุคคล การให้ความรู้ประชาชนเกี่ยวกับความจำเป็นและความสำคัญของการเข้ารหัสข้อมูล (Data Encryption) หรือการใช้กุญแจการเข้ารหัส (Encryption key) ซึ่งถือเป็นส่วนหนึ่งของระบบความปลอดภัยด้านข้อมูล (Data Security) เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล และรักษาความปลอดภัยของข้อมูลส่วนบุคคล ซึ่งแม้ว่าแพลตฟอร์มต่างชาติจะได้ข้อมูลไป เป็นข้อมูลที่ถูกเข้ารหัสอยู่ ไม่สามารถอ่านไม่ได้ หรืออ่านได้แต่ต้องใช้เวลาในการถอดรหัสนาน จนข้อมูลที่ได้มาไม่เป็นประโยชน์แล้ว เป็นต้น

3.6 การเพิ่มบทบาทของประเทศไทยในเวทีระดับโลกและความร่วมมือระหว่างประเทศ

ในช่วงที่ผ่านมา หน่วยงานในประเทศไทยที่ปฏิบัติงานร่วมกับสหภาพโทรคมนาคมนานาชาติ (International telecommunication union: ITU) ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ กสทช. ซึ่งผู้แทนประเทศไทยเคยได้เข้าร่วมเป็นกรรมการบริหารของ ITU ด้วย ในสมัยที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารยังไม่เปลี่ยนโครงสร้างมาเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อย่างไรก็ดี ITU เป็นหน่วยงานระดับนานาชาติเฉพาะทางที่กำหนดมาตรฐานสากลในส่วนที่เกี่ยวข้องกับระบบโทรคมนาคม รวมถึงระบบอินเทอร์เน็ต และความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งไม่ใช่หน่วยงานปฏิบัติการรับมือหรือโต้ตอบภัยคุกคามโดยตรง นอกจากนี้ หน่วยงานในประเทศไทยที่ปฏิบัติงานร่วมกับ ITU ไม่มีหน้าที่ในด้านการป้องกันและโต้ตอบภัยคุกคามทางไซเบอร์โดยตรง

ดังนั้น แนวทางการเพิ่มบทบาทของประเทศไทย จึงควรจัดตั้งหน่วยงานที่มีหน้าที่ความรับผิดชอบในการนำมาตรฐานของ ITU มาปฏิบัติ โดยควรจัดตั้งหน่วยงานในลักษณะของศูนย์รับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response team: CSIRT) โดยอาศัยอำนาจตามมาตรา 22 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ทำหน้าที่เฝ้าระวัง เตือนภัยล่วงหน้า สร้างระบบป้องกัน และปฏิบัติการโต้ตอบเหตุการณ์ความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ภายในประเทศ รวมถึงร่วมมือกับ CSIRT ในต่างประเทศ ซึ่งยึดถือแนวปฏิบัติตามมาตรฐานของ ITU เช่นเดียวกัน ทั้งนี้ CSIRT แตกต่างจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ซึ่งประเทศไทยอยู่ระหว่างจัดตั้ง และแตกต่างจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ซึ่งทำหน้าที่ติดตาม แนะนำ ประสานงาน และเผยแพร่ข่าวสารและเหตุการณ์ด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน

กลุ่มประเทศอาเซียน (ASEAN) ได้บรรลุข้อตกลงจากการประชุมสุดยอดผู้นำอาเซียนครั้งที่ 36 (The 36th ASEAN summit) จัดขึ้นที่ประเทศเวียดนาม เมื่อเดือนมิถุนายน 2563 ที่ผ่านมา ว่าจะทำให้ภูมิภาคเป็น One ASEAN Digital ซึ่งจะเป็นกรอบทิศทางให้เกิดความร่วมมือกันและการพัฒนาในอาเซียนด้าน Digital technology มากยิ่งขึ้น ในอนาคต เช่น การใช้ Digital technology เพื่อเพิ่มคุณภาพให้กับบริการสาธารณสุขทางอิเล็กทรอนิกส์ (e-Healthcare) การท่องเที่ยวเชิงสุขภาพ และการสื่อสาร โดยเฉพาะในช่วงของวิกฤตหรือช่วงของการแพร่ระบาดของโรคติดต่อร้ายแรง นอกจากนี้ ASEAN ยังให้ความสำคัญกับการสร้างความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และการสร้างความทนทาน

ต่อภัยคุกคามทางไซเบอร์ ทั้งในมิติด้านความร่วมมือด้านนโยบาย การพัฒนาขีดความสามารถ และเสนอให้มีการจัดตั้งคณะกรรมการความร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์ (ASEAN coordinating committee on cybersecurity: ASEAN-Cyber CC) รวมถึงการจัดทำโปรแกรมฝึกอบรมบุคลากรด้านไซเบอร์จาก 10 ชาติอาเซียน โดยจัดทำขึ้นที่ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan cybersecurity capacity building Centre: AJCCBC) ที่ตั้งอยู่ในจังหวัดกรุงเทพมหานคร ประเทศไทย และศูนย์ความร่วมมืออาเซียน-สิงคโปร์ เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Singapore Cybersecurity Centre of Excellence: ASCCE) ที่ตั้งอยู่ในประเทศสิงคโปร์

ทั้งนี้ ปัจจุบันศูนย์ AJCCBC มีหลักสูตรอบรมบุคลากรไซเบอร์ที่สำคัญ 3 หลักสูตร ประกอบด้วย (1) หลักสูตรการรับมือภัยคุกคาม (Cyber defense exercise with recurrence: CYDER) ที่เน้นการรับมือกับภัยคุกคามทางไซเบอร์ ซึ่งเป็นหลักสูตรที่ประสบความสำเร็จในประเทศญี่ปุ่นมาแล้ว (2) หลักสูตร Digital forensics เป็นหลักสูตรที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลจากการโจมตีทางไซเบอร์ ทั้งความรู้พื้นฐานและการลงมือปฏิบัติ (3) หลักสูตรการวิเคราะห์มัลแวร์ (Malware analysis) ที่จะเป็นการวิเคราะห์มัลแวร์ประเภทต่าง ๆ ตามเทรนด์ของภัยคุกคามทางไซเบอร์ โดยเนื้อหาหลักสูตรเหล่านี้จะทบทวนและปรับปรุงให้เป็นปัจจุบันทุกปีเพื่อให้ทันต่อเหตุการณ์และสามารถรองรับการรับมือกับภัยคุกคามประเภทใหม่ ๆ ได้ เหมาะกับเจ้าหน้าที่ด้านไอทีของหน่วยงานที่ต้องมีความรู้เพื่อรับมือภัยคุกคามไซเบอร์

นอกจากนี้ กลุ่มประเทศอาเซียนให้ความสำคัญกับเรื่องความมั่นคงปลอดภัยไซเบอร์อย่างมาก เห็นได้จากการกำหนดให้ “ความมั่นคงปลอดภัยทางสารสนเทศและการรับรองความปลอดภัย (Information security and assurance)” เป็น 1 ใน 8 ของยุทธศาสตร์ในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน ปี 2563 (The ASEAN ICT masterplan 2020) ซึ่งจะเน้นเรื่องการส่งเสริมความร่วมมือระหว่าง CERT ธรรมาภิบาลข้อมูล หรือการกำกับดูแลข้อมูล (Data Governance) และการระบุและปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อีกทั้งกลุ่มประเทศอาเซียนยังได้ร่วมกันจัดทำ ASEAN Cybersecurity cooperation strategy ซึ่งระบุถึงความร่วมมือระหว่างประเทศสมาชิกอาเซียนเพื่อเสริมสร้างความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ รวมถึงความร่วมมือกับ Dialogue Partners และผู้มีส่วนได้ส่วนเสียอื่น ๆ ด้วย

ดังนั้น แนวทางการเพิ่มบทบาทของประเทศไทย จึงควรส่งบุคลากรด้านไซเบอร์ของหน่วยงานภาครัฐในประเทศเข้าร่วมโปรแกรมฝึกอบรมบุคลากรด้านไซเบอร์ของศูนย์ AJCCBC และจัดตั้งหน่วยงานหลักที่รับผิดชอบในการเฝ้าระวังและรับมือกับภัยคุกคามไซเบอร์ทั้งในลักษณะของ CERT และ CSIRT เพื่อประสานความร่วมมือกับหน่วยงาน CERT และ CSIRT ในต่างประเทศ รวมถึงการทบทวนและปรับปรุงยุทธศาสตร์ชาติให้สอดคล้องกับแผนแม่บทและ

ยุทธศาสตร์อาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ การรักษาความเป็นส่วนตัว ข้อมูลส่วนบุคคล และอธิปไตยทางไซเบอร์ ซึ่งต้องร่วมมือตั้งแต่ระดับบุคคลที่เป็นผู้ใช้งาน องค์กรในภาคเอกชน หน่วยงานภาครัฐ และความร่วมมือระหว่างประเทศ

ในเวทีสหประชาชาติ (United nations: UN) ประเทไทยสนับสนุนการทำงานของกรอบ United nations open ended working group (UN OEG) และ United nations group of governmental experts (UN GGEs) ในเรื่องพฤติกรรมความรับผิดชอบของรัฐทางไซเบอร์ที่เป็นบรรทัดฐานทางสังคม (Cyber norms) ทั้งหมด 11 เรื่อง ดังนี้

1. การรักษาสันติภาพและความมั่นคงระหว่างประเทศ (International peace and security) และให้ความร่วมมือในการพัฒนาเสถียรภาพและความมั่นคงของการใช้เทคโนโลยีสารสนเทศ และการสื่อสาร และการป้องกันกิจกรรมทางเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นภัยคุกคามต่อสันติภาพและความมั่นคงระหว่างประเทศ

2. ในกรณีที่เกิดเหตุการณ์ผิดปกติหรือปัญหาด้านเทคโนโลยีสารสนเทศและการสื่อสาร รัฐพึงพิจารณาข้อมูลที่เกี่ยวข้อง ผลกระทบทุกมิติ ผลกระทบในวงกว้าง ผลกระทบต่อสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ และการสื่อสาร (ICT environment) รวมถึงลักษณะและความรุนแรงของผลกระทบ (Nature and extent of the consequences)

3. รัฐพึงไม่ยินยอมให้มีการใช้ดินแดนของรัฐในการกระทำความผิดทางเทคโนโลยีสารสนเทศ และการสื่อสาร (Wrongful acts using ICTs) ต่อรัฐอื่น

4. รัฐพึงพิจารณาแนวทางการสร้างความร่วมมือในการแลกเปลี่ยนข้อมูล (Exchange of information) ความช่วยเหลือ และการลงโทษอาชญากรและผู้ก่อการร้ายทางเทคโนโลยีสารสนเทศ และการสื่อสาร รวมถึงความร่วมมืออื่น ๆ ในการแก้ไขปัญหาภัยคุกคามไซเบอร์ และการพัฒนามาตรการรูปแบบใหม่ที่จำเป็น

5. รัฐพึงสร้างความมั่นคงในการใช้เทคโนโลยีสารสนเทศ และการสื่อสาร การเคารพสิทธิมนุษยชน (Human rights) ในระบบอินเทอร์เน็ต และเสรีภาพในการแสดงออก (Freedom of expression)

6. รัฐพึงไม่ดำเนินการหรือสนับสนุนกิจกรรมที่ขัดแย้งต่อข้อตกลงภายใต้กฎหมายระหว่างประเทศ (Obligations under international law) ซึ่งสร้างความเสียหายต่อโครงสร้างพื้นฐานที่สำคัญของรัฐอื่น หรือสร้างผลกระทบต่อการให้บริการสาธารณะ

7. รัฐพึงกำหนดมาตรการที่เหมาะสมในการคุ้มครองโครงสร้างพื้นฐานที่สำคัญจากภัยคุกคามทางเทคโนโลยีสารสนเทศ และการสื่อสาร (ICT threats)

8. รัฐพึงให้ความช่วยเหลืออย่างเหมาะสมแก่รัฐอื่น (Requests for assistance) ซึ่งประสบภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญ รวมถึงการให้ความช่วยเหลือในการลดผลกระทบของกิจกรรมที่ประสงค์ร้ายต่อรัฐอื่น (Malicious ICT acts) หรือการโจมตีโครงสร้างพื้นฐานพื้นฐานของรัฐอื่น ซึ่งเกิดขึ้นจากการกระทำภายในเขตแดนของรัฐ โดยคำนึงถึงอธิปไตยของรัฐ

9. รัฐพึงสนับสนุนให้ห่วงโซการผลิต (Supply chain) มีความซื่อสัตย์ต่อผู้บริโภคขั้นสุดท้าย เพื่อให้เกิดความเชื่อมั่นต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร และรัฐควรป้องกันการขยายตัวของเครื่องมือและเทคนิคที่ประสงค์ร้ายต่อระบบเทคโนโลยีสารสนเทศ และการสื่อสาร รวมถึงการใช้งานฟังก์ชั่นลับที่ประสงค์ร้าย (Hidden functions)

10. รัฐพึงจัดทำรายงานความเปราะบางด้านเทคโนโลยีสารสนเทศ และการสื่อสาร (ICT vulnerabilities) และแบ่งปันข้อมูลที่จำเป็นต่อการพื้นฟูและลดความเปราะบางดังกล่าว เพื่อกำจัดภัยคุกคามที่ส่งผลกระทบต่อระบบและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT-dependent infrastructure)

11. รัฐพึงไม่ปฏิบัติหรือสนับสนุนกิจกรรมที่ประสงค์ร้ายต่อระบบข้อมูล (Information systems) ของ CERTs หรือ CSIRTs ของรัฐอื่น และไม่ใช้ทีมโต้ตอบเหตุการณ์ในการปฏิบัติการเพื่อประสงค์ร้ายต่อกิจกรรมระหว่างประเทศ (Malicious international activity)

ดังนั้น ประเทศไทยควรมีการศึกษาแนวทางการดำเนินการพฤติกรรมความรับผิดชอบของรัฐทางไซเบอร์ที่เป็นบรรทัดฐานทางสังคม (Cyber Norms) ของ UN และความสอดคล้องกับกฎหมายภายในประเทศต่อไป

บรรณานุกรม

ภาษาไทย

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

ชนินทร เฉลิมทรัพย์, นาวาอากาศเอก. “แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2560.

ปรัชญา เฉลิมวัฒน์, พลตรี. “แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2560.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “การพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐเพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล “รู้ทัน Cyber”, 2560.

ยุทธนา เจียมตระการ. “การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2560.

อุดม ประตาทะยัง, พลเรือตรี. “แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, 2560.

สมาคมโทรคมนาคมแห่งประเทศไทย. “แนวทางการสร้างกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์”. การสัมนาทางวิชาการ แนวทางการพัฒนาบุคลากรเพื่อสนับสนุนเทคโนโลยีสารสนเทศและการสื่อสาร และอุตสาหกรรม, 2561.

กฎหมาย

“ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561 - 2580). (13 ตุลาคม 2561)”. ราชกิจจานุเบกษา. เล่ม 135 ตอนที่ 82ก.

“ประกาศสำนักนายกรัฐมนตรี เรื่อง แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (วันที่ 3 มกราคม 2563)”. ราชกิจจานุเบกษา. เล่ม 137 ตอนที่ 2 ง.

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562”. ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก.

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562”. ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (18 มิถุนายน 2550)”. ราชกิจจานุเบกษา. เล่ม 124 ตอนที่ 27 ก.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (24 มกราคม 2560)”. ราชกิจจานุเบกษา. เล่ม 134 ตอนที่ 10 ก.

ฐานข้อมูลอิเล็กทรอนิกส์

ความมั่นคงปลอดภัยและโครงสร้างพื้นฐานทางไซเบอร์, สำนักงาน. (Cybersecurity and Infrastructure Security Agency : CISA) “The National Strategy to secure Cyberspace”. (ออนไลน์). เข้าถึงได้จาก : https://www.us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf>

ภาษาอังกฤษ

Cabinet Office “National Cybersecurity Strategy Progress Report 2016 – 2021”. (Online). Available : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf, 2019.

Cybersecurity Agency of Singapore. “Singapore's Cybersecurity Strategy”. (Online). Available : <https://www.csa.gov.sg/-media/csa/documents/publications/singaporecybersecuritystrategy.pdf, 2016.

Cynthia E. Ayers. “Rethinking Sovereignty in the Context of Cyberspace : The Cyber Sovereignty Workshop Series”. Center for Strategic Leadership, United States Army. (Online). Available : <https://www.hsdl.org/?view&did=802916, 2559.

Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Malinauskaitė-van de Castel “A Model for the National Cybersecurity Strategy”. : Lithuanian Case. Journal of Security and Sustainability Issues. (Online). Available <https://www.researchgate.net/publication/3 1 6 0 1 8 0 0 2 _A_model_for_the_national_cyber_security_strategy_The_Lithuanian_case, 2560.

European Union Agency for Network and Information Security Agency. “NCSS Good Practice Guide Designing and Implementing National Cybersecurity

Strategies". (Online). Available : <https://www.enisa.europa.eu/publications /ncss-good-practice-guide/at_download/fullReport, 2016.

Exabeam expert. "The Complete Guide to CSIRT Organization : How to Build an Incident Response Team." (Online). Available : <https://www.exabeam. com/incident-response/csirt/, 2561.

Global Cybersecurity Capacity Centre. "Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition". University of Oxford. (Online). Available : <https://gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf, 2016.

Hao Yeli. "A Three-Perspective Theory of Cyber Sovereignty". The Fifth Domain. PRISM vol. 7 No. 2 2017. A Journal of the Center for Complex Operation. <https://www.cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective%20Theory.pdf, 2560.

HM Government. "National Cyber Strategy 2016-2021". (Online). Available : <https:// www.assets.publishing.service.gov.uk/government/uploads/system/upl oads/attachment_data/file/567242/national_cyber_security_strategy_201 6.pdf>

Infocomm Media Development Authority. "Internet Code of Practice". (Online). Available:https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Codes-of-Practice/Codes-of-Practice-Media/ PoliciesandContentGuidelinesInternetInterneCodeOfPractice.pdf

Information Security Audit and Control. "An Introduction to the Business Model for Information Security". United States of America. (Online). Available : <http://www.media.techtarget.com/Syndication/SECURITY/BusiModelforInfo Sec.pdf, 2552.

International Telecommunication Union. "Guide to Developing a National Cybersecurity Strategy. Strategic engagement in cybersecurity". (Online). Available : <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf, 2018.

Kantar GREYnJ United, Mindshare (Thailand). "Thailand COVID-19 Situation". (Online). Available:<https://www.marketingoops.com/reports/behaviors/wpp-roup-

social-distancing-covid-19-change-consumer-behavior-to-new-normal/, 2563).

Kaushik Sarker, Hasibur Rahman, Khandaker Farzana Rahman, Md. Shohel Arman, Saikat Biswas, Touhid Bhuiyan. “A Comparative Analysis of the Cybersecurity Strategy of Bangladesh”. International Journal on Cybernetics & Informatics (IJCI) Vol. 8, No.2, April 2019. (Online). Available : https://www.Researchgate .net/publication/332849592_A_Comparative_Analysis_of_the_Cyber_Security _Strategy_of_Bangladeshm, 2562.

Organisation for Economic Co-operation and Development. “The Role of Digital Platforms in the Collection of VAT/GST on Online Sales”. (Published on June 20, 2019) As presented for consideration at the fifth meeting of the Global Forum on VAT March 2019. (Online). Available : <http://www.oecd.org/ tax/consumption/the-role-of-digital-platforms-in-the-collection-of-vat-gst-on-online-sales.pdf, 2562.

Narmeen Shafqat, Ashraf Masood. “Comparative Analysis of Various National Cybersecurity Strategies”. International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016. (Online). Available : <https://www.academia.edu/21451805/Comparative_Analysis_of_Various _National_Cyber_Security_Strategies, 2559.

National Institute of Standards and Technology. “Framework for Improving Critical Infrastructure Cybersecurity”. Version 1.1. (Online). Available : <https:// www. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 2018.

Techtarget. “Computer Security Incident Response Team (CSIRT)”. Ultimate guide to cybersecurity incident response. (Online). Available : https://www.whatis. techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT, 2561.

United Kingdom’s Multi-stakeholder Advisory Group on Cyber issues. “Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015”. (Online).Available:<https://www.un.org/disarmament/wp-ontent/uploads/ 2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf, 2562.

We Are Social, Hootsuite. “DIGITAL 2020 THAILAND”. (Online). Available : https://www.datareportal.com/digital-in-thailand, 2019.

White Hourse. “National Cyber Strategy of the United States of America”. (Online). Available<https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 2018.

ประวัติย่อผู้วิจัย

ชื่อ : ปริญญา หอมเอนก (สุทัศน์ ณ อยุธยา)

วันเดือนปีเกิด : 29 สิงหาคม 2512

ประวัติการศึกษา : ปริญญาตรี วิศวกรรมไฟฟ้า วิศวกรรมศาสตรบัณฑิต (วศ.บ.) คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
: ปริญญาโท บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยอัสสัมชัญ
: ปริญญาเอก วิทยาศาสตรดุษฎีบัณฑิตกิตติมศักดิ์ สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

ประวัติการทำงานโดยย่อ : กรรมการและอุปนายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association: TISA)
: คนไทยคนแรกและคนเดียวที่ได้รับการคัดเลือกเป็นคณะกรรมการที่ปรึกษา (ISC)2 ประจำภูมิภาคเอเชียแปซิฟิก Asia-Pacific Advisory Council สถาบัน International Information Systems Security Certification Consortium
: คนไทยคนแรกและคนเดียวที่ได้รับใบรับรองความรู้ระดับสากลจากองค์กรด้านสารสนเทศระดับโลกมากที่สุดในประเทศไทย
: อาจารย์พิเศษ/วิทยากรบรรยายให้กับสถาบันต่าง ๆ อาทิเช่น Stanford University Palo Alto U.S.A., NIDA, SASIN, จุฬาลงกรณ์มหาวิทยาลัย
: นักเรียนทุน Eisenhower Fellows 2013
: ประธานกรรมการบริหาร บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด และบริษัท ไซเบอร์ตรอน จำกัด
: กรรมาธิการวิสามัญ ร่าง พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
: กรรมการตรวจสอบ และ กรรมการกำกับความเสี่ยง บริษัท ทุนธนชาตจำกัด (มหาชน)
: ที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ กองทัพอากาศ
: อดีตอนุกรรมการความมั่นคงในคณะกรรมการธุรกรรมอิเล็กทรอนิกส์
: อดีตที่ปรึกษา National Security และ Cybersecurity รัฐมนตรีว่าการกระทรวงยุติธรรม
: อดีตกรรมการผู้ทรงคุณวุฒิ สานักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

ตำแหน่งปัจจุบัน : ประธานกรรมการบริหารบริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด