ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับภัยคุกคามทางไซเบอร์

เอกสารวิจัยส่วนบุคคล

โดย

นายณัฐกานต์ อรวรรณนุกุล

ผู้อำนวยการฝ่ายส่งเสริมการขาย

บริษัท แอสตร้า เทคโนโลยี จำกัด

วิทยาลัยการทัพบก

กันยายน 2565

เอกสารวิจัยเรื่อง ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับภัยคุกคามทางไซเบอร์

โดย นาย ณัฐกานต์ อรวรรณนุกุล

อาจารย์ที่ปรึกษา พันเอก ชนะชัย พลเตชา

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2565 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ ดีมาก

พลตรี ..... **ผู้บัญชาการวิทยาลัยการทัพบก**

(วิชาติ เอี่ยมไพจิตร์)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก ..... **ประธานกรรมการ**

(ชนะชัย พลเตชา)

ว่าที่ร้อยโท ..... **ผู้ทรงคุณวุฒิที่ปรึกษา**

(อภิสิทธิ์ ไชยประสิทธิ์)

พันเอก ..... **กรรมการ**

(ปริญญา ฉายะพงษ์)

พันเอกหญิง ..... **กรรมการ**

(กัญญนัฏ แสงภัทรเนตร)

บทคัดย่อ

ผู้วิจัย นาย ณัฐกานต์ อรวรรณนุกูล

เรื่อง ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับภัยคุกคามทางไซเบอร์

วันที่ กันยายน 2565 **จำนวนคำ :** 19,782 **จำนวนหน้า :** 63

คำสำคัญ ภัยคุกคามทางไซเบอร์, ความมั่นคงปลอดภัยไซเบอร์,ความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

ชั้นความลับ ไม่มีชั้นความลับ

จากการที่รัฐบาลได้นำประเทศไทยเข้าสู่การปฏิรูปโครงสร้างเศรษฐกิจเพื่อก้าวข้าม “Thailand 3.0” ไปสู่ “Thailand 4.0” ทำให้เกิดอุตสาหกรรม 4.0 ที่ขับเคลื่อนด้วยเทคโนโลยี นวัตกรรม และความคิดสร้างสรรค์ รัฐได้เห็นถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์และได้ดำเนินการตามยุทธศาสตร์ชาติ 20 ปี แผนแม่บท พระราชบัญญัติ นโยบายและแผนปฏิบัติการสำหรับภาครัฐอย่างต่อเนื่องจนถึงปัจจุบันที่อินเทอร์เน็ตได้เชื่อมโยงอุปกรณ์ต่างๆรอบตัว (Internet of Things “IoT”) ในยุคอินเทอร์เน็ตในทุกสิ่ง (Internet of Things “IoT”) ที่มีการเชื่อมโยงเข้าด้วยกันด้วยไซเบอร์สเปซ (Cyber Space) การพัฒนาเทคโนโลยีการติดต่อสื่อสาร การทำธุรกรรมทางการเงินรวมถึงอุปกรณ์ต่างๆ ล้วนเชื่อมโยงเข้าสู่โลกอินเทอร์เน็ต จากการแพร่ระบาดของโรคติดเชื้อไวรัสโควิด-19 (Covid-19) ที่หลายองค์กรและทุกคนทั่วโลกต่างต้องทำงานทางไกล (Remote Working) จึงปฏิเสธไม่ได้เลยที่หลายองค์กรและทุกคนมีโอกาสที่จะถูกโจมตีและถูกคุกคามจนเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ (Cyber Threats) จากการเชื่อมโยงนี้ส่งผลให้เกิดภัยคุกคามทางด้านความมั่นคงปลอดภัยไซเบอร์ต่อภาครัฐ ภาคเอกชนและทุกคน ปัญหาเรื่องการเตรียมความพร้อม

องค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เพื่อรองรับภัยคุกคามทางไซเบอร์ จึงมีความสำคัญยิ่งสำหรับองค์กรและบุคลากรที่จะต้องตระหนักถึงรูปแบบการโจมตี ทำความเข้าใจเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ เตรียมพร้อมหลักการคืนสภาพ แสวงหาความรู้เพิ่มเติมเพื่อเตรียมการป้องกันรองรับภัยคุกคามทางไซเบอร์ (Cyber Threats) ก่อนที่จะไม่สามารถแก้ไขได้

ผลวิจัยสรุปว่า สามารถนำภาพรวมองค์ความรู้จากการวิจัยเป็นแนวทางพิจารณาให้เกิดประโยชน์ต่อความมั่นคงทางการทหาร ภาครัฐ เอกชน ทุกคนและสำหรับประเทศไทยได้

ABSTRACT

AUTHOR: Mr. Nattakarn Orawannukul

TITLE: An overview of organization and cyber security personnel guidelines in preparation to support cyber threats.

DATE: September, 2022 **WORD COUNT:** 19,782 **PAGES:** 63

KEY TERMS: Cyber Threats, Cyber Security, Cyber Security Infrastructure, Cybersecurity Training Courses

CLASSIFICATION: Unclassified

As the government has led Thailand to reform the economic structure to move beyond "Thailand 3.0" to "Thailand 4.0", resulting in Industry 4.0 driven by technology, innovation, and creativity, the state recognizes the importance of cybersecurity and has implemented a 20-years national strategy, master plan, statutory policies, and action plans for the public sector continuously until now, where the Internet of Things (IoT) connects people with this world via Cyber Space, the development of communication technology, financial transactions via application, and all devices are well-connect to the internet. The spread of the COVID-19 virus is changing how and where we work. Many organizations and people must work remotely (Remote Working). It is undeniable that many organizations and everyone could be attacked by Cyber Threats. Various types of cyber-threats can cause critical harm to the government sector, private sector, and everyone. To prepare organization infrastructure and enhance cybersecurity personnel skills to cope with these cyber threats, the organizations

and personnel must be aware of cyber-attack patterns, understand existing Cyber Security Technology, prepare for recovery principles, and seek more knowledge to prepare themself against cyber threats before the point of no return.

The research concluded that the overview from these studies is applicable as a guide to consider all benefits of the Thai military, government sectors, private sectors, individuals, and nation.

กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคลนี้สำเร็จได้ด้วยดี ด้วยความกรุณาจากประธานกรรมการ พันเอก ชนะชัย พลเตชา อาจารย์ที่ปรึกษางานวิจัย พันเอก ปริญญา ฉายะพงษ์ พันเอกหญิง กัญญนัฏ แสงภัทรเนตรและคณาจารย์ของวิทยาลัยการทัพบกทุกท่านที่กรุณาเสียสละเวลา แรงกายแรงใจ ให้ความรู้และประสบการณ์ที่ทรงคุณค่าอย่างสูง รวมทั้งผู้ทรงคุณวุฒิที่ปรึกษา ว่าที่ร้อยโท อภิสิทธิ์ ไชยประสิทธิ์ ที่กรุณาให้แนวคิดที่เป็นประโยชน์ในการจัดทำเอกสารวิจัยส่วนบุคคล นอกเหนือจากข้อแนะนำทางวิชาการ อันเป็นประโยชน์ในการวิจัยแล้ว ยังได้รับกำลังใจและคำชี้แนะที่เป็นประโยชน์ยิ่ง ทำให้เอกสารวิจัยส่วนบุคคลฉบับนี้เสร็จสมบูรณ์ จึงขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอขอบพระคุณคณาจารย์หลักสูตรหลักประจำวิทยาลัยการทัพบก ที่ได้ประสิทธิประสาทวิชาความรู้ อบรมสั่งสอนช่วยเหลือให้คำแนะนำและแบ่งปันประสบการณ์อันมีค่ายิ่ง แก่ผู้วิจัยมาโดยตลอด ขอขอบพระคุณเจ้าของหนังสือ วารสาร เอกสาร และงานวิจัย ทุกเล่มที่ช่วยให้งานวิจัยนี้มีความสมบูรณ์ และขอขอบคุณสมาชิกในครอบครัวที่เป็นกำลังใจ มีความห่วงใยและช่วยเหลือมาโดยตลอด

ขอขอบคุณผู้อยู่เบื้องหลังทุกท่านที่คอยเป็นกำลังใจ ในการทำวิจัยฉบับนี้ให้สำเร็จสมบูรณ์ ได้สมตามความมุ่งหวัง ความดีอันเกิดจากผลงานการวิจัยครั้งนี้ ผู้วิจัยขอมอบให้ผู้ที่มีส่วนร่วมในงานวิจัยดังกล่าวข้างต้นทุกท่านด้วยความเคารพรัก และหวังเป็นอย่างยิ่งว่างานวิจัยฉบับนี้ จะเป็นประโยชน์ ก่อให้เกิดผลดีต่อวิทยาลัยการทัพบก เหล่าทัพและประเทศชาติสืบไป

สารบัญ

หน้า

สารบัญ

หน้า

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

จากการที่รัฐบาลได้นำประเทศไทยไปสู่การปฏิรูปโครงสร้างเศรษฐกิจเพื่อก้าวข้าม “Thailand 3.0” ไปสู่ “Thailand 4.0” ที่ขับเคลื่อนด้วยเทคโนโลยี นวัตกรรม และความคิดสร้างสรรค์ ถึงปัจจุบันที่อินเทอร์เน็ตได้เชื่อมโยงอุปกรณ์ต่างๆรอบตัว (Internet of Things “IoT”) เข้าด้วยไซเบอร์สเปซ (Cyber Space) การพัฒนาเทคโนโลยีการติดต่อสื่อสาร การทำธุรกรรมทางการเงินรวมถึงอุปกรณ์ต่างๆ ล้วนเชื่อมโยงเข้าสู่โลกอินเทอร์เน็ต ตั้งแต่เดือนธันวาคม พ.ศ.2562 ที่เริ่มพบการแพร่ระบาดของโรคติดเชื้อไวรัสโควิด-19 (Covid-19) ทั่วโลก หลายองค์กรต่างให้บุคลากรของตนต้องทำงานทางไกล (Remote Working) จึงปฏิเสธไม่ได้เลยที่หน่วยงาน องค์กรและทุกคนมีโอกาสที่จะถูกโจมตีและถูกคุกคามจนเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ (Cyber Threats)

ประเทศไทยมีการใช้งานเทคโนโลยีด้านการสื่อสารโทรคมนาคมเป็นลำดับต้นๆในภูมิภาคอาเซียนและรัฐบาลดำเนินการเรื่อยมาในการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล[1] ที่เริ่มมีการเชื่อมต่อโครงสร้างพื้นฐานหลักของประเทศเข้าระบบเครือข่ายอินเทอร์เน็ตเพื่อยกระดับการบริหารงานของภาครัฐให้ก้าวสู่ความทันสมัยที่มาพร้อมกับความสะดวกสบายและรวดเร็วควบคู่ไปกับการให้บริการประชาชนด้วยระบบอิเล็กทรอนิกส์ที่มีประสิทธิภาพ มั่นคง ปลอดภัยและทั่วถึง อีกทั้งยังพัฒนาให้เกิดการบูรณาการระหว่างหน่วยงานภาครัฐด้วยการเชื่อมโยงข้อมูลของทุกภาคส่วนเข้าด้วยกัน โดยปัจจุบันแนวโน้มเทคโนโลยีที่สำคัญต่อการพัฒนาเพื่อมุ่งไปสู่การเป็นรัฐบาลดิจิทัล[1] มีรายละเอียดดังต่อไปนี้

การนำเทคโนโลยีการจำลองภาพหรือสถานการณ์เหมือนจริง(Virtual Reality “VR” และ Augmented Reality “AR”) มาปรับใช้เพื่อบริหารจัดการความปลอดภัยสาธารณะ การขยายพื้นที่การรักษาสุขภาพไปยังพื้นที่ห่างไกล (Telemedicine)

การนำเทคโนโลยีเชิงลึกด้านข้อมูลในเชิงพื้นที่ (Advanced Geographic Information System) มาใช้ในการบริหารจัดการ โดยสามารถประยุกต์ใช้สำหรับการจัดสรรทรัพยากรด้านการเกษตร การบริหารจัดการระบบคมนาคมขนส่ง และด้านอื่นๆ

การนำข้อมูลขนาดใหญ่ (Big Data) มาประมวลผลให้ได้หลายทางเลือกสำหรับการตัดสินใจและใช้เป็นเครื่องมือในการคาดการณ์-ประเมินสถานการณ์ สภาพธุรกิจการให้บริการ โดยอาศัยเทคโนโลยี IoT และ Smart Machine เพื่อให้การวิเคราะห์และตอบสนองต่อผู้รับบริการ ณ ปัจจุบันที่เกิดขึ้นจริง (Real-Time)

การเปิดเผยข้อมูล (Open Data) ที่เป็นประโยชน์แก่ผู้รับบริการ โดยให้บริการผ่านเว็บไซต์กลางและฐานข้อมูล เพื่อสร้างการเข้าถึงจากสาธารณะมากขึ้น และผลักดันให้เกิดการเชื่อมโยงข้อมูลที่เปิดเผยเหล่านั้นกับหน่วยงานทุกภาคส่วน

การนำเทคโนโลยีเครื่องจักรที่อาศัยเทคโนโลยีสารสนเทศทำให้เกิดความเป็นอัจฉริยะ (Smart Machine) หรือ เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence “AI”) มาปรับใช้เพื่อให้เกิดการบริหารจัดการและตอบสนองการให้บริการอัตโนมัติ โดยระบบ Smart Machine จะพัฒนาขึ้นและสามารถประเมินปัญหาและจัดการสมดุลตลอดห่วงโซ่การบริการ

การนำเทคโนโลยีในการบริการจัดการที่ครอบคลุมถึงการให้ใช้กำลังประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่างๆจากผู้ให้บริการ เพื่อลดความยุ่งยากในการติดตั้ง ดูแลระบบ (Cloud Computing) ทำให้สามารถลดต้นทุนในการดูแลระบบ และต้นทุนสำหรับการสร้างเครือข่ายด้วยตนเอง

การคำนึงถึงความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) โดยจัดทำมาตรฐานความปลอดภัยทางไซเบอร์ ปรับปรุงกฎระเบียบที่เกี่ยวข้องให้ทันต่อเหตุการณ์และมีความยืดหยุ่น อีกทั้งปรับเปลี่ยน Mindset ในการจัดการประเด็นด้านความปลอดภัยทางไซเบอร์

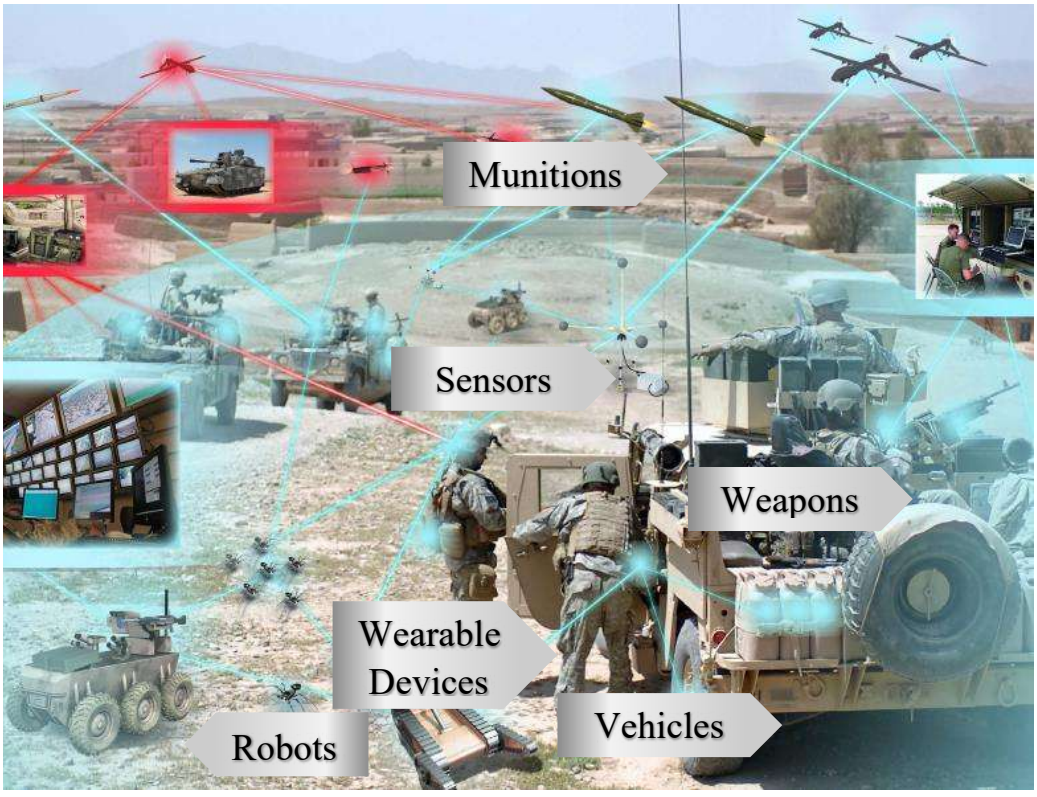
การนำเทคโนโลยีอุปกรณ์ที่สามารถเชื่อมต่อเข้าอินเทอร์เน็ตได้ตลอดเวลามาใช้ Internet of Things (IoT) เพื่อสร้างสภาพแวดล้อมให้ภาครัฐปรับเปลี่ยนรูปแบบบริการเป็นดิจิทัลมากยิ่งขึ้น ขณะเดียวกันเทคโนโลยีดังกล่าวยังสนับสนุนภาครัฐในด้านต่างๆ อาทิ การสื่อสาร การใช้เทคโนโลยีนอกสถานที่ เคลื่อนย้ายได้ (Mobility) การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) รวมไปถึงการประสานงานกับภาครัฐ ภาคเอกชน และพลเรือน

การประยุกต์ใช้เทคโนโลยีระบบการเก็บข้อมูล (Data Structure) ซึ่งไม่มีตัวกลาง แต่ข้อมูลที่ได้รับการปกป้องจะถูกแชร์และจัดเก็บเป็นสำเนาไว้ในเครื่องของทุกคน

ที่ใช้ฐานข้อมูลเดียวกันเสมือนห่วงโซ่ (Chain) ที่เรียกว่า Blockchain หรือ Distributed Ledger Technology ในการจัดเก็บข้อมูลและใช้ประโยชน์จากเครือข่ายเพื่อตรวจสอบความถูกต้อง และลดภาระการพึ่งพาคนกลางในการทำธุรกรรม ภายใต้ความปลอดภัยที่มีความน่าเชื่อถือ

ซึ่งถือได้ว่าจากการเชื่อมโยงนี้หากหน่วยงานภาครัฐ ภาคเอกชน และพลเรือนขาดความตระหนักถึงภัยคุกคามทางไซเบอร์ ไม่มีมาตราการป้องกันตามมาตราฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ ก็จะสามารถส่งผลให้เกิดภัยคุกคามที่มีความเสี่ยงในระดับสูงต่อระบบความมั่นคงปลอดภัยไซเบอร์อย่างหลีกหนีไม่ได้ อาจก่อให้เกิดความเสียหายทางเศรษฐกิจ สังคม ภาพลักษณ์ของประเทศและความมั่นคงปลอดภัยของชาติได้

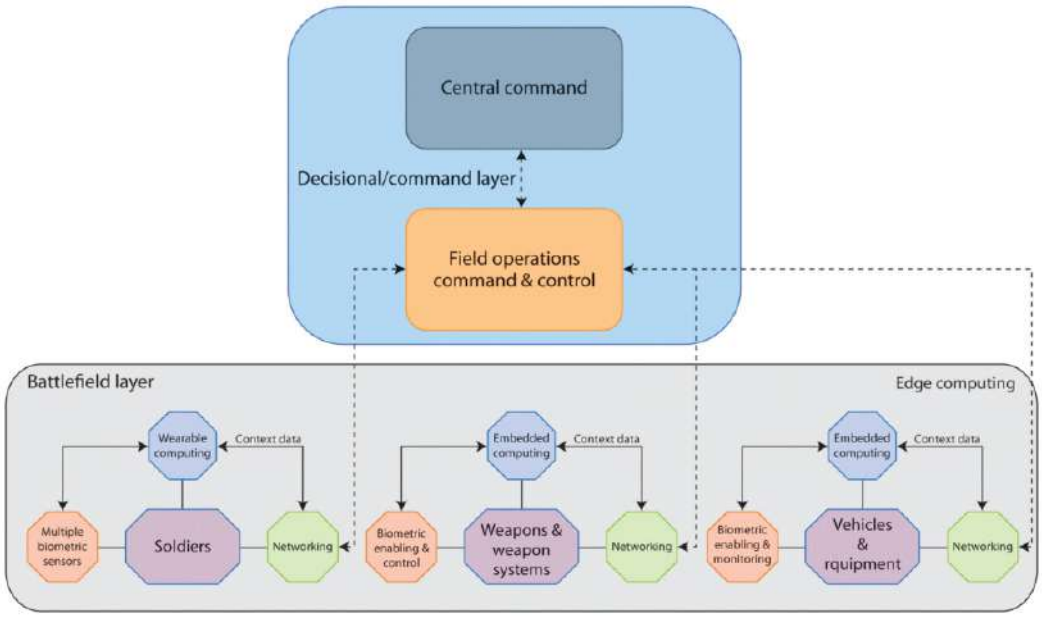
ด้วยเหตุนี้ความมั่นคงปลอดภัยไซเบอร์ได้บรรจุอยู่ในยุทธศาสตร์ชาติ 20 ปี 2561-2580 ด้านความมั่นคง ปัจจุบันความมั่นคงปลอดภัยทางไซเบอร์เป็นที่ประจักษ์แล้วว่าสามารถสร้างผลกระทบโดยตรงต่อความมั่นคงทางทหารและความมั่นคงของประเทศ



ภาพประกอบที่ 1 การเชื่อมโยงยุทโธปกรณ์ต่าง ๆ ในสนามรบเข้าเครือข่ายอินเทอร์เน็ต หรือ Internet of Battlefield Things **“IoBT”**

ชัดเจนมากขึ้น ซึ่งเห็นได้จากสงครามรัสเซีย – ยูเครน เพราะปัจจุบันยุทโธปกรณ์ต่าง ๆ อย่างอุปกรณ์ประจำกาย ระบบอำนวยการรบ อากาศยานไร้คนขับเป็นต้น ล้วนสามารถเชื่อมต่อเข้าโครงข่ายอินเทอร์เน็ตเพื่อให้ผู้บังคับบัญชาสามารถติดตามผล เห็นภาพจริงในสนามรบ เข้าใจสถานการณ์ที่เกิดขึ้นจริง ณ เวลาปัจจุบันทันทีทันใด (Real-Time) ทำให้สามารถตัดสินใจให้เกิดประสิทธิผลสูงสุดต่อสถานการณ์นั้น ๆ

การนำเทคโนโลยีอุปกรณ์เคลื่อนที่เพื่อการเชื่อมโยงยุทโธปกรณ์ต่าง ๆ ในสนามรบเข้าระบบสารสนเทศ ระบบสื่อสารและอินเทอร์เน็ต ซึ่งมีการส่งข้อมูลดิจิตอลผ่านระบบการสื่อสารแบบไร้สายเทคโนโลยี 5G ได้แบบทุกที่ตลอดเวลา เรียกว่า Internet of Battlefield Things “IoBT”[2]



ภาพประกอบที่ 2 โครงสร้างการเชื่อมโยงยุทโธปกรณ์ต่าง ๆ ในสนามรบเข้าเครือข่ายอินเทอร์เน็ต หรือ Internet of Battlefield Things **“IoBT”**

ในอนาคตอันใกล้สนามรบจะไม่มีเพียงแค่ยุทโธปกรณ์เท่านั้น หากเราสามารถนำทุกสรรพสิ่งรอบตัวในสรามรบเชื่อมต่อเข้าเป็นรูปแบบข้อมูลดิจิตอลได้ กองทัพจะสามารถนำข้อมูลในสนามรบผนวกเข้ากับฐานข้อมูลขนาดใหญ่ (BIG DATA) ของกองทัพ นำเข้าสู่กระบวนการวิเคราะห์ผ่านปัญญาประดิษฐ์ (Artificial Intelligence “AI”) สิ่งนี้จะช่วยให้ผู้บังคับบัญชานำข้อมูลมาวาดแผนการรบได้หลายทางเลือกจากข้อมูลหลายมิติอย่างชาญฉลาด ให้ได้มาซึ่งผลลัพธ์ที่เกิดประโยชน์สูงสุดต่อความมั่นคง ทั้งนี้

เป้าประสงค์นี้จะเกิดขึ้นได้นั้นขึ้นอยู่กับความก้าวหน้าด้านวิทยาศาสตร์ เทคโนโลยี ความพร้อมของระบบและกำลังพล/บุคลากร เหนือสิ่งอื่นใดคือนโยบายผนวกกับงบประมาณอย่างเป็นนัยยะสำคัญ[3]

ด้วยเหตุนี้ความมั่นคงปลอดภัยไซเบอร์จึงเป็นปัญหาความมั่นคงสำคัญที่ต้องได้รับการพัฒนาอย่างเร่งด่วนและต่อเนื่องในทุกภาคส่วน ดั่งที่มีการบรรจุอยู่ในยุทธศาสตร์ชาติ 20 ปี (2561-2580) ด้านความมั่นคง พระราชบัญญัติ แผนแม่บท นโยบายด้านความมั่นคงและแผนปฏิบัติการ ว่าด้วยความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัยเห็นความสำคัญต่อปัญหาเรื่องการเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับภัยคุกคามทางไซเบอร์ จึงมีความสนใจในการศึกษารูปแบบการโจมตีทางไซเบอร์ในปัจจุบันเพื่อสร้างการรับรู้ (Cyber Awareness) ศึกษายุทธศาสตร์ชาติ 20 ปี แผนแม่บท พระราชบัญญัติ นโยบายและแผนปฏิบัติการ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ศึกษาหลักการและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ ศึกษาหลักการคืนสภาพได้ทางไซเบอร์ ศึกษารูปแบบหลักสูตรการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับพัฒนาความมั่นคงปลอดภัยไซเบอร์องค์กรให้สูงขึ้น ศึกษายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ของภาครัฐและเอกชน ทั้งนี้เพื่อก่อให้เกิดภาพรวมองค์ความรู้ดังกล่าวสำหรับใช้เป็นแนวทางพิจารณาปรับใช้ให้เกิดประโยชน์สูงสุดต่อความมั่นคงของประเทศทั้งทางการทหาร ภาครัฐ ภาคเอกชนและพลเรือน

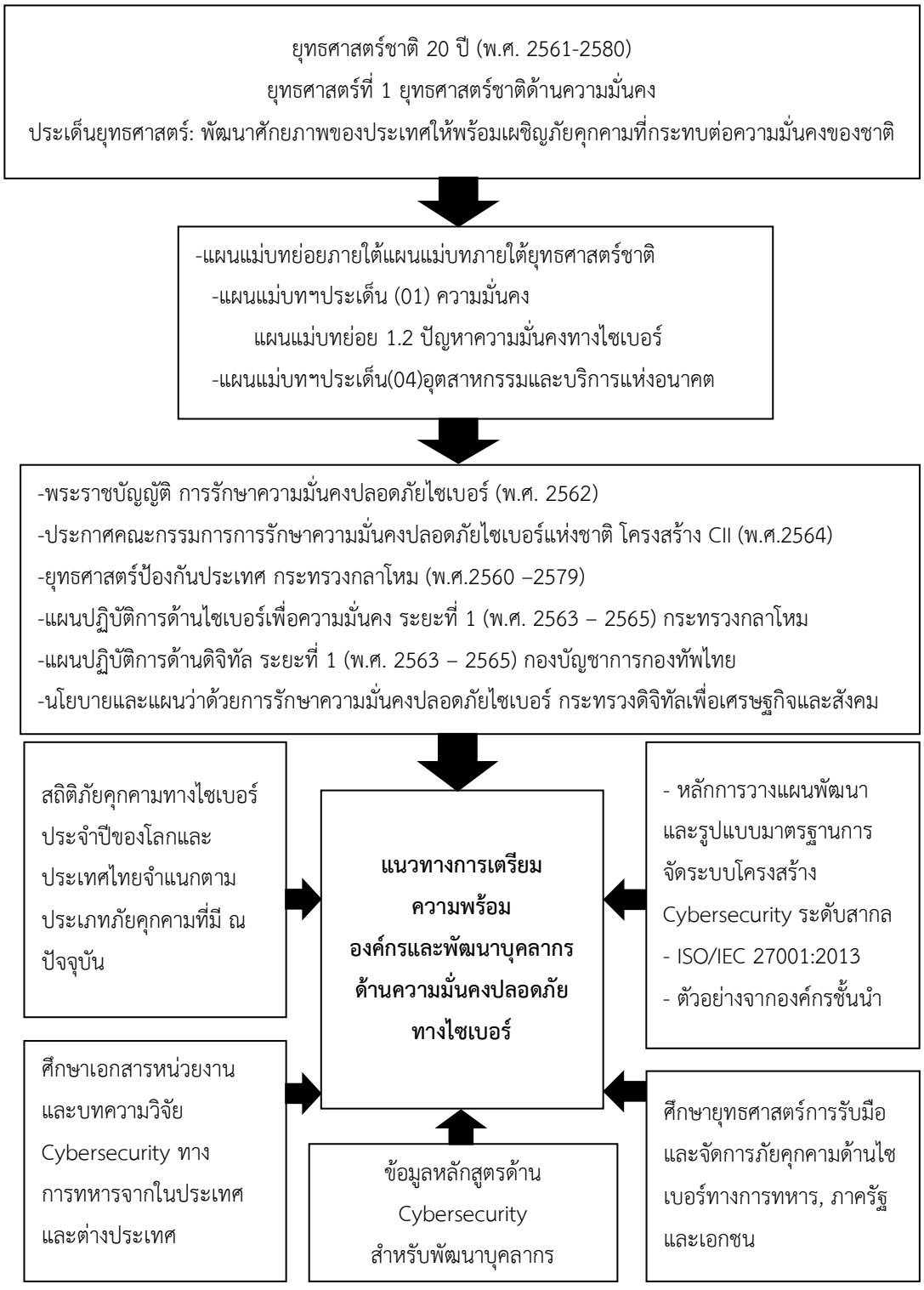
วัตถุประสงค์การวิจัย

1. ปัญหาการโจมตีทางไซเบอร์ในปัจจุบันมีรูปแบบใดบ้าง

2. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ทางการทหารและของประเทศมีอะไรบ้าง

3. ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อรองรับภัยคุกคามทางไซเบอร์เป็นอย่างไร

กรอบแนวคิดการวิจัย



ภาพประกอบที่ 3 กรอบแนวคิดการวิจัย

วิธีการศึกษา

1. แนวทางที่ใช้ในการศึกษา การวิจัยนี้ใช้รูปแบบการวิจัยเชิงยุทธศาสตร์โดยรูปแบบการวิจัยเอกสาร (Documentary Research) ตามรูปแบบที่วิทยาลัยการทัพบกกำหนด

2. ขอบเขตการศึกษา ทำการศึกษา ทบทวนแนวคิด หลักมาตรฐานสากล ยุทธศาสตร์ชาติ และการวิจัยที่เกี่ยวข้องเพื่อให้เกิดความรู้ ความเข้าใจในเรื่องที่เกี่ยวกับภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับภัยคุกคามทางไซเบอร์

3. การเก็บรวบรวมข้อมูล สืบค้นงานวิจัย เอกสารจากหน่วยงานความมั่นคง ภาครัฐ ภาคเอกชน บทความวิจัยต่างประเทศ และข้อมูลจากบริษัทชั้นนำผู้ให้บริการด้าน Cybersecurity ในต่างประเทศที่เกี่ยวข้อง นำผลการวิเคราะห์ที่ได้มาทำการสรุปเพื่อหาภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับภัยคุกคามทางไซเบอร์อย่างยั่งยืนต่อไป

4. การวิเคราะห์ข้อมูล ทำการวิเคราะห์ข้อมูลจากรวบรวมปัญหาการโจมตีทางไซเบอร์ในปัจจุบัน ยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง แผนปฏิบัติการด้านไซเบอร์ พระราชบัญญัติ เอกสารหน่วยงาน บทความวิจัยต่างประเทศ และข้อมูลจากภาคเอกชนที่ได้นำมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์มาปรับใช้กับองค์กร

ประโยชน์ที่ได้รับ

1. ได้รับทราบถึงรูปแบบภัยคุกคามและแนวทางป้องกันทางไซเบอร์
2. ทำให้ทราบถึงผลกระทบที่อาจเกิดจากภัยคุกคามทางไซเบอร์
3. ได้รับทราบถึงภาพรวมในการพัฒนาระบบโครงสร้างและบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สำหรับองค์กรเพื่อความมั่นคงทางไซเบอร์
4. ทำให้ทราบถึงภาพรวมแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานความมั่นคง ภาครัฐ และเอกชน

บทที่ 2

บทวิเคราะห์

โลกในปัจจุบันมีการเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็ว รัฐบาลเล็งเห็นถึงความสำคัญนี้และได้นำประเทศไทยเข้าสู่ “Thailand 4.0” ยุคไร้พรมแดนที่ซึ่งอินเทอร์เน็ตได้เข้ามาเป็นส่วนหนึ่งในการดำเนินชีวิตประจำวันของทุกคน การติดต่อสื่อสาร การทำธุรกรรมทางการเงิน การติดต่อและการทำธุรกรรมกับทางหน่วยงานราชการสามารถดำเนินผ่านการเชื่อมโยงเข้าสู่โลกอินเทอร์เน็ต ตั้งแต่ปีพ.ศ. 2562 จากการแพร่ระบาดของโรคติดเชื้อไวรัสโควิด-19 (Covid-19) ที่หลายองค์กรและทุกคนทั่วโลกต่างต้องทำงานทางไกล (Remote Working) ผ่านทางอินเทอร์เน็ตทำให้ทุกคนมีโอกาสที่จะถูกโจมตีและถูกคุกคามจนเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น เทคโนโลยีในปัจจุบันที่อุปกรณ์หลายอย่างรอบตัวเราเชื่อมต่อเข้ากับอินเทอร์เน็ตตลอดเวลา (Internet of Things “IoT”) อุปกรณ์เหล่านั้นอาจแฝงมาด้วยภัยคุกคามทางไซเบอร์ เช่น ไวรัส, มัลแวร์ และโปรแกรมประสงค์ร้ายต่าง ๆ ของผู้ไม่หวังดี โดยมีเป้าหมายเพื่อให้ได้มาซึ่งข้อมูล, การจารกรรมหรือสอดแนมข้อมูล, การหวังผลทางการเมือง, การทำลายระบบฐานข้อมูล, การปฏิบัติการข่าวสาร การค้า หรืออาจถึงขั้นการก่อการร้าย และการทำลายหน่วยงานที่เป็นโครงสร้างหลักพื้นฐานที่สำคัญของประเทศ ซึ่งสามารถส่งผลกระทบที่รุนแรงต่อความมั่นคงทางเศรษฐกิจและความมั่นคงของประเทศได้

ปัญหาการโจมตีทางไซเบอร์ในปัจจุบันมีรูปแบบใดบ้าง

จากศึกษารูปแบบการโจมตีทางไซเบอร์ในปัจจุบันมีหลายรูปแบบ มีการพัฒนาอยู่ตลอดเวลา ทวีความรุนแรงและซับซ้อนมากยิ่งขึ้นเรื่อย ๆ อย่างเช่น การสอดแนมข้อมูลผ่านอุปกรณ์ประเภท “IoT”(Internet of Things), การแพร่ระบาดของไวรัสเรียกค่าไถ่ (Ransomware), การโจมตีระบบแม่ข่ายคอมพิวเตอร์ให้ปฏิเสธหรือหยุดการให้บริการ “DDoS”(Distributed Denial-of-Service) และยุทธการทางข้อมูลข่าวสาร “IO” (Information Operation) การแพร่กระจายข้อมูลข่าวสารที่จัดทำขึ้นอย่างแนบเนียน (Fake News และ Deepfakes) เพื่อหวังผลให้เกิดการตอบสนองต่อข้อมูลข่าวสารในแนวทางที่ต้องการ เหตุการณ์ดังกล่าวเป็นเพียงตัวอย่างทั่วไปของสถานการณ์

ด้านไซเบอร์ในระดับโลก และสามารถนำสู่ความขัดแย้งระหว่างประเทศได้ในอนาคต ทั้งนี้สามารถจำแนกประเภทของการโจมตีทางไซเบอร์ในปัจจุบัน[17,43 ผนวก ก.] ได้ดังนี้

1. เนื้อหาที่เป็นภัย Abusive Content

2. โปรแกรมไม่พึงประสงค์ (Malicious Code)

3. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)

4. ความพยายามบุกรุก เข้าระบบ (Intrusion Attempts)

5. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)

6. การโจมตี สภาพความพร้อมใช้งาน ของระบบ (Availability)

7. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Content Security)

8. การฉ้อฉล ฉ้อโกงหรือหลอกลวง เพื่อผลประโยชน์ (Fraud)

9. การละเมิดนโยบายขององค์กร Policy Violation

10. ช่องโหว่ (Vulnerability); การโจมตีช่องโหว่ Log4Shell[12] การโจมตีแบบ Zero-day[13] การโจมตีด้วย STUXNET-WORM[19,20,ภาพประกอบที่4 ผนวก ก.และค.] และ Cryptojacking[22]

วิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ระดับโลก

จากการศึกษาผู้วิจัยพบว่าประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีและความพร้อมทางด้านไซเบอร์ต่างใช้ขีดความสามารถทางไซเบอร์ทั้งทางตรงและทางอ้อม เพื่อให้ได้เปรียบต่อประเทศอื่น เช่น การพยายามให้ได้มาซึ่งข้อมูลหรือการจารกรรมข้อมูลเพื่อวัตถุประสงค์ต่าง ๆ เพื่อให้ได้เปรียบทางการเมืองหรือทางการทหาร หรือแม้แต่การใช้ขีดความสามารถทางไซเบอร์มุ่งโจมตีต่อระบบสารสนเทศที่ใช้ควบคุมการทำงานของโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ระบบไฟฟ้า, ระบบประปา, ระบบท่อก๊าซ, ระบบสื่อสารโทรคมนาคม และอื่น ๆ เพื่อให้เกิดผลกระทบต่อการใช้ชีวิตของ

ประชาชน การกระทำดังกล่าวจะส่งผลกระทบโดยตรงต่อความน่าเชื่อถือ ภาพลักษณ์ เศรษฐกิจ สังคมต่อองค์กรนั้น ๆ หากแต่ยังส่งผลกระทบที่รุนแรงต่อประเทศด้วยเช่นกัน

การกำหนดระดับภัยคุกคามทางไซเบอร์ของสหประชาชาติ

ผู้ทำวิจัยได้ศึกษาสหภาพโทรคมนาคมระหว่างประเทศ (The Telecommunication Union "ITU")[4] ซึ่งเป็นหน่วยงานระดับนานาชาติภายใต้สหประชาชาติ ได้จัดอันดับความมั่นคงปลอดภัยไซเบอร์ของโลก โดยพิจารณาจากความพร้อม 5 ด้านที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือ (1) ด้านกฎหมาย (Legal Measures), (2) ด้านเทคนิค (Technical Measures), (3) การจัดองค์กร (Organizational Measures), (4) การพัฒนาบุคลากร (Capacity Building) และ(5) ความร่วมมือ (Cooperation) พบว่าประเทศที่มีความพร้อมทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Global scores and rank "GCI") โดย 3 ลำดับแรก ได้แก่ สหรัฐอเมริกา, สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ (ประเทศอังกฤษ) และราชอาณาจักรซาอุดิอาระเบีย ตามลำดับ

การกำหนดระดับภัยคุกคามทางไซเบอร์ของสหภาพยุโรป

ผู้ทำวิจัยได้ศึกษาหน่วยงานด้านความปลอดภัยทางไซเบอร์ของสหภาพยุโรป (The European Union Agency for Cybersecurity "ENISA") พบว่าเป็นหน่วยงานที่ถ่ายถอดองค์ความรู้และรับผิดชอบงานด้านความมั่นคงปลอดภัยไซเบอร์ในสหภาพยุโรป ให้คำแนะนำและแนวทางแก้ไขตลอดจนปรับปรุงความสามารถในการรักษาความปลอดภัยทางไซเบอร์สำหรับในกลุ่มประเทศสมาชิก นอกจากนี้ยังสนับสนุนการพัฒนาการตอบสนองความร่วมมือต่อเหตุการณ์หรือวิกฤตด้านความปลอดภัยทางไซเบอร์ข้ามพรมแดนขนาดใหญ่ตั้งแต่ปี พ.ศ.2562 เป็นต้นมาและปัจจุบันได้เผยแพร่รายงาน ENISA Threat Landscape Report 2021[21] ซึ่งเป็นการสรุปภาพรวมสถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในภูมิภาคยุโรป ตั้งแต่เดือน เมษายน 2563 จนถึงกลางเดือนกรกฎาคม 2564 ทาง ENISA ให้ข้อมูลสถิติของภัยคุกคามทางไซเบอร์ที่พบมากที่สุดในสหภาพยุโรป 3 อันดับแรก ได้แก่ การโจมตีแรนซัมแวร์ (Ransomware) เพื่อเรียกค่าไถ่ด้วยบิตคอยน์ (Bitcoin) หรือสกุลเงินคริปโต (Cryptocurrency), การโจมตีด้วยมัลแวร์ Malware และCryptojacking[22, ผนวก ก.] โดยเมื่อดูภาพรวมสถิติที่มีการโจมตีหน่วยงานที่

เป็นโครงสร้างพื้นฐานหลักในสหภาพยุโรป 3 อันดับแรกของหน่วยงานที่ถูกโจมตีได้แก่ หน่วยงานการให้บริการของภาครัฐ หน่วยงานให้บริการด้านดิจิทัล และ หน่วยงานที่เกี่ยวข้องกับสาธารณชน อย่างไรก็ตามจากสถานการณ์ดังกล่าวก็ทำให้บริษัทต่าง ๆ เริ่มให้ความสำคัญและเตรียมความพร้อมเพื่อรับมือภัยคุกคามทางไซเบอร์มากขึ้น[21]

การกำหนดระดับภัยคุกคามทางไซเบอร์ของประเทศสหรัฐอเมริกา

ผู้ทำวิจัยได้ค้นคว้าข้อมูลการกำหนดระดับภัยคุกคามทางไซเบอร์ของประเทศสหรัฐ ทำให้พบว่าเมื่อ 12 พฤษภาคม 2564 ประธานาธิบดี โจ ไบเดน สหรัฐอเมริกา ลงนามคำสั่งประธานาธิปดีในการยกระดับมาตรการป้องกันการโจมตีไซเบอร์รัฐบาลกลาง และหน่วยงานต่างๆ ในประเทศให้คุมเข้มมากยิ่งขึ้น หลังเกิดกรณีการโจมตีแรนซัมแวร์ (Ransomware) เรียกค่าไถ่บริษัทผู้ดูแลท่อส่งน้ำมันที่ใหญ่ที่สุดบริเวณชายชายฝั่งตะวันออกของสหรัฐฯ อย่าง Colonial Pipeline Co. จนนำไปสู่เหตุการความวุ่นวายและปัญหาการขาดแคลนน้ำมันที่เกิดขึ้นในช่วงระยะหนึ่ง

รายละเอียดในแถลงการณ์ของทำเนียบขาวสหรัฐฯ ระบุว่า สาเหตุของการลงนามในคำสั่งฉบับนี้ เนื่องจากที่ผ่านมาบริษัทหลายแห่งในสหรัฐฯ ไม่ว่าจะเป็น SolarWinds, Microsoft Exchange (Microsoft) และล่าสุด Colonial Pipeline ล้วนตกเป็นเป้าการโจมตี และตอกย้ำรัฐบาลสหรัฐฯ ว่าภาครัฐและเอกชนต้องเผชิญกับภัยคุกคามทางไซเบอร์หลากหลายรูปแบบอย่างต่อเนื่องและตลอดเวลา หากการป้องกันทางไซเบอร์ที่ไม่ดีพอก็จะเป็นช่องโหว่ที่ทำให้เกิดการโจมตีได้อีกในอนาคต จึงออกคำสั่งพิเศษมุ่งเน้นไปที่การยกระดับการป้องกันภัยไซเบอร์ของโครงข่ายรัฐบาลกลางให้ล้ำสมัยและให้เกิดความมั่นคงปลอดภัยมากยิ่งขึ้น ครอบคลุมไปถึงการเพิ่มความร่วมมือในกรณีการแชร์ข้อมูลข่าวสารระหว่างรัฐบาลและเอกชนถึงประเด็นภัยคุกคามทางไซเบอร์อื่นๆที่เกี่ยวข้อง และการเพิ่มอำนาจของสหรัฐฯ ในการตอบโต้กับการโจมตีทางไซเบอร์ที่ต้องเผชิญ[5,11]

ทั้งนี้เมื่อ 21 มีนาคม 2565 ประธานาธิบดี โจ ไบเดน สหรัฐอเมริกา ให้คำแถลงการณ์เรื่องความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ พิจารณาความเป็นไปได้ที่จะถูกสหพันธรัฐรัสเซียคุกคามทางไซเบอร์ จึงเสริมความแข็งแกร่งให้กับการป้องกันทางไซเบอร์ของประเทศ โดยกำหนดมาตรการรักษาความปลอดภัยทางไซเบอร์ที่ครอบคลุมสำหรับรัฐบาลกลางและภาคโครงสร้างพื้นฐานที่สำคัญ และสร้างความร่วมมือระหว่างภาครัฐและ

เอกชนที่เป็นนวัตกรรมและความคิดริเริ่ม เพื่อเพิ่มความปลอดภัยในโลกไซเบอร์ทั้งหมด โครงสร้างพื้นฐานที่สำคัญของชาติ และให้บริษัทต่างๆ รายงานเหตุการณ์ทางไซเบอร์ต่อรัฐบาลสหรัฐอเมริกาได้โดยตรง ทั้งนี้ก็เพื่อยับยั้ง ขัดขวาง การโจมตีทางไซเบอร์กับโครงสร้างพื้นฐานหลักที่สำคัญของชาติ โดยเร่งความพยายามในการล็อกประตูดิจิทัลของตนเพื่อป้องกันการโจมตีทางไซเบอร์ สหรัฐมีหน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (Cybersecurity & Infrastructure Security Agency "CISA")[7] ของ กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) เป็นองค์กรหลักในการบูรณาการร่วมกันระหว่างภาครัฐ ภาคเอกชนในเรื่องของโครงสร้างพื้นฐานหลัก เพื่อแบ่งปันข้อมูลอย่างรวดเร็วและรับคำแนะนำในการบรรเทาผลกระทบเพื่อช่วยปกป้องระบบและเครือข่ายที่เป็นโครงสร้างพื้นฐานหลักของประเทศ ทุกหน่วยงานที่เกี่ยวข้องต้องเตรียมรับมือกับภัยคุกคามที่กำหนดไว้ในยุคของปัจจุบัน ความระมัดระวังและความเร่งด่วนของทุกหน่วยงานที่เกี่ยวข้องในวันนี้สามารถป้องกันหรือบรรเทาการโจมตีได้ในวันพรุ่งนี้ได้[6]

จากแถลงการณ์ทั้งสองเรื่องข้างต้นแสดงถึงสหรัฐอเมริกาให้ความสำคัญต่อภัยคุกคามทางไซเบอร์ว่าเป็นอันตรายต่อความมั่นคงของชาติ เป็นภัยร้ายแรงสร้างความเสียหายในวงกว้างกระทบต่อพลเมืองเป็นจำนวนมาก ผู้วิจัยจึงทำการศึกษาหน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ[ผนวก จ. ภาพประกอบที่ 6] (Cybersecurity & Infrastructure Security Agency "CISA")[47] ซึ่งเป็นหน่วยงานหลักและได้กำหนดระดับภัยคุกคามไซเบอร์ที่มีผลต่อโครงสร้างพื้นฐานหลักของประเทศไว้ 5 ระดับ[7] ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติ (National Government) คือ ภัยที่เป็นอันตรายต่อประเทศชาติเป็นการปล่อยข่าวที่ไม่น่าเชื่อถือ การเข้าไปโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ในหน่วยงานของรัฐ หรือการเจาะระบบของโครงสร้างพื้นฐานที่เป็นระบบการเงินการธนาคาร และระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบประปา ซึ่งให้บริการกับประชาชนในประเทศ

2. ภัยจากการก่อการร้ายสากล (Terrorists) โดยเฉพาะกลุ่มก่อการร้ายต้องการโจมตีต่อประเทศคู่ขัดแย้ง ทางการเมือง มุ่งทำลายผลประโยชน์ทางการเมือง เพื่อสร้างความหวาดกลัวไปยังประชาชนในประเทศนั้น ๆ

3. ภัยจากสายลับหรือพวกจารกรรมข้อมูลในภาคอุตสาหกรรม และองค์กรเครือข่ายอาชญากรรม (Industries Spies and Organized Crime Groups) ซึ่งภัยด้านนี้จะกำหนดให้เป็นภัยคุกคามระดับกลางของประเทศ

4. ภัยจากกลุ่มแฮกเกอร์ (Hacktivist) ที่มีอุดมการณ์ซึ่งเกิดจากการรวมกลุ่มของพวกแฮกเกอร์ร่วมกันโจมตีเว็บไซต์ของรัฐบาลโดยมีแรงจูงใจจากอุดมการณ์ทางการเมืองหรือความคิดเห็นที่แตกต่างทางการเมือง เพราะกลุ่มแฮกเกอร์เหล่านั้นเห็นว่ารัฐหรือหัวหน้ารัฐบาลในประเทศนั้นๆ ได้ดำเนินนโยบายที่ขัดต่อสิทธิเสรีภาพในการแสดงออกหรือลิดรอนสิทธิเสรีภาพของบุคคล และการปิดกั้นสิทธิเสรีภาพทางการเมืองของประชาชน

5. ภัยจากกลุ่มแฮกเกอร์มือสมัครเล่น (Hackers) โดยกลุ่มแฮกเกอร์จะประชาสัมพันธ์ทางเว็บไซต์เพื่อรวบรวมพวกมือสมัครเล่นให้ร่วมกันโจมตีเว็บไซต์ของหน่วยงานภาครัฐ ภาคเอกชน และส่งผลกระทบอย่างกว้างขวางจนสร้างความเสียหายในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติที่ถูกโจมตีได้อย่างมหาศาล

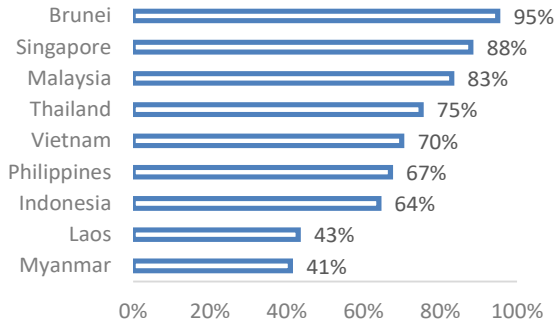
กล่าวโดยสรุปภัยคุกคามทางไซเบอร์ทั้ง 5 ประการได้เกิดขึ้นในประเทศมหาอำนาจทางทหารอย่างสหรัฐฯ กลุ่มประเทศในสหภาพยุโรป และตะวันออกกลางตลอดเวลา ทั้งที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศอย่างมาก จากภัยคุกคามที่เกิดขึ้นนี้สามารถนำมาเป็นบทเรียนและปรับใช้กับประเทศไทยที่ต้องการยกระดับและเพิ่มศักยภาพในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้เป็นอย่างดี

วิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ระดับภูมิภาค

จากการศึกษาสภาวะแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับภูมิภาคอาเซียนพบว่าสหภาพโทรคมนาคมระหว่างประเทศ (The Telecommunication Union “ITU”) ของสหประชาชาติได้จัดลำดับประเทศในกลุ่มเอเชียแปซิฟิกที่มีความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ (Global scores and rank “GCI”) โดย สาม

ลำดับแรก ได้แก่ สาธารณรัฐเกาหลี (เกาหลีใต้), สาธารณรัฐสิงคโปร์ และ ประเทศมาเลเซีย ตามลำดับ โดยประเทศไทยจัดอยู่ในลำดับที่ 9 จากจำนวนทั้งสิ้น 37ประเทศ[4]

ผู้วิจัยได้ค้นคว้าข้อมูลจากองค์การตำรวจอาชญากรรมระหว่างประเทศฝ่ายภูมิภาคอาเซียน (Interpol)[8] ซึ่งมีการศึกษาจำนวนผู้ใช้อินเทอร์เน็ตในภูมิภาคอาเซียนตั้งแต่ปี พ.ศ. 2563 ถึงปัจจุบัน พบว่าหลายประเทศในภูมิภาคอาเซียนมียอดผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นกว่า 63 เปอร์เซ็นต์ถือได้ว่าเติบโตเร็วที่สุดในโลกในยุค Covid-19



ภาพประกอบที่ 5 เปอร์เซ็นต์จำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้น พ.ศ.2563 ในกลุ่มประเทศสมาชิกอาเซียน

องค์การตำรวจอาชญากรรมระหว่างประเทศ ฝ่ายภูมิภาคอาเซียน (Interpol) ได้สรุปภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อภูมิภาคอาเซียนมากที่สุดตามลำดับ ได้แก่ 1.การหลอกลวงเพื่อผลประโยชน์ (Fraud) เป็นภัยคุกคามอันดับหนึ่งของภูมิภาค อย่าง 1.1)แก๊งคอลเซ็นเตอร์ Vishing หรือ Voice-Phishing ซึ่งมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์ ส่วน Smishing หรือ Short Message Service-Phishing เป็นการหลอกลวงโดยใช้ข้อความสั้น SMS เช่น การได้รับ SMS อ้างว่ามาจากธนาคารเพื่อแจ้งลูกค้าว่าบัญชีของท่านถูกระงับ กรุณาติดต่อกลับที่ 1.2)การหลอกลวงที่มีเป้าหมายชัดเจน Spear-phishing และ Whaling และรองลงมาคือ 2.การโจมตีแรนซัมแวร์ (Ransomware) เพื่อเรียกค่าไถ่ด้วยบิตคอยน์ (Bitcoin) หรือสกุลเงินคริปโต (Cryptocurrency) ด้วยเหตุนี้การสร้างความร่วมมือระดับภูมิภาคอาเซียนและความร่วมมือระหว่างประเทศเพื่อรับมือกับภัยคุกคามไซเบอร์และอาชญากรรมทางไซเบอร์ (Forge international and ASEAN cooperation to counter cyber threats and cybercrime)[55,56,57] เป็นสิ่งสำคัญ โดยเฉพาะการพัฒนาบุคลากรด้านไซเบอร์ การเพิ่ม

ประสิทธิภาพให้กับกระบวนการรายงานและการรับมือ การอาศัยความร่วมมือกับเครือข่าย การทำงานและการพัฒนาขีดความสามารถในการรับมือกับอาชญากรรมทางไซเบอร์ร่วมกันระหว่างประเทศ[8,55,56,57]

จากข้อมูลข้างต้นผู้วิจัยได้วิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ระดับภูมิภาคที่ปัจจุบันยังมีความขัดแย้งในภูมิภาคเอเชีย และการดำเนินยุทธศาสตร์ อินโดแปซิฟิก (Indo-Pacific Strategy) ของประเทศสหรัฐฯ ที่ต้องการร่วมมือกับประเทศพันธมิตรเพื่อพัฒนาแนวทางร่วมกันในการใช้เทคโนโลยีที่สำคัญ ตลอดจนอินเทอร์เน็ตและไซเบอร์สเปซ การเสริมสร้างระบบอินเทอร์เน็ตที่เปิดกว้าง ใช้งานร่วมกันได้ เชื่อถือได้และปลอดภัย รวมถึงประสานงานและการฝึกร่วมกับมิตรประเทศเพื่อให้เกิดองค์การมาตรฐานสากล ส่งเสริมมาตรฐานเทคโนโลยีที่เป็นไปตามฉันทามติและสอดคล้องกัน อีกทั้งอำนวยความสะดวกในการขับเคลื่อนนักวิจัยและเปิดการเข้าถึงข้อมูลทางวิทยาศาสตร์เพื่อการร่วมมือทำงานที่ทันสมัยต่อสถานการณ์ปัจจุบัน ตลอดจนดำเนินการนำกรอบปฏิบัติที่มีความรับผิดชอบและบรรทัดฐานที่เกี่ยวข้องไปปฏิบัติจริงในไซเบอร์สเปซ[9]

ผู้วิจัยสามารถสรุปได้ว่ามีความเป็นไปได้อย่างยิ่งที่อาจเป็นหนึ่งปัจจัยที่สามารถนำไปสู่การใช้ขีดความสามารถทางไซเบอร์คุกคามต่อกันตามความขัดแย้งของมิตรประเทศ เช่นในการแย่งชิงกรรมสิทธิ์บนหมู่เกาะในทะเลจีนใต้ การแข่งขันด้านเศรษฐกิจของประเทศมหาอำนาจในกลุ่มเอเชียตะวันออกเฉียงใต้ การพยายามขยายผลจากความขัดแย้งตามพื้นที่ชายแดนเพื่อให้เกิดภาพลักษณ์ที่เป็นลบต่อประเทศไทยเป็นต้น การที่ประเทศไทยมีบทบาททางด้านการเมืองระหว่างประเทศมากขึ้น รวมถึงการเป็นศูนย์กลางทางเศรษฐกิจและคมนาคมขนส่งในภูมิภาคอาเซียน ประจวบกับการได้รับความสนใจจากประเทศจีนและอินเดียในการเข้ามาขยายความสัมพันธ์ทางการค้าการรวมกลุ่มกันเป็นประชาคมเศรษฐกิจอาเซียน การเคลื่อนย้ายแรงงานอย่างเสรีในภูมิภาค ตลอดจนการเปลี่ยนแปลงขั้วอำนาจทางเศรษฐกิจที่อำนาจทางเศรษฐกิจของภูมิภาคเอเชียมีพลังมากขึ้น นอกจากนี้ภูมิภาคเอเชียตะวันออกเฉียงใต้ยังมีปัญหาความขัดแย้งทางวัฒนธรรมหรืออุดมการณ์ร่วมกันของกลุ่มคน การเชื่อมโยงระหว่างกลุ่มก่อการร้ายภายในภูมิภาคกับกลุ่มก่อการร้ายสากลที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงปลอดภัยไซเบอร์

ระหว่างประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ จึงเป็นเหตุให้ต้องตระหนักถึงสิ่งที่อาจเกิดขึ้นและควรเตรียมการรับมือ

วิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ระดับประเทศ

ผู้ทำวิจัยได้ค้นคว้าข้อมูลทำให้พบว่าปัจจุบันรัฐบาลให้ความสำคัญกับการพัฒนาและส่งเสริมทุกภาคส่วนให้มีการนำเทคโนโลยีดิจิทัลมาเป็นองค์ประกอบสำคัญในการขับเคลื่อนเพื่อเข้าสู่ยุครัฐบาลดิจิทัลและนำการปฏิรูปประเทศไปสู่การเป็นประเทศไทย 4.0 เพื่อสร้างระบบเศรษฐกิจและสังคมของประเทศที่ขับเคลื่อนด้วยนวัตกรรมและเทคโนโลยี[54,77,78,79] จากการจัดอันดับของสหภาพโทรคมนาคมระหว่างประเทศ หรือ The Telecommunication Union “ITU” ของสหประชาชาติ ได้จัดลำดับให้ประเทศไทยอยู่ในลำดับที่ 44 จากจำนวนทั้งสิ้น 182 ประเทศ[4] ส่งผลทำให้เป็นอีกหนึ่งปัจจัยที่ประเทศจะมีความเสี่ยงสูงขึ้นที่จะตกเป็นเป้าหมายในการก่อการร้ายทางไซเบอร์อย่างหลีกหนีไม่ได้ ผู้วิจัยได้ศึกษาสถิติภัยคุกคามไซเบอร์ของประเทศไทย[15] ตั้งแต่ปีพ.ศ.2560-2564 ดังตาราง

สถิติภัยคุกคาม ประจำปี พ.ศ. 2560-2564 (2017-2021)						
ประเภทภัยคุกคาม / ปี	**2560 (2017)**	**2561 (2018)**	**2562 (2019)**	**2563 (2020)**	**2564 (2021)**	**รวม**
Abusive content	-	1	124	4	14	143
Availability	540	-	79	101	5	725
Fraud	841	929	912	576	212	3,470
Information gathering	8	-	60	46	248	362
Information security	68	18	165	46	30	327
Intrusion Attempts	939	1,102	467	145	224	2,877
Intrusions	570	335	218	173	183	1,479
Malicious code	271	127	436	687	479	2,000
Vulnerability	-	-	-	471	674	1,145
Other	-	8	9	1	-	18
รวม	3,237	2,520	2,470	2,250	2,069	**12,546**

ตารางที่ 1 สถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ThaiCERT, ETDA

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

จากตารางพบว่าการละเมิดความเป็นส่วนตัวของข้อมูล[67] คือเป้าหมายหลักในการเกิดภัยคุกคามต่าง ๆซึ่งมักจะเป็นการขโมยข้อมูลส่วนบุคคลเพื่อนำไปใช้ในทางที่ผิดกฎหมาย อย่างการหลอกลวงเพื่อผลประโยชน์ Fraud เป็นภัยคุกคามความมั่นคงของประเทศเป็นอันดับหนึ่ง ด้วยเทคนิคการหลอกลวง Phishing ที่ใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลอื่น ๆ และนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน แก๊งคอลเซ็นเตอร์ Vishing และ Smishing เป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์และข้อความสั้น SMS การหลอกลวงที่มีเป้าหมายชัดเจน Spear-phishing และ Whaling อย่างองค์กร หรือบุคคลที่เป็นเป้าหมาย ส่วนใหญ่จะเป็นผู้ที่มีบทบาทสำคัญในองค์กร มีความสามารถหรือรู้วิธีการเข้าถึงข้อมูลสำคัญขององค์กร รวมถึงการพยายามเจาะข้อมูลองค์กรและการโจมตีด้วย มัลแวร์ (Malware) ประเภทเรียกค่าไถ่ (Ransomware) มีความรุนแรงมากยิ่งขึ้นถึงแม้จะมีระบบรักษาความปลอดภัยที่ดีแล้วก็อาจจะถูกโจมตีได้ผนวก ก.

นอกจากนี้เหตุจูงใจให้มีการโจมตีภัยทางไซเบอร์ของประเทศไทยไม่ใช่เฉพาะผลประโยชน์ทางการเงินเท่านั้น แต่ยังใช้เป็นเครื่องมือในการแสดงออกทางการเมืองของภาคประชาชน เช่น เหตุการณ์กลุ่ม F5 Army ที่โจมตีเว็บไซต์ของหน่วยงานภาครัฐด้วยการสร้างปริมาณ Traffic/Packet ที่ผิดปกติเพื่อก่อกวนในระบบ Network (Flood Network) หรือการ DoS (Denial of Service) รูปแบบหนึ่ง ทำให้มีการรับหรือส่ง Traffic เป็นจำนวนมาก ทำให้ระบบต้องทำงานหนักจากการบล็อคหรือป้องกัน Traffic ที่ผิดปกติจนส่งผลกระทบให้การใช้งานระบบช้าลงและหยุดทำงานในที่สุด ทั้งนี้เนื่องจากกลุ่มผู้ที่ต้องการแสดงออกมีความหวาดระแวงว่ารัฐบาลจะดำเนินการในเรื่อง Single gateway เพื่อดักรับข้อมูลของประชาชนบนอินเทอร์เน็ต การกระทำดังกล่าวเป็นการแสดงออกเชิงสัญลักษณ์ ซึ่งส่งผลกระทบต่อเศรษฐกิจ ความเชื่อมั่นและความน่าเชื่อถือในการขับเคลื่อนประเทศไทยในยุคดิจิทัลผนวก ข.

ทำให้ประเทศไทยมีความจำเป็นต้องเร่งรัดในการดำเนินแผนและพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อเป็นการรับมือ ปกป้องและลดความเสี่ยงจากภัยคุกคามและผลกระทบทางไซเบอร์ทั้งจากภายในและภายนอกประเทศที่สามารถส่งผลกระทบ[11,18, ผนวก ข.] ต่อความมั่นคงของภาครัฐ อย่างกรณีที่พบว่ามีข้อมูลการ

ปฏิบัติงานของเจ้าหน้าที่และแฟ้มของแพทย์ในการตรวจผู้ป่วยซึ่งมีฐานข้อมูล 10,095 ราย พร้อมชื่อ นามสกุล หมายเลขโทรศัพท์และรายละเอียดการเข้าออกโรงพยาบาลของกระทรวงสาธารณสุขถูกประกาศขายผ่านสื่อออนไลน์[16] ความมั่นคงทางเศรษฐกิจ อย่างเมื่อปี พ.ศ.2561 พบว่าความเสียหายทางเศรษฐกิจในประเทศไทยที่เป็นผลกระทบมาจากความมั่นคงปลอดภัยทางไซเบอร์สามารถส่งผลถึง 2.86 แสนล้านบาทหรือ 2.2 เปอร์เซ็นต์ของผลิตภัณฑ์มวลรวมของประเทศ ซึ่งคิดเป็นมูลค่า 14,360 ล้านล้านบาท[10] ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

ยุทธศาสตร์การจัดการภัยคุกคามทางไซเบอร์ทางการทหารและของประเทศมีอะไรบ้าง

ผู้วิจัยได้ทำการศึกษาและพบความสอดคล้องทางยุทธศาสตร์ชาติ และจำแนกแผนที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ ออกเป็น 3 ระดับ ประกอบด้วย

(1) ยุทธศาสตร์ชาติ

(2) แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนปฏิรูปประเทศ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ แผนความมั่นคง

(3) แผนปฏิบัติราชการของส่วนราชการ แผนปฏิบัติด้าน...เพื่อถ่ายทอดเป้าหมายและตัวชี้วัด รวมทั้งแนวทางการพัฒนาสู่การดำเนินการของหน่วยงาน ทางการพัฒนาสู่การดำเนินการของหน่วยงานอย่างเป็นระบบ

แผนระดับที่ 1

ยุทธศาสตร์ชาติ ระยะ 20 ปี พ.ศ. 2561-2580[58] เป็นเป้าหมายในการพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาล เพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกัน อันจะก่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว โดยประกอบด้วย 6 ยุทธศาสตร์ ได้แก่ 1)ยุทธศาสตร์ชาติด้านความมั่นคง 2) ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน 3)ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ 4)ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม 5)ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็น

มิตรต่อสิ่งแวดล้อมและ 6)ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

โดยมีประเด็นที่เกี่ยวข้องกับภัยคุกคามไซเบอร์และความมั่นคงปลอดภัยไซเบอร์อยู่ใน 2 ยุทธศาสตร์ คือ ยุทธศาสตร์ที่ 1 ด้านความมั่นคงและ ยุทธศาสตร์ที่ 2 ด้านการสร้างความสามารถในการแข่งขัน

แผนระดับที่ 2

1. แผนแม่บทภายใต้ยุทธศาสตร์ชาติ[58] 1)ประเด็นด้านความมั่นคง[68] 2)ประเด็นอุตสาหกรรมและบริการแห่งอนาคต 3)ประเด็นด้านโครงสร้างพื้นฐาน ระบบโลจิสติกส์[69] และดิจิทัลและ 4)ประเด็นการวิจัยและพัฒนานวัตกรรม

2. แผนปฏิรูปประเทศ ด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

3. แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 ยุทธศาสตร์ที่ 5 : การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน ยุทธศาสตร์ที่ 7 : การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์และ ยุทธศาสตร์ที่ 10 ความร่วมมือระหว่างประเทศเพื่อการพัฒนา

4. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ พ.ศ. 2562-2565 นโยบายความมั่นคงแห่งชาติที่ 10 เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์, นโยบายความมั่นคงแห่งชาติที่ 14 เสริมสร้างและพัฒนาศักยภาพ การป้องกันประเทศเพื่อพัฒนาศักยภาพการเตรียมความพร้อมของชาติในการเผชิญกับภาวะสงครามและวิกฤตการณ์ ความมั่นคงอย่างมีเอกภาพและประสิทธิภาพและ นโยบายความมั่นคงแห่งชาติที่ 16 เสริมสร้างดุลยภาพในการดำเนินความสัมพันธ์ระหว่างประเทศ

แผนระดับที่ 3

1. แผนเตรียมพร้อมแห่งชาติ (พ.ศ. 2560-2564) ยุทธศาสตร์ที่ 3 การเสริมสร้างความร่วมมือ การเตรียมพร้อมรับมือภัยคุกคามกับต่างประเทศ[71]

2. ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ 2560-2564) ทั้ง 8 ยุทธศาสตร์ สำนักงานสภาความมั่นคงแห่งชาติ[70]

ประเด็นยุทธศาสตร์ที่ 1 เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์[72]

ประเด็นยุทธศาสตร์ที่ 3 ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ 4 เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ 5 สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ 6 เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ 7 ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ 8 ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ในระดับภูมิภาคและระดับนานาชาติ

3. นโยบายละแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ 2561-2580)[69] เป็นแผนแม่บทหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศ ระยะ 20 ปี ที่กำหนดทิศทางการขับเคลื่อนการพัฒนาประเทศที่ยั่งยืนโดยใช้เทคโนโลยีดิจิทัล ซึ่งมีความสอดคล้องกับยุทธศาสตร์ชาติ และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ด้วย 6 ยุทธศาสตร์ ได้แก่ ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ, ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล, ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล, ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล, ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล, ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

4. แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ 5 ปี (พ.ศ. 2561 -2565)[74] เป้าหมาย : 5. สร้างความเชื่อมั่น โดยการขจัด ภัยคุกคามไซเบอร์การโจมตีเว็บไซต์ หน่วยงานภาครัฐ เนื้อหาไม่เหมาะสม ทางอินเทอร์เน็ต กลโกงออนไลน์/การฉ้อโกง รูปแบบใหม่ๆ ตลอดจนสร้างความเชื่อมั่น ให้กับภาคธุรกิจและประชาชนในการทำธุรกรรมออนไลน์และ เป้าหมาย : 6. พัฒนากำลังคนดิจิทัล โดยการพัฒนา ทักษะด้านดิจิทัลให้กับทุกอาชีพ เพื่อเพิ่มผลิตภาพแรงงานและการสร้างธุรกิจ รูปแบบใหม่และพัฒนาทักษะด้านดิจิทัล ของข้าราชการและบุคลากรภาครัฐ ตลอดจน สร้างความตระหนักให้ประชาชนใช้เทคโนโลยีดิจิทัลอย่างสร้างสรรค์[72]

จากการศึกษาแผนทั้ง 3 ระดับทำให้ทราบถึงยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ทางการทหารความสำคัญของแผนปฏิบัติราชการของส่วนราชการที่ได้รับการถ่ายทอดเป้าหมายและตัวชี้วัดมาจากแผนที่ 1และ2 การที่จะรวมทั้งแนวทางการพัฒนาไปสู่การดำเนินการของหน่วยงาน หนทางการพัฒนาสู่การดำเนินการของหน่วยงานอย่างเป็นระบบเป็นสิ่งสำคัญ

เพื่อให้เข้าใจยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ทางการทหารมากยิ่งขึ้นผู้วิจัยจึงทำการศึกษายุทธศาสตร์ป้องกันประเทศ พ.ศ. 2560-2579 กระทรวงกลาโหม[73]พบว่าเป็นกรอบสำคัญที่ นขต.กห. และเหล่าทัพ ใช้ยึดถือเป็น กรอบในการกำหนดความต้องการกำลังกองทัพและการดำเนินการด้านต่าง ๆ อันจะนำไปสู่การจัดทำแผนงาน/โครงการ เพื่อเสริมสร้างกำลังกองทัพให้มีขีดความสามารถในการรองรับสถานการณ์ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยมีประเด็นยุทธศาสตร์การป้องกันประเทศที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางไซเบอร์ ด้วยการดำเนินกลยุทธ์จัดเตรียมกำลัง เสริมสร้างพัฒนาให้กองทัพมีความพร้อมในการใช้กำลัง เพื่อการป้องกัน ป้องปราม แก้ไขและยุติความขัดแย้ง รวมทั้งให้ความสำคัญต่อการเตรียมความพร้อมของกองทัพในการเผชิญกับภัยคุกคามทางไซเบอร์ของประเทศ การวิจัยและพัฒนาวิทยาศาสตร์และเทคโนโลยีเพื่อการทหารและความมั่นคง และอุตสาหกรรมป้องกันประเทศ เพื่อให้เกิดความชัดเจนมากขึ้นผู้วิจัยจึงศึกษาเพิ่มเติมในส่วนของแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม[75]

วิเคราะห์แผนการพัฒนาทางไซเบอร์เพื่อความมั่นคงกระทรวงกลาโหมด้วยเครื่องมือ SWOT Analysis และ TOWS Matrix

จากการศึกษาสภาพแวดล้อมที่เกี่ยวข้องต่อการกำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศของกระทรวงกลาโหม โดยใช้การวิเคราะห์จากจุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) กำหนดปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในองค์กรด้วย 4M (Management, Machine, Money และ Man) และใช้การวิเคราะห์ปัจจัยภายนอกที่แสดงถึงโอกาสและอุปสรรคด้วย PEST (Policy, Economic, Social และ Technology) ประกอบด้วย การวิเคราะห์ปัจจัยภายใน (Internal Factors) และปัจจัยภายนอก (External Factors) ดังนี้

การวิเคราะห์สภาพแวดล้อมภายใน (Internal Environment)

การวิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศภายในของกระทรวงกลาโหม โดยใช้การวิเคราะห์สภาพแวดล้อมภายในตามหลัก 4M Analysis สามารถสรุปแยกเป็นจุดแข็งและจุดอ่อน สรุปได้ดังนี้

1. ด้านการบริหารจัดการ (Management)

1.1 จุดแข็ง; มีนโยบายและยุทธศาสตร์ที่ชัดเจนเกี่ยวกับการพัฒนางานทางไซเบอร์, มีโครงสร้างการจัดหน่วยงานที่รับผิดชอบงานทางไซเบอร์ที่ชัดเจนในทุกส่วนราชการ, มีคณะกรรมการ คณะอนุกรรมการ คณะทำงานระดับกระทรวงกลาโหม และมีระบบสารสนเทศ นขต.กห. ที่ได้รับการรับมาตรฐาน ISO 27001 : 2013

1.2 จุดอ่อน; โครงสร้างการจัดมีความซับซ้อนมีสายการบังคับบัญชายาว ทำให้ต้องใช้เวลาค่อนข้างมากในการดำเนินงานต่าง ๆ, ยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์, ขาดการบูรณาการข้อมูลร่วมกันระหว่างหน่วยงานรวมทั้งการยืนยันความถูกต้อง สมบูรณ์และเชื่อมโยงเป็นระบบเดียวกัน และบุคลากรผู้ใช้งานระบบคอมพิวเตอร์ยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์

2. ด้านอุปกรณ์และระบบ (Machine)

2.1 จุดแข็ง; ศูนย์ไซเบอร์ของ นขต.กห. มีเครื่องมือระบบตรวจจับและป้องกันการโจมตีทางไซเบอร์ที่ครอบคลุมเครือข่ายข้อมูลทั้งหมดภายในของแต่ละ นขต.กห

, หน่วยงานไม่สนับสนุนเครื่องคอมพิวเตอร์สำหรับใช้ในการปฏิบัติงานไม่เพียงพอ ทำให้ยากต่อการควบคุมความมั่นคงปลอดภัยไซเบอร์

2.2 จุดอ่อน; การติดตั้งใช้งานโปรแกรมละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์ส่วนหนึ่งของส่วนราชการ, ระบบงานที่พัฒนาขึ้นเองบางโปรแกรม ไม่ได้สอดคล้องตามมาตรฐานการรักษาความปลอดภัยสารสนเทศ

3. งบประมาณ (Money)

3.1 จุดแข็ง; มีการจัดสรรงบประมาณด้านไซเบอร์เป็นประจำทุกปี

3.2 จุดอ่อน; งบประมาณที่ได้รับไม่เพียงพอต่อการพัฒนาด้านไซเบอร์, ขาดการวางแผนในการขอรับการสนับสนุนงบประมาณที่ทำให้การรักษาความปลอดภัยไซเบอร์มีความไม่ต่อเนื่อง

4. บุคลากร (Man)

4.1 จุดแข็ง; มีบุคลากรผู้ปฏิบัติงานไซเบอร์

4.2 จุดอ่อน; ผู้ใช้งานระบบสารสนเทศส่วนใหญ่ยังขาดความตระหนักรู้ภัยคุกคามทางไซเบอร์, บุคลากรที่มีความรู้ความสามารถระดับสูงที่บรรจุตามหน่วยงาน ไม่เพียงพอต่อความต้องการ, บุคลากรผู้ใช้งานระบบคอมพิวเตอร์ยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์

การวิเคราะห์สภาพแวดล้อมภายนอก (External Environment)

การวิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศภายนอกของกระทรวงกลาโหม โดยใช้การวิเคราะห์สภาพแวดล้อมภายนอกตามหลัก PEST Analysis สามารถสรุปแยกเป็นโอกาสและอุปสรรค สรุปได้ดังนี้

1. นโยบาย กฎระเบียบ (Policy)

1.1 โอกาส; นโยบายในระดับรัฐบาลให้ความสำคัญต่อการปรับไปสู่รัฐบาลดิจิทัล

1.2 อุปสรรค; ปัญหาในขั้นตอนการตั้งงบประมาณ และการจัดซื้อจัดจ้างที่ล่าช้า, ระเบียบราชการไม่เอื้ออำนวยในการปฏิบัติงาน ในการจัดอุปกรณ์ระบบ

สารสนเทศ ที่ทันสมัยเข้ามาใช้งาน, การเปลี่ยนแปลงระดับนโยบายส่งผลต่อการดำเนินงานตามแผนงาน โครงการต้องปรับปรุงบ่อยครั้งขาดความต่อเนื่อง

2. เศรษฐกิจ (Economic)

2.1 โอกาส; แนวทางทิศทางเศรษฐกิจรองรับการเติบโตทางด้านเทคโนโลยีดิจิทัลมากขึ้น

2.2 อุปสรรค; การระบาดของโควิด – 19 ส่งผลกระทบกับการเติมโตทางด้านเศรษฐกิจ, การปรับเปลี่ยนรูปแบบการทำงานที่ใช้ระบบสารสนเทศเข้ามามีส่วนช่วยขับเคลื่อนธุรกิจมากขึ้นจึงเป็นโอสเกิดการโจมตีทางไซเบอร์ในรูปแบบใหม่ ๆ

3. สังคม วัฒนธรรม (Social)

3.1 โอกาส; การใช้สื่อ Digital ที่เพิ่มมากขึ้นในยุคปัจจุบัน

3.2 อุปสรรค; ความไม่เข้าใจในการใช้งานเทคโนโลยีที่มีความซับซ้อนรวมถึงภัยคุกคามที่คาดไม่ถึง

4. เทคโนโลยีสารสนเทศ (Technology)

4.1 โอกาส; ความก้าวหน้าและแนวโน้มของเทคโนโลยีที่เอื้อต่อการนำมาใช้ในหน่วยงาน, มีการนำเทคโนโลยีมาประยุกต์กับงานของกระทรวงได้หลากหลายมากขึ้น และการเข้ามาของเครือข่าย Government Cloud และBig Data ทำให้มีนวัตกรรมและช่องทางใช้งานเพิ่มขึ้น

4.2 อุปสรรค; มีการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็วทำให้หลายคนปรับตัวไม่ทัน, ข้อมูลถูกบิดเบือนหลายระดับ (Fake News และ Deepfake) ในเครือข่ายสังคมออนไลน์ (social media) ที่สร้างความสับสน ขัดแย้งและความเข้าใจที่ผิดเกี่ยวกับสถาบันพระมหากษัตริย์, ภัยคุกคามทางไซเบอร์ในภาพรวมระดับนาชาติได้ทวีความรุนแรงมากยิ่งขึ้น และแนวทางทิศทางเศรษฐกิจรองรับการเติบโตทางด้านเทคโนโลยีดิจิทัลมากขึ้น

จากการวิเคราะห์ จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) ซึ่งประกอบด้วยปัจจัยภายในและปัจจัยภายนอกที่ได้รับ นำเข้าสู่การวิเคราะห์ด้วยเครื่องมือ TOWS Matrix ตามขั้นตอนเพื่อกำหนดกลยุทธ์การพัฒนาไซเบอร์ของกระทรวงกลาโหมทั้ง 4 ด้าน โดยมีรายละเอียดดังนี้

1. กลยุทธ์เชิงรุก (Strength/Opportunities)

1.1พัฒนาโครงสร้างพื้นฐานและเทคโนโลยีทางไซเบอร์อย่างเป็นระบบ ให้สามารถสนับสนุนภารกิจอย่างมีประสิทธิภาพ พร้อมทั้งส่งเสริมหน่วยงานในสังกัดใช้งานระบบสารสนเทศอย่างปลอดภัยเพื่อป้องกันการถูกโจมตีทางไซเบอร์

1.2มุ่งเน้นการพัฒนาระบบป้องกันโจมตีทางไซเบอร์โดยการสร้างความร่วมมือด้านความมั่นคงไซเบอร์ระหว่างหน่วยงาน

2. กลยุทธ์เชิงรับ (Weakness/Threat)

2.1 จัดลำดับความสำคัญ ภารกิจ/แผนงาน/โครงการ/งาน ให้มีความเหมาะสมตามสถานการณ์ เช่น ความสำคัญของภารกิจความพร้อมของกำลังพล เครื่องมือและสถานภาพด้านงบประมาณ

2.2 การบูรณาการข้อมูลข่าวสารเครื่องมือ ให้สามารถใช้งานทรัพยากรร่วมกันระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการลงทุน

3. กลยุทธ์เชิงแก้ไข (Weakness/Opportunities)

3.1 พัฒนาการบริหารจัดการงานทางไซเบอร์ในภาพรวมของกระทรวงกลาโหมให้มีความเป็นเอกภาพ มีเป้าหมายและแผนระยะยาวที่ชัดเจน เป็นแนวทางการปฏิบัติให้หน่วยในสังกัดมีแนวทางพัฒนาเป็นไปในทิศทางเดียวกัน

3.2 พัฒนาการบริหารจัดการกำลังพลสังกัดกระทรวงกลาโหมที่มีคุณวุฒิประสบการณ์ทำงานทางไซเบอร์ และเทคโนโลยีที่เกี่ยวข้องให้มีประสิทธิภาพยิ่งขึ้น

3.3 การบูรณาการใช้งานกำลังพลระหว่างหน่วยงานมีการถ่ายทอดองค์ความรู้อย่างเป็นระบบเสริมสร้างขวัญกำลังใจให้กับผู้ปฏิบัติงานอย่างเหมาะสมเพื่อนำไปสู่การพัฒนาองค์ความรู้ทางไซเบอร์ อย่างยั่งยืน

4. กลยุทธ์เชิงแก้ไข (Weakness/Opportunities)

4.1 ส่งเสริมความร่วมมือการพัฒนาขีดความสามารถของกำลังพลร่วมกับหน่วยงานภายนอกที่มีความรู้และประสบการณ์

5. กลยุทธ์เชิงป้องกัน(Strength/Threat)

5.1 สร้างบทบาทนำและมีส่วนร่วมในฐานะหน่วยงานด้านความมั่นคง เพื่อสร้างความตระหนักถึงภัยคุกคามสมัยใหม่ เสริมสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการพัฒนาขีดความสามารถในการเฝ้าตรวจ ระวังป้องกัน และแก้ไขปัญหาภัยคุกคาม ตลอดจนเสริมสร้างขีดความสามารถให้มีความพร้อมรักษาอธิปไตยและพิทักษ์รักษาผลประโยชน์ของชาติอย่างเหมาะสม

5.2 รักษาสถานะภาพระบบสารสนเทศของ นขต.กห. ที่ได้รับการรับรองมาตรฐาน ISO 27001 : 2013

5.3 ดำรงสภาพการใช้งานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศให้มีความพร้อมใช้งานสนับสนุนภารกิจได้อย่างมีประสิทธิภาพ มีความคุ้มค่าสูงสุดด้านงบประมาณ

แนวทางการดำเนินการพัฒนาไซเบอร์ของกระทรวงกลาโหม ได้แก่

1. การพัฒนาศักยภาพไซเบอร์ด้วยกรอบการดำเนินการยกระดับความพร้อมหรือขีดความสามารถของหน่วยตามมาตรฐานสากล, การพัฒนาหลักนิยมทางไซเบอร์, การสนับสนุนบุคลากรที่ปฏิบัติการทางไซเบอร์ให้มีความรู้ความสามารถที่สูงขึ้น, การสนับสนุนการพัฒนาเครื่องมือและอุปกรณ์ในการปฏิบัติการไซเบอร์

2. การปฏิบัติการไซเบอร์ของกระทรวงกลาโหมด้วยกรอบการดำเนินการในกรอบของกฎหมายของกระทรวงกลาโหม โดยการสนับสนุนการดำเนินการของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.), การข่าวกรองในมิติไซเบอร์เพื่อสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหม, การตอบสนองต่อสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์ โดยการจัดตั้งหน่วยงานรับผิดชอบทางไซเบอร์อย่างน้อย 2 หน่วย ได้แก่ หน่วยที่ทำหน้าที่ตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ที่มีต่อระบบโครงสร้างพื้นฐานวิกฤติทางไซเบอร์ทางทหารซึ่งมีชื่อทางเทคนิคว่า Cybersecurity Operations Center (CSOC) และหน่วยที่ทำหน้าที่ตรวจประเมินและทดสอบความพร้อมในการจัดการภัยคุกคามไซเบอร์หรือ ตรวจสอบความปลอดภัยทางไซเบอร์แบบสุ่ม โดยดำเนินการในช่วงก่อนเกิดเหตุภัยคุกคามทางไซเบอร์และทำหน้าที่ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นแล้ว

ซึ่งมีชื่อทางเทคนิคว่า Computer Security Incident Response Team (CSIRT) ซึ่งทำงานในภาพรวมของกระทรวงกลาโหมภายใต้ชื่อ ในขั้นต้นว่า MODCSIRT (Ministryof Defence Computer Security Incident Response Team) หรือทีมเผชิญเหตุ / ตอบสนองเหตุภัยคุกคามทางไซเบอร์ของกระทรวงกลาโหม

3. ความร่วมมือด้านความมั่นคงไซเบอร์ด้วยกรอบการดำเนินการความร่วมมือด้านการป้องกันไซเบอร์กับต่างประเทศ โดยการกำหนดเป้าหมายและจัดลำดับความเป็นได้ในการใช้ความสัมพันธ์นั้นให้เกิดประโยชน์ โดยพิจารณาขยายความร่วมมือทางไซเบอร์ในกรอบการประชุมรัฐมนตรีกลาโหมอาเซียน การแสวงความร่วมมือด้านไซเบอร์กับกระทรวงกลาโหม มิตรประเทศ และความร่วมมือทางไซเบอร์กับหน่วยงานที่เกี่ยวข้องกับกระทรวงกลาโหม เพื่อให้เกิดการฝึก การแข่งขันระดับหน่วยประจำปีในระดับ บก.ทท.และ เหล่าทัพ กับมิตรประเทศ, มีการจัดกิจกรรมการประชุมในระดับบก.ทท.และเหล่าทัพกับมิตรประเทศ, ให้เกิดความร่วมมือในประเทศระหว่างหน่วยงานความมั่นคงปลอดภัย ไซเบอร์และหน่วยงานโครงสร้างพื้นฐานสำคัญ เพื่อการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์และการฝึก การรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศและระหว่างประเทศ โดยมีหน่วยงานที่เกี่ยวข้องกับการนำแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคงกระทรวงกลาโหมไปดำเนินการ ได้แก่ สำนักงานปลัดกระทรวงกลาโหม, กองบัญชาการกองทัพไทย, กองทัพบก, กองทัพเรือและกองทัพอากาศ

โครงการที่กองทัพบกได้รับมอบหมายให้ดำเนินการที่เกี่ยวข้องกับการนำแผนการพัฒนาทางไซเบอร์ ได้แก่

1. โครงการเสริมสร้างบุคลากรด้านเทคโนโลยีดิจิทัลและไซเบอร์ของกองทัพบก,
2. โครงการดำรงขีดความสามารถการปฏิบัติการทางไซเบอร์
3. โครงการเสริมสร้างขีดความสามารถ การปฏิบัติการทางไซเบอร์สำหรับกำลังพลกองทัพบก
4. โครงการศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSOC)กองทัพบกระยะที่ 3
5. โครงการจัดตั้งชุดรับมือเหตุการณ์ ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ระดับกองทัพบกและระดับกองทัพภาค

จากผลการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) กำหนดปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในองค์กรด้วย 4M (Management, Machine, Money และ Man) และใช้การวิเคราะห์ปัจจัยภายนอกที่แสดงถึงโอกาสและอุปสรรคด้วย PEST (Policy, Economic, Social และ Technology) ประกอบด้วย การวิเคราะห์ปัจจัยภายใน(Internal Factors) และปัจจัยภายนอก (External Factors) ของกระทรวงกลาโหม

ผู้วิจัยเห็นถึงความสำคัญจากผลวิเคราะห์ในเรื่องการปรับโครงสร้างการจัดองค์กรในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ให้ลดความซับซ้อนในสายการบังคับบัญชา ซึ่งในปัจจุบันใช้เวลาค่อนข้างมากในการดำเนินงาน เพิ่มการสร้างการตระหนักรู้ให้บุคลากรที่ยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์ ขาดนโยบายในการบูรณาการข้อมูลร่วมกันระหว่างหน่วยงานภายในกระทรวงกลาโหมและหน่วยงานอื่น ๆที่เกี่ยวข้องระหว่างภาครัฐ รวมทั้งการยืนยันความถูกต้อง สมบูรณ์และเชื่อมโยงเป็นระบบเดียวกันโดยมีการแชร์ข้อมูลถึงกัน ด้วยงบประมาณที่จำกัดจึงควรเร่งแก้ไขการติดตั้งใช้งานโปรแกรมละเมิดลิขสิทธิ์ให้ลงโปรแกรมลิขสิทธิ์ถูกต้องบนเครื่องคอมพิวเตอร์ของส่วนราชการเพื่อลดปัญหาการโจมตีจากผู้ประสงค์ร้าย

พิจารณาการบูรณาการระบบงานที่พัฒนาขึ้นเองบางโปรแกรมที่ใช้ OPEN SOURCE ที่ไม่ได้สอดคล้องตามมาตรฐานการรักษาความปลอดภัยสารสนเทศควรพิจารณาเร่งหาทางแก้ไขเพื่อให้ระบบมีความเสถียรภาพและปลอดภัยมากขึ้น (ของฟรีไม่มีในโลกซึ่ง OPEN SOURCE มักเป็นช่องโหว่ให้ผู้ไม่ประสงค์ดีใช้เข้าโจมตีได้) หากขาดผู้ชำนาญการ

ดำเนินโครงการดังกล่าว ควรพิจารณาให้ผู้ชำนาญการจากต่างประเทศ[89,90]ดำเนินการแก้ไข การปรับเปลี่ยนรูปแบบการทำงานที่ใช้ระบบสารสนเทศเข้ามามีส่วนช่วยขับเคลื่อนธุรกิจ มากขึ้นจึงเป็นโอกาสเกิดการโจมตีทางไซเบอร์ในรูปแบบใหม่ ๆมากขึ้นในยุคโควิด-19

การขาดบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีความชำนาญการ ระดับสูงเป็นสิ่งสำคัญ จึงควรพิจารณาในการสร้างความตระหนักรู้ถึงภัยคุกคามทางไซ เบอร์ให้กำลังพลทุกหน่วยเพื่อลดความเสี่ยงในการถูกคุกคาม และเร่งพัฒนาองค์ความรู้ กำลังพลด้านการปฏิบัติการไซเบอร์

วิเคราะห์การดำเนินการทางไซเบอร์เพื่อความมั่นคงกองบัญชาการกองทัพไทย[76]

เพื่อเป็นการรองรับกรอบการพัฒนางานด้านดิจิทัลในภาพรวมของ กระทรวงกลาโหม กองบัญชาการกองทัพไทยได้มีการกำหนดแนวทางการดำเนินการ พัฒนาที่สอดคล้องกันจำนวน 5 ด้าน ประกอบด้วย

1. ด้านการพัฒนากำลังพลด้านเทคโนโลยีดิจิทัล เพื่อให้กำลังพลใน ภาพรวมของกองบัญชาการกองทัพไทย จำนวน 6 กลุ่ม ที่มีการจัดแบ่ง ตามแผนพัฒนา ทักษะด้านดิจิทัลบุคลากรของกระทรวงกลาโหม พ.ศ.2563 – 2570 กำหนดประกอบด้วย ผู้บริหารระดับสูง (Executive), ผู้อำนวยการ (Management), ผู้ทำงานด้านนโยบายและ งานวิชาการ (Academic), ผู้ทำงานด้านบริการ(Service), ผู้ปฏิบัติงานด้านเทคโนโลยี ดิจิทัล(Technology Specialist) และผู้ปฏิบัติงานด้านอื่น (Others) มีความรู้ ความสามารถ ประสบการณ์คุณลักษณะ และสมรรถนะ ด้านดิจิทัลที่เหมาะสม สามารถ ปฏิบัติภารกิจต่าง ๆ ได้อย่างมีประสิทธิภาพ ส่วนราชการภายใน กองบัญชาการกองทัพ ไทย มีเครื่องมือ สำหรับใช้ในการพัฒนาขีดความสามารถกำลังพล ด้านเทคโนโลยีดิจิทัล ที่ เพียงพอและเหมาะสมต่อการใช้งาน

2. ด้านการปรับปรุงโครงสร้างการจัดหน่วย และ กฎ ระเบียบ ข้อบังคับ ด้านเทคโนโลยีดิจิทัล เพื่อปรับปรุงพัฒนาโครงสร้างการจัดของหน่วย และกฎ ระเบียบ ข้อบังคับ ด้านเทคโนโลยีดิจิทัล ให้มีความเหมาะสม เสริมสร้างขวัญ กำลังใจ ให้กับ ผู้ปฏิบัติงาน สามารถสนับสนุนการดำเนินงาน ด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

3. ด้านการพัฒนาและดำรงสภาพโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล เพื่อพัฒนาและดำรงสภาพโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลประกอบด้วย

ระบบสื่อสารโทรคมนาคม ระบบงานสารสนเทศ ระบบรักษาความปลอดภัยสารสนเทศ เทคโนโลยีภูมิสารสนเทศ ฐานข้อมูล ครุภัณฑ์คอมพิวเตอร์ ให้มีความพร้อมใช้งาน มีความครอบคลุมและเพียงพอต่อการใช้งานตามภารกิจ พร้อมทั้งสนับสนุนให้เกิดการบูรณาการโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลร่วมกันระหว่างหน่วยงาน มุ่งเน้นความคุ้มค่า ลดความซ้ำซ้อน และความปลอดภัยในการใช้งาน

4. ด้านการพัฒนาและประยุกต์ใช้เทคโนโลยีดิจิทัล เพื่อประยุกต์ใช้เทคโนโลยีดิจิทัลในการดำเนินงานด้านระบบควบคุมบังคับบัญชา, ระบบสารสนเทศ เพื่อการบริหารราชการทั่วไป, เทคโนโลยีภูมิสารสนเทศ, ระบบสารสนเทศเพื่อการฝึก ให้เกิดประโยชน์สูงสุด มีการปรับปรุงพัฒนาอย่างต่อเนื่องสามารถตอบสนองภารกิจในภาพรวมของกองบัญชาการกองทัพไทย ได้อย่างมีประสิทธิภาพ ตลอดจนมีการพัฒนาระบบการให้บริการสาธารณะหรือบริการภาครัฐ ที่เหมาะสมสอดคล้องกับความต้องการของประชาชน

5. ด้านการเสริมสร้างความร่วมมือกับหน่วยงานทั้งภายในและภายนอกประเทศ เพื่อให้มีการพัฒนาและเสริมสร้างความร่วมมือกับหน่วยงานทั้งภายในและภายนอกประเทศ ให้เกิดการพัฒนาขีดความสามารถกำลังพลและยกระดับการใช้งานเทคโนโลยีดิจิทัลระดับสูง ตลอดจนมีการบูรณาการการใช้งานทรัพยากรพื้นฐานเทคโนโลยีดิจิทัลที่จำเป็นร่วมกันบนพื้นฐาน ของความปลอดภัยในการใช้งาน รวมทั้งประสานความร่วมมือด้านการวิจัย พัฒนา และผลิต ในอุตสาหกรรมป้องกันประเทศ เพื่อนำไปสู่การพึ่งพาตนเอง ลดการพึ่งพาจากต่างประเทศ เพื่อประโยชน์สูงสุดของประเทศต่อไป

ทั้งนี้เพื่อเป็นการเน้นให้เกิดการบูรณาการความเป็นมาตราฐาน ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในกระทรวงกลาโหม ในการรับมือกับสงครามไซเบอร์ พัฒนาขีดความสามารถของศูนย์บัญชาการทางทหารและระบบควบคุมบังคับบัญชาของกองทัพไทย ตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ให้สามารถควบคุม อำนวยการ สั่งการ ต่อศูนย์ปฏิบัติการเหล่าทัพ อย่างมีประสิทธิภาพโดยมุ่งเน้นการพัฒนาระบบฐานข้อมูลทางทหาร การใช้ระบบแผนที่สถานการณ์ร่วม (Common Operational Picture “COP”) และระบบรายงานแลกเปลี่ยนข้อมูลข่าวสารทางทหาร (Message Text Format “MTF”) เพื่อให้สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูล ในทุกระดับได้อย่างเป็นรูปธรรม ตลอดจนให้ความสำคัญ

กับการสร้างความเสถียรและขยายขีดความสามารถ ตามความจำเป็นอย่างเหมาะสม พร้อมกับศึกษาแนวทางการพัฒนา Joint Tactical Data Link ในภาพรวมของกองทัพไทย เพื่อใช้สนับสนุน แนวความคิดการปฏิบัติที่ใช้เครือข่ายเป็นศูนย์กลางในการขับเคลื่อน การบูรณาการระบบโทรคมนาคมทหารร่วมของกองทัพไทยให้เสมือนเป็นระบบเดียวกัน (One Network) และสอดคล้องกับความเร่งด่วนตามแผนพัฒนาประเทศ

วิเคราะห์การดำเนินการทางไซเบอร์เพื่อความมั่นคงศูนย์ไซเบอร์กองทัพบก[84]

ผู้วิจัยได้ทำการศึกษาศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ซึ่งเป็นหน่วยขึ้นตรงต่อกองทัพบก (นขต.ทบ.) ในการรองรับการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่กระทบต่อความมั่นคงของชาติทั้งภายในและภายนอกประเทศโดยมุ่งเน้นไปที่ความมั่นคงทางทหารและการรักษาความสงบเรียบร้อยภายในประเทศรวมทั้งการทำงานที่สอดประสานกับหน่วยงานในเหล่าทัพและกระทรวงกลาโหม รวมถึงการร่วมมือกับหน่วยงานของภาครัฐและภาคเอกชนตลอดจนการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations ; NCO) ประกอบด้วย

1. กองปฏิบัติการไซเบอร์ทำหน้าที่เป็นศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังแจ้งเตือนป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์การเผชิญเหตุฉุกเฉินทางไซเบอร์ตลอดจนการพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุกเพื่อให้สามารถปฏิบัติการเชิงรุกและโต้ตอบโจมตีฝ่ายตรงข้ามได้ในกรณีจำเป็น

2. กองรักษาความมั่นคงปลอดภัยไซเบอร์ทำหน้าที่เสริมสร้างความรู้ความเข้าใจสร้างความตระหนักติดตามกำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัยรวมถึงการเฝ้าระวังแจ้งเตือนภัยคุกคามการติดตามสืบค้นและตรวจสอบช่องโหว่ของระบบโดยใช้เครื่องมือระบบตรวจหาการบุกรุกรวมถึงการกู้คืนสภาพเมื่อถูกโจมตี (Recovery) รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิทัล

3. กองสนับสนุนการปฏิบัติการข่าวสารไซเบอร์เพื่อให้การสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้องโดยทำหน้าที่เฝ้าระวังแจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ที่ส่งผลกระทบต่อสถาบันและความมั่นคงของชาติรวบรวมวิเคราะห์ทิศทางแนวโน้มโครงข่ายความสัมพันธ์ของข้อมูลประเภทสื่อและกลุ่มเป้าหมาย

ติดตามสืบค้นแหล่งที่มาและเป้าหมาย และกำหนดมาตรการป้องปรามตอบโต้สกัดกั้นตลอดจนพัฒนาโปรแกรมและเครื่องมือต่างๆเพื่อรองรับงานด้านไซเบอร์นอกจากนี้ยังได้เตรียมการด้านการพัฒนาเทคโนโลยีและนวัตกรรมต่างๆด้านไซเบอร์โดยแสวงหาความร่วมมือกับหน่วยงานต่างๆทั้งภายในกองทัพบก ภาครัฐและองค์กรเอกชนในด้านวิชาการการวิจัยพัฒนา (Research and Development “R&D”) การสัมมนาเชิงปฏิบัติการ (Workshop) และการฝึกปฏิบัติต่างๆโดยเฉพาะการฝึกซ้อมแผนเผชิญเหตุทางไซเบอร์ (Cyber Incident Action Plan Exercise) การฝึกซ้อมแผนฉุกเฉินทางไซเบอร์ (Cyber Emergency) รวมถึงการประสานงานเพื่อดำเนินการตามกฎหมายกับผู้ที่โจมตีระบบเครือข่ายคอมพิวเตอร์

ในส่วนเกี่ยวข้องกับการดำเนินการตามแผนการพัฒนาทางไซเบอร์เพื่อความมั่นคงกระทรวงกลาโหม พบว่าศูนย์ไซเบอร์กองทัพบกใช้มาตรฐานในการกำหนดระดับภัยคุกคามทางไซเบอร์[7] เฉกเช่นเดียวกับประเทศสหรัฐฯ โดยได้กำหนดระดับภัยคุกคามทางทางไซเบอร์เป็น 4 ด้าน ดังนี้

1. ด้านภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศหรือ ระดับชาติผู้ที่ก่อภัยคุกคามอาจใช้วิธีนำข่าวสารเหล่านั้นลงเผยแพร่ในเว็บไซต์ของประเทศตนเองเพื่อให้ข่าวสารเหล่านั้นเผยแพร่เข้ามาสู่ประเทศไทยจนส่งผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิดความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศไทย และการแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

2. ด้านภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ที่เป็นภัย คุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าว ไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัวจนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็น การปฏิบัติการข่าวสาร (Information Operation) ที่เป็นการปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมี การเผยแพร่ผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มมากขึ้น

3. ด้านภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติเป็นสิ่งที่กระทำได้ง่าย และยากต่อการดำเนินคดีต่อผู้กระทำผิด การเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์ การวิจารณ์สถาบันในทางเสื่อมเสีย ซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิด ไม่ได้อยู่ในประเทศไทยแต่ได้ใช้เว็บไซต์หรือสื่อสังคมออนไลน์ในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย

4. ด้านภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพไทย ทำให้ภาพลักษณ์ของผู้นำกองทัพไทยเสื่อมเสีย เสียหายหรือลดความน่าเชื่อถือในสังคมไทย รวมทั้งลดความเชื่อมั่นของประชาชนต่อการปกป้องประเทศไทย และการบังคับบัญชาของเหล่าทัพ ซึ่งส่งผลกระทบต่อการพิทักษ์อธิปไตยของชาติไทย

จากข้อมูลผู้วิจัยพบว่าศูนย์ไซเบอร์กองทัพบกควรพิจารณาเตรียมรับมือรูปแบบของภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนมากขึ้น ทวีคูณระดับความรุนแรงมากขึ้น โดยเฉพาะอย่างยิ่งการเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ที่สามารถส่งผลกระทบร้ายแรงต่อโครงสร้างพื้นฐานหลักของชาติอันเป็นพื้นฐานหลักความมั่นคงของประเทศ ณ ปัจจุบันซึ่งผลกระทบและมูลค่าความเสียหายมากขึ้นเรื่อย ๆ เพิ่มหลักการคืนสภาพ(Cyber Resilience)[ผนวก ฉ.]มาใช้ควบคู่กับการสร้างความตระหนักรู้ถึงความสำคัญในการเตรียมการ รับมือป้องกันภัยคุกคามทางไซเบอร์ (Cybersecurity Awareness) ไม่ว่าจะเป็นกำลังพล บุคลากรของภาครัฐ ภาคเอกชน และพลเรือน

ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับภัยคุกคามทางไซเบอร์

ผู้วิจัยได้ทำการศึกษารูปแบบมาตรฐานสากลและกรอบมาตรฐานสากลในการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ สามารถสรุปโดยแบ่งเป็นสองแบบ คือ สำหรับนำไปใช้ดำเนินการวางยุทธศาสตร์ชาติ และนำไปปรับใช้กับองค์กร ดังนี้

กรอบแนวคิดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับนำไปใช้ดำเนินการวางยุทธศาสตร์ชาติ ได้แก่

1.1 กรอบแนวคิดการพัฒนายุทธศาสตร์ของสหภาพโทรคมนาคมระหว่างประเทศของสหประชาชาติ (International Telecommunication Union: ITU) [28,29,30, ผนวก จ.] ผู้วิจัยได้สรุปตามแนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy)[28] ของสหประชาชาติ ซึ่งมีลักษณะสำคัญของคู่มือกรอบแนวคิดได้แบ่งองค์ประกอบที่สำคัญออกเป็น 3 ส่วน ได้แก่

1) ขั้นตอนของการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ
2) ลักษณะที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์
3) แนวปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

โดยมีแนวการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy)[28] เสนอขั้นตอนของการพัฒนายุทธศาสตร์ 5 ระยะ[ผนวก จ. ภาพประกอบที่ 7] ดังนี้ ระยะที่ 1: ระยะเริ่มต้น (Initiation), ระยะที่ 2: ระยะประเมินตรวจสอบและวิเคราะห์ (Stocktaking and Analysis), ระยะที่ 3: กำหนดยุทธศาสตร์ความมั่นคงไซเบอร์ระดับชาติ (Production of the national cybersecurity strategy), ระยะที่ 4: การขับเคลื่อนและใช้บังคับ (Implementation), ระยะที่ 5: การติดตามและประเมินผล (Monitoring and evaluation)

ลักษณะที่สำคัญตามคู่มือกรอบแนวคิดในการจัดทำยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) ได้เสนอลักษณะที่สำคัญของยุทธศาสตร์ 9 ประการ ดังนี้ 1. วิสัยทัศน์ของรัฐบาลและสังคมที่ชัดเจน (Clear vision), 2. ความเข้าใจต่อสภาพแวดล้อมทางไซเบอร์ของประเทศและการจัดลำดับประเด็นสำคัญของประเทศ (Comprehensive approach and tailored priorities), 3. การพัฒนายุทธศาสตร์จากการมีส่วนร่วมของทุกภาคส่วน (Inclusiveness), 4. การสร้างความมั่งคั่งทางเศรษฐกิจและสังคม (Economic and social prosperity), 5. สิทธิ

มนุษยชนขั้นพื้นฐาน (Fundamental human rights), 6. การบริหารความเสี่ยงและความทนทานต่อความเสี่ยง (Risk management and resilience), 7. กลไกขับเคลื่อนนโยบายที่เหมาะสม (Appropriate set of policy instruments), 8. บทบาทความเป็นผู้นำที่เด่นชัด การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน และการจัดสรรทรัพยากรที่ชัดเจน (Clear leadership, roles, and resource allocation) และ 9. สภาพแวดล้อมของความเชื่อมั่น (Trust environment)

แนวทางปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ (National Cybersecurity Strategy Good Practice)[32] มีปัจจัยสำคัญที่ทำให้ประเทศสามารถบรรลุตามเป้าหมายที่กำหนดขึ้นภายใต้ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ มีประสิทธิภาพประกอบด้วย 7 ปัจจัยที่สำคัญ ดังนี้ 1. การกำกับดูแลของภาครัฐ (Governance), 2. การบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Risk management in national cybersecurity), 3. การเตรียมความพร้อมและความทนทาน (Preparedness and resilience), 4. ระบบบริการโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical Infrastructure services and essential services), 5. ขีดความสามารถการพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ (Capability and capacity building and awareness raising), 6. กฎหมายและระเบียบกฎเกณฑ์ (Legislation and regulation) และ 7. ความร่วมมือระหว่างประเทศ (International cooperation)

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ITU มีหน่วยงานสถาบัน ITUAcademy เปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้อง โดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[31,32,44]

วิเคราะห์กรอบแนวคิด: สหภาพยุโรป

ผู้วิจัยได้ทำการศึกษากรอบแนวคิดของหน่วยงานด้านความมั่นคงปลอดภัยของเครือข่ายและข้อมูลของสหภาพยุโรป (European union agency for network and information security agency: ENISA) หน่วยงานได้จัดทำคู่มือแนวปฏิบัติที่ดีในการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับชาติ (Good practices in

innovation on cybersecurity under the National Cybersecurity Strategies “NCSS”) ในปี 2559 ซึ่งปรับปรุงจากคู่มือแนวปฏิบัติที่ดีฉบับปี 2563[32-38] เพื่อเป็นแนวทางให้กับประเทศสมาชิกของกลุ่มสหภาพยุโรปในการกำหนดยุทธศาสตร์ และการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันการโจมตี โครงสร้างพื้นฐานหลักของกลุ่มประเทศสมาชิกในสหภาพยุโรป[21,ผนวก จ. ภาพประกอบที่ 8] ประกอบด้วย

1. วัฏจักรของยุทธศาสตร์ พัฒนาเพื่อให้มีการตรวจสอบและทบทวนยุทธศาสตร์และนโยบายที่เกี่ยวข้องอย่างต่อเนื่อง โดยกำหนดให้วัฏจักรของยุทธศาสตร์ประกอบด้วย 4 ระยะ[ผนวก จ. ภาพประกอบที่ 9] **ได้แก่** ระยะที่ 1 พัฒนายุทธศาสตร์, ระยะที่ 2 ขับเคลื่อนยุทธศาสตร์ไปสู่การปฏิบัติ, ระยะที่ 3 ประเมินผลการปฏิบัติตามยุทธศาสตร์ และระยะที่ 4 การรักษาไว้ซึ่งยุทธศาสตร์ โดยมีการพัฒนายุทธศาสตร์

2. หลักการในการออกแบบและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 6 หลักการ ได้แก่

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

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

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

2.4 การกำหนดโครงสร้างการกำกับดูแลหน่วยงานภาครัฐที่ชัดเจน (Set a clear governance structure) โดยกำหนดหน่วยงานรับผิดชอบ บทบาทหน้าที่ ความรับผิดชอบ รวมถึงคณะกรรมการที่ทำหน้าที่สร้างความร่วมมือและประสานงานระหว่าง

หน่วยงานภาครัฐ การร่วมมือระหว่างภาครัฐและภาคเอกชน (Public Private Partnership: PPP)

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

2.6 การสร้างกลไกการแลกเปลี่ยนข้อมูลที่เชื่อถือได้ (Establish trusted information-sharing mechanisms) รวมถึงข้อมูลข่าวกรองที่สำคัญและข้อมูลจากทีมสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ เพื่อช่วยให้เข้าใจถึงสภาพแวดล้อมไซเบอร์ที่เปลี่ยนแปลงไป และสามารถลดความเสี่ยงและความเปราะบางที่มีอยู่ได้

3. เป้าหมายที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 15 ประการ โดยมีสาระสำคัญสรุปได้ ดังนี้ 1) การพัฒนาแผนรองรับสถานการณ์ฉุกเฉินทางไซเบอร์ของประเทศ (Develop national cyber contingency plans), 2) การคุ้มครองโครงสร้างพื้นฐานข้อมูลที่สำคัญยิ่งยวด (Protect critical information infrastructure), 3) การจัดการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ (Organize Cybersecurity exercises, 4) การกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ขั้นพื้นฐาน (Establish baseline security measures), 5) การสร้างกลไกการรายงานเหตุการณ์ (Establish incident reporting mechanisms), 6) การสร้างความตระหนักรู้ให้กับประชาชน เยาวชน และผู้บริโภค (Raise user awareness), 7) การจัดทำโครงการฝึกอบรมและหลักสูตรการศึกษา (Strengthen training and educational programmes), 8) การเพิ่มขีดความสามารถในการรับมือกับเหตุการณ์ (Establish an incident response capability) โดยจัดตั้งทีมสำหรับรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (CSIRT) ของประเทศ, 9) การแก้ไขปัญหาอาชญากรรมไซเบอร์ (Address cyber crime), 10) การสร้างความร่วมมือกับองค์กรระหว่างประเทศ (Engage in international cooperation), 11) การสร้างการร่วมมือระหว่างภาครัฐและเอกชน (Establish a public-private partnership), 12) การรักษาสมดุลระหว่างความมั่นคงปลอดภัยและความเป็นส่วนตัว (Balance security with privacy), 13) การสร้างความ

ร่วมมือระหว่างหน่วยงานภาครัฐ (Institutionalize cooperation between public agencies), 14) การเร่งการศึกษาวิจัยและพัฒนา (Foster R&D) และ15) การสร้างแรงจูงใจให้ภาคเอกชนในการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Provide incentives for the private sector to invest in security measures)

ในการจัดประเภทภัยคุกคามทางไซเบอร์ ENISA[21] ได้อ้างอิง MITRE[23,24] องค์กรไม่แสวงหาผลกำไรที่ก่อตั้งขึ้นเมื่อปี ค.ศ. 1958 ซึ่งมีจุดประสงค์เพื่อ “แก้ไขปัญหาเพื่อโลกที่ปลอดภัยกว่าเดิม” MITRE มีองค์ความรู้ขนาดใหญ่เกี่ยวเทคนิคการโจมตีและแนวทางการแก้ไขด้วย ATT&CK เป็นแพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ (Tactics, Techniques, Procedures “TTPs”) ที่แฮกเกอร์อร์นิยมใช้โจมตีระบบ Industrial Control System (ICS) ที่ใช้ควบคุมโครงสร้างพื้นฐานสำคัญของประเทศ ไม่ว่าจะเป็นระบบขนส่งพลังงาน โรงไฟฟ้า โรงกลั่นน้ำมัน ระบบบำบัดน้ำเสีย ระบบขนส่งมวลชน และอื่นๆ ภาครัฐและภาคเอกชนสามารถเพิ่มความปลอดภัยด้วย MITRE ATT&CK ซึ่งแบ่งเป็นหมวดหมู่ทั้งแบบ Enterprise, Mobile และ ICS[23,24, **ผนวก จ. ภาพประกอบที่ 10**

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ENISA มีการเปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[38,39]

วิเคราะห์กรอบแนวคิด: สหราชอาณาจักร

ผู้วิจัยได้ทำการศึกษาตามกรอบแนวคิดการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Cybersecurity Capacity Maturity Model for Nations “CMM”)[25, ผนวก จ. ภาพประกอบที่ 11 ซึ่งได้สร้างโดย Global Cybersecurity Capacity Centre, Department of Computer Science, มหาวิทยาลัย Oxford ประเทศอังกฤษ

กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีการวิเคราะห์ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ของประเทศและกำหนดระยะของการกำหนดยุทธศาสตร์ (Stage of maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ โดยตามกรอบแนวคิด

การสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีขีดความสามารถ[25, ผนวก จ. ภาพประกอบที่ 11] ประกอบด้วย มิติที่ 1 เป็นขีดความสามารถในการพัฒนานโยบายและยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ`(National Cybersecurity framework and policy), มิติที่ 2 เป็นขีดความสามารถด้านความรู้ความเข้าใจของประชาชนในเรื่องความเชื่อมั่นต่อบริการอินเทอร์เน็ต และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนโลกออนไลน์ (Cyber culture and society), มิติที่ 3 เป็นขีดความสามารถด้านความตระหนักรู้ (Awareness) ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ของภาครัฐภาคเอกชน และประชาชนทั่วไป (Cybersecurity education, training and skills), มิติที่ 4 เป็นขีดความสามารถในการออกแบบและบังคับใช้กฎหมาย รวมถึงการตัดสินคดีความที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Legal and regulatory frameworks), มิติที่ 5 เป็นขีดความสามารถด้านการใช้เทคโนโลยีที่มีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ (Standards, organizations, and technologies)

กรอบแนวคิดของ CMM ได้แบ่งระยะของการกำหนดยุทธศาสตร์ (Stage of Maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์[25, ผนวก จ. ภาพประกอบที่ 12] ประกอบด้วย 5 ระยะ ได้แก่

ระยะที่ 1 Start-up เป็นระดับที่เพิ่งเริ่มอภิปรายเกี่ยวกับแนวทาง การสร้างขีดความสามารถ แต่ยังไม่เริ่มดำเนินการ

ระยะที่ 2 Formative เป็นระดับที่เริ่มปรากฏแนวทางที่ชัดเจนแล้ว แต่ยังไม่จัดเป็นระเบียบหรือไม่เป็นหมวดหมู่

ระยะที่ 3 Established เป็นระดับที่เริ่มดำเนินการตามแนวทางแล้ว อยู่ในขั้นตอนของการตัดสินใจทางเลือกต่าง ๆ และ จัดสรรทรัพยากร

ระยะที่ 4 Strategic เป็นระดับที่มีการจัดลำดับความสำคัญของแนวทางว่าอยู่ในระดับองค์กรหรือในระดับชาติ และ

ระยะที่ 5 Dynamic เป็นระดับที่มีความชัดเจนในด้านกลไกนำไปสู่การเปลี่ยนแปลงยุทธศาสตร์ที่ขึ้นอยู่กับภัยคุกคามไซเบอร์ที่เกิดขึ้นจริงในปัจจุบัน

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ Global Cybersecurity Capacity Centre, Department of Computer Science, มหาวิทยาลัย Oxford ประเทศอังกฤษ มีพันธมิตรคือสถาบัน SANS ในการเปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[26,27]

กรอบแนวคิดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการนำไปปรับใช้กับองค์กร ดังนี้

วิเคราะห์กรอบแนวคิด: สหรัฐอเมริกา

จากการศึกษาแนวคิดกรอบโครงสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (National institute of standards and technology: NIST)[45,46] ประเทศสหรัฐอเมริกา เป็นหนึ่งในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นที่นิยมใช้อย่างมากในปัจจุบัน ไม่เพียงแค่องค์กรในประเทศสหรัฐอเมริกาเท่านั้น กรอบการทำงาน (framework) ดังกล่าวยังเป็นที่แพร่หลายทั่วโลก รวมไปถึงประเทศไทย หลายองค์กรเริ่มนำกรอบการทำงานนี้มาประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์

กรอบการทำงาน (framework) นี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ สามารถในไปกำหนดแนวทางบังคับใช้งาน และปรับปรุงแนวทางการรักษาความมั่นคงปลอดภัย ช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ ตอบสนองต่อภัยคุกคามและคืนสภาพได้อย่างรวดเร็วอย่างเป็นระบบ ในขณะที่ธุรกิจหรือหน่วยงานยังคงสามารถดำเนินการต่อไปได้อย่างเนื่อง ในกระบวนการควบคุมที่ใช้ในการปรับปรุงป้องกันโครงสร้างพื้นฐานสำคัญในองค์กรให้มีความมั่นคงปลอดภัยไซเบอร์ประกอบด้วย[45]

Core เป็นการระบุรายละเอียดกิจกรรมต่างๆ ที่สำคัญเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในกระบวนการต่างๆ ซึ่งอาจทำให้เกิดความเสี่ยงที่มีอยู่ในเกณฑ์ที่องค์กรยอมรับได้ให้สมบูรณ์ขึ้น

Implementation Tiers ระบุบริบทเพื่ออธิบายภาพความเสี่ยงและช่องว่าง กระบวนการ ด้านความมั่นคงปลอดภัยไซเบอร์ มุมมองในการจัดการความเสี่ยงที่

องค์กรยอมรับได้ โดยพิจารณาจากระดับความเข้มงวดที่เหมาะสมสำหรับโครงสร้างด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร

Profile ระบุความต้องการ เป้าหมาย วัตถุประสงค์ ความเสี่ยงที่ยอมรับและทรัพยากรที่สอดคล้องกับผลลัพธ์หรือเป้าหมายที่ Framework Core ได้แนะนำ อันเป็นเอกลักษณ์เฉพาะขององค์กรนั้น ๆ ส่วนใหญ่แล้วโปรไฟล์จะถูกใช้เพื่อระบุและจัดลำดับความสำคัญของกิจกรรมสำหรับการปรับปรุงความปลอดภัยทางไซเบอร์ในแต่ละโอกาสโดยการสร้าง “Current Profile” (โปรไฟล์ปัจจุบันขององค์กรที่กำลังเป็นอยู่) และ “Target Profile” (โปรไฟล์ที่องค์กรต้องการจะเป็นในด้านการรักษาความปลอดภัยไซเบอร์)

โดยกรอบการทำงานนี้มีจุดมุ่งหมายเพื่อลดและจัดการความเสี่ยง ปิดช่องว่างด้านความปลอดภัยทางไซเบอร์ให้ดีขึ้นในแต่ละกิจกรรมที่สำคัญขององค์กร เพื่อให้ไปถึงเป้าหมาย โดยแบ่งกรอบการทำงานที่สำคัญออกเป็น 5 ขั้นตอน[45,46, ผนวก จ. ภาพประกอบที่ 13] ประกอบด้วย

1. ระบุความเสี่ยง (Identify) ตัวช่วยกำหนดการควบคุมความเสี่ยงด้านความมั่นปลอดภัยไซเบอร์จะต้องมีการมุ่งเน้นและจัดระดับความสำคัญในการระบุความเสี่ยงที่เกี่ยวกับทรัพย์สิน ข้อมูล บุคลากรระบบที่มีความสำคัญที่อาจจะเกิดผลกระทบขึ้นในองค์กร

2. การป้องกัน (Protect) มาตรการป้องกันและรับมือที่เหมาะสมกับบริการที่สำคัญ เพื่อสนับสนุนเหตุการณ์ทางด้านความมั่นคงปลอดภัยไซเบอร์ ที่อาจจะเกิดขึ้นในอนาคต

3. การตรวจจับ (Detect) มาตรการตรวจจับและเฝ้าระวังเหตุการณ์ที่ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในองค์กรได้ทันท่วงทีและพร้อมรับมือกับเหตุการณ์ในอนาคต

4. การตอบสนอง (Respond) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุรับมือจะต้องได้รับการดำเนินการที่เหมาะสมและให้แน่ใจว่าตอบสนองต่อเหตุการณ์ได้ทันท่วงที เมื่อมีการตรวจพบภัยคุกคามไซเบอร์ในองค์กร

5. การกู้คืน (Recovery) มาตรการรักษาและฟื้นฟูความเสียหายที่เหมาะสมกับเหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นปกติภายในระยะเวลาที่เหมาะสม

ทั้งนี้แต่ละขั้นตอนหลักจะแบ่งออกเป็นขั้นตอนย่อย ๆ พร้อมระบุเอกสารอ้างอิง[ผนวก จ. ภาพประกอบที่ 14] เช่น ISO/IEC 27001:2013 , COBIT 5, NIST SP800-53 Rev.4 เพื่อให้สามารถนำกระบวนหรือแนวทางปฏิบัติจากเอกสารเหล่านั้นมาใช้เพื่อดำเนินการตามขั้นตอนต่อไปได้ทันที

มาตรฐาน ISO/IEC 27001:2013 (Information Security Management System)[40,41,ผนวก จ. ภาพประกอบที่ 16] คือ ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ “ISMS” เป็น มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งใช้หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Information Security) ที่มีองค์ประกอบ 3 ส่วน ได้แก่ “CIA”[ผนวก จ. ภาพประกอบที่ 17] 1.Confidentiality คือการรักษาความลับของสารสนเทศ กล่าวได้ว่าถ้าข้อมูลสารสนเทศนั้นถูกกำหนดให้เข้าถึงได้เฉพาะคนกลุ่มหนึ่ง ก็จะต้องมีเฉพาะคนกลุ่มนั้นเท่านั้นที่จะสามารถเข้าถึงข้อมูลสารสนเทศนั้นได้ ทั้งนี้ผู้ที่ไม่ได้อยู่ในคนกลุ่มนั้นจะต้องไม่สามารถเข้าถึงข้อมูลได้โดยเด็ดขาด 2.Integrity คือความถูกต้องของข้อมูลสารสนเทศ กล่าวได้ว่าข้อมูลสารสนเทศจะต้องคงความถูกต้องสมบูรณ์เสมอ โดยจะถูกเปลี่ยนแปลง แก้ไข หรือลบได้ด้วยเฉพาะผู้ที่ได้รับสิทธิอย่างถูกต้องเท่านั้น 3.Availability คือความพร้อมใช้งานของเทคโนโลยีสารสนเทศ กล่าวได้ว่าเมื่อผู้มีสิทธิต้องการเข้าถึงสารสนเทศนั้น ๆ ต้องการเข้าถึงหรือใช้งานสารสนเทศ จะต้องเข้าถึงได้ทุกครั้งที่ต้องการ

ผนวกกับระบบมาตรฐาน ISO/IEC 27001:2013 มีการประยุกต์ใช้หลักการ “PDCA” (Plan- Do -Check- Action)[40,ผนวก จ. ภาพประกอบที่ 15] อันเป็นหลักการสำคัญในการบริหารจัดการที่ใช้กันแพร่หลาย โดยหลักการ PDCA จะกำหนดมาตรฐานการดำเนินการให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2013 อาทิเช่น การจัดทำนโยบาย กระบวนการ การกำหนดหน้าที่ความรับผิดชอบ การควบคุม การตรวจสอบ การประเมินความเสี่ยง การวางแผนความต่อเนื่องทางธุรกิจ การจัดการเหตุการณ์ที่เกี่ยวข้องกับมั่นคงปลอดภัยได้ ทั้งนี้เมื่อนำมาใช้ในองค์กรที่ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานได้ทั้งภาครัฐและภาคเอกชน [42]

มีหลักสูตรการเรียนรู้ด้านมาตรฐาน ISO 27001:2013 และอื่น ๆ โดยบริษัทเอกชนที่จดทะเบียนจัดตั้งโดย Royal Charter (จาก British Standard Standards Association “BSI”)[42]

กรอบแนวคิดในการเตรียมพร้อมและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการนำไปปรับใช้กับองค์กร

สหรัฐฯมีหน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน (Cybersecurity & Infrastructure Security Agency “CISA”)[47] ของ กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) เป็นองค์กรหลักในการบูรณาการร่วมกันระหว่างภาครัฐ ภาคเอกชนในเรื่องของโครงสร้างพื้นฐานหลัก ซึ่งมีหน่วยงาน National Initiative for Cybersecurity Careers and Studies “NICCS” ที่ออกแบบกรอบแนวคิดในการเตรียมพร้อมและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการนำไปปรับใช้กับองค์กร (NICE Framework หรือ National Initiative for Cybersecurity Education “NICE”) หน่วยงานนี้มีหน้าที่แนะนำงานและสายงานที่เกี่ยวข้องกับ Cybersecurity และให้การบริการฝึกอบรมงานด้านการรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานสำคัญ (Critical Information Infrastructure : CII) แก่บุคลากรภาครัฐและเอกชน[48,49,50]

หลักสูตรการฝึกอบรมและแนวทางหน้าที่การงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับกำลังพลทางการทหาร โดยกระทรวงกลาโหมสหรัฐฯแผนกไซเบอร์(DoD CYBER) ซึ่งได้ออกแบบกรอบแนวคิดในการเตรียมพร้อมและพัฒนากำลังพลด้านความมั่นคงปลอดภัยไซเบอร์ (DoD Cyber Workforce Framework)[51,52,53]บนพื้นฐานของกรอบแนวคิดในการเตรียมพร้อมและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการนำไปปรับใช้กับองค์กร (NICE Framework หรือ National Initiative for Cybersecurity Education “NICE”)[49,50]

การเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กรภาครัฐและภาคเอกชน

พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ ตราขึ้นเพื่อให้ประเทศไทยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ มีผลบังคับใช้ ตั้งแต่วันที่ 27 พฤษภาคม พ.ศ.2562[59] สาระสำคัญคือ แนวทางในการจัดการ การป้องกัน การรับมือ และการลดความเสี่ยงทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ความสามารถของบุคลากร และผู้เชี่ยวชาญ รวมถึงการให้ความรู้ และความตระหนักถึงภัยไซเบอร์อีกด้วยการวางรากฐานระบบรักษาความปลอดภัยทางไซเบอร์ให้กับองค์กรต่างๆ ทั้งภาครัฐ ภาคเอกชน ในกลุ่มหน่วยงานที่เป็นโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Information Infrastructure : CII)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือ National Cybersecurity Agency “NCSA” เป็นหน่วยงานกลางผู้สร้างกลไกขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศ เพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น การดำเนินงานดังกล่าวต้องอาศัยผู้เชี่ยวชาญเฉพาะด้าน และมีกลไกการทำงานที่มีความคล่องตัวพร้อมสำหรับการปฏิบัติงาน ทั้งด้านนโยบายเทคโนโลยี การวิจัยพัฒนาและกฎหมาย[60]

ตั้งแต่ปี 2564 สกมช. ได้ดำเนินการจัดทำแผนและนโยบายระดับประเทศ จัดทำกรอบดำเนินการต่าง ๆ เพื่อดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ทั้ง 7 ภาคส่วน[61,62,72] ได้แก่

1. หน่วยงานด้านความมั่นคงภาครัฐ ได้แก่ สำนักงานปลัดกระทรวงกลาโหม, สำนักงานตำรวจแห่งชาติ และสำนักงานสภาความมั่นคงแห่งชาติ
2. หน่วยงานด้านบริการภาครัฐที่สำคัญ ได้แก่ กระทรวงการคลัง, กรมศุลกากร, กรมการปกครอง, สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) และกรมชลประทาน

3. หน่วยงานด้านการเงินการธนาคาร ได้แก่ ธนาคารแห่งประเทศไทย, สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ได้แก่ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม แห่งชาติ (กสทช.)[83]
5. หน่วยงานด้านขนส่งและโลจิสติกส์ ได้แก่ สำนักงานตำรวจแห่งชาติ, กรมการขนส่งทางราง, สำนักงานปลัดกระทรวงคมนาคม[80] และสำนักงานการบินพลเรือนแห่งประเทศไทย
6. ด้านพลังงานและสาธารณูปโภค ได้แก่ กระทรวงพลังงาน และการประปาส่วนภูมิภาค
7. ด้านสาธารณสุข ได้แก่ สำนักงานปลัดกระทรวงสาธารณสุข และสำนักงานคณะกรรมการอาหารและยา

ดำเนินการสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ให้บุคลากรประจำองค์กรที่เป็น CII ทั้ง 7 ภาคส่วน ตามแนวทางปฏิบัติของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งเป็นแผนพัฒนาและปฏิบัติระยะยาวภายใต้การดูแลเชิงปฏิบัติการของ สกมช. เพื่อให้เกิดผลสัมฤทธิ์ในการป้องกันตัวเองตลอดจนแก้ไขภัยทางไซเบอร์รูปแบบต่าง ๆ[62]

จัดให้มีการเร่งรัดพัฒนาบุคลากรด้านไซเบอร์ โดยมีเป้าหมายกว่า 2,000 คน สำหรับปี 2564 ถึงปี 2565 ได้พัฒนาระดับผู้บริหาร ระดับผู้เชี่ยวชาญ จัดโปรแกรมสัมมนาเพื่อพัฒนาบุคลากรอย่างต่อเนื่อง มีโครงการพัฒนาความรู้ในบุคคลทั่วไป ตลอดจนนักเรียน นักศึกษา มีโครงการจัดแข่งขันทักษะทางไซเบอร์ในระดับมัธยม มหาวิทยาลัย ตลอดจนบุคคลทั่วไป ซึ่งได้รับความสนใจเป็นอันมาก เนื่องจากเป็นเส้นทางสายอาชีพกระแสใหม่ มีรายได้ดี เป็นที่ต้องการสูงจึงเกิดการผลักดันให้เกิดความต้องการศึกษาด้านไซเบอร์ซิเคียวริตี้ที่ประเทศยังขาดแคลน รวมถึงการฝึกร่วมภาครัฐและCII[62,63,64,65]

การแสวงหาความร่วมมือกับองค์กรทั้งในประเทศและต่างประเทศ ตลอดจนกระทรวงต่าง ๆ ซึ่งขณะนี้มีการร่าง MOU กับประเทศอิสราเอล จีน อังกฤษ ญี่ปุ่น และอีกหลายประเทศ

สำหรับประเทศไทย พ.ร.บ.ไซเบอร์ ได้แบ่งภัยคุกคามไซเบอร์เป็น 3 ระดับ

1. ระดับไม่ร้ายแรง ส่งผลให้เกิดความด้อยประสิทธิภาพในการให้บริการอิเล็กทรอนิกส์

2. ภัยไซเบอร์ระดับร้ายแรง มีการโจมตีระบบจนเกิดความเสียหายไม่สามารถทำงานต่อได้
3. ระดับวิกฤต ระบบล้มเหลวจนรัฐทำงานจากส่วนกลางไม่ได้ ส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศทั้งระบบ

ซึ่ง พ.ร.บ.ไซเบอร์ ให้อำนาจ สกมช. ในการเข้าตรวจสอบหรือจัดการแก้ปัญหาการโจมตีไซเบอร์เฉพาะที่มีการถูกโจมตีระดับร้ายแรงและระดับวิกฤต ตั้งแต่ต้นปี 2564ถึงปัจจุบัน สกมช. ได้เข้าร่วมแก้ปัญหาในหน่วยงานหรือองค์กรต่าง ๆ จนผ่านพ้นวิกฤตหลายหน่วยงาน

“Thailand Computer Emergency Response Team” (ThaiCERT)

“ไทยเซิร์ต” (ThaiCERT) ภายใต้การกำกับดูแลของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. มีชื่ออย่างเป็นทางการว่า“ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบ คอมพิวเตอร์ประเทศไทย” หรือ Thailand Computer Emergency Response Team “ThaiCERT” มีพันธกิจในการแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยทั้งที่ได้รับแจ้งและตรวจพบเองในขอบเขตครอบคลุมระบบเครือข่ายอินเทอร์เน็ตและเว็บไซต์ภายใต้โดเมนเนม (Domain Name) ของประเทศไทย(.th) โดยทำงานร่วมกับหน่วยงานในเครือข่ายและ หน่วยงานที่เกี่ยวข้อง อีกทั้งให้ความสำคัญกับการพัฒนาบุคลากรเพื่อเพิ่มขีดความ สามารถด้านการรักษาความมั่นคงปลอดภัยภายในประเทศไทย และให้คำปรึกษาแก่ หน่วยงานที่เป็นโครงสร้างพื้นฐานสารสนเทศสำคัญของประเทศ (Critical Information Infrastructure : CII) ในเรื่องของการป้องกันและแก้ไขปัญหาภัยคุกคามไซเบอร์ เพื่อรักษาความต่อเนื่องในการดำเนินภารกิจของหน่วยงานนั้น ๆ

ไทยเซิร์ต (ThaiCERT)[77,78,81] มีภารกิจหลักในการรับมือกับสถานการณ์ภัยคุกคามไซเบอร์ของประเทศไทย ด้วยการประสานระหว่างบุคลากรผู้เชี่ยวชาญ กระบวนการทำงาน ที่ได้รับมาตรฐาน เทคโนโลยีทันสมัยที่นำมาประยุกต์ใช้ในงาน และเครือข่าย ความร่วมมือจากทั่วโลก เพื่อเชื่อมโยงการทำงานให้มีประสิทธิภาพสูงสุดและสามารถรับมือภารกิจที่สำคัญได้ อย่างต่อเนื่อง

หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานหรือองค์กรที่มีบทบาทสำคัญประกอบด้วย 3 หน่วยงาน ได้แก่

ทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response team: CSIRT)

ทีมรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams: CERTs)

ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (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

หน่วยงานที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.)[84] เป็นหน่วยรับผิดชอบงานด้านไซเบอร์ ได้พัฒนาการฝึกอบรมกำลังพลของกองทัพบกระดับนายทหารสัญญาบัตรและชั้นประทวน ทั้งหมด 7 หลักสูตร

ศูนย์ไซเบอร์กองทัพบกจะเน้นไปในด้านความมั่นคงทางไซเบอร์ความมั่นคงทางด้านทหารความมั่นคงของชาติเป็นภารกิจที่สำคัญและได้ทำงานประสานกับหน่วยงานรัฐอื่นๆ อีกเช่นหน่วยงานไทยเซิร์ต (ThaiCERT) ซึ่งเป็นหน่วยงานสำคัญของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เป็นองค์การมหาชนสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจ

และสังคมมี หน้าที่สำคัญในการรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์ต่างๆเพื่อให้การทำธุรกรรมทางออนไลน์มีความมั่นคงปลอดภัยซึ่งปัจจุบันนี้ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มมากขึ้นในประเทศไทยและมีความซับซ้อนสังคมไทยจึงต้องตื่นตัวเฝ้าระวังและหาทางรับมือกับภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้น

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือ National Cybersecurity Agency : NCSA เสนอ 6 หลักสูตร ในโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) ระยะที่ 1[65, ผนวก ช.] เพื่อยกระดับศักยภาพบุคลการด้านไซเบอร์ตามแนวทางมาตรฐานสากล ภายใต้โครงการฯ มีความมุ่งมั่นในการส่งเสริมการสอบใบประกาศนียบัตรและใบรับรองความเชี่ยวชาญไซเบอร์ที่เป็นที่ยอมรับในระดับสากล ซึ่งการจัดทำหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับพื้นฐานและระดับผู้เชี่ยวชาญได้ดำเนินการสอดคล้องตามแนวทางมาตรฐาน NICE ซึ่งเป็นมาตรฐานในการพัฒนาบุคลการด้าน Cybersecurity และแนวคิดสมรรถนะวิชาชีพ (Competency-based) ซึ่งประกอบด้วย องค์ประกอบ KSA ได้แก่ องค์ความรู้ (Knowledge) ทักษะ (Skill) และความสามารถ (Abilities) ที่เกี่ยวข้องด้าน Cybersecurity เพื่อให้เกิดผลลัพธ์สำคัญที่จะบรรลุผลสัมฤทธิ์ตามวัตถุประสงค์ในการฝึกทักษะ ยกระดับศักยภาพ และขีดความสามารถของบุคลการด้านไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) และหน่วยสำคัญ ๆ ของประเทศ ให้มีความรู้ความสามารถตามมาตรฐานสากล ทัดเทียมกับการพัฒนาด้านนี้ของประเทศอื่นในภูมิภาค

หลักสูตรการเรียนรู้ด้านรัฐบาลดิจิทัล (E-Learning) สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy “TDGA” ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นศูนย์กลางการพัฒนาทักษะด้านดิจิทัลสำหรับข้าราชการและบุคลากรภาครัฐของประเทศไทย[79,88]

บทที่ 3

บทอภิปรายผล

จากผลการศึกษาวิจัยในบทที่ 2 ผู้วิจัยสามารถอภิปรายผลตามวัตถุประสงค์การวิจัย โดยแนวทางการอภิปรายผลวิจัยได้นำข้อมูลยุทธศาสตร์ชาติ 20 ปี แผนแม่บท พระราชบัญญัติ นโยบายและแผนปฏิบัติการ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ศึกษาหลักการกรอบแนวคิดด้านความมั่นคงปลอดภัยไซเบอร์ รูปแบบหลักสูตรการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับพัฒนาความมั่นคงปลอดภัยไซเบอร์องค์กรและกำลังพลให้สูงขึ้นและศึกษายุทธศาสตร์การจัดการภัยคุกคามทางไซเบอร์ของภาครัฐและเอกชน มาวิเคราะห์ เปรียบเทียบ และรองรับผลงานวิจัย มีรายละเอียด ดังนี้

1. ปัญหาการโจมตีทางไซเบอร์ในปัจจุบันมีรูปแบบใดบ้าง

ผลการวิจัยพบว่าปัญหาการโจมตีทางไซเบอร์ในปัจจุบันที่มีลักษณะการโจมตีเหมือนกันทั่วโลก ได้แก่ 1.การหลอกลวงเพื่อผลประโยชน์ (Fraud) เช่น 1.1)แก๊งคอลเซ็นเตอร์ Vishing หรือ Voice-Phishing ซึ่งมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์ ส่วน Smishing หรือ Short Message Service-Phishing เป็นการหลอกลวงโดยใช้ข้อความสั้น SMS เช่น การได้รับ SMS อ้างว่ามาจากธนาคารเพื่อแจ้งลูกค้าว่าบัญชีของท่านถูกระงับ กรุณาติดต่อกลับที่ หรือคุณได้รับรางวัลให้กดลิงค์ตามที่ส่งมา 1.2)การหลอกลวงที่มีเป้าหมายชัดเจน Spear-phishing และ Whaling และรองลงมาคือ2.การโจมตีแรนซัมแวร์ (Ransomware) เพื่อเรียกค่าไถ่ด้วยบิตคอยน์ (Bitcoin) หรือสกุลเงินคริปโต (Cryptocurrency) 3.การโจมตีระบบแม่ข่ายคอมพิวเตอร์ให้ปฏิเสธหรือหยุดการให้บริการ “DDoS”(Distributed Denial-of-Service) และ 4.ยุทธการทางข้อมูลข่าวสาร “IO” (Information Operation) การแพร่กระจายของข่าวปลอม ข่าวลวงหรือข้อมูลข่าวสารที่จัดทำขึ้นอย่างแนบเนียน (Fake News และ Deepfakes) เพื่อหวังผลให้เกิดการตอบสนองต่อข้อมูลข่าวสารในแนวทางที่ต้องการ

จากภัยคุกคามทั้งหมดที่กล่าวมาล้วนมีการพัฒนารูปแบบการโจมตีอย่างต่อเนื่อง พึงคำนึงไว้เสมอว่าการโจมตีเหล่านี้สามารถเกิดขึ้นกับอุปกรณ์ IoT ได้ทั้งหมด ไม่ได้เกิดขึ้นแค่เพียงคอมพิวเตอร์ เพราะปัจจุบันอุปกรณ์รอบตัวเรานั้นได้มีการพัฒนาให้มี

การเชื่อมต่อเข้าระบบอินเทอร์เน็ตตลอดเวลา สามารถส่งข้อมูล ชี้แจงสถานะ บอกพิกัดตำแหน่งอย่างปัจจุบันทันด่วน (Realtime) อย่างโทรศัพท์มือถือ (Smartphone), นาฬิกา (Smart Watch), คอมพิวเตอร์พกพา (iPad, Surface), กล้อง CCTV, รถยนต์ส่วนบุคคล เป็นต้น ดังนั้นการที่จะยับยั้งการโจมตีเหล่านี้ได้คือการปิดช่องโหว่โดยการสร้างความตระหนักรู้ให้กำลังพล บุคลากรขององค์กรถึงภัยคุกคามทางไซเบอร์ ณ ปัจจุบัน การสร้างความตระหนักรู้ถึงผลกระทบที่จะเกิดขึ้นหากถูกคุกคามทางไซเบอร์ และองค์กรควรมีการจัดตั้งหน่วยงาน อย่างทีมรับมือกับสถานการณ์ความมั่นคงที่เกี่ยวกับคอมพิวเตอร์ (Computer security incident response team: CSIRT) หรือทีมรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams: CERTs) หรือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (Security Operations Center: SOC) ทั้งนี้ขึ้นอยู่กับขนาดขององค์กร หน่วยงานนั้น ๆ

เมื่อพิจารณาวัตถุประสงค์หลักและความสำคัญแล้ว CERT มีหน้าที่หลักในการจัดเก็บ รวบรวม และเผยแพร่ข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ ไม่มีความจำเป็นต้องมีปฏิบัติการเพื่อรับมือ หรือโต้ตอบกับเหตุการณ์ภัยคุกคามทางไซเบอร์ ในขณะที่ CSIRT มีหน้าที่หลักในการรับมือและโต้ตอบเหตุการณ์ภัยคุกคามทางไซเบอร์ และกำจัดภัยคุกคามทางไซเบอร์ รวมถึงการฟื้นฟูคืนสภาพจากความเสียหาย อย่างไรก็ดี การทำหน้าที่ของ CSIRT และ CERT อาจมีหน้าที่บางส่วนที่เหมือนกันได้ เช่น การทำความเข้าใจกับเหตุการณ์ และการให้คำแนะนำ เป็นต้น นอกจากนี้ ในส่วนของศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระดับองค์กร (SOC) มีหน้าที่ติดตามเหตุการณ์ ลงทุนในระบบป้องกันโครงสร้างพื้นฐานด้านสารสนเทศขององค์กร และพัฒนาขีดความสามารถของบุคลากรด้านการป้องกันเครือข่ายและระบบระดับองค์กร

2. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ทางการทหารและของประเทศมีอะไรบ้าง

จากการศึกษายุทธศาสตร์ชาติ 20 ปี แผนแม่บท พระราชบัญญัติ นโยบายและแผนปฏิบัติการ ยุทธศาสตร์ชาติ 20 ปี[58] ได้ระบุถึงหน่วยงานความมั่นคงของแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ตามมติ ครม. วันที่ 3 ธันวาคม 2562 อันประกอบด้วย สำนักนายกรัฐมนตรี, สำนักงานสภาความมั่นคงแห่งชาติ, กระทรวงมหาดไทย, กอง

อำนวยการรักษาความมั่นคงภายในราชอาณาจักร, สำนักงานตำรวจแห่งชาติ, กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สำนักข่าวกรองแห่งชาติและกระทรวงการต่างประเทศ เป็นรากแก้วของหน่วยงานที่มีความเกี่ยวข้องกับมั่นคงของชาติ และรากฝอยที่เชื่อมโยงหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยพบความเชื่อมโยงของหน่วยงานที่เกี่ยวข้องในปัจจุบัน ดังนี้

1. สำนักนายกรัฐมนตรี

2. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช)

3. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

4. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ. หรือ ETDA) / ThaiCERT

    4.1 สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa)

    4.2 สถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ (สวข.)

    4.3 สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร. หรือ DGA)

    4.4 ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data) “BIG DATA”

จากการศึกษาหน่วยงานดังกล่าว การแลกเปลี่ยนข้อมูลบนพื้นฐานแพลตฟอร์มเดียวกันเพื่อรักษามาตรฐานความมั่นคงปลอดภัยไซเบอร์ในระดับเดียวกันมีความสำคัญยิ่ง อีกทั้งต้องมีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐและเอกชน เพื่อยกระดับความพร้อมรับมือภัยคุกคามทางไซเบอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานสารสนเทศที่สำคัญของประเทศ เพื่อให้สอดคล้องกับพรบ.ไซเบอร์ฯ ปัจจุบันการดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำขาดการบูรณาการร่วมกัน แม้ว่าในปัจจุบันความเสี่ยงด้านความปลอดภัยไซเบอร์มากขึ้นและเห็นได้ชัด แม้องค์กรต่าง ๆ มีการรักษาความปลอดภัยแบบแยกส่วน และบางครั้งมีความขัดแย้งกัน ประกอบกับการขาดแคลนกำลังพลและบุคลากรที่มีความรู้ มีทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำให้ปัจจุบันหลายหน่วยงาน องค์กรขาดองค์ความรู้ความไม่เข้าใจถึงภัยคุกคามทางไซเบอร์ในปัจจุบันและไม่สามารถจัดการกับความเสี่ยงได้

อย่างมีประสิทธิภาพ แสดงให้เห็นถึงการขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์ และการพัฒนาบุคลากรด้านนี้ ที่ปัจจุบันยังไม่ทันต่อความต้องการของประเทศ

ด้วยเหตุนี้จากการวิเคราะห์ผู้วิจัยพบว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือ National Cybersecurity Agency "NCSA" เป็นหน่วยงานกลางผู้สร้างกลไกขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือสนับสนุนหน่วยงานภาครัฐ ภาคเอกชนและหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศของประเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น การดำเนินงานดังกล่าวต้องอาศัยผู้เชี่ยวชาญเฉพาะด้าน และมีกลไกการทำงานที่มีความคล่องตัวพร้อมสำหรับการปฏิบัติงาน ทั้งด้านนโยบายเทคโนโลยี การวิจัยพัฒนาและกฎหมาย

ดำเนินการสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ให้บุคลากรประจำองค์กรที่เป็น CII ทั้ง 7 ภาคส่วน เพื่อให้เกิดผลสัมฤทธิ์ในการป้องกันตัวเองตลอดจนแก้ไขภัยทางไซเบอร์รูปแบบต่าง ๆ และเร่งรัดพัฒนาบุคลากรด้านไซเบอร์ โดยมีเป้าหมายกว่า 2,000 คน ตั้งแต่ปีพ.ศ. 2564 ถึงปี พ.ศ. 2565 ได้พัฒนาระดับผู้บริหาร 70 คน ระดับผู้เชี่ยวชาญ 300 คน จัดโปรแกรมสัมมนาเพื่อพัฒนาบุคลากรอย่างต่อเนื่อง มีโครงการพัฒนาความรู้ พร้อมประกาศนียบัตรระดับสากลให้กับบุคคลทั่วไป ตลอดจนนักเรียนนักศึกษา กำลังพลและบุคลากร CII[62,63,64,65] จัดให้มีโครงการจัดแข่งขันทักษะทางไซเบอร์ในระดับมัธยม มหาวิทยาลัย ตลอดจนบุคคลทั่วไป ซึ่งได้รับความสนใจเป็นอันมาก เนื่องจากเป็นเส้นทางสายอาชีพกระแสใหม่ มีรายได้ดี เป็นที่ต้องการสูงจึงเกิดการผลักดันให้เกิดความต้องการศึกษาด้านไซเบอร์ซิเคียวริตี้ที่ประเทศยังขาดแคลน ควบคู่กับการแสวงหาความร่วมมือกับองค์กรทั้งในประเทศและต่างประเทศ ตลอดจนกระทรวงต่าง ๆ ซึ่งขณะนี้มีการร่าง MOU กับประเทศอิสราเอล จีน อังกฤษ ญี่ปุ่นและอีกหลายประเทศ เพื่อสร้างความเป็นมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศ[55,56,57]

3. ภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อรองรับภัยคุกคามทางไซเบอร์เป็นอย่างไร

ผลการวิจัยพบว่าภาพรวมแนวทางในระดับมาตรฐานสากลมีการเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อรองรับภัยคุกคามทางไซเบอร์ ประเทศไทยได้ดำเนินการตามกรอบโครงสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (National institute of standards and technology: NIST) ประเทศสหรัฐอเมริกา[45,46] ซึ่งเป็นหนึ่งในกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นที่นิยมใช้อย่างมากในปัจจุบัน ไม่เพียงแค่องค์กรในประเทศสหรัฐอเมริกาเท่านั้น กรอบการทำงาน (framework) ดังกล่าวยังเป็นที่แพร่หลายทั่วโลก หลายองค์กรในประเทศที่จัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ “CII”[47,48]เริ่มนำกรอบการทำงานนี้มาประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์ ประกอบกับการใช้มาตรฐาน มาตรฐาน ISO/IEC 27001:2013 (Information Security Management System)[72,**ผนวก จ. ภาพประกอบที่ 16**] คือ ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ “ISMS” เป็น มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งใช้หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Information Security) ที่มีองค์ประกอบ 3 ส่วน ได้แก่ C (การรักษาความลับ หรือ Confidentiality), I (ความถูกต้องของข้อมูลสารสนเทศ หรือ Integrity) และ A (ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ หรือ Availability) “CIA” ผนวกกับการประยุกต์ใช้หลักการ “PDCA” (Plan- Do -Check- Action)[**ผนวก จ. ภาพประกอบที่ 15,17**] อันเป็นหลักการสำคัญในการบริหารจัดการที่ใช้กันแพร่หลาย โดยหลักการ PDCA จะกำหนดมาตรฐานการดำเนินการให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2013 อาทิเช่น การจัดทำนโยบาย กระบวนการ การกำหนดหน้าที่ความรับผิดชอบ การควบคุม การตรวจสอบ การประเมินความเสี่ยง การวางแผนความต่อเนื่องทางธุรกิจ การจัดการเหตุการณ์ที่เกี่ยวข้องกับมั่นคงปลอดภัยได้ ทั้งนี้เมื่อนำมาใช้ในองค์กรที่ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานได้ทั้งภาครัฐและภาคเอกชน

เมื่อนำมาเปรียบเทียบแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศในประเทศแล้วผู้วิจัยพบว่าแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากร ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อรองรับภัยคุกคามทางไซเบอร์ มีกรอบการดำเนินการในทิศทางเดียวกันคือ มีมาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดำเนินการเพื่อจัดการภัยคุกคามทางไซเบอร์ (incident handling) โดยแบ่งขั้นตอนการดำเนินการออกได้เป็น 4 ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดดังนี้[59,60,61,62]

ภาพประกอบที่ 18 ขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)

ขั้นตอนที่ 1 การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ

ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

ขั้นตอนที่ 3 การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์, และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ขั้นตอนที่ 4 การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทำงไซเบอร์ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินมาตรการดูแลและรับมือภัยคุกคามไซเบอร์ตามขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle) กับหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ทั้ง 7 ภาคส่วน[61] ได้แก่

1. หน่วยงานด้านความมั่นคงภาครัฐ ได้แก่ สำนักงานปลัดกระทรวงกลาโหม, สำนักงานตำรวจแห่งชาติ และสำนักงานสภาความมั่นคงแห่งชาติ
2. หน่วยงานด้านบริการภาครัฐที่สำคัญ ได้แก่ กระทรวงการคลัง, กรมศุลกากร, กรมการปกครอง, สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) และกรมชลประทาน
3. หน่วยงานด้านการเงินการธนาคาร ได้แก่ ธนาคารแห่งประเทศไทย, สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ได้แก่ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม แห่งชาติ (กสทช.)
5. หน่วยงานด้านขนส่งและโลจิสติกส์ ได้แก่ สำนักงานตำรวจแห่งชาติ, กรมการขนส่งทางราง, สำนักงานปลัดกระทรวงคมนาคม และสำนักงานการบินพลเรือนแห่งประเทศไทย
6. ด้านพลังงานและสาธารณูปโภค ได้แก่ กระทรวงพลังงาน และการประปาส่วนภูมิภาค

7. ด้านสาธารณสุข ได้แก่ สำนักงานปลัดกระทรวงสาธารณสุข และสำนักงานคณะกรรมการอาหารและยา

งานวิจัยที่สนับสนุนการศึกษาแนวทางพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

ผู้วิจัยได้ศึกษาแนวทางพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ พบว่าปัจจัยทางด้านการขาดกำลังพลและบุคลากรที่มีความชำนาญการด้านความมั่นคงปลอดภัยไซเบอร์เป็นจำนวนมากในหลายหน่วยงาน การขาดแคลนกำลังพลและบุคลากรดังกล่าวมีระบุหนทางในการแก้ไขปัญหาดังกล่าวอยู่ในยุทธศาสตร์ชาติ 20ปีอย่างชัดเจนไม่ว่าจะด้านความมั่นคง ด้านการสร้างความสามารถในการแข่งขัน ด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ด้านการสร้างโอกาสและความเสมอภาคทางสังคม และด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ ล้วนมีการกำหนดนโยบายและยุทธศาสตร์ในการส่งเสริมการพัฒนากำลังพล บุคลากรให้เกิดความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์และส่งเสริมในการพัฒนาการเรียนรู้เพิ่มเติมให้กับกำลังพลบุคลากรของตนเพื่อให้เกิดการพัฒนา ให้สามารถรับการปรับเปลี่ยนเข้าสู่การทำงานในยุคดิจิทัล โดยเห็นได้ชัดช่วงธันวาคม พ.ศ.2562 ถึง พ.ศ.2565 ที่มีภาวะวิกฤติการแพร่ระบาดของโรคติดเชื้อไวรัสโควิด-19 (Covid-19) ทั่วโลก หลายหน่วยงานต่างให้บุคลากรของตนต้องทำงานทางไกล (Remote Working) จึงปฏิเสธไม่ได้เลยที่หลายหน่วยงานปรับเปลี่ยนเข้าสู่การทำงานในยุคดิจิทัล (Digital transformation)

ในขณะเดียวกันในอนาคตอันใกล้กำลังพลและบุคลากรที่มีความรู้ ความชำนาญการด้านความมั่นคงปลอดภัยไซเบอร์รุ่นใหม่จะเพิ่มมากขึ้น เหตุเพราะพ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งแสดงให้เห็นถึงเป้าหมายในอนาคตของประเทศที่ให้ความสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ ส่งผลให้เกิดความสนใจและมีตอบรับในการเร่งรัดพัฒนากำลังพลและบุคลากรด้านไซเบอร์อย่างมาก มีจัดโปรแกรมสัมมนาเพื่อพัฒนาบุคลากรอย่างต่อเนื่อง มีโครงการพัฒนาความรู้ในบุคคลทั่วไป ตลอดจนนักเรียน นักศึกษา มีโครงการจัดแข่งขันทักษะทางไซเบอร์ในระดับมัธยม มหาวิทยาลัย ตลอดจนบุคคลทั่วไป หลายมหาวิทยาลัยมีการเปิดหลักสูตรปริญญาด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งได้รับความสนใจเป็นอันมาก เนื่องจากเป็นเส้นทางสายอาชีพ

กระแสใหม่ มีรายได้ดี เป็นที่ต้องการสูงจึงเกิดการผลักดันให้เกิดความต้องการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ขึ้นเพื่อแก้ปัญหาความขาดแคลนด้านกำลังพลและบุคลากรดังกล่าว

ทั้งนี้ผลการศึกษาวิจัยข้างต้นมีความสอดคล้องกับงานวิจัย ดังต่อไปนี้

พลตรี ปรัชญา เฉลิมวัฒน์ (2560)[85] ได้ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมความพร้อมต่อภัยคุกคามไซเบอร์ในระดับชาติ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ๆ ทั้งปัจจัยด้านเวลาการพัฒนาและด้านการเสริมสร้างกำลังพลไซเบอร์ในรูปแบบกองกำลังผสมพลเรือน ตำรวจ ทหาร และการพิจารณาใช้ข้อกฎหมายที่เกี่ยวข้องกับการเตรียมกำลังพลสำรองในระดับชาติ

ผลการศึกษาพบว่า แนวทางในการพัฒนากำลังพลด้านไซเบอร์จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งของบุคลากรด้านไซเบอร์ให้กับประเทศชาติ ซึ่งหากนำไปใช้ปฏิบัติได้จะทำให้สามารถลดปัญหาการขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความ “ยั่งยืน” ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี

ข้อเสนอแนะสำหรับการพัฒนากำลังพลด้านไซเบอร์ ประกอบด้วย 1) การกำหนดแนวทางในการจัดการกำลังพลสำรองที่ปลดประจำการ (ผ่านการเกณฑ์ทหารไปแล้ว) แต่ทำงานในสาขาที่เกี่ยวข้องอยู่แล้ว พิจารณาการเรียกเข้ามาเพื่อเป็นผู้ฝึกให้กับ “ทหารใหม่ไซเบอร์” ได้เป็นอย่างดี โดยที่เขาเหล่านั้นก็ถือได้ว่ามารับใช้ประเทศชาติในอีกทางหนึ่งในมิติของไซเบอร์ 2) การกำหนดนโยบายกำลังพลสำรองไซเบอร์ เพื่อนำทหารกองหนุน/กองเกินที่มีประสบการณ์ด้านไซเบอร์มาประกอบกำลังในสถานการณ์ฉุกเฉินและการทำให้บุคลกรไซเบอร์สามารถทำงานได้ ทั้งภาครัฐและเอกชน อาศัยหลักการ “แบ่งเวลา” ตามความเหมาะสมหรือความต้องการของบุคคลนั้น ๆ 3) การจัดตั้งคณะทำงานเพื่อหาแนวทางร่วมกันระหว่างหน่วยที่เกี่ยวข้องเพื่อให้ได้ข้อสรุปการบริหารจัดการกำลังพลสำรองไซเบอร์ 4) การยื่นข้อเสนอพิเศษให้บุคลากรที่มีพื้นฐานด้านคอมพิวเตอร์อยู่แล้ว เป็นการสร้างทางเลือกให้แก่ผู้ที่คิดจะหลีกเลี่ยงการเกณฑ์ทหารด้วยมีภาพลักษณ์ของการฝึกทหารใหม่ที่มีการใช้ความรุนแรง แต่สามารถเข้ารับการเกณฑ์ทหาร

ด้วยการฝึกแบบพิเศษ เพื่อให้สามารถเข้าทำการในลักษณะปฏิบัติการไซเบอร์ได้ ทั้งในหน่วยทหารและองค์กรที่มีความต้องการบุคลากรด้านไซเบอร์

พลเรือตรี อุดม ประตาทะยัง (2560)[86] ได้ศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษาแนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต

ผลการศึกษาพบว่า การมีหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศเพื่อการป้องกันภัยคุกคามทางไซเบอร์ และประสานงานทั้งภายในและระหว่างประเทศ ในการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์มีความสำคัญอีกทั้งต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐและเอกชน เพื่อยกระดับความพร้อมรับมือภัยคุกคามทางไซเบอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ถึงแม้ว่าในปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์มากขึ้น แต่องค์กรต่าง ๆ มีการรักษาความปลอดภัยแบบแยกส่วน และบางครั้งมีความขัดแย้งกัน ประกอบกับการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์ และการพัฒนาบุคลากรด้านนี้ ยังไม่ทันต่อความต้องการของประเทศ องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์ เนื่องจากกลัวการเสียชื่อเสียง นอกจากนี้ ร่างพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันนั้น อาจยังขาดองค์ประกอบที่สำคัญหลายประการ

นาวาอากาศเอก ชนินทร เฉลิมทรัพย์ (2560)[87] ได้ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กรการบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการศึกษาค้นคว้า นโยบาย ยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยผลการศึกษาพบว่า การศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กรการบูรณาการการบริหารจัดการ และการรักษาความมั่นคงปลอดภัยไซ

เบอร์ จำเป็นต้องมีองค์กรที่นำเทคนิคการบริหารจัดการมาใช้ ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้น การบูรณาการ การบริหารจัดการ ต้องมีเจ้าภาพที่ชัดเจน ทำงานแบบมุ่งเน้นผลงานตามยุทธศาสตร์ โดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุเป้าหมาย สำหรับภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคาม ที่มีการเปลี่ยนแปลงไปจากเดิม มีรูปแบบการโจมตีที่หลากหลาย การวางแผนป้องกัน คือ การปรับกลยุทธ์ในการรับมือและใช้ระบบมาตรฐานทางไซเบอร์ (ISO/IEC 27001 : 2013) หรือมาตรฐานที่จะถูกพัฒนาขึ้นต่อไป มาช่วยดำเนินการบริหารจัดการ แต่ปัจจัยในการดำเนินงานที่สำคัญที่สุดคือมนุษย์ การศึกษาแนวนโยบายและยุทธศาสตร์ตลอดจนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่า กระทรวงกลาโหมใช้แนวความคิดในการป้องกันทางไซเบอร์ เช่นเดียวกับการศึกษามั่นคงของประเทศ โดยเน้นการป้องกันเชิงรุก การผนึกกำลังป้องกันประเทศ และ การร่วมมือด้านความมั่นคงทางไซเบอร์ โดยได้จัดตั้งส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity operation center : CSDC) เชิงรับและส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer security incident response team : CSIRT) สำหรับกระทรวงดิจิทัลฯ ได้กำหนดกรอบแนวคิดและนโยบายในระดับชาติกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure : CII) ของประเทศ กำหนดแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard operating procedure : SOP) รวมทั้งเสนอแนวความคิดในการจัดตั้ง Cybersecurity agency (CSA) หน้าที่เป็นหน่วยงานกลาง ในการประสานงานและเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์

จิตสุภา ฤทธิผลิน 2564[83] ได้ศึกษาเกี่ยวกับกลยุทธ์การคืนสภาพได้ทางไซเบอร์ ซึ่งเป็นแนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล การเตรียมความพร้อมขององค์กรในการรับมือกับภัยคุกคามทางไซเบอร์นั้นเป็นสิ่งที่องค์กรสามารถดำเนินการได้ ควรเริ่มตั้งแต่ระดับนโยบายแล้วถ่ายทอดลงสู่ระดับปฏิบัติการ การที่องค์กรมีทักษะที่ดีในการรับมือ แก้ไข และเยียวยาจากเหตุการณ์ทางไซเบอร์ หรือที่เรียกว่าการคืนสภาพได้ทางไซเบอร์ (Cyber resilience) ถือว่าเป็นสภาวะที่องค์กรมีความทนทานซึ่งประกอบด้วยความคล่องตัว (Agility) และ ความทนทาน (Robustness) ต่อภัยคุกคามทาง

ไซเบอร์ จะช่วยให้องค์กรสามารถป้องกัน ตรวจจับ และ ตอบสนองต่อการถูกโจมตีทางไซเบอร์และกลับคืนสู่สภาพปกติได้อย่างรวดเร็ว

การคืนสภาพได้ทางไซเบอร์มีผลโดยตรงต่อการหน่วยงานและองค์กร ช่วยสร้างความเชื่อมั่นในพร้อมของหน่วยงาน ทำให้เกิดความได้เปรียบได้ เนื่องจากบุคคลภายนอกจะพบว่าองค์กรมีความพร้อมในการปรับตัวและฟื้นตัวจากการโจมตีได้อย่างรวดเร็ว จึงพบได้ว่าหลายองค์กรเริ่มมีความตระหนักเกี่ยวกับความปลอดภัยของเทคโนโลยีสารสนเทศ และเริ่มมีการนำมาตรฐานความปลอดภัยระดับสากลมาใช้เป็นกรอบแนวทางกันมากเพราะสามารถช่วยให้องค์กรสามารถบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

บทที่ 4

บทสรุป

จากยุทธศาสตร์ชาติ 20 ปี พ.ศ. 2561 – 2580 ซึ่งมีเป้าหมายให้บรรลุเป็นรูปธรรมชัดเจน คือ “ประเทศชาติมั่นคง ประชาชนมีความสุข” มั่นคง โดยยึดถือแนวทางการดำเนินการ หรือแนวความคิดทางยุทธศาสตร์ จำนวน 3 แนวความคิด ได้แก่ 1) การป้องกันเชิงรุก (Active Defence), 2) การผนึกกำลังป้องกันประเทศ (United Defence), และ 3) การสร้างความร่วมมือด้านความมั่นคง (Security Cooperation) จึงเป็นยุทธศาสตร์ที่หน่วยงานภาครัฐทุกหน่วยพึงปฏิบัติให้บรรลุเป้าหมาย และให้เกิดความมั่นคงสูงสุด

การวิจัยเรื่องภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นการศึกษาปัญหาการโจมตีทางไซเบอร์ในปัจจุบัน ศึกษายุทธศาสตร์การจัดการภัยคุกคามทางไซเบอร์ทางการทหารและของประเทศ และศึกษาภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เพื่อรองรับภัยคุกคามทาง ไซเบอร์ (Cyber) พร้อมกับการวิเคราะห์ความสอดคล้องและเปรียบเทียบข้อมูล ยุทธศาสตร์ชาติ 20 ปี แผนแม่บท พระราชบัญญัติ นโยบายและแผนปฏิบัติการ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ จนนำมาสู่บทสรุปผลการวิจัยและข้อเสนอแนะ เพื่อตอบโจทย์ตาม ยุทธศาสตร์ที่ 1 ด้านความมั่นคงและ ยุทธศาสตร์ที่ 2 ด้านการสร้างความสามารถในการแข่งขัน ผู้วิจัยสามารถสรุปผลการศึกษาและข้อเสนอแนะได้ดังนี้

สรุปผลการวิจัย

ในยุคที่อินเทอร์เน็ตในทุกสิ่ง (Internet of Things “IoT”) ที่มีการเชื่อมโยงอุปกรณ์ต่างๆเข้าด้วยกันด้วยไซเบอร์สเปซ (Cyber Space) การพัฒนาเทคโนโลยีการติดต่อสื่อสาร การทำงานระยะไกล การทำธุรกรรมทางการเงินรวมถึงอุปกรณ์ต่างๆ ล้วนเชื่อมโยงเข้าสู่โลกอินเทอร์เน็ต ยุทธศาสตร์ของทั้งภาครัฐ ภาคเอกชน และพลเรือน ควรคำนึงถึงการรักษาความปลอดภัยบนโลกไซเบอร์ของตนเป็นหลักตามกรอบยุทธศาสตร์ชาติ 20ปีที่ได้วางไว้ และควรกำหนดแนวทางการปฏิบัติ แบ่งออกเป็น 5 รูปแบบ เพื่อการเพิ่ม

ประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้ 1) การบูรณาการความร่วมมือทางไซเบอร์ การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ หน่วยงานภาคเอกชน และภาคประชาชน 2) การวางระบบป้องกันภัยคุกคามทางไซเบอร์ 3) สร้างความตระหนักและให้ความรู้แก่ผู้บริหาร ผู้ปฏิบัติและผู้ใช้งานของหน่วยงานภาครัฐ ภาคเอกชนและพลเรือน 4) การสร้าง การเพิ่มกำลังพลและบุคลากรที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ 5) ความร่วมมือด้านความมั่นคงทางไซเบอร์ภายในและระหว่างประเทศ

ด้วยเหตุนี้จึงควรกำหนดแนวทางในการขับเคลื่อนยุทธศาสตร์ฯ ให้ชัดเจนไม่ทับซ้อนกันเพราะการกำหนดแนวทางการขับเคลื่อนยุทธศาสตร์เพื่อนำยุทธศาสตร์ไปสู่หนทางการปฏิบัตินั้นมีความสำคัญยิ่งต่อความสำเร็จและล้มเหลวต่อยุทธศาสตร์ชาติ การมุ่งมั่นที่จะช่วยให้เกิดการสร้างสรรค์นวัตกรรม การเจริญเติบโตทางเศรษฐกิจ และความเจริญรุ่งเรืองให้กับประเทศพร้อมกับการรักษาความมั่นคงปลอดภัยบนโลกไซเบอร์ที่แข็งแกร่ง จะสามารถช่วยให้การพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ด้านนี้ ให้เกิดความทันสมัย แข่งขันบนเวทีโลกได้และตอบสนองต่อยุทธศาสตร์ไทยแลน์4.0 ที่เกี่ยวโยงถึงระบบเศรษฐกิจของประเทศและนำพาไปสู่ความมั่นคงแห่งชาติสืบไป

ข้อเสนอแนะ

กระทรวงกลาโหม กองบัญชาการกองทัพไทยและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรเป็นหลักในการบูรณาการความมั่นคงปลอดภัยทางไซเบอร์สำหรับ เหล่าทัพ, ภาครัฐ, ภาคเอกชน และพลเรือน เพื่อให้เกิดเป็นรูปธรรม โดยเฉพาะการส่งเสริมให้เกิดการตระหนักถึงภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยไซเบอร์แก่กำลังพลและบุคลากรทั่วไป โดยการจัดทำโครงการกระจายความรู้พื้นฐานด้านภัยคุกคามทางไซเบอร์ เริ่มจากในหน่วยงานการศึกษาเช่น โรงเรียนทหาร โรงเรียนเตรียมทหาร ซึ่งสามารถเริ่มให้ความรู้พื้นฐานการรักษาความปลอดภัยทางไซเบอร์เพื่อรองรับงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพได้ในอนาคต นอกจากนี้ควรส่งเสริมให้เกิดหลักสูตรการฝึกร่วมระหว่าง สกมช. กับ หลักสูตร เสนาธิการทหาร (วสท.), วิทยาลัยการทัพบก (วทบ.), วิทยาลัยการทัพเรือ (วทร.) และวิทยาลัยการทัพอากาศ (วทอ.)พร้อมกับหน่วยงานโครงสร้างพื้นฐานสารสนเทศสำคัญของประเทศทุกปี

[65,66,91,92] โดยเป็นการจัดการฝึกแก้ไขสถานการณ์ฉุกเฉิน และการฝึกร่วมของวิทยาลัยการทัพ ซึ่งการฝึกจำลองสถานการณ์การต่อต้านการก่อการร้ายทางไซเบอร์หรือการทำสงครามไซเบอร์นี้จะช่วยส่งเสริมการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ เพิ่มพูนทักษะในการรับมือต่อสถานการณ์ เพื่อให้ผู้เข้ารับการฝึกทั้งระดับผู้บริหารและระดับหัวหน้าจากหน่วยต่างๆ ได้รับประสบการณ์ในการบัญชาการภายใต้สถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ สามารถถ่ายทอดและใช้ประโยชน์ในการบริหารหน่วยงาน ส่งเสริมองค์ความรู้ให้กำลังพลและบุคลากรให้ทราบถึงความสำคัญในการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์และสามารถนำไปปฏิบัติใช้ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

เนื้อหาในเอกสารวิจัยฉบับนี้ เน้นการภาพรวมแนวทางการเตรียมความพร้อมองค์กรและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีรูปแบบการปฏิบัติที่เป็นไปในแนวทางเดียวกัน ส่งเสริมให้เกิดการตะหนักถึงภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์และก่อให้เกิดประสิทธิภาพสูงสุดในการปฏิบัติการป้องกันภัยความมั่นคงปลอดภัยทางไซเบอร์

ด้วยเหตุนี้จึงควรมีการพัฒนาต่อยอดจากการวิจัยครั้งนี้ ในเรื่องการเสริมสร้างความพร้อมของบุคลากรด้านไซเบอร์ เพื่อรองรับการทำงานในหน่วยงานโครงสร้างพื้นฐานสารสนเทศหลักของประเทศ ซึ่งประเทศไทยยังขาดความพร้อมของบุคลากรด้านไซเบอร์ในระดับปฏิบัติการและระดับเชี่ยวชาญ พร้อมด้วยการศึกษาการบูรณาการร่วมกันบนแพตฟอร์มที่เป็นอนึ่งเดียวกันเพื่อให้เกิดประโยชน์สูงสุด ทั้งนี้เพื่อตอบสนองแนวคิดยุทธศาสตร์ชาติ ได้แก่ 1.การป้องกันเชิงรุก (Active Defence) 2. การผนึกกำลังป้องกันประเทศ (United Defence) และ3. การสร้างความร่วมมือด้านความมั่นคง (Security Cooperation) โดยทั้ง 3 แนวความคิดนี้จะยึดมั่นในแนวความคิดเชิงป้องกัน (Preventive) เป็นหลัก อีกทั้งการสร้างความตระหนักรู้ของหน่วยงานรัฐและเอกชนให้ความสำคัญกับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์อย่างเต็มที่ และการสร้างแรงจูงใจให้กับกำลังพลและบุคลากรเรื่องการเสริมความรู้เพื่อเพิ่มศักยภาพด้านไซเบอร์ให้กับตนเองอย่างการสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากลจะส่งผลให้เกิดความมั่นคงของประเทศอย่างยั่งยืน

เอกสารอ้างอิง

1. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) [อินเทอร์เน็ต]. แผนปฏิบัติการ ระยะ 3ปี พ.ศ.2563-2565. กรุงเทพฯ; 2563 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

2. Alexander Kott. The Internet of Battle Things. [Internet]. RESEARCHGATE; 2016 [cited 2022 May 20]. Available from:

3. Lori Cameron, Internet of Things Meets the Military and Battlefield “Connecting Gear and Biometric Wearables for an IoMT and IoBT”. [Internet] Computer.org; 2020. [cited 2022 May 20]. Available from:

4. Global Cybersecurity Index. [Internet] International Telecommunication Union; 2021. [cited 2022 May 20]. Available from:

5. FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks, “Statements and Releases”. [Internet] The White House; May 12, 2021 [cited 2022 May 20]. Available from:

6. Statement by President Biden on our Nation’s Cybersecurity, “Statements and Releases”.[Internet] The White House; March 21, 2022 [cited 2022 May 20]. Available from:

7. Cybersecurity & Infrastructure Security Agency: Cyber Threat Source Descriptions. [Internet] Cybersecurity & Infrastructure Security Agency “CISA” [cited 2022 May 20]. Available from:

8. Asean Cyberthreat assessment. [Internet]. INTERPOL; 2021 [cited 2022 May 20]. Available from:

9. Indo-Pacific Strategy of The United States. [อินเทอร์เน็ต] สถานฑูตสหรัฐฯและสถานกงสุลในประทศไทย; 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

10. ผลสำรวจโดยไมโครซอฟท์และฟรอสต์ แอนด์ ซัลลิแวนชี้ ภัยคุกคามทางไซเบอร์สามารถสร้างความเสียหายทางเศรษฐกิจ ให้องค์กรไทยถึง 2.86 แสนล้านบาท. [อินเทอร์เน็ต] Techtalkthai; 2018. [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

11. In Focus: Cyber Attack-คลื่นใต้น้ำแห่งยุคดิจิทัลที่ต้องจับตามอง. [อินเทอร์เน็ต] สำนักข่าวอินโฟเควสท์; 2564 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

12. The Crowdstrike global Threat Report. [Internet] Crowdstrike; 2021 [cited 2022 May 20]. Available from:

13. WHAT IS A ZERO - DAY EXPLOIT ? [Internet] Crowdstrike; 2022 [cited 2022 May 20]. Available from:

14. ZERODIUM Exploit Acquisition Program. [Internet] ZERODIUM; 2022 [cited 2022 May 20]. Available from:

15. สถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ThaiCERT. [อินเทอร์เน็ต] ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน); 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

16. อนุทินยอมรับฐานข้อมูลคนไข้ถูกเจาะ สั่งยกระดับการป้องกันระบบคอมพิวเตอร์ สธ. [อินเทอร์เน็ต] สำนักข่าว BBC NEWS; 7กันยายน 2564 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

17. ประเภทและตัวอย่างภัยคุกคาม ThaiCERT Annual Report 2017. [อินเทอร์เน็ต] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ); 2017, หน้า 82 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. [ภาคผนวก ก.] เข้าถึงได้จาก

18. ลำดับเหตุการณ์การโจมตีทางไซเบอร์ที่สำคัญในประเทศไทย ThaiCERT Annual Report 2017. [อินเทอร์เน็ต] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน); 2017 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. [หน้า23-24] เข้าถึงได้จาก

19. Reuters Staff, Suspected cyber attack hits Iran oil industry. [Internet] REUTERS; April 23, 2012. [cited 2022 May 20]. Available from:

20. ภัยร้าย STUXNET ระเบิดนิวเคลียร์แห่งโลกไซเบอร์. [อินเทอร์เน็ต] บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน); 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

21. ENISA THREAT LANDSCAPE REPORT 2021 วารสาร [อินเทอร์เน็ต] European Union Agency for Cybersecurity [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

22. ทำความรู้จักภัยคุกคามรูปแบบใหม่ Crytojacking [อินเทอร์เน็ต] บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน); 2018 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

23. WORAPON H, MITRE ATT&CK คืออะไร? แล้วมีประโยชน์อย่างไร? [อินเทอร์เน็ต] BLOG.ESET; 2020 [cited 2022 May 20]. เข้าถึงได้จาก

24. MITRE, ATT&CK Enterprise Framework. [Internet] MITRE; 2021 [cited 2022 May 20]. Available from:

25. Cybersecurity Capacity Maturity Model for Nation (CMM), 2021 EDITION [Internet] Global Cyber Security Capacity Centre, Oxford Martin School; 2021 [cited 2022 May 20]. Available from:

26. 20 Coolest Careers in Cybersecurity, | SANS Training [Internet]. 2021 [cited 2022 May 20]. Available from:

27. Cybersecurity Courses & Certifications, | SANS Training [Internet]. 2021 [cited 2022 May 20]. Available from:

28. Guide to Developing a National Cybersecurity Strategy, 2nd Edition “NCS”. [Internet] International Telecommunication Union (ITU); 2021 [cited 2022 May 20]. Available from:

29. ITU Cybersecurity programme: CIRT framework. [Internet] International Telecommunication Union (ITU); 2021 [cited 2022 May 20]. Available from:

30. ITU CIRTs World-wide Status. [Internet] International Telecommunication Union (ITU); 2022 [cited 2022 May 20]. Available from:

31. Cybersecurity Training & Exercises, | ITUAcademy [Internet]. 2022 [cited 2022 May 20]. Available from:

32. First NCSS Good Practice Guide, Natioanl Cyber Security Strategy Good Practice Guide 2012 for EU Member States and EFTA countries. [Internet] European Union Agency for Cybersecurity (ENISA); 2012 [cited 2022 May 20]. Available from:

33. National Cyber Security Strategies: An Implementation Guide. [Internet] European Union Agency for Cybersecurity (ENISA); 2012 [cited 2022 May 20]. Available from:

34. Good practices in innovation on Cybersecurity under the NCSS. [Internet] European Union Agency for Cybersecurity (ENISA); 2019 [cited 2022 May 20]. Available from:

35. National Capabilities Assessment Framework. [Internet] European Union Agency for Cybersecurity (ENISA); 2020 [cited 2022 May 20]. Available from:

36. Good practices in innovation on cybersecurity under the NCSS. [Internet] European Union Agency for Cybersecurity (ENISA); 2020 [cited 2022 May 20]. Available from:

37. Good practices in innovation on Cybersecurity under the NCSS. [Internet] European Union Agency for Cybersecurity (ENISA); 2019 [cited 2022 May 20]. Available from:

38. Raising Awareness of Cybersecurity. [Internet] European Union Agency for Cybersecurity (ENISA); 2021 [cited 2022 May 20]. Available from:

39. Training for Cybersecurity Specialists, | enisa (European Union Agency for Cybersecurity) [Internet]. 2022 [cited 2022 May 20]. Available from:

40. ISO/IEC 27001:2013 (Information Security Management System). [Internet] The British Standard Institution (bsi); 2022 [cited 2022 May 20]. Available from:

41. นันทนิตร์ มีพร้อม, นักตรวจสอบภายใน: มาตรฐาน ISO/IEC 27001 : 2013. [Internet] มหาวิทยาลัยมหิดล; 2022 [cited 2022 May 20]. Available from:

42. BSI Training Academy Course Portfolio (Information Security Management System). [Internet] The British Standard Institution (bsi); 2022 [cited 2022 May 20]. Available from:

43. Appendix C - Incident Classification. [Internet] The European Computer Security Incident Response Team Network (eCSIRT); 2022 [cited 2022 May 20]. Available from:

44. NCI Academy, C4ISR & Cyber | Training Catalogue – 2021 [cited 2022 May 20]. Available from:

45. Getting Started with the NIST Cybersecurity Framework. [Internet] National Institute of Standards and Technology (NIST); 2022 [cited 2022 May 20]. Available from:

46. Framework for Improving Critical Infrastructure Cybersecurity. [Internet] National Institute of Standards and Technology (NIST); 2022 [cited 2022 May 20]. Available from:

47. CISA Cybersecurity Framework, | Infrastructure [Internet]. 2021 [cited 2022 May 20]. Available from:

48. Critical Infrastructure Training, | Training [Internet]. 2021 [cited 2022 May 20]. Available from:

49. Workforce Framework for Cybersecurity (NICE Framework). [Internet] National Initiative for Cybersecurity Careers and Studies (NICCS); 2022 [cited 2022 May 20]. Available from:

50. Introduction to NICE Cybersecurity Workforce Framework. [Internet] National Institute of Standards and Technology U.S. Department of Commerce ; 2022 [cited 2022 May 20]. Available from:

51. The DoD Cyber Workforce Framework [Internet] DoD CYBER EXCHANGE; 2022 [cited 2022 May 20]. Available from:

52. Interagency Federal Cyber Career Pathways Initiative. [Internet] DoD CYBER; 2020 [cited 2022 May 20]. Available from:

53. DoD Cybersecurity Policy Chart [Internet] DoD CYBER; 2020 [cited 2022 May 20]. Available from:

54. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. ภาวะสังคมไทยไตรมาสหนึ่ง [อินเทอร์เน็ต] สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ; 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

55. ลัฐกา เนตรทัศน์, อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์. [อินเทอร์เน็ต] Law for ASEAN สำนักงานคณะกรรมการกฤษฎีกา (ประเทศไทย); 2563 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

56. สมดุลความมั่นคงปลอดภัยไซเบอร์กับการค้าระหว่างประเทศในอาเซียน. [อินเทอร์เน็ต] โพสต์ทูเดย์ดอทคอม; 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

57. ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์. [อินเทอร์เน็ต] สำนักเลขาธิการอาเซียนแห่งชาติ; 2020 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

58. ราชกิจจานุเบกษา, ประกาศ เรื่อง ยุทธศาสตร์ชาติ พ.ศ. 2561-2580 เล่ม 135 ตอนที่ 82 ก หน้าที่ 1, ราชกิจจานุเบกษา 13 ตุลาคม 2561 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

59. ราชกิจจานุเบกษา, พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เล่ม 136 ตอนที่ 69 ก หน้าที่ 20, ราชกิจจานุเบกษา 27 พฤษภาคม 2562 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

60. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ.2564 เล่ม 138 ตอนพิเศษ 194 หน้าที่ 14, ราชกิจจานุเบกษา 23 สิงหาคม 2564 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก 

61. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ.2564 เล่ม 138 ตอนพิเศษ 194 ง. หน้าที่ 14, ราชกิจจานุเบกษา 23 สิงหาคม 2564 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

62. การประชุมเตรียมความพร้อมเป็นหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามผลการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2564. [อินเทอร์เน็ต] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ; 2564 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

63. การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์. [อินเทอร์เน็ต] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ; 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

64. แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2565 – 2570 [อินเทอร์เน็ต] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

65. NCSA ชู 6 หลักสูตร ในโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ยกระดับศักยภาพให้ทัดเทียมต่างประเทศ [อินเทอร์เน็ต] adslthailand.com; 2564 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

66. (ร่าง) แผนรับมือเหตุการณ์ทางไซเบอร์ สำหรับการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2565, [อินเทอร์เน็ต] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

67. ราชกิจจานุเบกษา, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เล่ม 136 ตอนที่ 69 ก หน้าที่ 52, ราชกิจจานุเบกษา 27 พฤษภาคม 2562 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

68. สำนักงานสภาความมั่นคงแห่งชาติ, แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (1) ประเด็น ความมั่นคง พ.ศ. 2561-2580 [อินเทอร์เน็ต] สำนักงานสภาความมั่นคงแห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

69. สำนักงานสภาความมั่นคงแห่งชาติ, แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (7) ประเด็น โครงสร้างพื้นฐาน ระบบโลจิสติกส์ และดิจิทัล พ.ศ. 2561-2580 [อินเทอร์เน็ต] สำนักงานสภาความมั่นคงแห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

70. สำนักงานสภาความมั่นคงแห่งชาติ, ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 –2564 [อินเทอร์เน็ต] สำนักงานสภาความมั่นคงแห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

71. สำนักงานสภาความมั่นคงแห่งชาติ, สำนักนายกรัฐมนตรี แผนเตรียมพร้อมแห่งชาติ พ.ศ.2560-2564 [อินเทอร์เน็ต] สำนักงานสภาความมั่นคงแห่งชาติ [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

72. นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสำหรับองค์กร ตามแนวทางของมาตรฐาน ISO 27001 สำนักงานสภาความมั่นคงแห่งชาติ. [อินเทอร์เน็ต] มหาวิทยาลัยบูรพา; 2559 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

73. กระทรวงกลาโหม, ยุทธศาสตร์ป้องกันประเทศ พ.ศ. 2560-2579 [อินเทอร์เน็ต] กระทรวงกลาโหม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

74. แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ 5 ปี (พ.ศ. 2561 -2565), สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. [อินเทอร์เน็ต] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม; 2561 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

75. กระทรวงกลาโหม, แผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง (พ.ศ. 2566 – 2570) [อินเทอร์เน็ต] กระทรวงกลาโหม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

76. กองบัญชาการกองทัพไทย, แผนปฏิบัติการด้านดิจิทัล ระยะที่ 1 พ.ศ. 2563 – 2565 [อินเทอร์เน็ต] กองบัญชาการกองทัพไทย [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

77. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [อินเทอร์เน็ต] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

78. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [อินเทอร์เน็ต] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

79. แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ระยะ 3 ปี พ.ศ.2559-2561 [อินเทอร์เน็ต] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

80. กระทรวงคมนาคม, แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562-2566 [อินเทอร์เน็ต] กระทรวงคมนาคม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

81. นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ 2561-2580) [อินเทอร์เน็ต] สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

82. ราชกิจจานุเบกษา, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ พ.ศ. 2564 เล่ม 138 ตอนที่ 303 ง หน้าที่ 3, ราชกิจจานุเบกษา 11 ธันวาคม 2562 [อินเทอร์เน็ต] ราชกิจจานุเบกษา [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

83. จิตสุภา ฤทธิผลิน, กลยุทธ์การคืนสภาพได้ทางไซเบอร์: แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล. [อินเทอร์เน็ต] สำนักเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ; 2021 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

84. อริย์ธัช แก้วเกาะสะบ้า, ศูนย์ไซเบอร์กองทัพบก. [อินเทอร์เน็ต] สำนักงานเลขาธิการสภาผู้แทนราษฎร; 2560 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

85. ปรัชญา เฉลิมวัฒน์ พล.ต. แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อการเตรียมพร้อมรับภัยคุกคามระดับชาติ. [อินเทอร์เน็ต] วิทยาลัยป้องกันราชอาณาจักร; 2560 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

86. อุดม ประตาทะยัง, พล.ต. แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ ความมั่นคงปลอดภัยทางไซเบอร์. [อินเทอร์เน็ต] วิทยาลัยป้องกันราชอาณาจักร; 2560 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

87. ชนินทร เฉลิมทรัพย์, น.อ. แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ. [อินเทอร์เน็ต] วิทยาลัยป้องกันราชอาณาจักร; 2560 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

88. หลักสูตรทางด้านดิจิทัล. [อินเทอร์เน็ต] สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy; 2565 [เข้าถึงเมื่อ 13 พฤษภาคม 2565]. เข้าถึงได้จาก

89. Thales CDSDP Conference, Thales a global and trusted partner in Cybersecurity, Lisbon 2017 - Part1 [Internet]. Thales; 2021 [cited 2022 May 20]. Available from:

90. Thales CDSDP Conference, Thales a global and trusted partner in Cybersecurity, Lisbon 2017 - Part2 [Internet]. Thales; 2021 [cited 2022 May 20]. Available from:

91. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน หน่วยที่ 11 ระบบตรวจจับการบุกรุก [อินเทอร์เน็ต] Thailand National Cyber Academy, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ; 2565 [เข้าถึงเมื่อ 30 พฤษภาคม 2565]. เข้าถึงได้จาก

92. หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน หน่วยที่ 16 การจัดการเหตุขัดข้อง [อินเทอร์เน็ต] Thailand National Cyber Academy, สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ; 2565 [เข้าถึงเมื่อ 30 พฤษภาคม 2565]. เข้าถึงได้จาก

ผนวก ก.

จำแนกประเภทของการโจมตีทางไซเบอร์ในปัจจุบัน ได้ดังนี้

ภัยจากการบุกรุกหรือเจาะเข้าระบบ (Intrusion Attempts)

การโจมตีระบบโดยอาศัยช่องโหว่ในซอฟต์แวร์ หรือ ฮาร์ดแวร์ (Exploit Vulnerability) เป็นพฤติกรรมที่มีการพยายามใช้ช่องทางต่าง ๆ โจมตีมายังเป้าหมาย อาจเป็นช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชันต่าง ๆ ที่เพิ่งมีการค้นพบ หรือเป็นช่องโหว่เดิมที่มีอยู่ในระบบ หากเป้าหมายไม่ได้ทำการปิดช่องโหว่หรือแก้ไขก็อาจตกเป็นเหยื่อได้ รวมถึงการพยายามเข้าถึงเครือข่ายจาก IP ต้องสงสัย การเปิด Known Port โดยไม่จำกัดการเข้าใช้งาน เมื่อมีข้อมูลเหล่านี้แล้วแฮกเกอร์ (Hacker) จะทดลองเจาะเข้ามายังเครือข่าย ดังนั้นการหมั่นปรับปรุง Firmware และระบบปฏิบัติการเพื่อปิดช่องโหว่เหล่านี้ให้ได้มากที่สุดจึงเป็นเรื่องสำคัญเสมอ

การพยายามแสดงตนแทนเจ้าของบัญชี Login Attempt สาเหตุหลักยังคงมาจาก Human Error หรือเกิดจากตัวผู้ใช้งาน อาทิ การลืมรหัสผ่าน การจดจำ User และ Password ไว้ในระบบแล้วไม่ได้ Update เมื่อทำการเปลี่ยนรหัสผ่าน ฯลฯ ภัยคุกคามชนิดนี้จะยังไม่มีอันตรายแต่อาจทำให้เกิดความน่ารำคาญใจแก่ผู้ใช้งานหรือเจ้าของระบบเท่านั้น อย่างไรก็ตาม จากข้อมูลสถิติยังมีการตรวจพบความพยายาม Login และเข้าจากภายนอกผ่านช่องทาง Internet Access มายังระบบที่ต้องเปิดให้ผู้ใช้งาน หรือผู้ใช้บริการเข้าถึง ดังนั้น ทุกหน่วยงาน บริษัท หรือองค์กรต่าง ๆ ควรปฏิบัติตามนโยบายความมั่นคงปลอดภัยเกี่ยวกับ Password หรือรหัสผ่านอย่างเคร่งครัด รวมถึงหมั่นตรวจสอบว่าเป็นการพยายามเข้าถึงระบบจากภายนอกที่ผิดปกติหรือไม่ อีกทั้ง ควรมีแผนรับมือและจัดการกับเหตุการณ์ที่เกิดขึ้น เพื่อป้องกันผลกระทบและความเสียหายที่อาจเกิดขึ้นในอนาคต

การโจมตีด้วยโค้ด Malicious Code

การโจมตีด้วยโปรแกรมไม่พึงประสงค์ สาเหตุหลักมาจากพนักงานขององค์กรเองที่ขาดความรู้ความเข้าใจ และความตระหนักทางด้าน Cyber Security รวมถึงการควบคุม Policy ที่ไม่รัดกุม ส่งผลให้มีมัลแวร์หลุดรอดเข้ามายังระบบจนส่งผลให้เกิด

ความเสียหายหนักตามมา ไม่ว่าจะเป็นการโดนโจมตีจาก Ransomware ไวรัส และโทรจันที่ยังมีให้พบได้อยู่เสมอ

ความพร้อมในการใช้งาน / ในการให้บริการ Availability

พฤติกรรมการสร้างปริมาณ Traffic/Packet ที่ผิดปกติเพื่อก่อกวนในระบบ Network (Flood Network) หรือการ DoS (Denial of Service) รูปแบบหนึ่ง โดยมีสาเหตุ มาจากการติดมัลแวร์ หรือการโจมตีผ่านช่องโหว่ต่าง ๆ ทำให้มีการรับหรือส่ง Traffic เป็นจำนวนมาก จนทำให้รบกวนการทำงานของอุปกรณ์ด้านความปลอดภัย (Security Device) ในระบบได้ เช่น อุปกรณ์ Firewall ต้องทำงานหนักจากการบล็อคหรือป้องกัน Traffic ที่ผิดปกติ จนส่งผลกระทบให้การใช้งานระบบช้าลง หรือแม้กระทั่งหยุดทำงานได้

การเก็บรวบรวมข้อมูล Information Gathering

ยังคงเป็นพฤติกรรมพื้นฐานของการเจาะระบบที่ Hacker หรือผู้ไม่หวังดีจะกระทำเพื่อหาข้อมูลเบื้องต้น การเก็บข้อมูลของเป้าหมายไม่ว่าจะเป็นจากการใช้เครื่องมือเฉพาะเจาะจงเพื่อค้นหา หรือแม้แต่ข้อมูลการประกาศรับสมัครงานขององค์กรเอง สิ่งเล็ก ๆ น้อย ๆ เหล่านี้ ล้วนเป็นช่องทางในการต่อยอดให้เหล่า Hacker เข้าถึงระบบของเราได้

การละเมิดนโยบายขององค์กร Policy Violation

การละเมิดนโยบายขององค์กร อาจจะด้วยความไม่ตั้งใจของพนักงาน เช่น การพยายามใช้งาน USB ซึ่งมักจะเป็นหนึ่งในช่องทางการแพร่มัลแวร์ การเข้าเว็บไซต์ต้องห้าม การแอบติดตั้งโปรแกรม หรือมาจากการโจมตีของผู้ไม่หวังดี เช่น การพยายามเข้าใช้งานระบบนอกเวลางานซึ่งเข้าถึงจากต่างประเทศ

Trojan.Multi.BroSubsc.gen

เป็นโทรจันชนิดหนึ่งที่ช่วยให้ Hacker สามารถฝัง Backdoor ไว้ในเครื่องเหยื่อได้ ซึ่งช่องทางการแพร่กระจายมาจากการดาวน์โหลดโปรแกรมปลอม ไฟล์แนบหลอกลวง เว็บไซต์ที่ไม่ปลอดภัย หรือโฆษณาหลอกลวงต่าง ๆ จุดมุ่งหมายของโทรจันประเภทนี้คือการเก็บข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยการแอบติดตั้ง Ransomware หรือ ไวรัสอื่น ๆ เพื่อขโมยข้อมูล ความน่ากลัวของมัลแวร์ชนิดนี้คือ การดัก

ปล้นเบราเซอร์และเริ่มแสดงโฆษณาที่แสนน่ารำคาญโดยใช้ข้อมูลจาก Browser History ซึ่งโฆษณาเหล่านี้ล้วนแฝงไปด้วยมัลแวร์

Backdoor: Andromeda.Botnet

เป็นโทรจันที่อยู่ในตระกูลAndromeda ทำตัวเป็น Backdoor สำหรับแฮกเกอร์ไว้ Remote เข้าเครื่องเหยื่อและมีหลายความสามารถ ไม่ว่าจะเป็นการติดตั้งมัลแวร์ตัวอื่นเพิ่มเติม หรือการขโมยข้อมูลต่างๆ จากเครื่องของเหยื่อออกไป สาเหตุการแพร่กระจายส่วนใหญ่มาจากไฟล์แนบที่มากับอีเมลหลอกลวง

W32/Khalesi.XB!tr

จัดอยู่ในกลุ่มของโทรจันเช่นกัน พฤติกรรมโดยทั่วไปคือการ Remote เข้าเครื่องเหยื่อจากระยะไกล เก็บข้อมูลจากแป้นพิมพ์ เก็บข้อมูลของเครื่องคอมพิวเตอร์ ดาวโหลด/อัปโหลดไฟล์ ติดตั้งมัลแวร์ตัวอื่นลงบนเครื่องเหยื่อ ใช้เป็น Bot เพื่อทำการโจมตี DoS ไปยังเครื่องเป้าหมาย

Backdoor: Backdoor.DoublePulsar

ถูกค้นพบในเดือนมีนาคม พ.ศ. 2560 (ค.ศ.2017) และถูกนำมาใช้ร่วมกับ WannaCry Ransomware ในเดือนพฤษภาคม พ.ศ. 2560 (ค.ศ.2017) DoublePulsar ใช้ช่องโหว่เก่าในระบบปฏิบัติการ Windows ในการฝังตัวเข้ามายังระบบ พฤติกรรมเหมือนกับโทรจันตัวอื่น ๆ คือการ Remote เข้ามาควบคุมเครื่อง

HEUR:Trojan.Script.Generic

โทรจันที่จัดเป็น Ransomware ชนิดหนึ่งแพร่ระบาดผ่านทางอีเมลหลอกลวง ที่แนบไฟล์ Ransomware หรือลิ้งก์หลอกลวงมาด้วย เพื่อให้เหยื่อหลงกลและกดดาวน์โหลด Ransomware มาที่เครื่อง จากนั้นจะทำการเข้ารหัสไฟล์และเรียกค่าไถ่

การหลอกลวงเพื่อผลประโยชน์ Fraud

เทคนิคการหลอกลวง Phishing โดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน

หน้าเว็บไซต์ปลอมบางหน้าจะใช้วิธีการที่แยบยล นั่นคือการฝังโทรจันที่สามารถขโมยข้อมูลที่ต้องการมากับหน้าเว็บไซต์ปลอมนั้นด้วย เช่น โทรจันที่ทำหน้าที่เป็น Key-logger ซึ่งจะคอยติดตามว่าผู้เสียหายพิมพ์คีย์บอร์ดอะไรบ้าง เป็นต้น เมื่อผู้เสียหายหลงกล กดลิงก์ตามเข้ามาที่หน้าเว็บไซต์ปลอมก็จะติดโทรจันชนิดนี้ไปโดยอัตโนมัติ และหากผู้เสียหายทำการล็อกอินเข้าใช้งานระบบใด ๆ ข้อมูลชื่อผู้ใช้ และรหัสผ่าน ของระบบนั้นก็จะถูกส่งไปยังผู้ประสงค์ร้าย

แก๊งคอลเซ็นเตอร์ Vishing และ Smishing พฤติกรรมของแก๊งเหล่านี้เข้าข่ายของ Vishing หรือ Voice-Phishing ซึ่งมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์ ส่วน Smishing หรือ Short Message Service-Phishing เป็นการหลอกลวงโดยใช้ข้อความสั้น SMS เช่น การได้รับ SMS อ้างว่ามาจากธนาคารเพื่อแจ้งลูกค้าว่าบัญชีของท่านถูกระงับ กรุณาติดต่อกลับที่หมายเลข ดังต่อไปนี้ ซึ่งเมื่อโทรตามหมายเลขที่ระบุไว้ ก็จะเข้าสู่กระบวนการ Vishing ต่อไป

การหลอกลวงที่มีเป้าหมายชัดเจน Spear-phishing และ Whaling เป็นกลวิธีของ Phishing ในการนำไปใช้งาน ผู้ประสงค์ร้ายมุ่งเป้าหมายที่องค์กร หรือบุคคลที่เป็นเป้าหมายชัดเจนอยู่แล้ว บุคคลที่มักตกเป็นเป้าหมายส่วนใหญ่จะเป็นผู้ที่มีบทบาทสำคัญในองค์กร มีความสามารถหรือรู้วิธีการเข้าถึงข้อมูลสำคัญขององค์กร การหลอกลวงแบบ Phishing ที่มีเป้าหมายชัดเจนนี้มีคำเรียกเฉพาะคือ Spear-phishing และหากเป้าหมายของ Spear-phishing นี้เป็นบุคคลที่มีตำแหน่งสูงหรือเป็นบุคคลสำคัญในองค์กรจะเรียกการหลอกลวงนี้ว่า Whaling (บุคคลสำคัญเป็นปลาตัวโตเสมือนปลาวาฬ)

ช่องโหว่ Log4Shell[12]

ช่องโหว่ที่ทำให้แฮกเกอร์สามารถเจาะระบบเข้ามาแฮกแอปพลิเคชันหลาย ๆ ตัวที่พัฒนาด้วยภาษา Java และมีการรับค่าจากผู้ใช้งาน (User Input) เข้าไปใช้ในฟังก์ชันการบันทึก Log ของ Java Library ที่ชื่อว่า Apache Log4J อาจจะตั้งใจเขียนโค้ดเองเพื่อ Log หรือว่ามี Library อื่น ๆที่ไปดึงมาใช้ทำการ Log ให้โดยเราไม่รู้ตัวก็ได้ เช่น VMware vCenter และแอปที่พัฒนาด้วย Web Framework ชั้นนำของโลก Java อย่าง Apache Strut และ Spring ก็มีความเสี่ยงจะใช้ log4j

Cryptojacking[22]

เป็นภัยคุกคามไซเบอร์ที่เจ้าของเว็บไซต์หรือแฮกเกอร์แอบรันสคริปต์บางอย่างบนเว็บเบราเซอร์ของผู้ใช้ เพื่อให้พวกเขาสามารถใช้ทรัพยากรบนเครื่องของผู้เข้าชมเว็บไซต์ในการขุดเหมืองเงินดิจิทัล เช่น Bitcoin หรือ Monero เพื่อสร้างรายได้ให้แก่ตนเอง อาจเรียกได้ว่าเป็นการขโมยทรัพยากรคอมพิวเตอร์มาใช้งานโดยที่ผู้ใช้ไม่รู้ตัว สามารถสังเกตได้หากอยู่ ๆ พบว่าอินเทอร์เน็ตเล่นได้ช้าลง คอมพิวเตอร์ทำงานช้าลง เครื่องร้อน และได้ยินเสียงพัดลมทำงานอย่างหนัก อาจหมายความว่ามีโอกาสสูงคอมพิวเตอร์ที่ใช้งานอยู่ที่จะตกเป็นเหยื่อของการโจมตีแบบ Cryptojacking แล้ว

การโจมตีแบบ Zero-day[13]

การโจมตีข้อบกพร่องของซอฟต์แวร์หรือฮาร์ดแวร์ที่มีช่องโหว่ทำให้เกิดเป็นช่องทางใช้สำหรับการโจมตี โดยข้อบกพร่องหรือช่องโหว่ที่กล่าวถึงนั้นเป็นช่องโหวใหม่ที่แฮกเกอร์เพิ่งค้นพบและใช้เป็นจุดเข้าโจมตี เท่ากับว่านักพัฒนาซอฟต์แวร์จะมีเวลาในการแก้ไขหาทางปิดช่องโหว่ดังกล่าวเหลือแค่เพียง "Zero-day" หรือ "0 วัน" เท่านั้น การใช้คำว่า Zero-day จะมีคำที่ควบคู่ตามมาด้วย ซึ่งมีความหมายแตกต่างกัน ดังต่อไปนี้

Zero-day Vulnerability หมายถึง ช่องโหวในซอฟต์แวร์ หรือฮาร์ดแวร์ที่นักพัฒนาค้นพบ เพราะถูกแฮกเกอร์ใช้ในการโจมตี ช่องโหว่ลักษณะนี้จัดว่าค่อนข้างอันตราย เพราะยังไม่มีแพทช์ (โปรแกรมPatch) แก้ไขออกมาให้อัปเดต แฮกเกอร์จึงมีโอกาสประสบความสำเร็จในการโจมตีสูงมาก

Zero-day Exploit หมายถึง วิธีการที่แฮกเกอร์โจมตีระบบ โดยอาศัยช่องโหว่ที่ไม่เคยถูกค้นพบมาก่อน

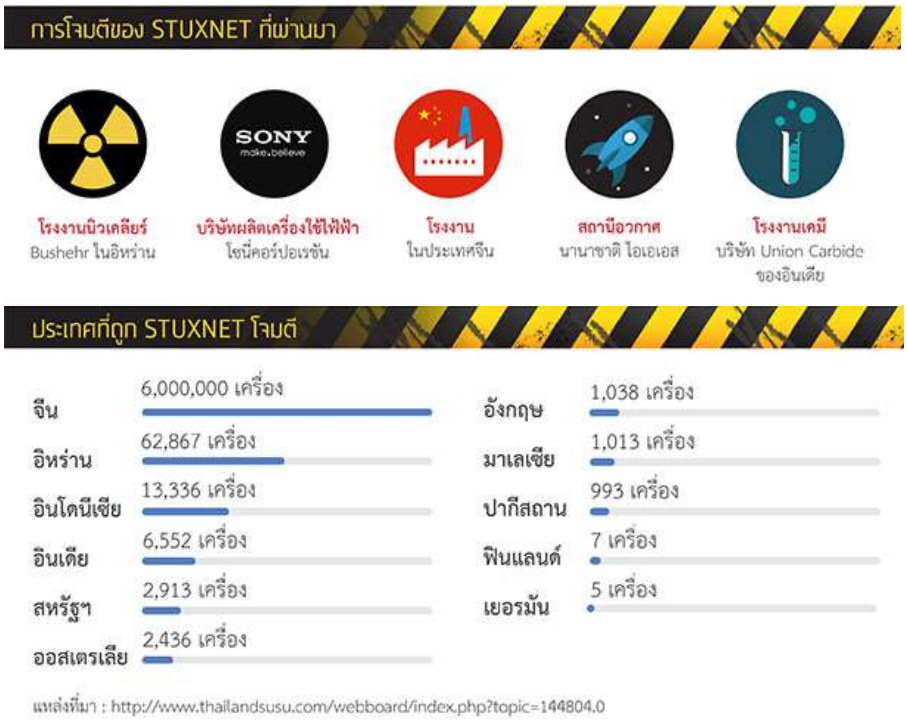
Zero-Day Attack หมายถึง การที่แฮกเกอร์ใช้ Zero-day Exploit สร้างความเสียหาย หรือขโมยข้อมูล จากอุปกรณ์ที่มีช่องโหว่ โดยการใช้ malware

อย่างไรก็ตามบ่อยครั้งที่ นักเจาะระบบ หรือ แฮกเกอร์ (Hacker) จะเป็นผู้ที่ค้นพบช่องโหว่ก่อนที่ผู้พัฒนาซอฟต์แวร์หรือฮาร์ดแวร์จะไหวตัวทัน ในช่วงเวลาดังกล่าวที่ช่องโหว่ยังเปิดโล่งโจ้งอยู่ แฮกเกอร์ก็จะสร้างโค้ดใหม่ขึ้นมาเพื่อหาประโยชน์จากช่องโหว่ดังกล่าว หรือที่เรียกกันว่าการ Exploit code

Exploit Code จะถูกใช้เหมือนเป็นใบเบิกทางในการทำอาชญากรรมไซเบอร์ได้หลากหลายวิธี อาจจะลงมือด้วยตนเอง, ส่งมัลแวร์ (Malware) ไปบุก, สร้างฐาน บอตเน็ต (Botnet) นำช่องโหว่ไปวางจำหน่ายบน เว็บมืด (Dark Web) หรือนำไปขายให้กลุ่มที่รับซื้อเพื่อการวิจัยด้านความปลอดภัยอย่าง ZERODIUM[14]

เมื่อช่องโหว่เริ่มเป็นที่รู้จัก ผู้พัฒนาจะพยายามหาทางปิดช่องโหว่เพื่อหยุดการโจมตี ถึงกระนั้นการปิดช่องโหว่ก็ไม่ใช่เรื่องง่ายเพราะจำเป็นต้องใช้เวลาค้นคว้าว่าการโจมตีที่เกิดขึ้นได้เพราะช่องโหว่อะไร มีองค์ประกอบอะไรที่เกี่ยวข้องบ้าง ซึ่งมันอาจจะใช้เวลาเป็นวันจนถึงเป็นเดือนกเป็นได้ กว่าที่นักพัฒนาจะสามารถพัฒนาแพทช์ (โปรแกรม Patch) แก้ไขได้สำเร็จ และที่ควรตระหนักเป็นอย่างยิ่ง คือ ไม่ใช่ว่าผู้ใช้ทุกคนที่จะรับรู้ถึงปัญหานี้และทำการอัปเดตแพทช์ (โปรแกรมPatch) เพื่อปิดช่องโหว่ดังกล่าว

STUXNET Worm, Zero-Day[20] STUXNET ภัยร้ายไซเบอร์ระดับโลกในรูปแบบของ Worm โดยจะเน้นโจมตีบนช่องโหว่ระบบปฏิบัติการ มุ่งหวังเพื่อทำลายระบบควบคุม (Programmable Logic Controller : PLC) และประมวลผลในโรงงานอุตสาหกรรม



ภาพประกอบที่ 4 การโจมตีทางไซเบอร์ (Cyber warfare) ระดับโลก - STUXNET

ผนวก ข.

ลำดับเหตุการณ์การโจมตีทางไซเบอร์ที่สำคัญของประเทศไทย[18]

มิถุนายน พ.ศ. 2555

ผู้ให้บริการชื่อโดเมนไทย (.th) ถูกเจาะระบบและแก้ไข ข้อมูลที่อยู่เว็บไซต์ขององค์กรใหญ่หลายแห่ง

กุมภาพันธ์ พ.ศ. 2556

เว็บไซต์ของตลาดหลักทรัพย์ในอเมริกา เอเชีย รวมถึงไทย ถูกโจมตีด้วย DDoS โดยกลุ่ม Anonymous ทำให้บริการขัดข้องหลายชั่วโมง ซึ่งส่งผลกระทบด้านเศรษฐกิจ

ตุลาคม พ.ศ. 2558

ธนาคารพาณิชย์ 5 ธนาคาร ได้รับจดหมายอิเล็กทรอนิกส์ ข่มขู่เรียกเงินเป็น Bitcoins เพื่อแลกกับการไม่ถูกโจมตี DDoS จากกลุ่ม Armada Collective

สิงหาคม พ.ศ. 2559

ตู้ ATM ของธนาคารออมสิน จำนวน 21 ตู้ถูกโจมตีด้วยมัลแวร์ และลอบขโมยเงิน 12 ล้านบาท ซึ่งเป็นมัลแวร์ที่คล้ายกับที่ใช้โจมตี ATM ในไต้หวันในปีเดียวกัน

ธันวาคม พ.ศ. 2559

ปรากฏการณ์ทางสังคมที่แสดงออกผ่านไซเบอร์ เมื่อกลุ่ม “พลเมืองต่อต้าน Single Gateway #opsinglegateway” รณรงค์ให้มีการโจมตี DDoS กับเว็บไซต์ของหน่วยงานรัฐ ทำให้หลายระบบสำคัญของรัฐขัดข้อง และพบการเจาะฐานข้อมูลเพื่อโจรกรรมข้อมูลมาเผยแพร่ รวมถึงใช้ปฏิบัติการข่าวสาร IO ในการลดความน่าเชื่อถือของรัฐบาล

พฤษภาคม พ.ศ.2560:

พบการแพร่ระบาดของ WannaCry ในเครื่องคอมพิวเตอร์กว่า 200,000 เครื่อง จาก 112 ประเทศรวมถึงประเทศไทย ผ่านช่องโหว่ในโพรโทคอล SMB

กรกฎาคม พ.ศ. 2561

ข้อมูลลูกค้าสินเชื่อที่อยู่อาศัยของธนาคารกรุงไทย และ ข้อมูลลูกค้าบริการหนังสือค้ำประกันของธนาคารกสิกรไทย ถูกโจรกรรมข้อมูล ถึงแม้จะไม่มีมูลค่าความเสียหายเป็น

ตัวเลข แต่ก็สร้างความเสียหายทางชื่อเสียงและความน่าเชื่อถือของกิจการธนาคารอย่างมาก

มกราคม พ.ศ.2561:

พบมัลแวร์ที่ใช้ขุดเงินดิจิทัลสกุลเงิน Monero ส่งผลให้เครื่องทำงานช้าลง มัลแวร์ดังกล่าวถูกดาวน์โหลดในประเทศไทยกว่า 3.5ล้านครั้ง

เมษายน พ.ศ.2561:

เครื่องคอมพิวเตอร์ในไทยถูกใช้เป็นฐานการโจมตี หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานอื่นๆกว่า 17ประเทศ และผู้ให้บริการโทรคมนาคมตั้งค่าระบบเก็บกู้ข้อมูลไม่เหมาะสมทำให้สาธารณะสามารถเข้าถึงข้อมูลลูกค้า เช่น สำเนาบัตรประชาชน พาสปอร์ต กว่า 46,000 ไฟล์

พฤษภาคม พ.ศ.2561:

มัลแวร์ VPN Filter แพร่ระบาดในอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ (Internet of Things “IoT”) กว่า500,000 เครื่องใน 54 ประเทศรวมถึงประเทศไทย

กรกฎาคม พ.ศ.2561:

ข้อมูลลูกค้าธนาคารรวมกว่า 123,000 รายหลุด

ตุลาคม พ.ศ.2561:

Facebook แถลงเรื่องข้อมูลผู้ใช้หลุดมีผลกระทบประมาณ 30ล้านบัญชี และบริษัท Mandiant ระบุพบมัลแวร์ที่ใช้ในการแอบส่งข้อมูลโจมตีระบบหน่วยงานภาครัฐสำคัญ

กันยายน พ.ศ.2564:

ข้อมูลการปฏิบัติงานของเจ้าหน้าที่และแฟ้มของแพทย์ในการตรวจผู้ป่วยซึ่งมีฐานข้อมูล 10,095 รายพร้อมชื่อ นามสกุล หมายเลขโทรศัพท์และรายละเอียดการเข้าออกโรงพยาบาลของกระทรวงสาธารณสุขถูกประกาศขายผ่านสื่อออนไลน์

ผนวก ค.

ลำดับเหตุการณ์การโจมตีทางไซเบอร์ที่สำคัญของโลก

พ.ศ.2552: STUXNET Worm, Zero-Day[19,20]

เหตุไฟไหม้โรงงานนิวเคลียร์อิหร่านเกิดจากการก่อวินาศกรรมทางไซเบอร์ สำนักข่าวรอยเตอร์ รายงานช่วงปลายปี พ.ศ.2552 ถึงต้นปี พ.ศ.2553 เกิดเหตุไฟไหม้โรงงานนิวเคลียร์ Natanz ของอิหร่านทำให้อาคารหนึ่งชั้นถูกเผาบางส่วน แต่ยังไม่มีรายงานผู้บาดเจ็บหรือเสียชีวิต อาคารดังกล่าวถือเป็นศูนย์กลางของโครงการเสริมสมรรถนะแร่ยูเรเนียมของอิหร่าน

ทางการอิหร่านเร่งสืบสวนหาสาเหตุของเพลิงไหม้พบว่าอาจเป็นการก่อวินาศกรรมทางไซเบอร์ โดยพบว่ามีการโจมตีมุ่งเป้าหมายต่อเครื่องปั่นหมุนเหวี่ยงเพื่อเสริมสมรรถนะแร่ยูเรเนียม โดยได้รับการยืนยันว่าถูกโจมตีโดย Stuxnet Worm สันนิฐานว่าอาจเป็นการก่อวินาศกรรมทางไซเบอร์กระทำโดยไม่ประเทศอิสราเอล ก็สหรัฐฯ นาย Behrouz Kamalvandi โฆษกขององค์กรพลังงานปรมาณูของอิหร่านได้ระบุว่า อิหร่านจำต้องชะลอการพัฒนาและผลิตเครื่องปั่นหมุนเหวี่ยง แต่อิหร่านก็จะนำเครื่องจักรที่ใหญ่กว่าและทันสมัยกว่าเข้ามาทดแทนเครื่องที่เสียหาย

Stuxnet Worm อาจเกิดจากการที่มีเจ้าหน้าในโรงงานนิวเคลียร์อิหร่านได้นำแฟลชไดร์ฟซึ่งถูกเก็บจากพื้นที่สาธารณะ (Public Zone) ขององค์กรมาเสียบกับคอมพิวเตอร์ในโรงงานนิวเคลียร์ทำให้มัลแวร์ (worm) ในแฟลช์ไดร์ฟกระจายตัว และเข้าสู่ระบบเครือข่ายภายใน โดยมีเป้าหมายเข้าควบคุมโปรแกรมควบคุมเครื่องจักร (Programmable Logic Controller : PLC) เพื่อสั่งการให้เครื่องจักรในโรงงานทำงานเกินปกติจนเกิดข้อผิดพลาดจนเครื่องจักรเสียหาย ถือเป็นการโจมตีทางไซเบอร์ครั้งแรกของโลกที่สร้างความเสียหายทางกายภาพได้

กันยายน: พ.ศ. 2555

ปฏิบัติการ “Operation Ababil” ของสถาบันการเงินสำคัญในสหรัฐฯ เช่น New York Stock Exchange, J.P. Morgan Chase, Bank of America และอีก

หลายแห่ง ถูกโจมตี DDoS โดยกลุ่ม Qassam Cyber Fighters ทำให้การบริการเว็บไซต์หยุดชะงัก

กันยายน พ.ศ. 2559

แฮคเกอร์ปล่อย มัลแวร์ Mirai ใช้ช่องโหว่ในอุปกรณ์ IoT โจมตีเครื่องให้บริการชื่อโดเมน ทำให้ไม่สามารถเข้าถึงเว็บไซต์ กระทบผู้ใช้งานทั่วโลก

กันยายน พ.ศ. 2559

ธนาคารกลางบังคลาเทศ ถูกมิจฉาชีพลักลอบโอนเงินจากธนาคาร จำนวน 81 ล้านเหรียญสหรัฐอเมริกา ทำให้ธนาคารเกิดความเสียหาย

พฤษภาคม พ.ศ. 2560

มัลแวร์WannaCry โจมตีหน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยมากกว่า 69,000 ราย ไม่สามารถรับบริการได้ และเกิดการแพร่กระจายไปมากกว่า 150 ประเทศ

กรกฎาคม พ.ศ. 2560

ข้อมูลส่วนบุคคลของผู้บริโภคชาวสหรัฐอเมริกาของบริษัท Equifax รั่วไหล จำนวน 145 ล้านคน

พฤศจิกายน พ.ศ. 2560

บริษัท Uber ถูกโจรกรรมข้อมูลส่วนบุคคลของคนขับรถและผู้ใช้บริการ จำนวน 53 ล้านคน

มกราคม พ.ศ. 2561

ข้อมูลผู้ใช้บริการ Florida Medicaid ของสหรัฐอเมริกา รั่วไหล จำนวน 30,000 คน

มกราคม พ.ศ. 2561

ระบบฐานข้อมูลประชาชนของอินเดียพบช่องโหว่ และทำให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูลประชาชนของอินเดียโดยไม่ได้รับอนุญาต จำนวนกว่า 1,000 คน

ผนวก ง.

ผลกระทบจากภัยคุกคามไซเบอร์ 5 อันดับแรนซัมแวร์เรียกค่าไถ่แพงที่สุดในโลก[11]

แรนซัมแวร์ (Ransomware) มักมีเป้าหมายในการโจมตีองค์กร บริษัททั้งเล็กและใหญ่ จนนำไปสู่การชัตดาวน์ (Shutdown) หรือหยุดดำเนินการการให้บริการชั่วคราว ซึ่งสร้างความเสียหายทางธุรกิจตามมาอย่างเลี่ยงไม่ได้ สำหรับการใช้แรนซัมแวร์เพื่อเรียกค่าไถ่ที่สร้างความเสียหายมากที่สุดในโลก 5 อันดับแรกช่วงปีพ.ศ.2563-2564 ได้แก่

CWT Global (4.5 ล้านดอลลาร์) บริษัทธุรกิจท่องเที่ยวของสหรัฐรายนี้ สูญเงินราว 4.5 ล้านดอลลาร์ให้กับแกงค์ Ragnar Locker เมื่อเดือนก.ค. 2563 โดยคาดกันว่า แฮกเกอร์กลุ่มนี้ได้ลบข้อมูลในคอมพิวเตอร์ถึง 30,000 เครื่องและเจาะข้อมูลของบริษัทไปได้ 2 เทระไบต์ รวมถึงข้อมูลการเงิน, เอกสารระบบความปลอดภัย และข้อมูลส่วนบุคคลของพนักงาน

Colonial Pipeline (4.4 ล้านดอลลาร์) บริษัทโคโลเนียล ไปป์ไลน์ เหยื่อผู้เคราะห์ร้ายที่เพิ่งผ่านพ้นเหตุโจมตีทางไซเบอร์ฝีมือของกลุ่มดาร์กไซด์เมื่อไม่นานมานี้ สูญเงินไปราว 4.4 ล้านดอลลาร์ อย่างไรก็ดี เจ้าหน้าที่ตำรวจของรัฐบาลกลางสหรัฐสามารถตามยึดบิตคอยน์มูลค่ากว่า 2.3 ล้านดอลลาร์จากเงินค่าไถ่จำนวนดังกล่าว

Brenntag (4.4 ล้านดอลลาร์)ผู้จำหน่ายสารเคมีสัญชาติเยอรมนีถูกโจมตีด้วยแรนซัมแวร์โดยกลุ่มดาร์กไซด์เช่นเดียวกัน ในช่วงเวลาไล่เลี่ยกับการโจมตีระบบท่อส่งน้ำมันของโคโลเนียล ไปป์ไลน์ ในตอนแรกนั้น แฮกเกอร์กลุ่มนี้เรียกค่าไถ่เป็นเงินบิตคอยน์สูงถึง 7.5 ล้านดอลลาร์ ก่อนจะเจรจาต่อรองเหลือ 4.4 ล้านดอลลาร์ เพื่อแลกกับข้อมูลที่ถูกขโมยไป 150 กิกะไบต์

Travelex (2.3 ล้านดอลลาร์) ปลายปี 2562 ช่วงที่หลายคนกำลังมีความสุขก่อนเข้าสู่เทศกาลปีใหม่ ฝ่ายไอทีของบริษัทผู้ให้บริการแลกเปลี่ยนเงินตราของอังกฤษรายนี้ ต้องสาละวนอยู่กับการไล่ล่าแรนซัมแวร์ที่ปั่นป่วนระบบคอมพิวเตอร์ของบริษัท ก่อนจะกู้คืนข้อมูลกลับมาได้ในอีกเกือบสองสัปดาห์ต่อมา โดยบริษัทยอมจ่ายค่าไถ่เป็นเงิน 2.3 ล้านดอลลาร์เพื่อให้ระบบกลับมาใช้การได้ ว่ากันว่า พนักงานต้องหันมาทำงานโดยใช้กระดาษ

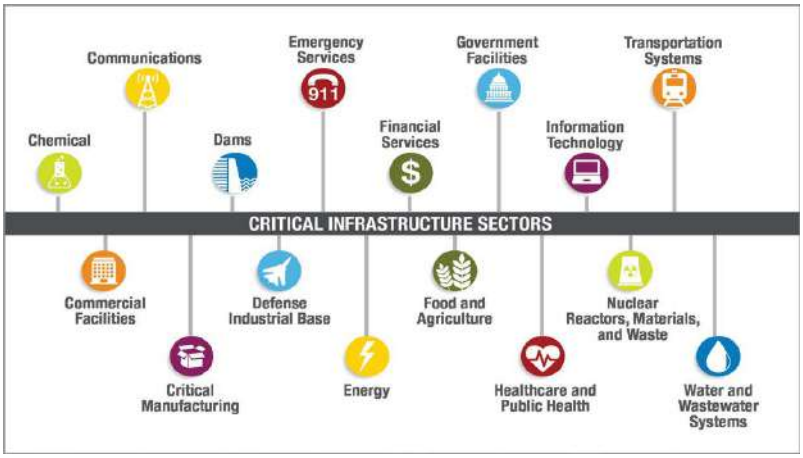
และปากกาแทนคอมพิวเตอร์ ยิ่งไปกว่านั้น เหตุการณ์ในครั้งนี้ยังสร้างความเสียหายต่อภาพลักษณ์และความน่าเชื่อถือของบริษัทเป็นอย่างมาก

มหาวิทยาลัยแคลิฟอร์เนีย ซานฟรานซิสโก (UCSF) (1.4 ล้านดอลลาร์) ในเดือนมิ.ย. 2563 UCSF ยอมจ่ายเงิน 1.4 ล้านดอลลาร์เพื่อแลกกับการให้แฮกเกอร์ปลดล็อกระบบหลังงัดข้อกันนานร่วมเดือน โดยในเบื้องต้นนั้น คาดว่าแฮกเกอร์เรียกค่าไถ่เป็นเงินราว 3 ล้านดอลลาร์ โดยในช่วงการเจรจาต่อรองนั้น ผู้ดูแลระบบนั้นได้พยายามสกัดกั้นการโจมตีไม่ให้แรนซัมแวร์เจาะเข้าสู่เครือข่ายหลักของ UCSF ได้ อย่างไรก็ดี แม้วิธีดังกล่าวจะช่วยป้องกัน ไม่ให้หน่วยงานภายในบางส่วนของ UCSF ถูกโจมตี รวมไปถึงการปฏิบัติงานส่งต่อผู้ป่วยและงานด้านโควิด-19 แต่เซิร์ฟเวอร์ของโรงเรียนแพทย์ในมหาวิทยาลัยก็ยังถูกเจาะเข้ารหัสได้เป็นผลสำเร็จ

ผนวก จ.

หน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (Cybersecurity & Infrastructure Security Agency “CISA”) ซึ่งเป็นหน่วยงานหลักและได้กำหนดกรอบการดำเนินการความมั่นคงปลอดภัยไซเบอร์แต่ละหน่วยงานที่เป็นโครงสร้างพื้นฐานหลักของประเทศสหรัฐฯไว้[7,47] เช่น

1. อุตสาหกรรมเคมีภัณฑ์ Chemical Framework Guidance [pdf]
2. ธุรกิจการค้า Commercial Facilities Framework Guidance [pdf]
3. โรงงานอุตสาหกรรม Critical Manufacturing Framework Guidance [pdf]
4. เขื่อน Dams Framework Guidance [pdf]
5. อุตสาหกรรมป้องกันประเทศ Defense Industrial Base Framework Guidance [pdf]
6. บริการฉุกเฉินในภาวะวิกฤติ Emergency Services Framework Guidance [pdf]
7. หน่วยงานภาครัฐ Federal Framework Guidance DRAFT [pdf]
8. สาธารณสุข Healthcare & Public Health Framework Guidance [pdf]
9. พลังงานนิวเคลียร์ Nuclear Framework Guidance [pdf]
10. คมนาคมขนส่ง Transportation Systems Framework Guidance [pdf]
11. ระบบน้ำและปประปา Water & Wastewater Systems [link: American Water Works Association Cybersecurity Guidance & Tool]



ภาพประกอบที่ 6 กลุ่มหน่วยงานที่เป็นโครงสร้างพื้นฐานที่สำคัญ

แนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy)

สหภาพโทรคมนาคมระหว่างประเทศ หรือ The Telecommunication Union “ITU” ของสหประชาชาติ มีกรอบแนวคิดการพัฒนายุทธศาสตร์ร่วมกับสำนักเลขาธิการประเทศเครือจักรภพ (Commonwealth secretariat: ComSec) ธนาคารโลก (World bank) องค์การนาโต (NATO) องค์กรโทรคมนาคมประเทศเครือจักรภพ (Commonwealth telecommunication organization: CTO) หน่วยงานความมั่นคงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของนาโต (Cooperative cyber defence centre of excellence: CCD COE) องค์กรระหว่างประเทศ และบริษัทที่ปรึกษาจากภาคเอกชนชั้นนำ จัดทำและเผยแพร่คู่มือกรอบแนวคิดในการจัดทำยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) สำหรับผู้นำประเทศและผู้กำหนดนโยบาย ในปี 2564[26] โดยแนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy) มีลักษณะสำคัญของคู่มือกรอบแนวคิดได้แบ่งองค์ประกอบที่สำคัญออกเป็น 3 ส่วน ได้แก่

1) ขั้นตอนของการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ
2) ลักษณะที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์
3) แนวปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเนื้อหาที่สำคัญ ดังนี้

ขั้นตอนของการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ

คู่มือแนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy) เสนอขั้นตอนของการพัฒนายุทธศาสตร์ 5 ระยะ ดังนี้[28]

ระยะที่ 1: ระยะเริ่มต้น (Initiation) ประกอบด้วย การระบุหน่วยงานรับผิดชอบหลัก (Identifying the lead project authority), การแต่งตั้งคณะกรรมการ

ขับเคลื่อน (Establishing a steering committee), การระบุหน่วยงานหรือผู้มีส่วนเกี่ยวข้องในการพัฒนายุทธศาสตร์ (Identifying stakeholders to be involved in the development of the Strategy), การวางแผนการพัฒนายุทธศาสตร์ (Planning the development of the strategy)

ระยะที่ 2: ระยะประเมินตรวจสอบและวิเคราะห์ (Stocktaking and Analysis) ประกอบด้วย การประเมินสภาวะความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Assessing the national cybersecurity landscape)และการประเมินสภาวะความเสี่ยงทางไซเบอร์ (Assessing the cyber-risk landscape)

ระยะที่ 3: กำหนดยุทธศาสตร์ความมั่นคงไซเบอร์ระดับชาติ (Production of the national cybersecurity strategy) ประกอบด้วย การยกร่างยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Drafting the national cybersecurity strategy), การปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องทุกภาคส่วน (Consulting with a broad range of stakeholders), การขอความเห็นชอบยุทธศาสตร์ (Seeking formal approval), การเผยแพร่ยุทธศาสตร์ให้มีผลใช้บังคับ (Publishing the strategy)

ระยะที่ 4: การขับเคลื่อนและใช้บังคับ (Implementation) ประกอบด้วย การพัฒนาแผนปฏิบัติงาน (Developing the action plan), การพิจารณาโครงการนำร่องที่สามารถนำไปปฏิบัติได้จริง (Determining initiatives to be implemented), การจัดสรรทรัพยากรบุคลากรและงบประมาณเพื่อการขับเคลื่อนแผนปฏิบัติงาน (Allocating human and financial resources for the implementation), การกำหนดกรอบระยะเวลา และตัวชี้วัด (Setting timeframes and metrics)

ระยะที่ 5: การติดตามและประเมินผล (Monitoring and evaluation), การกำหนดขั้นตอนการดำเนินงาน (Establishing a formal process), การติดตามความคืบหน้าของการขับเคลื่อนยุทธศาสตร์ (Monitoring the progress of the implementation of the strategy), การประเมินผลการขับเคลื่อนยุทธ์ศาสตร์ (Evaluating the outcome of the strategy)

ลักษณะที่สำคัญของยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

คู่มือกรอบแนวคิดในการจัดทำยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (National cybersecurity strategy) เสนอลักษณะที่สำคัญของยุทธศาสตร์ 9 ประการ ดังนี้

1. วิสัยทัศน์ของรัฐบาลและสังคมที่ชัดเจน (Clear vision)

2. ความเข้าใจต่อสภาพแวดล้อมทางไซเบอร์ของประเทศและการจัดลำดับประเด็นสำคัญของประเทศ (Comprehensive approach and tailored priorities)

3. การพัฒนายุทธศาสตร์จากการมีส่วนร่วมของทุกภาคส่วน (Inclusiveness)

4. การสร้างความมั่งคั่งทางเศรษฐกิจและสังคม (Economic and social prosperity)

5. สิทธิมนุษยชนขั้นพื้นฐาน (Fundamental human rights)

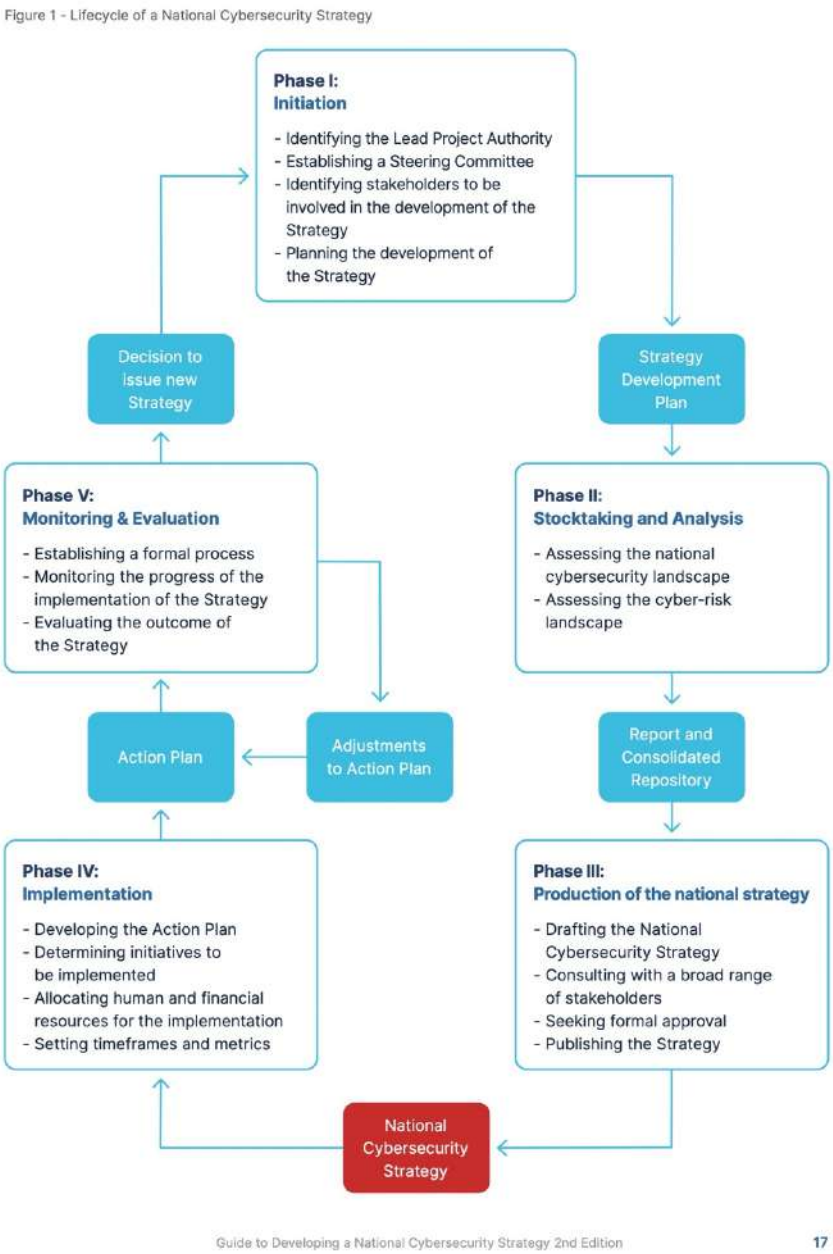
6. การบริหารความเสี่ยงและความทนทานต่อความเสี่ยง (Risk management and resilience)

7. กลไกขับเคลื่อนนโยบายที่เหมาะสม (Appropriate set of policy instruments)

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

9. สภาพแวดล้อมของความเชื่อมั่น (Trust environment)

ภาพประกอบแสดงการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับชาติ (Lifecycle of a National Cybersecurity Strategy) ของสหประชาชาติ



ภาพประกอบที่ 7

ภาพประกอบแสดงการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับชาติ

แนวปฏิบัติที่ดีเกี่ยวกับปัจจัยสำคัญที่จะทำให้ประเทศบรรลุเป้าหมายของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ (National Cybersecurity Strategy Good Practice)

ตามแนวปฏิบัติที่ดี (Good-practice) ปัจจัยสำคัญที่ทำให้ประเทศสามารถบรรลุตามเป้าหมายที่กำหนดขึ้นภายใต้ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ ประกอบด้วย 7 ปัจจัยที่สำคัญ ดังนี้

1. การกำกับดูแลของภาครัฐ (Governance)

2. การบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Risk management in national cybersecurity)

3. การเตรียมความพร้อมและความทนทาน (Preparedness and resilience)

4. ระบบบริการโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Critical Infrastructure services and essential services)

5. ขีดความสามารถการพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ (Capability and capacity building and awareness raising)

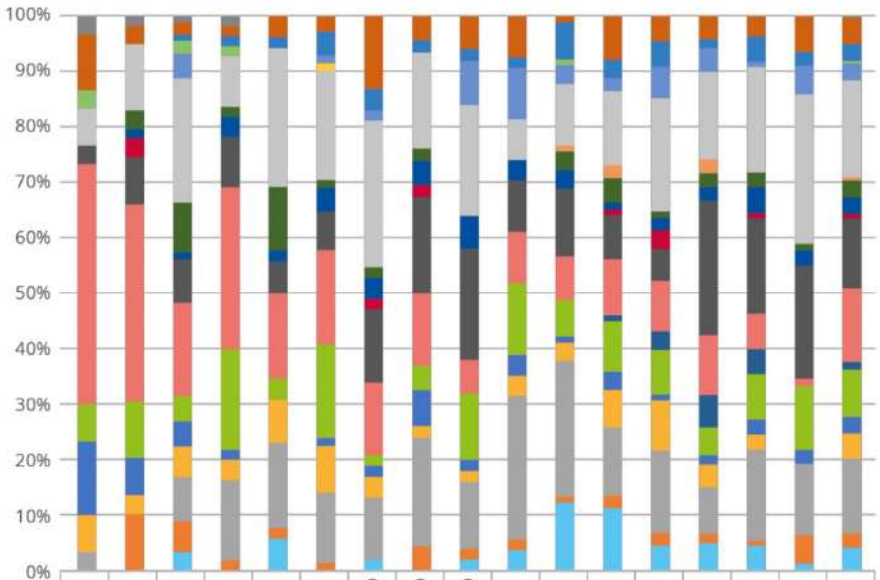
6. กฎหมายและระเบียบกฎเกณฑ์ (Legislation and regulation)

7. ความร่วมมือระหว่างประเทศ (International cooperation)

วิเคราะห์กรอบแนวคิด: สหภาพยุโรป

ภาพประกอบที่ 8 สถิติหน่วยงานโครงสร้างพื้นฐานหลักของสหภาพยุโรปที่ถูกโจมตีห้วงเดือน เมษายน 2563 จนถึงกลางเดือน กรกฎาคม 2564 จัดทำโดยโดยหน่วยงานหน่วยงานด้านความปลอดภัยทางไซเบอร์ของสหภาพยุโรป (The European Union Agency for Cybersecurity “ENISA”)[21]

Figure 3: Timeline of observed incidents related to prime ETL threats in terms of the affected sector.



	4/20	5/20	6/20	7/20	8/20	9/20	10/20	11/20	12/20	1/21	2/21	3/21	4/21	5/21	6/21	7/21	Total
Water utilities	1	1	1	1													4
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	54
Targeted individuals			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Space	1		2	1							1						5
Software supply chain			4			1	1		4	5	3	2	5	5	1	4	35
Semiconductor						1											1
Public administration/ Government	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	198
Postal & Courier Services											1	2		3			6
Military		2	8	1	6	1	1	1			3	4	1	3	3	1	35
Media/Entertainment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	33
Legal		2					1	1				1	3		1		9
Healthcare/Medical	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	143
General public	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	151
Food												1	3	7	5		16
Finance/Banking	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	97
Energy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	33
Education/Academic	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		52
Digital Service Providers	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	152
Construction		6	5	1	1	1		2	1	1	1	2	2	2	1	4	30
All Sectors			3		3		1		1	2	11	10	4	6	5	1	47

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

หน่วยงานได้จัดทำคู่มือแนวปฏิบัติที่ดีในการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับชาติ (Good practices in innovation on cybersecurity under the National Cyber Security Strategies “NCSS”) ในปี 2559 ซึ่งปรับปรุงจากคู่มือแนวปฏิบัติที่ดีฉบับปี 2563[32-38] เพื่อเป็นแนวทางให้กับประเทศสมาชิกของกลุ่มสหภาพยุโรปในการกำหนดยุทธศาสตร์ และการขับเคลื่อนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

Figure 2-1 – NCSS lifecycle

ภาพประกอบที่ 9

1. วัฏจักรของยุทธศาสตร์ พัฒนาเพื่อให้มีการตรวจสอบและทบทวนยุทธศาสตร์และนโยบายที่เกี่ยวข้องอย่างต่อเนื่อง โดยกำหนดให้วัฏจักรของยุทธศาสตร์ประกอบด้วย 4 ระยะ ได้แก่

ระยะที่ 1 พัฒนายุทธศาสตร์ โดยมีการปรับปรุงยุทธศาสตร์ให้สอดคล้องกับสภาพและสถานการณ์ปัจจุบัน

ระยะที่ 2 ขับเคลื่อนยุทธศาสตร์ไปสู่การปฏิบัติ โดยมีการปรับแผนปฏิบัติงานให้สอดคล้องกับสภาพและสถานการณ์ปัจจุบัน

ระยะที่ 3 ประเมินผลการปฏิบัติตามยุทธศาสตร์ โดยมีการทบทวนยุทธศาสตร์เป็นระยะ

ระยะที่ 4 การรักษาไว้ซึ่งยุทธศาสตร์ โดยมีการพัฒนายุทธศาสตร์

2. หลักการในการออกแบบและพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 6 หลักการ ได้แก่

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

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

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

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

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

2.6 การสร้างกลไกการแลกเปลี่ยนข้อมูลที่เชื่อถือได้ (Establish trusted information-sharing mechanisms) รวมถึงข้อมูลข่าวกรองที่สำคัญและข้อมูลจากทีมสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ เพื่อช่วยให้เข้าใจถึงสภาพแวดล้อมไซเบอร์ที่เปลี่ยนแปลงไป และสามารถลดความเสี่ยงและความเปราะบางที่มีอยู่ได้

3. เป้าหมายที่สำคัญของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ 15 ประการ โดยมีสาระสำคัญสรุปได้ ดังนี้

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

3.2 การคุ้มครองโครงสร้างพื้นฐานข้อมูลที่สำคัญยิ่งยวด (Protect critical information infrastructure) โดยระบุถึงประเภทของโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญยิ่งยวด และกำหนดมาตรการลดความเสี่ยง

3.3 การจัดการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ (Organize Cybersecurity exercises) โดยระบุถึงกระบวนการขั้นตอนและขีดความสามารถที่ต้องได้รับการทดสอบก่อนเกิดเหตุการณ์ และจัดตั้งทีมรับมือที่กำหนดอำนาจหน้าที่ความรับผิดชอบไว้อย่างชัดเจน

3.4 การกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ขั้นพื้นฐาน (Establish baseline security measures) หรือหลักเกณฑ์ระดับความปลอดภัยขั้นต่ำที่ทุกภาคส่วนต้องปฏิบัติตาม เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถตรวจสอบและบ่งชี้ถึง ขีดความสามารถของตนเองได้ และทำให้สามารถจัดลำดับความสำคัญของการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ได้

3.5 การสร้างกลไกการรายงานเหตุการณ์ (Establish incident reporting mechanisms) เพื่อสร้างความเข้าใจต่อภาพรวมสถานการณ์ภัยคุกคามไซเบอร์ ช่วยให้

สามารถประเมินผลกระทบได้ ได้ทราบถึงความเปราะบางและรูปแบบของการโจมตีทางไซเบอร์ ทำให้สามารถปรับปรุงแผนการรับมือให้เป็นปัจจุบันได้

3.6 การสร้างความตระหนักรู้ให้กับประชาชน เยาวชน และผู้บริโภค (Raise user awareness) โดยระบุถึงช่องว่างของความรู้ความเข้าใจหรือความตระหนักรู้จากปัญหาจากการใช้งานระบบอินเทอร์เน็ต และเติมเต็มช่องว่างนั้นด้วยการให้ความรู้และการสร้างความตระหนักรู้ ผ่านการรณรงค์ การจัดกิจกรรม การจัดการประชุม และปรับปรุงเว็บไซต์ของหน่วยงานภาครัฐ ให้ครอบคลุมเนื้อหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การอภิปราย การบรรยาย และการสัมมนาผ่านเว็บไซต์ เป็นต้น

3.7 การจัดทำโครงการฝึกอบรมและหลักสูตรการศึกษา (Strengthen training and educational programmes) ซึ่งเป็นส่วนหนึ่งของสาขาวิทยาการคอมพิวเตอร์ โดยปรับปรุงเนื้อหาให้ทันต่อสถานการณ์อย่างต่อเนื่อง เพิ่มขีดความสามารถให้กำลังแรงงานการรักษาความมั่นคงปลอดภัยทางข้อมูล ส่งเสริมให้นักศึกษาเข้าร่วมในสาขาวิชาว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ สนับสนุนให้เกิดความเชื่อมโยงกันระหว่างการรักษาความปลอดภัยทางข้อมูล ในแวดวงวิชาการ และอุตสาหกรรมความมั่นคงปลอดภัยในการรักษาความมั่นคงปลอดภัยทางข้อมูล

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

3.9 การแก้ไขปัญหาอาชญากรรมไซเบอร์ (Address cyber crime) โดยอาศัยความร่วมมือของทุกภาคส่วนและสังคม การบัญญัติกฎหมาย และการเพิ่มประสิทธิภาพของหน่วยงานด้านการบังคับใช้กฎหมาย

3.10 การสร้างความร่วมมือกับองค์กรระหว่างประเทศ (Engage in international cooperation) เพื่อสร้างองค์ความรู้พื้นฐานร่วมกัน และช่วยส่งเสริมผลประโยชน์ร่วมกันในการรับมือกับภัยคุกคามไซเบอร์และอาชญากรรมทางไซเบอร์ โดย

ระบุประเทศพันธมิตรและแง่มิติที่ต้องการสร้างความร่วมมือ และกำหนดหน่วยงานภายในประเทศให้มีหน้าที่ความรับผิดชอบในการสร้างความร่วมมือระหว่างประเทศ

3.11 การสร้างการร่วมมือระหว่างภาครัฐและเอกชน (Establish a public-private partnership) ซึ่งมักจะเป็นผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญของประเทศ โดยการประสานงานและร่วมมือระหว่างภาครัฐและเอกชนช่วยทำให้รัฐบาลเข้าใจถึงความต้องการของภาคเอกชน และความท้าทายที่ภาคเอกชนต้องเผชิญ การรร่วมมือระหว่างภาครัฐและเอกชน จะช่วยให้เกิดการรวมกลุ่มของผู้เชี่ยวชาญและทรัยากรที่จำเป็นในการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์และการสร้างความทนทานต่อภัยคุกคามทางไซเบอร์

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

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

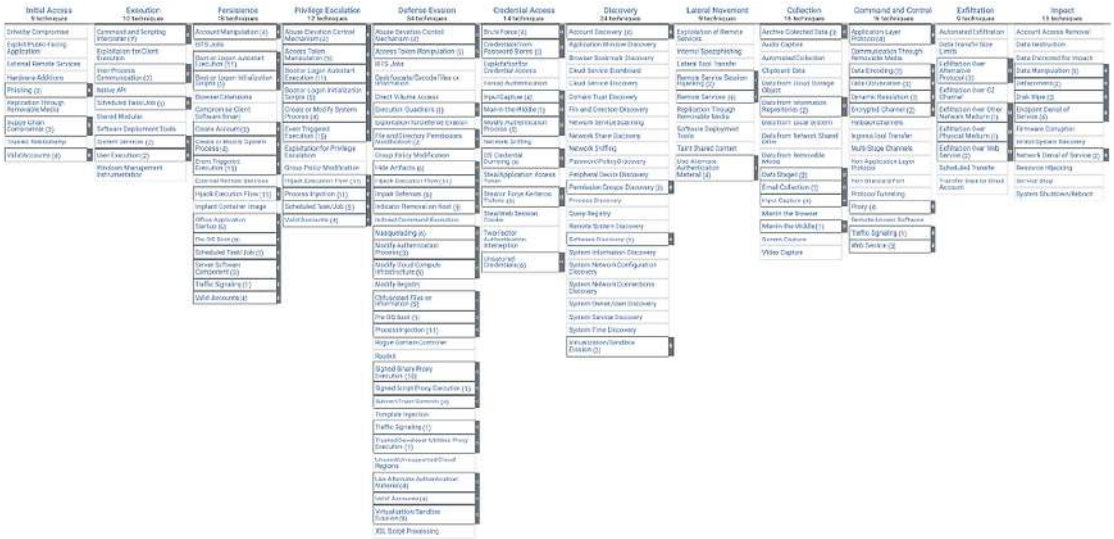
3.14 การเร่งการศึกษาวิจัยและพัฒนา (Foster R&D) เครื่องมือในการตรวจสอบ และป้องกันการโจมตีทางไซเบอร์รูปแบบใหม่ ๆ รวมถึงการระบุถึงสาเหตุของความเปราะบางต่อการโจมตีทางไซเบอร์

3.15 การสร้างแรงจูงใจให้ภาคเอกชนในการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Provide incentives for the private sector to invest in security measures) วิธีที่ง่ายที่สุดในการกระตุ้นให้ภาคเอกชนลงทุนด้านการรักษาความ

มั่นคงปลอดภัยไซเบอร์ คือ การใช้บังคับตามกฎหมาย อย่างไรก็ดี รัฐบาลมักจะใช้วิธีการสร้างแรงจูงใจให้ภาคเอกชนมากกว่า เช่น สิทธิประโยชน์ทางภาษี การให้เงินช่วยเหลือ และการสนับสนุนเงินทุนวิจัยและพัฒนา เป็นต้น

ในการจัดประเภทภัยคุกคามทางไซเบอร์ ENISA[21] ได้อ้างอิง MITRE[23,24] องค์กรไม่แสวงหาผลกำไรที่ก่อตั้งขึ้นเมื่อปี ค.ศ. 1958 ซึ่งมีจุดประสงค์เพื่อ “แก้ไขปัญหาเพื่อโลกที่ปลอดภัยกว่าเดิม” ปัจจุบัน MITRE มีองค์ความรู้ขนาดใหญ่เกี่ยวเทคนิคการโจมตีและแนวทางการแก้ไขด้วย ATT&CK เป็นแพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ (Tactics, Techniques, Procedures “TTPs”) ที่แฮกเกอร์อร์นิยมใช้โจมตีระบบ Industrial Control System (ICS) ที่ใช้ควบคุมโครงสร้างพื้นฐานสำคัญของประเทศ ไม่ว่าจะเป็นระบบขนส่งพลังงาน โรงไฟฟ้า โรงกลั่นน้ำมัน ระบบบำบัดน้ำเสีย ระบบขนส่งมวลชน และอื่นๆ ภาครัฐและภาคเอกชนสามารถเพิ่มความปลอดภัยด้วย MITRE ATT&CK ซึ่งแบ่งเป็นหมวดหมู่ทั้งแบบ Enterprise, Mobile และ ICS[23,24]

โดยมีตัวอย่างของ กลยุทธ์สำหรับ Enterprise-Windows[23] ประกอบด้วย 12 กลยุทธ์[24] ดังนี้



ภาพประกอบที่ 10 ตัวอย่างกลยุทธ์ ATT&CK สำหรับ
Enterprise-Windows ประกอบด้วย 12 กลยุทธ์ โดย องค์กร MITRE

1. Initial Access เป็นกลยุทธ์ที่แฮกเกอร์พยายามที่จะเข้าไปยังระบบเครือข่ายของเหยื่อ คือการหาช่องทางในการโจมตีเหยื่อ ประกอบด้วย 9 เทคนิค และ 10 เทคนิคย่อย (เวอร์ชั่น 6 มี 11 เทคนิค)

2. Execution เป็นกลยุทธ์ที่แฮกเกอร์พยายามให้มัลแวร์ทำงานที่ระบบเครือข่ายของเหยื่อ คือวิธีการติดตั้งมัลแวร์ลงบนเครื่องต่างๆ ในระบบเครือข่าย ประกอบด้วย 10 เทคนิค และ 18 เทคนิคย่อย (เวอร์ชั่น 6 มี 34 เทคนิค)

3. Persistence เป็นกลยุทธ์ที่แฮกเกอร์พยายามให้มัลแวร์สามารถทำงานอยู่ในเครือข่ายได้เสมอ ประกอบด้วย 18 เทคนิค และ 65 เทคนิคย่อย (เวอร์ชั่น 6 มี 63 เทคนิค)

4. Privilege Escalation เป็นกลยุทธ์ที่แฮกเกอร์พยายามยกระดับสิทธิในระบบเครือข่ายให้สูงขึ้น คือหา user ที่มีสิทธิสูงในระบบเครือข่าย เช่น root หรือ admin เป็นต้น ประกอบด้วย 12 เทคนิค และ 75 เทคนิคย่อย (เวอร์ชั่น 6 มี 61 เทคนิค)

5. Defense Evasion เป็นกลยุทธ์ที่แฮกเกอร์หลีกเลี่ยงการตรวจจับจากระบบรักษาความปลอดภัยในเครื่อง หรือในเครือข่าย ประกอบด้วย 34 เทคนิค และ 101 เทคนิคย่อย (เวอร์ชั่น 6 มี 73 เทคนิค)

6. Credential Access เป็นกลยุทธ์ที่แฮกเกอร์พยายามที่จะขโมย username และ password ที่มีการใช้งานอยู่ในระบบเครือข่าย ประกอบด้วย 14 เทคนิค และ 32 เทคนิคย่อย (เวอร์ชั่น 6 มี 23 เทคนิค)

7. Discovery เป็นกลยุทธ์ที่แฮกเกอร์พยายามหาข้อมูลว่าในระบบเครือข่ายของเหยื่อว่ามีสิ่งใดที่มีประโยชน์ต่อการโจมตี ประกอบด้วย 24 เทคนิค และ 11 เทคนิคย่อย (เวอร์ชั่น 6 มี 25 เทคนิค)

8. Lateral Movement เป็นกลยุทธ์ที่แฮกเกอร์พยายามเคลื่อนย้ายตัวเองไปยังเครื่องอื่นๆ ที่อยู่ในระบบเครือข่ายของเหยื่อ ประกอบด้วย 9 เทคนิค และ 12 เทคนิคย่อย (เวอร์ชั่น 6 มี 20 เทคนิค)

9. Collection เป็นกลยุทธ์ที่แฮกเกอร์พยายามรวบรวมข้อมูลที่น่าสนใจทั้งหมดที่อยู่ในระบบเครือข่าย ประกอบด้วย 16 เทคนิค และ 15 เทคนิคย่อย (เวอร์ชั่น 6 มี 14 เทคนิค)

10. Command and Control เป็นกลยุทธ์ที่แฮกเกอร์พยายามสื่อสารกับเครื่องภายในที่ถูกบุกรุกไปแล้ว เพื่อควบคุมให้ทำสิ่งอื่นต่อไปได้ ประกอบด้วย 16 เทคนิค และ 22 เทคนิคย่อย (เวอร์ชั่น 6 มี 22 เทคนิค)

11. Exfiltration เป็นกลยุทธ์ที่แฮกเกอร์พยายามขโมยข้อมูลที่สำคัญออกไปจากระบบเครือข่ายของเหยื่อ ประกอบด้วย 9 เทคนิค และ 7 เทคนิคย่อย (เวอร์ชั่น 6 มี 10 เทคนิค)

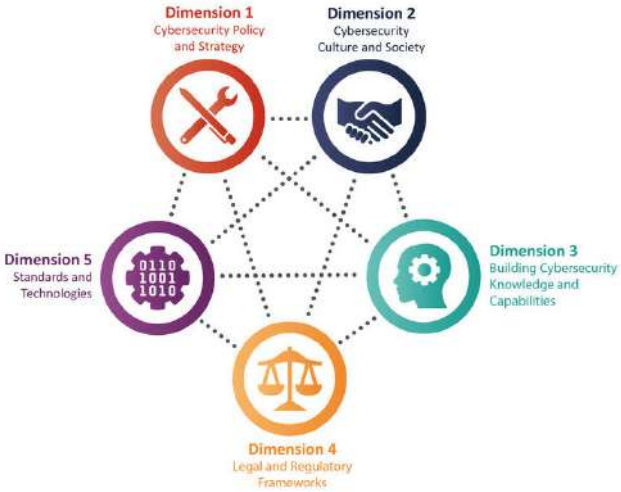
12. Impact เป็นกลยุทธ์ที่แฮกเกอร์พยายามจัดการ ขัดขวาง หรือทำลายระบบ และข้อมูลภายในเครือข่ายของเหยื่อ ประกอบด้วย 13 เทคนิค และ 13 เทคนิคย่อย (เวอร์ชั่น 6 มี 16 เทคนิค)

ซึ่งแต่ละกลยุทธ์จะมีข้อมูลของเทคนิคที่แฮกเกอร์นิยมใช้ทั้งหมด รวมถึงอธิบายถึงกระบวนการทำงานในแต่ละเทคนิคเพื่อให้สามารถนำไปปรับการป้องกันทางไซเบอร์ของตนได้อีกด้วย

วิเคราะห์กรอบแนวคิด: สหราชอาณาจักร

ผู้วิจัยได้ทำการศึกษาตามกรอบแนวคิดการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Cybersecurity Capacity Maturity Model for Nations “CMM”)[25] ซึ่งได้สร้างโดย Global Cyber Security Capacity Centre, Department of Computer Science, มหาวิทยาลัย Oxford ประเทศอังกฤษ โดยที่กระบวนการในการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีการวิเคราะห์ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ของประเทศ และกำหนดระยะของการกำหนดยุทธศาสตร์ (Stage of maturity) ด้านการดูแลความ

มั่นคงปลอดภัยทางไซเบอร์ โดยตามกรอบแนวคิดการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีขีดความสามารถ ประกอบด้วย



ภาพประกอบที่ 11

มิติตามกรอบแนวคิดการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มิติที่ 1 National Cybersecurity framework and policy

เป็นขีดความสามารถในการพัฒนานโยบายและยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ`ความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ การบริหารจัดการในภาวะวิกฤต การปกป้องโครงสร้างพื้นฐานที่สำคัญ การเตือนภัยล่วงหน้า การฟื้นฟูหรือซ่อมแซมความเสียหาย รวมถึงความสามารถในการพัฒนานโยบายความมั่นคงที่มีประสิทธิภาพในการปกป้องและทนทานต่อภัยคุกคาม

มิติที่ 2 Cyber culture and society

เป็นขีดความสามารถด้านความรู้ความเข้าใจของประชาชนในเรื่องความเชื่อมั่นต่อบริการอินเทอร์เน็ต บริการอิเล็กทรอนิกส์ของภาครัฐ และพาณิชย์อิเล็กทรอนิกส์ และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนโลกออนไลน์ ความเข้าใจของประชาชนในเรื่องความเสี่ยงที่เกี่ยวข้องกับโลกไซเบอร์ต่าง ๆ กลไกการให้ผู้ใช้งานรายงานอาชญากรรมทางไซเบอร์ รวมถึงบทบาทของเครือข่ายสังคมออนไลน์ต่อการเปลี่ยนแปลงทัศนคติ และพฤติกรรมของผู้ใช้งาน

มิติที่ 3 Cybersecurity education, training and skills

เป็นขีดความสามารถด้านความตระหนักรู้ (Awareness) ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ของภาครัฐภาคเอกชน และประชาชนทั่วไป ตลอดจนการเข้าถึงและคุณภาพของการให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชนและประชาชนทั่วไป

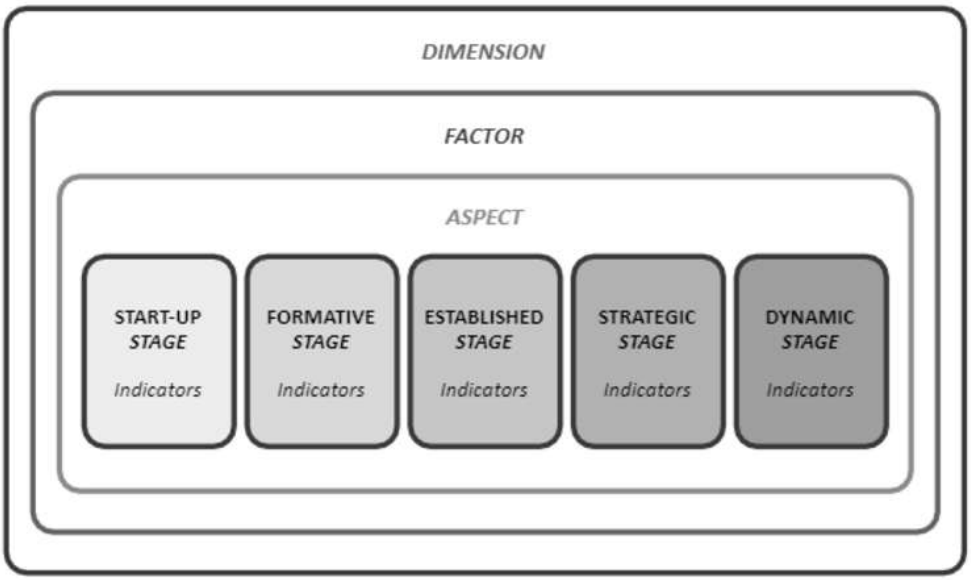
มิติที่ 4 Legal and regulatory frameworks

เป็นขีดความสามารถในการออกแบบและบังคับใช้กฎหมาย รวมถึงการตัดสินคดีความที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล และการคุ้มครองความเป็นส่วนตัว (Privacy protection) ถือว่าเป็นอีกมิติที่มีความจำเป็นต้องพัฒนาเพื่อให้เท่าทันการเปลี่ยนแปลงทางดิจิทัล (Digital transformation) ที่กำลังเกิดขึ้นและส่งผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วโลก

มิติที่ 5 Standards, organizations, and technologies

เป็นขีดความสามารถด้านการใช้เทคโนโลยีที่มีประสิทธิภาพเพื่อรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ให้กับประชาชนทั่วไป องค์กร โครงสร้างพื้นฐานของประเทศ มาตรฐานและการถอดบทเรียนจากกรณีศึกษาที่ดี ด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอ

กรอบแนวคิดของ CMM ได้แบ่งระยะของการกำหนดยุทธศาสตร์ (Stage of Maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ ออกเป็น 5 ระยะดังนี้ส่วนระยะของการกำหนดยุทธศาสตร์ ประกอบด้วย 5 ระยะ ได้แก่



ภาพประกอบที่ 12 ระยะของการกำหนดยุทธศาสตร์ (Stage of Maturity) ของ CCM

ระยะที่ 1 Start-up เป็นระดับที่เพิ่งเริ่มอภิปรายเกี่ยวกับแนวทาง การสร้างขีดความสามารถ แต่ยังไม่เริ่มดำเนินการ

ระยะที่ 2 Formative เป็นระดับที่เริ่มปรากฏแนวทางที่ชัดเจนแล้ว แต่ยังไม่จัดเป็นระเบียบหรือไม่เป็นหมวดหมู่

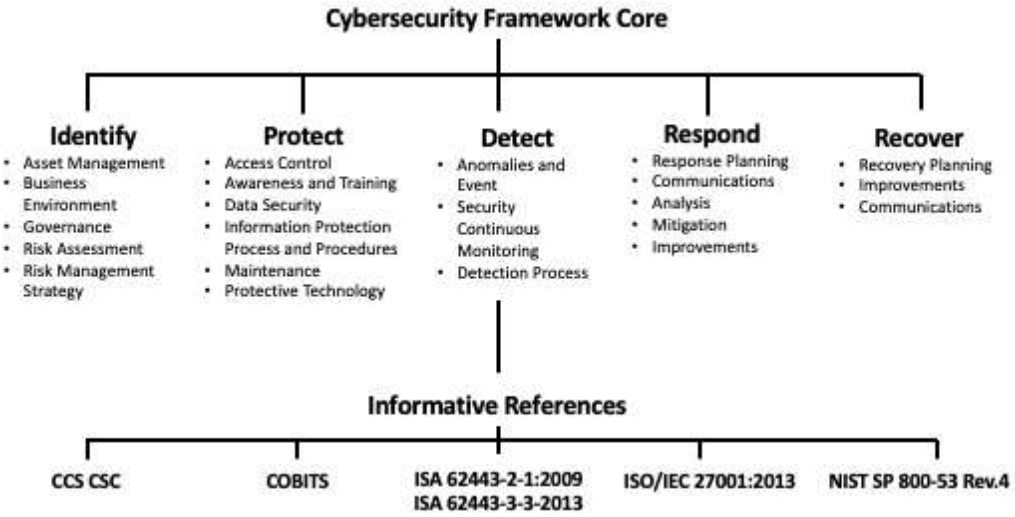
ระยะที่ 3 Established เป็นระดับที่เริ่มดำเนินการตามแนวทางแล้ว อยู่ในขั้นตอนของการตัดสินใจทางเลือกต่าง ๆ และ จัดสรรทรัพยากร

ระยะที่ 4 Strategic เป็นระดับที่มีการจัดลำดับความสำคัญของแนวทางว่าอยู่ในระดับองค์กรหรือในระดับชาติ และ

ระยะที่ 5 Dynamic เป็นระดับที่มีความชัดเจนในด้านกลไกนำไปสู่การเปลี่ยนแปลงยุทธศาสตร์ที่ขึ้นอยู่กับภัยคุกคามไซเบอร์ที่เกิดขึ้นจริงในปัจจุบัน

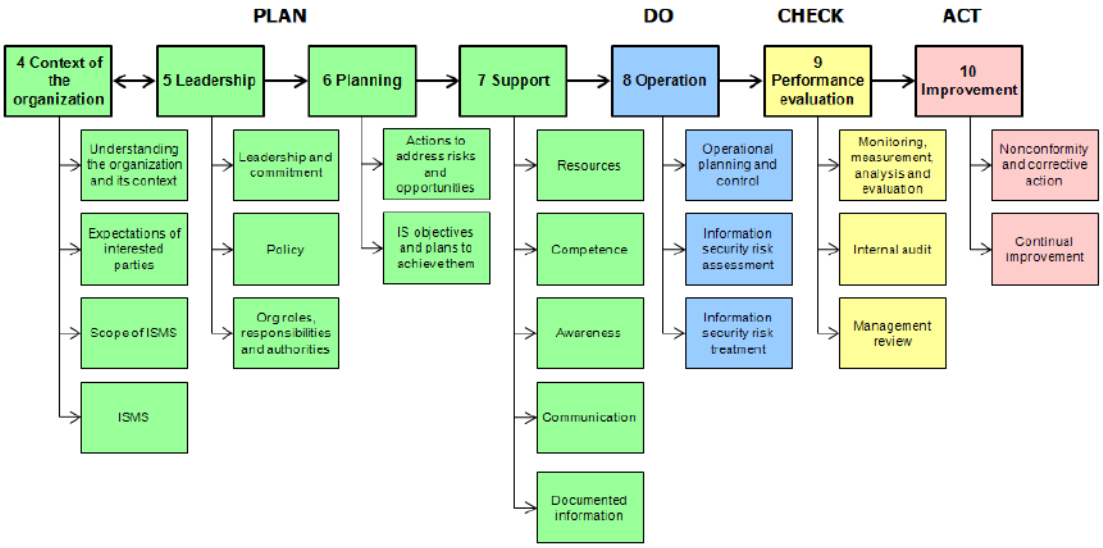
กรอบโครงสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity framework) ของสถาบันมาตรฐานและเทคโนโลยี (National institute of standards and technology: NIST) ประเทศสหรัฐอเมริกา[45,46]

ภาพประกอบที่ 13 กรอบการทำงานด้านความมั่นคงไซเบอร์



ภาพประกอบที่ 14 กรอบการทำงานด้านความมั่นคงไซเบอร์

มาตรฐาน ISO/IEC 27001:2013 (Information Security Management System)



ภาพประกอบที่ 15 มาตรฐาน ISO/IEC 27001:2013[41,72]

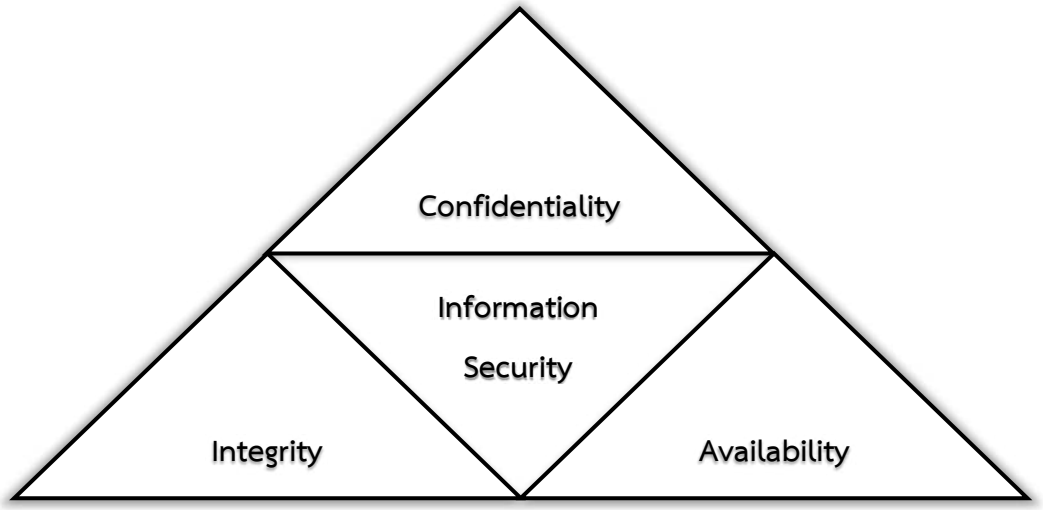
ประยุกต์ใช้หลักการ “PDCA” (Plan- Do -Check- Action)

ภาพประกอบที่ 16 ระบบมาตรฐานด้านความปลอดภัยสารสนเทศ “ISMS”

(Information Security Management System)

CIA TRIAD หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ

หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ (Information Security) ที่มีองค์ประกอบ 3 ส่วน ได้แก่



ภาพประกอบที่ 17 CIA TRIAD
หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ

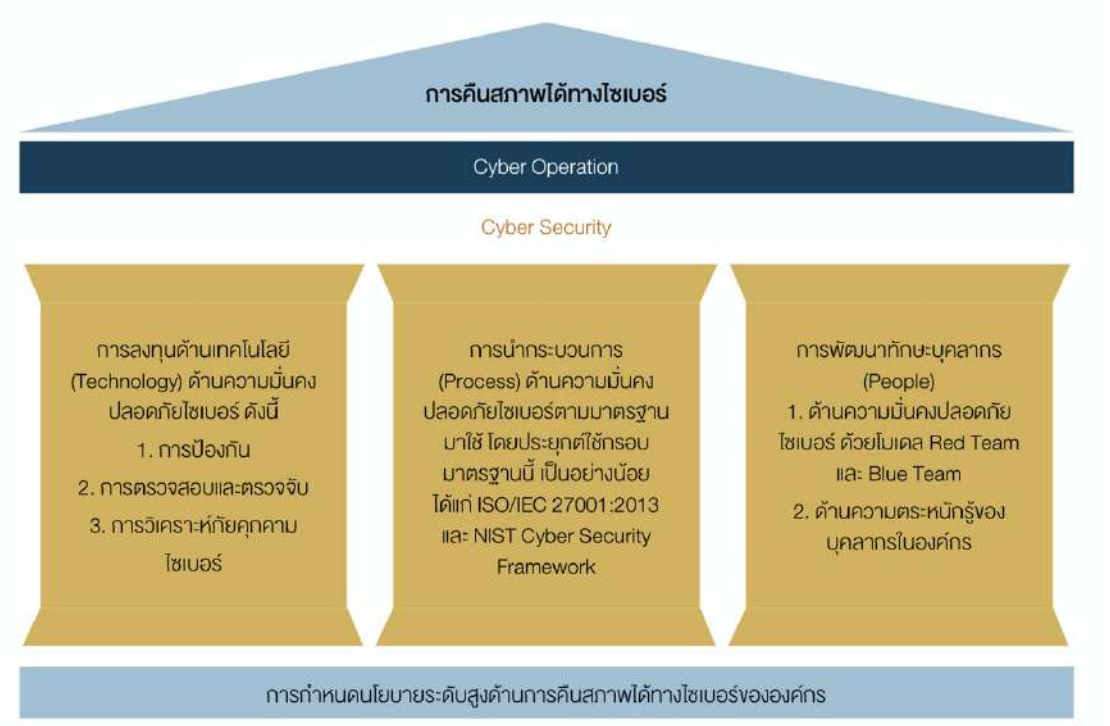
1.Confidentiality คือการรักษาความลับของสารสนเทศ กล่าวได้ว่าถ้าข้อมูลสารสนเทศนั้นถูกกำหนดให้เข้าถึงได้เฉพาะคนกลุ่มหนึ่ง ก็จะต้องมีเฉพาะคนกลุ่มนั้นเท่านั้นที่จะสามารถเข้าถึงข้อมูลสารสนเทศนั้นได้ ทั้งนี้ผู้ที่ไม่ได้อยู่ในคนกลุ่มนั้นจะต้องไม่สามารถเข้าถึงข้อมูลได้โดยเด็ดขาด

2.Integrity คือความถูกต้องของข้อมูลสารสนเทศ กล่าวได้ว่าข้อมูลสารสนเทศจะต้องคงความถูกต้องสมบูรณ์เสมอ โดยจะถูกเปลี่ยนแปลง แก้ไข หรือลบได้ด้วยเฉพาะผู้ที่ได้รับสิทธิอย่างถูกต้องเท่านั้น

3.Availability คือความพร้อมใช้งานของเทคโนโลยีสารสนเทศ กล่าวได้ว่าเมื่อผู้มีสิทธิต้องการเข้าถึงสารสนเทศนั้น ๆ ต้องการเข้าถึงหรือใช้งานสารสนเทศ จะต้องเข้าถึงได้ทุกครั้งที่ต้องการ

ผนวก ฉ.

Cyber Resilience[83] (หรือ Cyber Resiliency) คือ ความสามารถในการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ จึงกล่าวได้ว่า Cyber Resilience มุ่งเน้นไปในเรื่องความพร้อมหรือการปรับตัวเพื่อรับมือกับสถานการณ์ที่เกี่ยวข้องกับภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้เสมอ ซึ่งจะแตกต่างกับ Cyber Security ที่เน้นไปในทางการป้องกันเพื่อไม่ให้เกิด ในปัจจุบัน Cyber Resilience เริ่มเข้ามามีบทบาทมากขึ้น เนื่องจากมีภัยคุกคามทางไซเบอร์ที่หลากหลายรูปแบบและมักจะมาพร้อมกับเทคโนโลยีใหม่ ๆ ที่บางครั้งเราก็ไม่อาจป้องกันได้ทั้งหมด ดังนั้นทุกองค์กรจึงจำเป็นต้องมีกระบวนการจัดการ มีการวางแผนการรับมือเพื่อให้ธุรกิจดำเนินไปได้อย่างต่อเนื่อง



ภาพประกอบที่ 18 แนวคิดกลยุทธ์การคืนสภาพได้ทางไซเบอร์

การใช้หลักการของ Cyber Resilience ทำให้องค์กรสามารถเตรียมตัวรับมือกับภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ได้ดีขึ้น ซึ่งสอดคล้องกับหลักการมาตรฐานสากล ได้แก่ The National Institute of Standards and Technology (NIST) Framework, Center for Internet Security (CIS) Critical Security Controls และ ISO/IEC 27001 เป็นต้น

ผนวก ช.

หลักสูตรการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

สหประชาชาติ

1. สหภาพโทรคมนาคมระหว่างประเทศ หรือ The Telecommunication Union “ITU” ของสหประชาชาติ ว่าด้วยกรอบแนวทางการพัฒนายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ (Guide to Developing a National Cybersecurity Strategy)

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ITU มีหน่วยงานสถาบัน ITUAcademy เปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[31]

สหภาพยุโรป

2. หน่วยงานด้านความมั่นคงปลอดภัยของเครือข่ายและข้อมูลของสหภาพยุโรป (The European union agency for network and information security agency: ENISA) จัดทำคู่มือแนวปฏิบัติที่ดีในการกำหนดยุทธศาสตร์ความมั่งคงปลอดภัยไซเบอร์ระดับชาติ (Good practices in innovation on cybersecurity under the National Cyber Security Strategies “NCSS”)

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ENISA มีการเปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[88] และใช้แพลตฟอร์มของ MITRE ATT&CK[24] ในการแก้ไข จัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ (Tactics, Techniques, Procedures “TTPs”) ที่แฮกเกอร์นิยมใช้โจมตีระบบ Industrial Control System (ICS) ที่ใช้ควบคุมโครงสร้างพื้นฐานสำคัญของประเทศ ไม่ว่าจะเป็นระบบขนส่งพลังงาน โรงไฟฟ้า โรงกลั่นน้ำมัน ระบบบำบัดน้ำเสีย ระบบขนส่งมวลชน และอื่นๆ ภาครัฐและภาคเอกชนสามารถเพิ่มความปลอดภัยด้วย MITRE ATT&CK ซึ่งแบ่งเป็นหมวดหมู่ทั้งแบบ Enterprise, Mobile และ ICS[23,24,]

สหราชอาณาจักร

3. ศูนย์Global Cyber Security Capacity Centre, Department of Computer Science, มหาวิทยาลัย Oxford ประเทศอังกฤษ มีการวิเคราะห์ขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity capacity) ของประเทศและกำหนดระยะของการกำหนดยุทธศาสตร์ (Stage of maturity) ด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ โดยตามกรอบแนวคิดการสร้างความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ Global Cyber Security Capacity Centre, Department of Computer Science, มหาวิทยาลัย Oxford ประเทศอังกฤษ มีพันธมิตรคือสถาบัน SANS ในการเปิดหลักสูตร CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[26,27]

4. หลักสูตรการเรียนรู้ด้านมาตรฐาน ISO 27001:2013 และอื่น ๆ โดยบริษัทเอกชนที่จดทะเบียนจัดตั้งโดย Royal Charter (จาก British Standard Standards Association “BSI”)[42]

สหรัฐอเมริกา

5. หน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (Cybersecurity & Infrastructure Security Agency “CISA”)

ด้านการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ CISA มีสถาบันฝึกอบรม CISA TRAINING เปิดหลักสูตร Infrastructure Training และ CYBERSECURITY และอื่น ๆ ที่เกี่ยวข้องโดยสามารถเลือกเรียนทางไกลผ่านระบบอินเทอเน็ตได้[48,51,52,53]

ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.)

ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.)[84] เป็นหน่วยรับผิดชอบงานด้านไซเบอร์ได้พัฒนาการฝึกอบรมกำลังพลของกองทัพบกระดับนายทหารสัญญาบัตรและชั้นประทวนทั้งหมด 7 หลักสูตรดังนี้

หลักสูตรที่ 1 คือการปฏิบัติการด้านไซเบอร์เบื้องต้นประกอบไปด้วยการปฏิบัติการไซเบอร์(Kali Linux) การเจาะระบบเบื้องต้นองค์ประกอบพื้นฐานของ Information Security ประเภทภัยคุกคาม(Threat) ขั้นตอนการโจมตี Ethical Hacker 9 ขั้นตอน Network Mapping และการทำ Scanning เบื้องต้น

หลักสูตรที่ 2 การปฏิบัติการไซเบอร์ขั้นสูงศึกษาช่องโหว่ระบบปฏิบัติการต่างๆขั้นตอนการทดสอบการเจาะระบบข้อมูลของผู้ทดสอบเจาะระบบโปรมแกรมทดสอบการเจาะระบบ (Metasploit Framework) การโจมตี Web Application

หลักสูตรที่ 3-4 การรักษาความปลอดภัยทางไซเบอร์ (Cyber Security) สำหรับนายทหารสัญญาบัตรและนายทหารชั้นประทวนการติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายให้ปลอดภัยการรักษาความปลอดภัย Intrusion Detection System (IDS) ระบบตรวจจับการบุกรุกเป็นระบบที่ใช้สำหรับการเฝ้าระวังและแจ้งเตือนภัยถ้ามีการบุกรุก Internet Service Provider (ISP) ระบบการเชื่อมต่อเครือข่ายอินเทอร์ เน็ตเพื่อเปิดใช้งานกับเว็บไซต์ต่างๆ Intrusion Prevention System (IPS) การหยุดการบุกรุกจะใช้หลักการที่ เรียกว่า “Inline” หรือที่เรียกว่า “Gateway IDS” ซึ่งก็คือการนำ IPS ไปกั้นกลางบนเส้นทางการส่งข้อมูลโดยไม่ต้องมีการกำหนดหมายเลขไอพีให้กับ IDS/IPS เป็นระบบรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์เพื่อเป็นเครื่องมือสำหรับการสืบสวนบุคคลที่โจมตีบุกรุกเก็บสถิติ เกี่ยวกับการโจมตีและนำข้อมูลไปวิเคราะห์ภัยคุกคามและเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยเช่นไฟร์วอลเป็นต้น Firewall, Virus, Malware, Ransomware และการป้องกันการโจมตี Web Application กฎหมายอาชญากรรมทางไซเบอร์

หลักสูตรที่ 5-6 นายทหารรักษาความปลอดภัยไซเบอร์และเจ้าหน้าที่รักษาความปลอดภัยของนายทหารชั้นประทวนฝึกอบรมความตะหนักและการรักษาความ

ปลอดภัยทางด้านไซเบอร์คอมพิวเตอร์และระบบปฏิบัติ การระบบเครือข่ายคอมพิวเตอร์ (Computer Network) VA and Penetration Tesing, Vulnerability Scaning, Penetration Testing, Log Analysis

หลักสูตรที่ 7 การบริหารจัดการข่าวสารทางไซเบอร์ของนายทหารระดับชั้นสัญญาบัตรและนายทหารชั้นประทวนโดยฝึกอบรมพื้นฐานด้านการข่าว และวงรอบข่าวกรองหลักการประชาสัมพันธ์ และการสื่อสารมวลชนกฎหมายที่เกี่ยวข้องกับพระราชบัญญัติ คอมพิวเตอร์และพระราชบัญญัติลิขสิทธิ์เทคนิคการโฆษณาประชาสัมพันธ์ทางอินเทอร์เน็ตรูปแบบต่างๆ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือ National Cyber Security Agency : NCSA มี 6 หลักสูตร ในโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) ระยะที่ 1[65] เพื่อยกระดับศักยภาพบุคลการด้านไซเบอร์ตามแนวทางมาตรฐานสากล ภายใต้โครงการฯ มีความมุ่งมั่นในการส่งเสริมการสอบใบประกาศนียบัตรและใบรับรองความเชี่ยวชาญไซเบอร์ที่เป็นที่ยอมรับในระดับสากล ซึ่งเป็นหัวใจหลักในการยกระดับศักยภาพบุคลากรด้านไซเบอร์ของประเทศไทยให้ทัดเทียมกับนานาอารยประเทศ การจัดทำหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับพื้นฐานและระดับผู้เชี่ยวชาญ ได้ดำเนินการสอดคล้องตามแนวทางมาตรฐาน NICE ซึ่งเป็นมาตรฐานในการพัฒนาบุคลการด้าน Cybersecurity และแนวคิดสมรรถนะวิชาชีพ (Competency-based) ซึ่งประกอบด้วย องค์ประกอบ KSA ได้แก่ องค์ความรู้ (Knowledge) ทักษะ (Skill) และความสามารถ (Abilities) ที่เกี่ยวข้องด้าน Cybersecurity ความสอดคล้องของหลักสูตรเพื่อเตรียมความพร้อมในการสอบใบประกาศนียบัตรสากลมี อย่างหลักสูตรด้านความมั่นคงปลอดภัยระดับพื้นฐาน มีความสอดคล้องต่อการเตรียมความพร้อมเพื่อการสอบใบประกาศนียบัตรสากล EC-Council Security Specialist (ECSS) ของสถาบัน EC-Council, หลักสูตรด้านความมั่นคงปลอดภัยระดับผู้เชี่ยวชาญ มีความสอดคล้องต่อการเตรียมความพร้อมในการสอบใบ

ประกาศนียบัตรสากล Security+ ของสถาบัน CompTIA, หลักสูตรด้านความมั่นคงปลอดภัยระดับผู้เชี่ยวชาญเฉพาะด้าน มีความสอดคล้องต่อการเตรียมความพร้อมเพื่อการสอบประกาศนียบัตร CISSP (Certified Information Systems Security Professional) ของสถาบัน (ISC)2 โดยเป้าหมายหลักของโครงการฯ ต้องการให้เกิดผลลัพธ์สำคัญที่จะบรรลุผลสัมฤทธิ์ตามวัตถุประสงค์ในการฝึกทักษะ ยกระดับศักยภาพ และขีดความสามารถของบุคลการด้านไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure)[66,91,92] และหน่วยสำคัญ ๆ ของประเทศ ให้มีความรู้ความสามารถตามมาตรฐานสากล ทัดเทียมกับการพัฒนาด้านนี้ของประเทศอื่นในภูมิภาค

ประวัติย่อผู้วิจัย

ยศ ชื่อ นายณัฐกานต์ อรวรรณนุกุล

วัน เดือน ปีเกิด 22 กุมภาพันธ์ 2523

ประวัติสำเร็จการศึกษา

พ.ศ. 2544	ระดับเตรียมอุดมศึกษา เอกภาษาฝรั่งเศส โรงเรียนนวมินทราชินูทิศเตรียมอุดมศึกษาน้อมเกล้า
พ.ศ. 2546	ปริญญาตรี สาขาบริหารธุรกิจระหว่างประเทศ BBA ภาคภาษาอังกฤษ มหาวิทยาลัยหอการค้าไทย.
พ.ศ. 2546	หลักสูตรฝึกอบรมเชิงปฏิบัติการ Business Knowledge Enhancement ภาคภาษาอังกฤษ มหาวิทยาลัยหอการค้าไทย.
พ.ศ. 2552	ปริญญาโท สาขา บริหารธุรกิจมหาบัณฑิต การตลาด มหาวิทยาลัยรามคำแหง.
พ.ศ. 2554	หลักสูตรฝึกอบรมกลยุทธ์และการบริหารจัดการระบบขนส่ง Logistic: Strategy & Management ภาคภาษาอังกฤษ จุฬาลงกรณ์มหาวิทยาลัย

ประวัติการทำงาน

พ.ศ. 2548 - 2554	ผู้จัดการโครงการ (Project Manager), SmartSpa (London, UK) Ltd.
พ.ศ. 2554 - 2557	ผู้อำนวยการฝ่ายต่างประเทศ (Director of International Affairs), บริษัท G.E.T. Solutions Co., Ltd.

ตำแหน่งปัจจุบัน

พ.ศ. 2557 - 2565	ผู้อำนวยการฝ่ายส่งเสริมการขาย, บริษัท แอสตร้า เทคโนโลยี จำกัด