แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม

โดย

พลตรี ชาติชาย ชัยเกษม
ผู้อำนวยการศูนย์ไซเบอร์ทหาร
กองบัญชาการกองทัพไทย

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๓
ประจำปีการศึกษา พุทธศักราช ๒๕๖๓ – ๒๕๖๔

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม” ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยี ของ พลตรี ชาติชาย ชัยเกษม เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๓ ประจำปีการศึกษา พุทธศักราช ๒๕๖๓ - ๒๕๖๔

พลโท

(วิโรจน์ เกิดแสง)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอแห่งชาติเพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย พลตรี ชาติชาย ชัยเกษม **หลักสูตร** วปอ. **รุ่นที่** ๖๓

ภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันได้ทวีความรุนแรงและมีความซับซ้อนมากขึ้นอย่างต่อเนื่อง ที่ส่งผลกระทบตั้งแต่ในระดับบุคคล ระดับองค์กรทั้งภาครัฐฯ และภาคเอกชน ระดับประเทศ และระดับโลก ทั้งนี้ หัวใจของการรับมือกับเหตุการณ์การถูกโจมตีทางไซเบอร์ในระดับองค์กรขนาดใหญ่ที่มีการนำเอาระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) ระบบควบคุมการทำงานของเครื่องจากหรือกลไกขนาดใหญ่ด้วยระบบเครือข่ายคอมพิวเตอร์ (Operational Technology : OT)และระบบอินเตอร์เน็ตสรรพสิ่ง (Internet of Things : IOT) ที่มีมูลค่าสูงมาใช้ในการทำให้การปฏิบัติงานขององค์กรเกิดความมีประสิทธิภาพและมีความสะดวกสบายมากยิ่งขึ้น ซึ่งองค์กรดังกล่าวจำเป็นอย่างยิ่งที่จะต้องปกป้องระบบต่าง ๆ ด้วยศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC)

ทั้งนี้ มีความสับสนกันอย่างมากสำหรับแนวทางในการจัดตั้ง และการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศ (National Cybersecurity Operations Center : NCOC) ว่าควรจะมีลักษณะของการดำเนินการเช่นไร จะเป็นเหมือนกับการจัดตั้ง CSOC ขององค์กรขนาดใหญ่ทั่วไป หรือจะมีลักษณะพิเศษเป็นอย่างไร ซึ่งหลายประเทศและรวมทั้งประเทศไทยยังมีการดำเนินการที่ไม่ค่อยจะถูกต้องนัก ดังนั้นงานวิจัยฉบับนี้จึงมีความตั้งใจจะค้นหาปัญหาที่เกิดขึ้น วิธีการที่ควรจะนำมาเป็นตัวเลือกในการดำเนินการสำหรับ NCOC และแนวทางที่จะเสนอแนะให้ประเทศไทยดำเนินการจัดตั้ง NCOC ที่เป็นรูปธรรมและมีประสิทธิภาพ

ABSTRACT

Title The guidance for setting up Thailand National Cybersecurity Operations Center – NCOC – in order to properly solve the critical cybersecurity incidents at the national level

Field Science and Technology

Name Major General Chartchai Chaigasam **Course** NDC **Class** 63

Cybersecurity Threat is, now a day, becoming more and more aggressive and complicated. It impacts to every level from people to organizations, the nations, and the world. One of the best techniques for the large organizations that implement a lot of information technologies (IT), operational technologies (OT) and internet of things (IOT) as a part of their organizations' systems to handle and respond to the cybersecurity threats is Cyber Security Operations Center (CSOC)

There are a lot of confusion for many countries including Thailand of how to set up and operate the National Cybersecurity Operations Center (NCOC) at the national level. Should the NCOC set up and operate just like the CSOC of the large organizations? Is there some special characteristics for the NCOC at the national level? Therefore, this research would try to find out about the problems, the course of action of how to set up the NCOC, and then offer the most appropriate guidance to set up the NCOC for Thailand.

คำนำ

การวิจัยแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The guidance for setting up Thailand National Cybersecurity Operations Center – NCOC – in order to properly solve the critical cybersecurity incidents at the national level) ซึ่งแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) สามารถดำเนินการได้ใน ๒ รูปแบบหลัก ๆ ได้แก่ การตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) และแบบแยกการ (Decentralize) โดยที่การตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการนั้น มีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรทางคอมพิวเตอร์จากทุก ๆ หน่วยงานที่มีระบบการป้องกัน เฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ไปยังศูนย์กลางเฝ้าระวังภัยคุกคามทางไซเบอร์เพียงที่เดียว ทั้งนี้ประเทศไทยได้มีการริเริ่มที่จะนำเอาแนวคิดของการจัดศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ มาดำเนินการแล้วเช่นกัน ซึ่งถือว่าเป็นเป็นแนวคิดที่ดีที่มีความพยายามทำให้เกิดการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ขึ้นในระดับประเทศ แต่แนวทางในการดำเนินการที่สามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศได้อย่างเป็นรูปธรรมและมีประสิทธิภาพนั้น อาจสามารถดำเนินการได้หลายรูปแบบ

ผู้วิจัยจึงเห็นถึงความสำคัญของแนวทางการตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์แห่งชาติหรือศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ที่จะต้องเป็นกลไกหลักในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents)

ผู้วิจัยหวังเป็นอย่างยิ่งว่า เอกสารวิจัยฉบับนี้จะเป็นประโยชน์ต่อผู้เกี่ยวข้องและผู้ที่สนใจในการนำผลการวิจัยพร้อมทั้งข้อเสนอแนะไปใช้เป็นกรอบแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่สามารถปฏิบัติงานได้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ

พลตรี

(ชาติชาย ชัยเกษม)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๓
ผู้วิจัย

กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณคณาจารย์ทุกท่านของวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ที่ได้กรุณาประสิทธิ์ประสาทวิชาความรู้ให้ โดยเฉพาะอย่างยิ่งความรู้เกี่ยวกับในเรื่อง ยุทธศาสตร์ และการแก้ไขปัญหาภัยพิบัติรูปแบบต่าง ๆ ในระดับประเทศ ตลอดจนแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ซึ่งได้นำมาประยุกต์ใช้ในการจัดทำเอกสารวิจัยนี้

เอกสารวิจัยฉบับนี้ สำเร็จลุล่วงไปได้ด้วยดีด้วยความสนับสนุนช่วยเหลือจากอาจารย์ที่ปรึกษาวิจัย ได้แก่ พล.ต.กิติชาติ นิลขำ และ พ.อ.หญิง อัจริย์กุล อำไพ วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ และท่านผู้ให้ข้อมูลจากการเก็บข้อมูลวิจัย ทั้งจากการสัมภาษณ์เชิงลึก (In - Depth Interview) และการสนทนากลุ่ม (Focus Group Discussion) ตลอดจนท่านผู้ทรงคุณวุฒิ ได้แก่ พล.ท.ดร.ปรัชญา เฉลิมวัฒน์ เลขาฯ สกมช. และผู้มีส่วนเกี่ยวข้องกับงานวิจัยทุกท่าน ที่ให้ความกรุณาสนับสนุนการศึกษาด้วยความปรารถนาดีตลอดมา ซึ่งเป็นความภาคภูมิใจของผู้วิจัยจึงทำให้เกิดความมุ่งมั่นที่จะศึกษาจนประสบผลสำเร็จ เพื่อนำความรู้และประสบการณ์ที่ได้รับมาใช้ในการปฏิบัติหน้าที่ ตลอดจนพัฒนาหน่วยงานและประเทศชาติต่อไป

พลตรี

(ชาติชาย ชัยเกษม)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๓
ผู้วิจัย

สารบัญ

	หน้า
บทคัดย่อ	**ก**
คำนำ	**ค**
กิตติกรรมประกาศ	**ง**
สารบัญ	**จ**
สารบัญตาราง	**ช**
สารบัญแผนภาพ	**ซ**
ประมวลคำย่อ	**ญ**
บทที่ ๑ บทนำ	**๑**
ความเป็นมาและความสำคัญของปัญหา	๑
วัตถุประสงค์ของการวิจัย	๗
ขอบเขตของการวิจัย	๗
วิธีดำเนินการวิจัย	๘
ประโยชน์ที่ได้รับจากการวิจัย	๑๒
คำจำกัดความ	๑๒
บทที่ ๒ ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง	**๑๔**
แนวคิดและทฤษฎีสำคัญที่เกี่ยวข้อง	๑๔
กฎหมายและหลักการสำคัญต่าง ๆ ที่เกี่ยวข้อง	๓๑
งานวิจัยที่เกี่ยวข้อง	๔๓
กรอบแนวคิดของการวิจัย	๔๕
บทที่ ๓ แนวทางการดำเนินการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ	**๔๗**
ขั้นตอนในการดำเนินการวิจัย	๔๗
ขอบเขตของการวิจัย	๕๒
เครื่องมือที่ใช้ในการรวบรวมข้อมูลสำหรับการวิจัย	๕๓
การวิเคราะห์ข้อมูล	๕๕
สรุป	๕๖

สารบัญ (ต่อ)

		หน้า
บทที่ ๔	**วิเคราะห์แนวทางในการจัดตั้งและการปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ**	**๕๗**
	สรุปผลการวิเคราะห์ข้อมูล	๕๗
บทที่ ๕	**สรุป อภิปรายผลและข้อเสนอแนะ**	**๗๕**
	สรุป	๗๖
	อภิปรายผลการวิจัย	๘๐
	ข้อเสนอแนะ	๘๖
บรรณานุกรม		**๘๘**
ภาคผนวก		**๙๑**
ประวัติย่อผู้วิจัย		**๙๕**

สารบัญตาราง

หน้า

ตารางที่

๔ - ๑ รายชื่อผู้ให้สัมภาษณ์เชิงลึก (In - Depth Interview) ๖๐
๔ - ๒ รายชื่อผู้เข้าร่วมการสนทนากลุ่ม (Focus Group) ๖๗

สารบัญแผนภาพ

หน้า

แผนภาพที่

๒ - ๑ กรอบแนวคิดของการวิจัย ๔๕
๓ - ๑ เก็บรวบรวมข้อมูลวิจัย ๔๙
๔ - ๕ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการความมั่นคงปลอดภัย
ทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ ๖๔
๔ - ๖ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางความมั่นคงปลอดภัย
ทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ ๖๕
๕ - ๑ แนวทางการจัดตั้งศูนย์บริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์
ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC)
ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทั้ง ๘ ประเภท ๘๓
๕ - ๒ ตัวอย่างการจัดตั้ง JCOC ของหน่วยงานด้านความมั่นคงของรัฐ ๘๕

สารบัญตาราง

หน้า

ตารางที่

๔ - ๑ รายชื่อผู้ให้สัมภาษณ์เชิงลึก (In - Depth Interview) ๖๐
๔ - ๒ รายชื่อผู้เข้าร่วมการสนทนากลุ่ม (Focus Group) ๖๗

สารบัญแผนภาพ

หน้า

แผนภาพที่

๒ - ๑ กรอบแนวคิดของการวิจัย ๔๕
๓ - ๑ เก็บรวบรวมข้อมูลวิจัย ๔๙
๔ - ๕ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการความมั่นคงปลอดภัย
ทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ ๖๔
๔ - ๖ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางความมั่นคงปลอดภัย
ทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ ๖๕
๕ - ๑ แนวทางการจัดตั้งศูนย์บริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์
ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC)
ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทั้ง ๘ ประเภท ๘๓
๕ - ๒ ตัวอย่างการจัดตั้ง JCOC ของหน่วยงานด้านความมั่นคงของรัฐ ๘๕

คำอธิบายคำย่อ

ภาษาไทย

กมช.	ย่อมาจาก	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ตร.	ย่อมาจาก	สำนักงานตำรวจแห่งชาติ
ทบ.	ย่อมาจาก	กองทัพบก
ทร.	ย่อมาจาก	กองทัพเรือ
ทอ.	ย่อมาจาก	กองทัพเรือ
บก.ทท.	ย่อมาจาก	กองบัญชาการกองทัพไทย
ปปช.	ย่อมาจาก	คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
ปปส.	ย่อมาจาก	คณะกรรมการป้องกันและปราบปรามยาเสพติด
พ.ร.บ.	ย่อมาจาก	พระราชบัญญัติ
สกมช.	ย่อมาจาก	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
สป.	ย่อมาจาก	สำนักงานปลัดกระทรวงกลาโหม

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเราไม่สามารถปฏิเสธได้ว่าเทคโนโลยีสารสนเทศ (Information Technology : IT) และระบบเครือข่ายอินเทอร์เน็ต (Internet) มีบทบาทที่สำคัญอย่างมากกับชีวิตของมนุษย์ หรืออาจจะถือได้ว่าเป็นปัจจัยที่ห้าที่สำคัญสำหรับการดำรงชีวิตของมนุษย์ ที่นอกเหนือจากปัจจัยสี่อัน ได้แก่ อาหาร ที่อยู่อาศัย เครื่องนุ่งห่ม และยารักษาโรคเลยก็ได้ ทั้งนี้ เทคโนโลยีสารสนเทศและอินเทอร์เน็ตนั้นได้กลายเป็นสิ่งที่สำคัญต่อการดำรงชีวิตของมนุษย์ทั้งในด้านการใช้ชีวิต การทำงาน การเรียน การแพทย์ การธนาคารและอื่น ๆ อีกมากมาย อีกทั้งเทคโนโลยีสารสนเทศได้นำไปสู่การพัฒนาสิ่งใหม่ ๆ ให้เกิดขึ้นมาเพื่อทำให้ชีวิตของมนุษย์มีความสะดวกสบายมากยิ่งขึ้นแทบทุกวัน ยิ่งไปกว่านั้นเทคโนโลยีสารสนเทศยังสามารถที่จะเป็นเครื่องมือในการช่วยให้การทำงาน หรือแก้ไขปัญหาต่าง ๆ ของมนุษย์ได้อย่างมากมาย เช่น อุปกรณ์ เครื่องมือ เครื่องจักรวัสดุ หรือแม้กระทั่งสิ่งที่จับต้องไม่ได้ อันได้แก่ ระบบเครือข่ายสารสนเทศทั้งที่เป็นระบบปิด หรือระบบที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ระบบโปรแกรมและ Applications ต่าง ๆ หรือกระบวนการต่าง ๆ ด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำรงชีวิตของมนุษย์เกิดความสะดวกสบายมากยิ่งขึ้น

ยิ่งไปกว่านั้น ยังมีเทคโนโลยีอีกกลุ่มหนึ่งที่มีความสำคัญเป็นอย่างมาก ที่เป็นการรวมเอาเทคโนโลยีสารสนเทศหรือระบบ IT มาร่วมทำงานและประสานการปฏิบัติกับภาคอุตสาหกรรม เพื่อให้การผลิตหรือการควบคุมการทำงานของระบบงานภาคอุตสาหกรรมให้มีประสิทธิภาพมากกว่าในอดีต โดยเรียกเทคโนโลยีกลุ่มนี้ว่า เทคโนโลยีเชิงปฏิบัติงาน (Operational Technology : OT) ซึ่งเป็นทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่ใช้ในการควบคุมระบบอุตสาหกรรม เช่น ระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งทำหน้าที่เป็นรากฐานสำคัญในการควบคุมการทำงานของระบบโครงสร้างพื้นฐานที่สำคัญต่าง ๆ รวมถึงอุตสาหกรรมที่จำเป็นต่อความปลอดภัยและคุณภาพชีวิตที่ดีของประชาชน อันได้แก่ โรงไฟฟ้า โรงงานผลิต ระบบสาธารณูปโภค การประปา ด้านสาธารณสุข การคมนาคมขนส่ง และอื่น ๆ

ทั้งนี้ ระบบ OT จะแตกต่างจากระบบ IT แบบดั้งเดิม เนื่องจาก OT จะต้องรวมกระบวนการของการทำงานของแต่ละอุตสาหกรรม และระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ที่อาจมี Protocol ในการทำงานของแต่ละระบบที่แตกต่างกันไปเข้าด้วยกัน เพื่อออกแบบมาเป็นระบบที่ใช้ในการพัฒนาทรัพยากร และระบบบริหารการผลิตที่มีประสิทธิภาพ มีส่วนประกอบต่าง ๆ อันรวมถึง

เครื่องจักรหรือเครื่องยนต์นานาประเภท ตลอดจนระบบเซ็นเซอร์หรือแม้แต่หุ่นยนต์ซึ่งเป็นองค์ประกอบที่จำเป็นในโครงสร้างพื้นฐานที่สำคัญของแต่ละอุตสาหกรรมดังกล่าว ซึ่งอาจจะไม่พบในระบบ IT ประเภทดั้งเดิม

อีกเทคโนโลยีหนึ่งที่มีสำคัญและมีบทบาทต่อการใช้ชีวิตของมนุษย์โดยทั่วไปอย่างมากในปัจจุบัน ได้แก่ อินเทอร์เน็ตในทุกสรรพสิ่ง (Internet of Things : IoT) ที่อุปกรณ์ต่าง ๆ และสิ่งต่าง ๆ ได้ถูกเชื่อมโยงเอาทุกสิ่งทุกอย่างเข้ากับระบบอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การเปิด - ปิด อุปกรณ์เครื่องใช้ไฟฟ้า การสั่งการเปิดไฟฟ้าภายในบ้าน รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องมือทางการเกษตร อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านอุปกรณ์มือถือหรืออุปกรณ์สื่อสารแบบอื่น ๆ ที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต เป็นต้น

ทั้งนี้ นอกจากเรื่องของการให้บริการด้านเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ (Computer Networks) และสิ่งต่าง ๆ ที่กล่าวมาแล้วในขั้นต้น ไม่ว่าจะเป็นระบบ IT OT และ IoT หรือเทคโนโลยีอื่น ๆ ที่มีการเอาระบบเครือข่ายคอมพิวเตอร์เข้ามาใช้ด้วยก็ตาม สิ่งที่มีความจำเป็นอย่างยิ่งในสถานการณ์ปัจจุบัน ซึ่งมีผู้ไม่หวังดีที่อาจพยายามแสวงประโยชน์เพื่อตนเองหรือกลุ่มของตนเองต่อระบบเครือข่ายคอมพิวเตอร์ ได้แก่ เรื่องของ **“การรักษาความมั่นคงปลอดภัยทางไซเบอร์” หรือ Cybersecurity** ซึ่งมีความจำเป็นอย่างมากที่ทุกระบบไม่ว่าจะเป็นระบบ IT OT IOT หรือระบบเครือข่ายเทคโนโลยีสารสนเทศใด ๆ ก็ตาม มีความจำเป็นอย่างยิ่งที่จะต้องคำนึงถึงเรื่องของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่จะเป็นการทำให้ระบบ IT OT IOT และระบบเครือข่ายคอมพิวเตอร์ในรูปแบบต่าง ๆ มีความปลอดภัยจากภัยคุกคามทางไซเบอร์ ซึ่งจำเป็นอย่างยิ่งที่จะต้องมีผนวกการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในเรื่องของบุคลากร (People) กระบวนการดำเนินการ (Process) และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ (Technology) เชื่อมต่อทั้งในทางกายภาพ (Physical) และทางตรรกะ (Logical) เข้ากับระบบเครือข่ายด้านคอมพิวเตอร์ หรือระบบควบคุมของเครือข่ายด้านคอมพิวเตอร์ในรูปแบบต่าง ๆ ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ เครือข่ายทางคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ หรือแม้แต่เครื่องจักร เครื่องมือแพทย์ เครื่องใช้ภายในบ้าน อุปกรณ์ทางการเกษตร และสิ่งอื่น ๆ อีกมากมายที่ช่วยให้มนุษย์ใช้ชีวิตได้อย่างสะดวกสบายมากยิ่งขึ้น ให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถบริหารจัดการได้อย่างเป็นระบบ

ทั้งนี้ ภายใต้ความสะดวกสบายและประโยชน์มากมายที่มนุษย์ได้รับจากการเกิดขึ้นของระบบ IT OT IOT และระบบเครือข่ายคอมพิวเตอร์ในรูปแบบต่าง ๆ ย่อมมีความเสี่ยงและอันตรายที่เกิดขึ้นมาในโลกอย่างมากมาย ทั้งในปัจจุบันและในอนาคต จากการเกิดขึ้นมาของภัยคุกคามทางไซเบอร์ในหลากหลายรูปแบบ ทั้งในเรื่องของการถูกโจรกรรมข้อมูลที่สำคัญ การทำลายข้อมูล การทำให้การบริการต่าง ๆ หยุดชะงัก การเปลี่ยนแปลงข้อมูล หรือแม้แต่การทำให้เสียชื่อเสียง การทำให้ขาดความน่าเชื่อถือ ที่อาจจะนำมาเป็นเครื่องมือทางการเมือง ในการปลุกระดม การสร้างกระแส

หรือแม้แต่การหวังผลทางการทหาร จากการเกิดขึ้นของสงครามในรูปแบบใหม่ที่เรียกว่า สงครามทางไซเบอร์ (Cyberwarfare) ซึ่งในปัจจุบันนี้ในทางการทหารได้ถือว่า มิติทางไซเบอร์เป็นมิติที่ ๕ ของการรบในสงครามรูปแบบต่าง ๆ จากเดิมที่เคยพิจารณาและการทำการรบกันเพียงในมิติทางบก มิติทางน้ำ มิติทางอากาศ และมิติทางอวกาศเท่านั้น ปัจจุบันจะต้องคำนึงถึงมิติทางไซเบอร์ในการวางแผนและการปฏิบัติการในสนามรบรูปแบบต่าง ๆ เข้าไปด้วย ทั้งนี้ ในสถานการณ์ของความขัดแย้งทางการเมืองทั้งในประเทศและในระดับนานาชาติ บ่อยครั้งที่เมื่อเกิดความขัดแย้งและการเจรจาทางการทูตไม่สำเร็จ สงครามไซเบอร์จะถูกนำมาใช้เป็นเทคนิค หรือเป็นอำนาจกำลังรบสำคัญที่นำมาโจมตีและเป็นเครื่องมือในการทำให้ฝ่ายตรงข้ามเกิดความเสียหาย เพื่อแสวงหาข้อได้เปรียบและข้อยุติที่ฝ่ายที่มีอำนาจกำลังรบทางไซเบอร์สูงกว่า จะเป็นฝ่ายที่ได้เปรียบอย่างมากของสงครามทั้งที่เป็นอยู่ในปัจจุบันและในอนาคต

ในปัจจุบันหลายประเทศและหลายหน่วยงานเริ่มมีการตระหนักถึงความรุนแรงของภัยคุกคามทางไซเบอร์ จนทำให้เกิดการตื่นตัวและปรับตัวกันอยู่เป็นอย่างมากในหลาย ๆ หน่วยงาน แต่ในขณะเดียวกันก็ยังมีหน่วยงานอีกไม่น้อยที่ยังไม่ได้แม้แต่จะเริ่มต้น เนื่องจากขาดความรู้ความเข้าใจ งบประมาณ และการขาดแคลนบุคลากรผู้ปฏิบัติงานที่เป็นผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งอาจจะส่งผลให้หน่วยงานดังกล่าวตกเป็นเป้าหมายของผู้ไม่หวังดีในการโจมตีทางไซเบอร์เพื่อวัตถุประสงค์ที่แตกต่างกันไปของแฮกเกอร์ (Hackers)

ประเทศไทยได้มีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยที่ พ.ร.บ. ไซเบอร์ฯ ฉบับนี้มีวัตถุประสงค์เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure : CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น ๘ กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงาน และสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม[๑] ให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น พร้อมทั้งมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการถูกบุกรุกหรือถูกโจมตีทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ ตลอดจนความมั่นคงทางระบบเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศได้อย่างทันท่วงที

ทั้งนี้ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ได้กำหนดให้ทุกหน่วยงานที่ถือว่าเป็นสาธารณูปโภคสำคัญของประเทศ จะต้องมีกลไกและการบริหารจัดการที่นำไปสู่การแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานของตน และอาจส่งผลกระทบต่อประเทศ

---

[๑] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ในภาพรวม ทั้งก่อน ระหว่าง และหลังจากการถูกโจมตีหรือถูกบุกรุกทางไซเบอร์ ซึ่งหน่วยงานดังกล่าวอาจจำเป็นต้องจัดตั้งกลไกในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้นมาด้วยศักยภาพของหน่วยงานของตนเอง หรือจ้างหน่วยงานเอกชนเข้ามาดำเนินการให้ ซึ่งในทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นมีความจำเป็นที่จะต้องดำเนินการใน ๓ ส่วนพร้อม ๆ กันไป ได้แก่ ด้านบุคลากร (People) ด้านกระบวนการบริหารจัดการ (Processes) และด้านเทคโนโลยี (Technologies) โดยกรอบแนวคิดของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานและนิยมใช้กันอยู่ในทุกประเทศทั่วโลก ได้แก่ การดำเนินตามหลักการทำงานของ National Institute of Standards and Technology (NIST) Cybersecurity Framework[๒] โดยจะมีกลไกในการดำเนินการหลักอยู่ด้วยกัน ๕ กลุ่มงาน ได้แก่ การทำความเข้าใจกับระบบเทคโนโลยีสารสนเทศของหน่วยงานตนเอง และเข้าใจรูปแบบของการถูกโจมตีทางไซเบอร์ต่อระบบดังกล่าว (Identify) จากนั้นก็จะเข้าสู่ระบบของการป้องกัน (Protection) การเฝ้าระวังและตรวจจับ (Detection) การแก้ไขปัญหา (Respond) และการกู้คืนให้ระบบกลับมาใช้งานได้อย่างเป็นปกติ กรณีไม่สามารถรับมือกับการถูกโจมตีทางไซเบอร์ได้อย่างสมบูรณ์ (Recovery)

โดยทั่วไปแล้วในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น หน่วยงานหรือองค์กรต่าง ๆ มักจะมีการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operation Center - CSOC) ขึ้นมา เพื่อทำหน้าที่รับผิดชอบในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามกรอบแนวคิดของ NIST Cybersecurity Framework ในการรับมือกับภัยคุกคามทางไซเบอร์ และยิ่งไปกว่านั้นถ้าหน่วยงานใดที่ต้องการความน่าเชื่อถือทางในด้านการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อาจจำเป็นจะต้องมีการดำเนินการให้องค์กรของตนเอง ผ่านการประเมินโดยองค์กรที่ทำหน้าที่เป็น Certification Body (CB) ให้เป็นไปตามมาตรฐานสากลในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น ISO/IEC27001[๓] ร่วมด้วย

การจัดตั้งศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ อาจสามารถดำเนินการได้ใน ๒ รูปแบบหลัก ๆ ได้แก่ การตั้งศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) และแบบแยกการ

---

[๒] National Institute of Standards and Technology. “หลักการทำงานของ NIST Cybersecurity Framework.” (ออนไลน์). เข้าถึงได้จาก : https://www.nist.gov/cyberframework, ๒๕๖๓.

[๓] “มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS).” (ออนไลน์). เข้าถึงได้จาก : https://www.iso.org/isoiec-27001-information-security.html, ๒๕๖๓.

(Decentralize) โดยที่การตั้งศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการนั้น มีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรจากทุก ๆ หน่วยงานที่สำคัญในระดับประเทศ ที่เมื่อถูกโจมตีหรือบุกรุกทางไซเบอร์แล้วจะส่งผลกระทบในภาพรวมของประเทศเป็นวงกว้าง โดยหน่วยงานดังกล่าวจะต้องส่งข้อมูลการจราจรจากระบบการป้องกัน เฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของตนเอง ไปยังศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ที่ทำหน้าที่เป็นศูนย์กลางในการเฝ้าระวังภัยคุกคามทางไซเบอร์เพียงที่เดียวทั้งนี้ ประเทศไทยนั้นได้มีการริเริ่มที่จะนำเอาแนวคิดดังกล่าว มาจัดตั้งเป็น NCOC แบบรวมการมาแล้ว ซึ่งเป็นการดำเนินการของหน่วยงานระดับประเทศหน่วยงานหนึ่งภายใต้การกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในอดีต ที่ได้มีการจัดทำโครงการระบบการป้องกันและติดตามรักษาความปลอดภัยทางไซเบอร์ สำหรับองค์กรและหน่วยงานของรัฐที่ไม่สามารถดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ด้วยตัวเอง ซึ่งถือว่าเป็นเป็นแนวคิดที่ดีสำหรับความพยายามที่จะทำให้เกิดการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศขึ้น แต่ประสิทธิภาพของการดำเนินการที่นำไปสู่การแก้ไขปัญหาการถูกโจมตีทางไซเบอร์ที่เป็นรูปธรรมนั้นยังเป็นที่กังขาอยู่เป็นอย่างมาก

ทั้งนี้ การดำเนินการของ NCOC แบบรวมการนั้น มีความจำเป็นที่จะต้องมีข้อมูลการจราจรทางคอมพิวเตอร์ที่มีจำนวนมากเพียงพอต่อการวิเคราะห์ มีระบบตรวจจับภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพในการประมวลผลข้อมูลจำนวนมหาศาล และมีบุคลากรที่เชี่ยวชาญจำนวนมากพอในการวิเคราะห์ข้อมูล และดำเนินการแก้ไขปัญหาการถูกบุกรุกทางไซเบอร์ได้อย่างทันท่วงที แต่ข้อด้อยของการตั้ง NCOC แบบรวมการ มาจากที่หน่วยงานแต่ละหน่วยงานมีข้อมูลที่สำคัญต่างกันและการป้องกันข้อมูลที่สำคัญก็ต่างกันด้วย การส่งข้อมูลจราจรคอมพิวเตอร์ไปวิเคราะห์ ตรวจจับภัยคุกคามทางไซเบอร์ที่จะนำไปสู่การแก้ปัญหาการถูกโจมตีหรือการถูกบุกรุกทางไซเบอร์อาจจะไม่ตรงจุดเท่าที่ควร

ยิ่งไปกว่านั้น ในปัจจุบันยังไม่มีอุปกรณ์ที่สามารถวิเคราะห์ภัยคุกคามจากข้อมูลการจราจรคอมพิวเตอร์จำนวนมหาศาลได้อย่างแม่นยำ เช่น การนำระบบ SIEM (Security Information and Event Management) ที่เป็นระบบจัดเก็บ ตรวจสอบ และวิเคราะห์ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเครือข่ายขององค์กร เพื่อนำเอาข้อมูลเหล่านั้นไปใช้ในการตรวจจับและโต้ตอบการถูกโจมตีที่เกิดขึ้น แต่ในความเป็นจริงแล้วระบบ SIEM นั้น เป็นระบบที่เหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรของหน่วยงานขนาดเล็กถึงขนาดกลาง (Small and Medium - Sized Enterprise) เพียงหน่วยงานเดียวหรือไม่กี่หน่วยงาน ที่มีข้อมูลการจราจรรวมกันแล้วไม่มากเกินไป ที่จะนำข้อมูลดังกล่าวมาวิเคราะห์ให้เห็นถึงภัยคุกคามทางไซเบอร์ที่เข้ามาสู่ระบบขององค์กรได้อย่างแท้จริง

ส่วนการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) อีกรูปแบบหนึ่ง คือการดำเนินการแบบแยกการ ซึ่งอาจจะเป็นการดำเนินการโดยให้แต่ละกลุ่มที่มีการดำเนินการทางธุรกิจหรือวัตถุประสงค์ขององค์กรที่คล้ายกันตามหน่วยงานโครงสร้าง

พื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ดำเนินการตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ร่วม (Joint Cybersecurity Operations Center : JCOC) ของกลุ่มตนเอง หรืออาจจะลงลึกถึงหน่วยงานของตนเองสามารถแยกดำเนินการเองในลักษณะของการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ย่อยไปเลย ถ้ามีความพร้อมทั้งด้านงบประมาณ และกำลังพลเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เพียงพอ ส่วนหน่วยกลางใหญ่หรือ JCOC เป็นเพียงแค่ส่วนงานที่คอยบูรณาการให้เกิดการกระจายหรือแชร์ข้อมูลด้านไซเบอร์ที่สำคัญร่วมกัน และบูรณาการให้เกิดการพึ่งพาอาศัยกันตลอดจนช่วยกันแก้ไขปัญหาที่เกิดขึ้นเท่านั้น ซึ่งการดำเนินการในลักษณะนี้อาจสามารถแก้ปัญหาและรับมือภัยคุกคามทางไซเบอร์ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพในเชิงลึกได้มากกว่า แต่อาจจะต้องใช้เวลาในการสร้างศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ให้มีความพร้อมทั้งด้านบุคลากรทางไซเบอร์ ระบบการบริหารจัดการ และระบบเทคโนโลยีต่าง ๆ ที่จะเลือกมาใช้ในการดำเนินการ ซึ่งปัญหาใหญ่มักจะอยู่ที่การขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่จะมาเป็นผู้ควบคุมระบบต่าง ๆ ให้สามารถดำเนินการได้จริงอย่างมีประสิทธิภาพ

จากเหตุผลดังกล่าว ผู้วิจัยจึงเห็นถึงความสำคัญของแนวทางการตั้งศูนย์ปฏิบัติการเฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ที่จะต้องเป็นกลไกหลักในระดับประเทศ ในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ซึ่งภายหลังจากการออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๒ แล้ว ประเทศไทยได้มีการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ขึ้นเพื่อทำหน้าที่เป็นหน่วยงานหลักที่จะทำหน้าที่รับผิดชอบและบริหารจัดการให้เกิดการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศ และระดับนานาชาติอย่างเป็นระบบ แต่อย่างไรก็ตามหัวใจของการดำเนินการและรับมือกับภัยคุกคามทางไซเบอร์ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ คือ CSOC (Cyber Security Operations Center) ที่จะเป็นส่วนงานของการทำหน้าที่ในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้เป็นไปตามมาตรฐานสากล ที่ประกอบด้วยการ Identify, Protect, Detect, Response และ Recovery ให้กับองค์กรที่นำระบบเครือข่ายเทคโนโลยีสารสนเทศมาใช้บริหารจัดการทางธุรกิจ หรือการปฏิบัติงานขององค์กร แต่การที่ดำเนินการด้าน CSOC ของ สกมช. ในระดับประเทศนั้น ยังไม่มีการออกแบบหรือวางแนวทางในการดำเนินการอย่างชัดเจนในระดับประเทศ

ดังนั้นงานวิจัยฉบับนี้จึงมุ่งเน้นและมีความต้องการที่จะเพื่อศึกษาถึงปัญหาและรูปแบบของการดำเนินการของ CSOC ในระดับประเทศ ที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ปี พ.ศ. ๒๕๖๒ ตลอดจนศึกษาแนวทางการทำงานของศูนย์ปฏิบัติการทางไซเบอร์ ในรูปแบบต่าง ๆ ที่ใช้กันอยู่ในระดับนานาชาติ และในท้ายที่สุดก็จะนำเสนอรูปแบบ ตลอดจนแนวทางในการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังและแก้ไข

ปัญหาทางไซเบอร์แห่งชาติ หรือ NCOC เพื่อรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศสำหรับประเทศไทย ให้สามารถปฏิบัติงานได้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒. เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ที่เป็นแบบรวมการและแยกการ

๓. เพื่อเสนอแนวทางในการจัดตั้งและดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

ขอบเขตของการวิจัย

๑. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้มุ่งเน้นศึกษาถึงทฤษฎีและหลักการในการดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เอกสารงานวิจัยที่เกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ ยุทธศาสตร์ด้านไซเบอร์ กฎหมายต่าง ๆ ที่เกี่ยวข้องในการปฏิบัติงานของเจ้าหน้าที่ ข้อมูลพื้นฐานที่เกี่ยวกับศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์และศูนย์ปฏิบัติการร่วมทางไซเบอร์ โครงสร้างการจัดระเบียบปฏิบัติ เพื่อนำข้อมูลที่รวบรวมได้ มาออกแบบสำหรับเป็นแนวทางในการดำเนินการตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับประเทศ

๒. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

กลุ่มตัวอย่าง การเลือกกลุ่มตัวอย่าง (Sampling) โดยเลือกกลุ่มตัวอย่างประเภทการเลือกกลุ่มตัวอย่างที่เป็นตัวแทน (Typing Cases Sampling) เป็นลักษณะการเลือกแบบเจาะจง (Purposive Sampling) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และผู้มีประสบการณ์ในด้านการบริหารจัดการหรือรับมือภัยคุกคามทางไซเบอร์มาแล้วเท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๘ ท่าน และสรรหาผู้เข้าร่วมในการสนทนากลุ่มอีกจำนวนประมาณ ๕ - ๑๐ ท่าน จากกลุ่มประชากรที่เกี่ยวข้องในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่ได้กำหนดให้มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ไว้จำนวน ๘ ประเภท

๓. ขอบเขตเวลา

ทำการศึกษาในช่วงตั้งแต่เดือน ธันวาคม ๒๕๖๓ ถึง พฤษภาคม ๒๕๖๔

วิธีดำเนินการวิจัย

งานวิจัยเรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The Guidance For Setting Up Thailand National Cybersecurity Operations Center – NCOC – In Order To Properly Solve The Critical Cybersecurity Situation At The National Level) ” จะเป็นการดำเนินการในลักษณะของการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยกระบวนการศึกษาทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องกับเรื่องที่ศึกษา เพื่อให้ได้กรอบแนวคิดในการวิจัยที่เกิดจากกระบวนการวิเคราะห์และสังเคราะห์ กรอบแนวคิดงานวิจัยหลังจากนั้นจะแบ่งการเก็บข้อมูล เพื่อการวิจัยออกเป็น ๔ ส่วนหลัก ๆ ได้แก่ การวิจัยเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่ม (Focus Group Discussion) และการสังเกตการณ์ (Observation) เพื่อหาข้อมูลของปัญหาในการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์แห่งชาติ ตลอดจนแนวทางในการดำเนินการที่เป็นรูปธรรมและมีประสิทธิภาพต่อไปในอนาคต

๑. แหล่งข้อมูล

๑.๑ แหล่งข้อมูลปฐมภูมิ (Primary Data) จะได้จากการสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่ม (Focus Group Discussion) และการสังเกตการณ์ (Observation) จากกลุ่มเป้าหมายที่เป็นกลุ่มตัวอย่าง (Sampling) โดยเลือกกลุ่มตัวอย่างประเภทที่เป็นตัวแทน (Typing Cases Sampling) เป็นลักษณะการเลือกแบบเจาะจง (Purposive Sampling) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และผู้มีประสบการณ์ในด้านการบริหารจัดการ หรือรับมือภัยคุกคามทางไซเบอร์มาแล้วเท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๘ ท่าน และสรรหาผู้เข้าร่วมในการสนทนากลุ่มอีกจำนวนประมาณ ๕ - ๑๐ ท่าน จากกลุ่มประชากรที่เกี่ยวข้องในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่ได้กำหนดให้มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ไว้จำนวน ๘ ประเภท

๑.๒ ข้อมูลทุติยภูมิ (Secondary Data) จะได้จากการทบทวนวรรณกรรม ตลอดจนค้นคว้าจากเอกสาร ตำรา เว็บไซต์ และงานวิจัยที่เกี่ยวข้อง

๒. การเก็บรวบรวมข้อมูล

๒.๑ การดำเนินวิจัยจากเอกสารต่าง ๆ ที่เกี่ยวข้อง (Documentary Research)

เพื่อให้ทราบถึงแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้องในเรื่องของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ในหลากหลายรูปแบบ

ตลอดจนวิเคราะห์หาข้อเด่นและข้อด้อยของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ทั้งที่เป็นแบบรวมการและแบบแยกการ

๒.๒ การสัมภาษณ์เชิงลึก (In - depth Interview)

จะเป็นการดำเนินการสัมภาษณ์กลุ่มเป้าหมาย ทั้งบุคคลที่เป็นผู้เชี่ยวชาญและมีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์จริง ๆ เท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๘ ท่าน จากตัวแทนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยเป็นการสัมภาษณ์แบบกึ่งโครงสร้าง หรือการสัมภาษณ์แบบชี้นำ (Guided Interview) กล่าวคือเป็นการสัมภาษณ์ที่มีการใช้คำสำคัญ (Keywords) มาประกอบในการสัมภาษณ์มีการร่างข้อคำถามที่มีลักษณะปลายเปิดพร้อมกับลักษณะของข้อคำถามที่มีความยืดหยุ่น พร้อมที่จะมีการปรับเปลี่ยนถ้อยคำของข้อคำถามให้มีความสอดคล้องกับผู้ให้สัมภาษณ์แต่ละคนในแต่ละสถานการณ์ได้ตอบข้อคำถามอันทำให้ได้มาซึ่งข้อมูลที่มีความหลากหลายในมิติต่าง ๆ และข้อเท็จจริงในทางปฏิบัติที่มีทั้งมิติของความลึกและมิติของความกว้างในเรื่องที่เกี่ยวข้องกับงานวิจัย เพื่อใช้เป็นข้อมูลในการวิเคราะห์และศึกษาปัจจัยสำคัญทำให้สามารถนำข้อมูลที่ได้มาวิเคราะห์หาแนวทาง และรูปแบบของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพต่อไป

๒.๓ การสนทนากลุ่มเฉพาะ (Focus Group Discussion)

ในการสนทนากลุ่มที่ผู้วิจัยจะทำการรวบรวมข้อมูลจากการสนทนากับกลุ่มผู้ให้ข้อมูลในประเด็นปัญหา โดยผู้วิจัยได้ออกแบบโครงสร้างของข้อคำถามเพื่อนำไปใช้ในการประชุมสนทนากลุ่มซึ่งการใช้กระบวนการการเลือกกลุ่มแบบเจาะจงในการสำรวจข้อมูล จำนวน ๕ - ๘ ท่าน จากตัวแทนศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย ศูนย์ไซเบอร์กองทัพบก ศูนย์ไซเบอร์กองทัพอากาศ ศูนย์ไซเบอร์กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ ศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ตลอดจนหน่วยงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายนอกกระทรวงกลาโหม เพื่อประมวลแนวคิดและสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ เพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคต

๒.๔ การสังเกตการณ์ (Observation)

จะเป็นการใช้ข้อมูลของการสังเกตจากตัวนักวิจัยเองที่เป็นผู้มีความรู้และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับกองทัพไทย ในระดับประเทศ และในระดับนานาชาติ มานานกว่า ๗ ปี ตลอดจนเป็นผู้มีส่วนร่วมในการร่างกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ และเป็นผู้ร่วมจัดตั้ง สกมช. ตั้งแต่เริ่มต้นจนถึงปัจจุบัน

ทั้งนี้ การสัมภาษณ์เชิงลึก การสนทนากลุ่ม และการสังเกตการณ์ จะมีรายละเอียดของการดำเนินการที่ประกอบด้วย การศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง, การกำหนดกรอบแนวคิดในการวิจัย, การกำหนดประชากรและกลุ่มตัวอย่าง, กำหนดเครื่องมือที่ใช้ในการวิจัย, การประมวลผลและการวิเคราะห์ข้อมูล

๓. เครื่องมือที่ใช้ในการรวบรวมข้อมูล

๓.๑ การวิจัยจากเอกสาร (Documentary Research) จะเป็นการทำการวิจัยจากเอกสารต่าง ๆ ที่เกี่ยวข้องกับหัวข้อการวิจัย เพื่อให้มาซึ่งแนวคิด และทฤษฎีที่เกี่ยวข้องกับการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ตลอดจนหาแนวทางและองค์ความรู้เกี่ยวกับการจัดตั้งและการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC)

๓.๒ การสัมภาษณ์เชิงลึก (In - Depth Interview) ประกอบด้วยประเด็นคำถามสำคัญ ๔ ข้อ ได้แก่

๓.๒.๑ หน่วยของท่านมีการรับมือภัยคุกคามทางไซเบอร์อย่างไร และถ้าไม่สามารถรับมือหรือแก้ปัญหาภัยคุกคามทางไซเบอร์ได้ มีแนวทางที่จะดำเนินการต่อไปอย่างไร

๓.๒.๒ ท่านคิดว่าอะไรคือปัญหา การจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมศูนย์และแบบกระจายศูนย์

๓.๒.๒.๑ บุคลากร (People) ทั้งผู้ปฏิบัติงาน และผู้บังคับบัญชา

๓.๒.๒.๒ กระบวนการ (Process) และงบประมาณ (Budget)

๓.๒.๒.๓ เทคโนโลยี (Technology)

๓.๒.๓ ท่านคิดว่าโมเดลการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) มีกี่แบบ แต่ละแบบมีข้อเด่นและข้อด้อยอย่างไร

๓.๒.๔ ท่านคิดว่า โมเดลการจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) ควรเป็นอย่างไร

๓.๓ การสนทนากลุ่มเฉพาะ (Focus Group Discussion) ประกอบด้วยประเด็นคำถามสำคัญ ๔ ข้อ ได้แก่

๓.๓.๑ แนวทางในการรับมือกับภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างไรและในกรณีที่หน่วยงานหรือองค์กรไม่สามารถแก้ไขปัญหาภัยคุกคามทางไซเบอร์ได้ด้วยตนเอง ควรมีการดำเนินการต่อไปอย่างไร

๓.๓.๒ อะไรคือปัญหาของการจัดตั้งหน่วยงานเพื่อนำไปสู่การบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมศูนย์ และแบบกระจายศูนย์

๓.๓.๒.๑ บุคลากร (People) ทั้ง ผู้ปฏิบัติงาน และผู้บังคับบัญชา

๓.๓.๒.๒ กระบวนการ (Process) และงบประมาณ (Budget)

๓.๓.๒.๓ เทคโนโลยี (Technology)

๓.๓.๓ รูปแบบของการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศของประเทศไทย (NCOC) มีได้กี่แบบ แต่ละแบบมีแนวทางในการดำเนินการอย่างไร และมีข้อดีข้อเสียอย่างไร

๓.๓.๔ รูปแบบของการจัดตั้งและการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย (NCOC) ควรจะเป็นอย่างไร

๓.๔ การเก็บรวบรวมข้อมูลจากสังเกตมีวิธีดำเนินการเก็บรวบรวมข้อมูล โดยการสังเกตจากตัวนักวิจัยเอง ซึ่งมีความรู้ และประสบการณ์ด้านจัดการภัยคุกคามทางไซเบอร์ในระดับกองทัพไทยและระดับประเทศ จาก ๒ สถานการณ์ ดังนี้

๓.๔.๑ การสังเกตจากการปฏิบัติงานจริงด้านการรับมือและจัดการภัยคุกคามทางไซเบอร์ของกองบัญชาการกองทัพไทย และกองทัพไทย ซึ่งถือเป็นหน่วยงานที่ถูกกำหนดให้เป็นสาธารณูปโภคพื้นฐานสำคัญของประเทศ

๓.๔.๒ การสังเกตจากการฝึกการปฏิบัติการทางไซเบอร์ประจำปีของกองทัพไทย ซึ่งกองบัญชาการกองทัพไทยได้จัดมาอย่างต่อเนื่องเป็นเวลา ๕ ปี ซึ่งเป็นการฝึกการปฏิบัติการและแก้ไขสถานการณ์ด้านไซเบอร์ทั้งในระดับกองทัพไทย ร่วมกับหน่วยงานที่เกี่ยวข้องที่สำคัญทั้งหมดในระดับประเทศ

๔. วิธีการประมวลผลและการวิเคราะห์ข้อมูล

เป็นการวิเคราะห์ข้อมูลในงานเชิงคุณภาพ ซึ่งจะใช้วิธีการวิเคราะห์ข้อมูลเชิงเนื้อหา (Content Analysis) ที่ได้จากกระบวนการสัมภาษณ์และกระบวนการกลุ่มย่อย (Focus Group)

๔.๑ จัดระเบียบข้อมูล (Data) ในรูปของบันทึกเป็นคำพูด นำมาถอดเทป และพิมพ์บันทึกสรุปใจความการสนทนากลุ่ม

๔.๒ พัฒนาข้อมูลไปสู่มโนทัศน์ (Concept) โดยการนำเสนอและแสดงข้อมูลเชิงพรรณนาซึ่งมาจากการกลั่นความคิดและหาความสัมพันธ์เชื่อมโยงของข้อมูลที่ถูกต้องและตรงประเด็นตามกรอบความคิด

๔.๓ จัดมโนทัศน์เข้าสู่หมวดหมู่ (Categories) โดยสรุปข้อมูลเป็นหมวดหมู่เพื่อจำแนกให้อยู่ในขอบเขตและครอบคลุมในประเด็นที่กำหนด เพื่อตอบวัตถุประสงค์ของการวิจัย

๔.๔ จัดทำข้อเสนอเชิงทฤษฎี (Proposal) ที่ได้จากการจัดกระบวนการกลุ่ม

๔.๕ ภายหลังจากการเก็บรวบรวมข้อมูลทั้ง ๔ วิธีการ ได้แก่ การดำเนินการวิจัยจากเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่มเฉพาะ (Focus Group Discussion) และการสังเกตการณ์ (Observation) เพื่อให้ทราบถึงแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้องในเรื่องของการดำเนินการ ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติในหลากหลายรูปแบบ จะมีการนำเอาข้อมูลที่ได้จากการเก็บรวบรวมข้อมูลไปวิเคราะห์หาจุดเด่นและจุดด้อยของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ทั้งที่เป็นแบบรวมการ และแบบแยกการ และประมวล

แนวคิดและสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ นำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ และเพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคต

ประโยชน์ที่ได้รับจากการวิจัย

๑. ได้ทราบความเป็นมาและปัญหาในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

๒. ได้ทราบความเหมือน ความต่าง และข้อดีข้อเสียการดำเนินงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติในแบบรวมการและแยกการ

๓. ได้แนวทางในการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์แห่งชาติได้ในอนาคต

๔. งานวิจัยฉบับนี้จะเป็นแนวทางให้กับหน่วยงานที่ถือเป็นสาธารณูปโภคพื้นฐานสำคัญของประเทศได้เข้าใจถึงปัญหาในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเป็นแนวทางในการดำเนินการจัดตั้งหน่วยงานของตนเพื่อการรับมือกับภัยคุกคามทางไซเบอร

๕. งานวิจัยฉบับนี้จะเป็นแนวทางให้กับ สกมช. ในการนำไปใช้ในการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์แห่งชาติได้ในอนาคต

๖. งานวิจัยฉบับนี้จะทำให้ผู้ที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตลอดจนผู้ที่สนใจสามารถเข้าใจถึงแนวทางในการบริหารจัดการและการปฏิบัติการทางไซเบอร์ในระดับประเทศ มีความเข้าใจระบบการบริหารจัดการด้านไซเบอร์ในระดับประเทศที่เป็นไปในทิศทางเดียวกันและจะนำไปสู่การทำงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ในระดับประเทศร่วมกันได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

คำจำกัดความ

การปฏิบัติการทางไซเบอร์

หมายถึง การใช้ขีดความสามารถทางไซเบอร์ที่หลากหลายเพื่อให้สามารถบรรลุภารกิจต่าง ๆ ที่ได้รับมอบ ทั้งภายในมิติทางไซเบอร์และผ่านมิติทางไซเบอร์

การรักษาความมั่นคงปลอดภัยทางไซเบอร์

หมายถึง หลักการ มาตรการ กระบวนการ และแนวทางปฏิบัติเพื่อปกป้องมิติไซเบอร์จากการโจมตีทางไซเบอร์

โครงสร้างพื้นฐานที่สำคัญอย่างมาก (Critical Infrastructure)

หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งของรัฐ ซึ่งใช้ระบบสารสนเทศในการควบคุมการปฏิบัติงาน มักใช้ในการให้บริการประชาชน ได้แก่ ระบบการจ่ายกระแสไฟฟ้า ระบบการบริหารจัดการน้ำ ระบบบริหารด้านการเงิน ระบบการให้บริการอินเทอร์เน็ต ระบบการสื่อสารทั้งภาคพื้นดินและดาวเทียม ระบบกิจการวิทยุและโทรทัศน์ ระบบการขนส่งมวลชน ระบบควบคุมการจราจรทางบกและทางอากาศ เป็นต้น

ภัยคุกคามทางไซเบอร์

หมายถึง การกระทำใด ๆ ที่มุ่งต่อระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมโยงติดกันรวมทั้งฐานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ ระบบดังกล่าวไม่สามารถปฏิบัติการได้ตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกจารกรรมหรือถูกทำลาย รวมทั้งการแสวงใช้ประโยชน์ เครือข่ายคอมพิวเตอร์เพื่อก่ออาชญากรรมหรือจุดประสงค์ไม่ดี

มิติทางไซเบอร์ หมายถึง มิติที่มีการประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์ (Electronics) และหลักการด้านสเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ในการจัดเก็บแก้ไขหรือแลกเปลี่ยนข้อมูล ผ่านระบบเครือข่ายหรือโครงสร้างพื้นฐานทางกายภาพ (Physical Infrastructures)

ศูนย์ปฏิบัติการร่วมทางไซเบอร์

หมายถึง หน่วยงานที่มีหน้าที่ วางแผน อำนวยการ ประสานงาน กำกับดูแล และควบคุมการปฏิบัติด้านไซเบอร์ ให้กับหน่วยรอง ตั้งแต่ยามปกติและในสภาวะวิกฤต ตามที่ได้รับมอบหมาย และควบคุม อำนวยการ สั่งการต่อหน่วยงานไซเบอร์ของหน่วยรองที่จัดตั้งขึ้นตามแผนรับมือเหตุการณ์ด้านไซเบอร์ของหน่วยงาน หรือองค์กรขนาดใหญ่

บทที่ ๒
ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่อง แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The Guidance For Setting Up Thailand National Cybersecurity Operations Center – NCOC – In Order To Properly Solve The Critical Cybersecurity Situation At The National Level) ผู้วิจัยได้ศึกษาค้นคว้า วิเคราะห์ และสังเคราะห์ องค์ความรู้ จากเอกสาร แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องดังนี้

แนวคิดและทฤษฎีสำคัญที่เกี่ยวข้อง

๑. เทคโนโลยีสำคัญต่าง ๆ ที่เกี่ยวข้องในปัจจุบัน

๑.๑ เทคโนโลยีสารสนเทศ (Information Technology : IT)

ในปัจจุบันเทคโนโลยีสารสนเทศ มีบทบาทในการดำเนินชีวิตประจำวันของมนุษย์และการดำเนินกิจกรรมต่าง ๆ เนื่องจากความสามารถในการเข้าถึงแหล่งข้อมูล ในการส่งหรือสื่อสารข้อมูลได้เพิ่มขึ้นด้วยวิวัฒนาการ ด้านการสื่อสารโทรคมนาคม และคอมพิวเตอร์ ทำให้สามารถสื่อสารโต้ตอบและส่งข่าวสารในรูปแบบต่าง ๆ ทั้งที่เป็นแบบเนื้อหา ภาพ และเสียง ไปให้ผู้รับคนอื่นได้และสื่อสารโต้ตอบกันได้ทันเวลา

การพัฒนาเทคโนโลยี ในทศวรรษที่ ๒๐๒๐ จะเป็นช่วงของการเปลี่ยนแปลงเทคโนโลยีด้านต่าง ๆ โดยเป็นพื้นฐานที่จะนำไปสู่ยุคดิจิทัล จนได้รับการพัฒนาให้สามารถเข้าถึงประสาทสัมผัสของมนุษย์ได้ ซึ่ง Ericsson เรียกเทคโนโลยีนี้ว่า “อินเทอร์เน็ตของความรู้สึก” Internet of Senses โดยทิศทางของการพัฒนาเทคโนโลยีไปสู่อินเทอร์เน็ตของความรู้สึก ประกอบด้วย [๑]

๑.๑.๑ ลักษณะข้อมูลของทศวรรษหน้า

การพัฒนาเทคโนโลยีที่นำมาใช้ในการวิเคราะห์ข้อมูลให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งเรียกว่าเป็นยุค Analytics ๔.๐ โดยมีการนำ AI (Artificial Intelligence), Machine Learning และ Data Science มาใช้ในการวิเคราะห์ข้อมูล ในส่วนของการเก็บข้อมูลจะใช้ระบบคลาวด์ แบบกระจายศูนย์ (Distributed Cloud System) เพื่อให้รวบรวมข้อมูลได้มากขึ้น

---

[๑] สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช). “แนวโน้มเทคโนโลยีที่มีผลกระทบต่ออุตสาหกรรมสื่อสารของประเทศไทย”.

๑.๑.๒ การพัฒนาระบบเครือข่ายตามความต้องการของผู้ใช้

การสร้างแอพพลิเคชั่นใหม่ ๆ เกี่ยวกับการปกป้องข้อมูล การปรับปรุงโครงสร้างพื้นฐานและการเสริมสร้างขีดความสามารถให้ระบบงาน การพัฒนาเครือข่าย โดยนักพัฒนาเทคโนโลยีพยายามที่จะคิดค้นระบบเครือข่ายตามความต้องการของผู้ใช้ เช่น มีการนำระบบ AI และ Machine Learning มาใช้เพื่อสามารถคาดการณ์ดำเนินการ ตรวจหาและแก้ไขความผิดปกติได้โดยอัตโนมัติทำให้เครือข่ายมีประสิทธิภาพในการส่งข้อมูลได้มากขึ้น

๑.๑.๓ การประยุกต์ใช้เทคโนโลยีเป็นแบบ Hyper Automation

ระบบอัตโนมัติมีอิทธิพลเป็นอย่างมาก ต่อการเปลี่ยนแปลงอุตสาหกรรม การทำงานและการใช้ชีวิตประจำวัน มาตั้งแต่ศตวรรษที่ ๒๐ ในปัจจุบันมีการพัฒนาระบบอัตโนมัติมีทิศทางเป็นแบบ Hyper Automation คือผู้พัฒนาซอฟต์แวร์ จะนำเทคโนโลยีอื่น ๆ เช่น AI, Machine Learning เข้ามาใส่ในระบบอัตโนมัติ ทำให้การทำงานของอุปกรณ์และเครื่องจักรมีความเป็นอัตโนมัติทุกขั้นตอน

๑.๑.๔ การเพิ่มมาตรการรักษาความปลอดภัย

มาตรการรักษาความปลอดภัยดิจิทัลที่ใช้อยู่ในปัจจุบัน เช่น การตรวจจับการบุกรุกแบบเสมือน การยืนยันตัวตนด้วยฮาร์ดแวร์เพื่อตรวจสอบอัตลักษณ์ของผู้ใช้งาน อาจเป็นเครื่องมือที่เพียงพอสำหรับการใช้งานในปัจจุบัน แต่ในขณะเดียวกันผู้บุกรุกทางไซเบอร์ได้พยายามหาวิธีใหม่ ๆ ในการก่ออาชญากรรม จึงได้มีการพัฒนาระบบรักษาความปลอดภัยดิจิทัล โดยนำ AI และ Machine Learning มาใช้และมีการดำเนินการพัฒนาอย่างต่อเนื่อง

๑.๑.๕ เทคโนโลยีที่ใส่ใจสิ่งแวดล้อม

การพัฒนาเทคโนโลยีในทศวรรษนี้ ใส่ใจเรื่องสิ่งแวดล้อมมากยิ่งขึ้น โดยเทคโนโลยีต่าง ๆ เช่น AI, IoT (Internet of Things) จะถูกพัฒนาและนำมาประยุกต์ในอุปกรณ์ต่าง ๆ เพื่อช่วยตรวจจับหรือลดมลพิษมากยิ่งขึ้น

๑.๑.๖ การพัฒนาเทคโนโลยีเพื่อทดแทนแรงงานที่ขาดแคลน

จากการขาดแคลนแรงงานในหลายอาชีพทำให้ผู้พัฒนาเทคโนโลยีให้ความสนใจ และพยายามพัฒนาเทคโนโลยีให้สามารถทดแทนแรงงานในสายอาชีพเหล่านั้น

ในส่วนของแผนแม่บทเทคโนโลยีสารสนเทศ และการสื่อสารของประเทศไทย พ.ศ.๒๕๕๗ – ๒๕๖๑ (ฉบับที่ ๓) กล่าวว่า เทคโนโลยีสารสนเทศ และการสื่อสาร ถือเป็นเครื่องมือสำคัญที่ทำให้บุคคลสามารถนำมาประยุกต์ใช้สำหรับการดำรงชีวิต และการประกอบอาชีพได้ โดยในแผนแม่บทเทคโนโลยีสารสนเทศ และการสื่อสาร ของประเทศไทย พ.ศ. ๒๕๕๗-๒๕๖๑ (ฉบับที่ ๓) ที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดทำยุทธศาสตร์การพัฒนา ๔ ด้าน ประกอบด้วย [๒]

---

[๒] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. “แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ ๓) ของประเทศไทย พ.ศ.๒๕๕๗ - ๒๕๖๑”.

๑.๑.๖.๑ การพัฒนาทุนมนุษย์ให้เข้าถึงและรู้เท่าทัน ICT (Information and Communication Technology)

เพื่อการดำรงชีวิต และการประกอบอาชีพอย่างพอเพียง ด้วยแนวคิดสร้างสรรค์เชิงนวัตกรรม มีส่วนร่วมในการพัฒนาและใช้ประโยชน์จากบริการ ICT (Participatory People)

๑.๑.๖.๒ การพัฒนาโครงสร้างพื้นฐานที่คุ้มค่าและพอเพียง (Optimal Infrastructure)

มีแผนงานหลักอยู่ที่การพัฒนาโครงข่ายหลักระหว่างประเทศ การขยายจุดให้บริการและปรับปรุงคุณภาพ Free Wi-Fi ในที่สาธารณะโดยไม่คิดค่าบริการและจัดทำชุดเครื่องมือมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นพื้นฐาน (Standard Security Toolkit) สำหรับหน่วยงานภาครัฐ และเอกชน โดยเฉพาะอุตสาหกรรมขนาดกลาง และขนาดย่อมให้สามารถนำไปใช้ในการตรวจสอบและเสริมสร้างการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน

๑.๑.๖.๓ การยกระดับบริการทางอิเล็กทรอนิกส์ของภาครัฐ

โดยการมีส่วนร่วมของชุมชนและท้องถิ่นให้มีการรักษาความมั่นคงปลอดภัย โดยมีแผนงานหลัก คือ การประเมินระดับวุฒิภาวะ (Maturity) ของ e-Service ในด้านต่าง ๆ ทั้งในระดับประเทศ และหน่วยงานระดับกรมในทุกกระทรวง การจัดตั้งหรือปรับปรุงเว็บไซต์กลางของภาครัฐตามแนวทาง Open Government

๑.๑.๖.๔ การพัฒนาขีดความสามารถของธุรกิจ

ส่งเสริมให้มีการประยุกต์ใช้ ICT เพื่อให้มีศักยภาพในการแข่งขันในตลาดในระดับภูมิภาคและระดับสากล โดยมีแผนงานหลัก คือการจัดตั้ง One Stop Service ในการให้บริการข้อมูล ข่าวสารรวมทั้งการจดทะเบียน เพื่ออำนวยความสะดวกในการจัดตั้งและประกอบธุรกิจ ICT ในประเทศไทย (Facilitation Desk for ICT Business Start - up Program) รวมถึงการจัดตั้งกองทุน ICT เพื่อการพัฒนา ICT ในภาคธุรกิจและการส่งเสริมอุตสาหกรรม ICT

๑.๒ เทคโนโลยีเชิงปฏิบัติการ (Operational Technology : OT)

เทคโนโลยีเชิงปฏิบัติการ (Operational Technology : OT) คือ ฮาร์ดแวร์ และซอฟต์แวร์ที่ใช้ในระบบควบคุมอุตสาหกรรม เช่น SCADA ซึ่งจะทำหน้าที่เป็นรากฐานของโครงสร้างพื้นฐานหลักที่สำคัญต่าง ๆ รวมถึงอุตสาหกรรมที่จำเป็นต่อความปลอดภัยและคุณภาพชีวิตที่ดีของประชาชน ได้แก่ โรงไฟฟ้า โรงงานผลิต ระบบสาธารณูปโภค การประปา ด้านสาธารณสุข การคมนาคมขนส่ง และอื่น ๆ [๓]

---

[๓] FORTINET. “What Is Operational Technology (OT)? Retrieved by 10 September 2020.” (Online). Available : https://www.fortinet.com/solutions/industries/scada-industrial-control- systems/what-is-ot-security, 2014.

เทคโนโลยีปฏิบัติการ (OT) ประกอบด้วย ระบบควบคุมอุตสาหกรรม (ICS : Industrial Control System) ซึ่งเป็นองค์ประกอบหลัก ได้แก่ อุปกรณ์ระบบการควบคุมและเครือข่ายประเภทต่าง ๆ ที่จัดการกระบวนการทางอุตสาหกรรมที่หลากหลาย สิ่งที่พบบ่อยที่สุด คือ ระบบควบคุมกำกับดูแลและระบบเก็บข้อมูล (SCADA : Supervisory Control and Data Acquisition) และระบบควบคุมแบบกระจาย (DCS : Decentralized Control System) โดย SCADA เป็นระบบรวบรวมข้อมูลจากเซ็นเซอร์ซึ่งมักจะอยู่ที่ไซต์แบบกระจายและส่งไปยังคอมพิวเตอร์ส่วนกลางที่จัดการและควบคุมข้อมูลส่วน DCS ใช้เพื่อจัดการตัวควบคุมภายในหรืออุปกรณ์ของระบบการผลิตในที่เดียว

โดยระบบเทคโนโลยีปฏิบัติการ (OT) จะแตกต่างจากระบบไอทีแบบดั้งเดิม เพราะระบบเทคโนโลยีปฏิบัติการ (OT) จะรวมกระบวนการและระบบต่าง ๆ เข้าด้วยกันเพื่อออกแบบมาเป็นระบบที่ใช้ในการพัฒนาทรัพยากรและระบบบริหารการผลิตที่มีประสิทธิภาพมีส่วนประกอบต่าง ๆ รวมถึงเครื่องยนต์นานาประเภท วาล์ว เซ็นเซอร์และหุ่นยนต์ซึ่งเป็นองค์ประกอบที่จำเป็นในโครงสร้างพื้นฐานสำคัญดังกล่าวซึ่งอาจจะไม่พบในระบบไอทีประเภทดั้งเดิม

ในส่วนของระบบความปลอดภัยของเทคโนโลยีเชิงปฏิบัติการ (OT) โดย Gartner ได้ให้คำจำกัดความของระบบความปลอดภัยของเทคโนโลยีเชิงปฏิบัติการ หมายถึง แนวทางปฏิบัติและเทคโนโลยีที่ใช้เพื่อ ปกป้องบุคคล ทรัพย์สิน และข้อมูล, ตรวจสอบและ/หรือควบคุมอุปกรณ์ทางกายภาพ กระบวนการและเหตุการณ์ต่าง ๆ และเริ่มการเปลี่ยนแปลงของรัฐในระบบ OT ขององค์กร” โซลูชั่นการรักษาความปลอดภัย OT ประกอบด้วยเทคโนโลยีด้านความปลอดภัยที่หลากหลายตั้งแต่ ไฟร์วอลล์รุ่นใหม่ (NGFW : Next Generation Firewall) ไปจนถึงระบบข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (SIEM : Security Information and Event Management) ไปจนถึงการเข้าถึงและการจัดการข้อมูลประจำตัวและอื่น ๆ อีกมากมาย [๔]

๑.๓ Internet of Things หรือ IoT

เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things - IoT) นับเป็นเทคโนโลยีที่จะนำมาซึ่งความสะดวกสบายในชีวิตประจำวัน และทำให้ประชาชนมีคุณภาพชีวิตที่ดีขึ้น นอกจากนี้ยังเป็นเทคโนโลยีที่สร้างความได้เปรียบทางธุรกิจเนื่องจาก สามารถจัดเก็บและรวบรวมข้อมูลที่นำมาใช้ประโยชน์ได้อย่างมหาศาล โดย Garther ได้ทำการวิเคราะห์เกี่ยวกับกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศในปี ๒๕๕๘ พบว่าหนึ่งในแนวโน้มของวิวัฒนาการของเทคโนโลยีที่จะเข้ามามีบทบาทเกี่ยวกับการดำเนินชีวิตของมนุษย์ ได้แก่ เทคโนโลยีภายใต้แนวความคิดที่ เรียกว่า internet of Things :

---

[๔] Earl Perkins. (๒๐๑๔). “Operational Technology Security – Focus on Securing Industrial Control and Automation Systems.” (Online). Available : https://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security- focus-on-securing-industrial-control-and-automation-systems/, 2014.

IoT เป็นแนวทางที่เกิดจากการรวมกันของข้อมูล การบริการที่สร้างบนรากฐานของทุกอย่างที่เชื่อมต่อกันด้วยระบบดิจิทัล [๕]

๑.๓.๑ ความหมายและความสำคัญของ Internet of Things

Internet of Things คือ “อินเทอร์เน็ตของทุกสิ่ง” ซึ่ง “ทุกสิ่ง” หรือ “Thing” หมายถึงวัตถุ สิ่งของ เครื่องใช้ต่าง ๆ ที่ไม่ใช่อุปกรณ์สื่อสาร คอมพิวเตอร์ แท็บเล็ต สมาร์ทโฟน หรือโน้ตบุ๊ก เท่านั้นที่สามารถเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตได้ แต่ยังหมายถึง วัตถุ เครื่องมือ เครื่องใช้ในชีวิตประจำวัน เช่น ตู้เย็น โทรทัศน์ รถยนต์ นาฬิกาข้อมือ สามารถเชื่อมต่อกับระบบอินเทอร์เน็ตได้ ซึ่งการเชื่อมต่อทำให้เกิดการติดต่อสื่อสารกันโดยอัตโนมัติ และเกิดขึ้นได้ตลอดเวลา ส่งผลทำให้เกิดข้อมูลมหาศาลทำให้เราสามารถนำข้อมูลเหล่านี้มาใช้ประโยชน์ได้อีกมากมาย [๖]

เทคโนโลยี Internet of Things หรือ IoT คือ กรอบแนวคิดของระบบโครงข่ายที่รองรับการเชื่อมต่อกับอุปกรณ์หลากหลายชนิด ทั้งคอมพิวเตอร์ โทรศัพท์เคลื่อนที่ อุปกรณ์โครงข่าย อุปกรณ์อิเล็กทรอนิกส์ เซนเซอร์ และวัตถุต่าง ๆ เข้าด้วยกัน ส่งผลให้ระบบต่าง ๆ สามารถติดต่อสื่อสารและทำงานร่วมกันได้อย่างเป็นอัตโนมัติอีกทั้งยังส่งผลให้มนุษย์สามารถเข้าถึงข้อมูลได้หลากหลายมากยิ่งขึ้น การควบคุมอุปกรณ์และระบบต่าง ๆ มี ประสิทธิภาพมากขึ้น

๑.๓.๒ รูปแบบการเชื่อมต่ออุปกรณ์ IoT เข้ากับโครงข่าย Internet

IoT เป็นผลสืบเนื่องของการพัฒนาระบบอินเทอร์เน็ต ซึ่งมีวัตถุประสงค์เพื่อการสร้างโครงข่ายเพื่อเชื่อมโยงอุปกรณ์ที่มีมาตรฐานแตกต่างกันให้สามารถสื่อสารกันได้ โดย IoT จะเปิดโอกาสให้มีการเชื่อมต่อในรูปแบบที่หลากหลายมากยิ่งขึ้น และรองรับอุปกรณ์ที่พัฒนาโดยผู้ผลิตที่มีเทคโนโลยีแตกต่างกันมากกว่าเดิม ซึ่งรูปแบบการเชื่อมต่ออุปกรณ์ต่าง ๆ เข้ากับโครงข่ายอินเทอร์เน็ต มีดังนี้[๗]

๑.๓.๒.๑ การเชื่อมต่อผ่านอุปกรณ์สื่อสารระยะสั้น (Short - Range Devices)

ซึ่งเป็นรูปแบบการเชื่อมต่ออุปกรณ์ในระยะสั้นมากและใช้กำลังส่งต่ำมาก ส่วนใหญ่เหมาะสำหรับการสื่อสารในพื้นที่ครอบคลุมขนาดเล็กซึ่งอยู่ในลักษณะการเชื่อมต่อระหว่างอุปกรณ์ (Peer - to - Peer)

---

[๕] Andrew Spender. “Gartner’s Top 10 Strategic Technology Trends for 2558.” (Online). Available : https://ph01.tci-thaijo.org/index.php/JIE/article/view/137017, 2558

[๖] วอนชนก ไชยสุนทร. “Internet of Things เมื่อทุกสิ่งเชื่อมต่ออินเทอร์เน็ต. วารสารคุรุศาสตร์อุตสาหกรรม.” (Online). เข้าถึงได้จาก : https://ph01.tci-thaijo.org/index.php/JIE/article/view/137017, 2558

[๗] สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ. “เทคโนโลยี Internet of Things และนโยบาย Thailand ๔.๐.” ๒๕๖๐.

๑.๓.๒.๒ การเชื่อมต่อผ่านโครงข่ายโทรศัพท์เคลื่อนที่

ซึ่งเป็นรูปแบบการให้บริการที่มีพื้นที่ครอบคลุมกว้างโดยอาศัยการเชื่อมต่ออุปกรณ์เครื่อง ลูกข่าย IoT เข้ากับโครงสร้างพื้นฐานของระบบโทรศัพท์เคลื่อนที่ที่มีอยู่แล้ว

๑.๓.๒.๓ การเชื่อมต่อผ่านโครงข่าย LPWAN (Low Power Wide Area Network)

เป็นรูปแบบการเชื่อมต่อผ่านโครงข่ายกำลังส่งต่ำบริเวณกว้าง LPWAN โดยเน้นใช้งานในลักษณะการสื่อสารแบบ Narrow Band หรือ Ultra Narrow Band ที่มีอัตราการส่งข้อมูลต่ำมาก ประหยัดพลังงานมาก และมีราคาอุปกรณ์ต่อหน่วยที่ต่ำ

๑.๓.๒.๔ การเชื่อมต่อผ่านเครือข่ายสื่อสารดาวเทียม

ซึ่งเหมาะสมกับการใช้งานที่มีพื้นที่ครอบคลุมการให้บริการที่กว้างมาก แต่การเชื่อมต่อดังกล่าวจะมีระยะเวลาการตอบสนอง (Latency) ที่ช้ากว่าการเชื่อมต่อรูปแบบอื่น ๆ เนื่องจากระยะเวลาที่สัญญาณเดินทาง ไป - กลับ ระหว่างอุปกรณ์สื่อสารภาคพื้นโลก

๑.๓.๓ การประยุกต์ใช้ Internet of Things หรือ IoT

ในปัจจุบันมีการนำ Internet of Things หรือ IoT มาประยุกต์ใช้กับงานด้านต่าง ๆ ดังนี้

๑.๓.๓.๑ การเกษตรแม่นยำ (Precision Farming)

เป็นระบบที่มีการทำงานร่วมกันของระบบเซ็นเซอร์ที่วัดความชื้น ปริมาณแสงแดด อุณหภูมิ ระบบฐานข้อมูลพืชและระบบให้น้ำ ปรับปริมาณแสง และระบบปรับอุณหภูมิที่ทำงานสอดคล้องกัน เพื่อสร้างสภาวะแวดล้อมที่เหมาะสมต่อการเจริญเติบโตของพืชมากที่สุด และแม่นยำที่สุด

๑.๓.๓.๒ อินเทอร์เน็ตอุตสาหกรรม (Industrial Internet)

เป็นโครงข่ายข้อมูลขนาดใหญ่ที่เชื่อมต่ออุปกรณ์ต่าง เช่น เครื่องจักร เครื่องวัดและระบบการควบคุมในระบบอุตสาหกรรมเข้าด้วยกัน โดยการส่งข้อมูลผ่านโครงข่ายจะช่วยให้อุปกรณ์และระบบต่าง ๆ มีการทำงานที่แม่นยำมากยิ่งขึ้น สามารถทำงานสอดคล้องกันได้โดยไม่ต้องการเก็บข้อมูลเกี่ยวกับสภาพของเครื่องจักร เช่น อุณหภูมิ การสั่น การหมุน

๑.๓.๓.๓ ระบบคมนาคมและการจัดการโลจิสติกส์โครงข่าย IOT

มีบทบาทในการพัฒนาระบบคมนาคมและการจัดการโลจิสติกส์ โดยจะช่วยสนับสนุนให้มีการเชื่อมต่อข้อมูลระหว่างยานพาหนะด้วยกันหรือ ระหว่างยานพาหนะและระบบควบคุมการจราจรอื่น ตัวอย่างเช่น การจราจร ระบบสัญญาณ ระบบข้อมูลสภาพจราจร หรือการนำเอาระบบดังกล่าวมาใช้กับระบบขนส่งมวลชนที่จะช่วยให้การบริการมีความปลอดภัย สะดวก และตรงเวลามากยิ่งขึ้น ทำให้การจัดการสินค้าคงคลังมีประสิทธิภาพมากยิ่งขึ้น

๑.๓.๓.๔ ระบบการจัดการพลังงาน และสาธารณูปโภค (Utility Management)

มีการนำระบบ IoT มาประยุกต์ใช้เกี่ยวกับการตรวจวัดระยะไกล (Telemetry) เช่น ระบบ Smart Meter ซึ่งมีความสามารถในการวัดปริมาณการใช้สาธารณูปโภค หรือวัดคุณภาพสาธารณูปโภค ก่อนจะส่งข้อมูลดังกล่าวไปยังหน่วยประมวลผลกลางเพื่อใช้ในการวิเคราะห์ในภาพรวมต่อไป

๑.๓.๓.๕ ระบบสาธารณสุขอัจฉริยะ (Smart Health)

ใช้อุปกรณ์ IoT เป็นที่เก็บข้อมูลทางด้านสุขภาพ และสัญญาณทางร่างกาย (Bio Signals) เช่น สัญญาณชีพจร ความดันโลหิต คุณภาพการนอน การเคลื่อนที่การหายใจ ผ่านการใช้อุปกรณ์สวมใส่ (Wearable Devices) เพื่อรวบรวมและประมวลผลออกมาเป็นข้อมูลสุขภาพและอาการเจ็บป่วย ซึ่งสามารถเก็บข้อมูลการเจ็บป่วยที่มีประโยชน์ต่อการวินิจฉัยก่อนที่คนไข้มาถึงการดูแลของแพทย์ การคาดการณ์และการวินิจฉัยการเจ็บป่วยล่วงหน้า (Predictive Diagnostic) และมีการแจ้งเตือนการเจ็บป่วยทันที

๑.๓.๓.๖ ระบบเทคโนโลยีการเงิน (Fintech)

เทคโนโลยี Internet of Things (IoT) มีบทบาทสนับสนุนเทคโนโลยีทางการเงินได้หลายรูปแบบ เช่น ระบบการจ่ายเงินอัตโนมัติ (Auto - Payment) ในร้านค้าปลีก ระบบการจ่ายเงินโดยผ่านอุปกรณ์สวมใส่ (Wearable Devices) และโทรศัพท์เคลื่อนที่และทำงานร่วมกับอุปกรณ์อื่น ๆ เช่น ในโรงงานอุตสาหกรรม สำหรับการสั่งซื้อ และจ่ายเงินวัสดุอุปกรณ์และวัตถุดิบอย่างอัตโนมัติ

๑.๓.๔ ข้อควรตระหนักของ Internet of Things

เทคโนโลยีที่มีคุณประโยชน์มากมายและช่วยอำนวยความสะดวกสบายในชีวิตประจำวันแก่ผู้ใช้มากมาย แต่การจะใช้งาน IoT ได้อย่างมีประสิทธิภาพนั้นประเทศไทยจะต้องเร่งจัดสรรคลื่นความถี่ให้เพียงพอกับการใช้งานในอนาคตอันใกล้ เพื่อรองรับปริมาณการสื่อสารขนาดมหาศาลและหนาแน่นในทุกพื้นที่ นอกจากนี้ควรเตรียมการรับมือภัยคุกคามจากการโจมตีทางไซเบอร์ นอกจากนี้ผู้ใช้งานและผู้พัฒนาเทคโนโลยี ควรตระหนักและร่วมมือกันพัฒนา Internet of Things เกี่ยวกับประเด็นต่าง ๆ ในแต่ละด้าน โดยมีด้านความปลอดภัยอุปกรณ์ ด้านข้อมูลส่วนบุคคลของข้อมูล ด้านเทคโนโลยีการสื่อสารโทรคมนาคม และด้านมาตรฐานและวิวัฒนาการทางด้านเทคโนโลยี

๒. ภัยคุกคามทางไซเบอร์

๒.๑ ภัยคุกคามทางไซเบอร์ซึ่งเป็นที่รู้จักกันโดยทั่วไป (Known Threats)

ภัยคุกคามที่เกิดขึ้นกับข้อมูลหรือสารสนเทศ หรือการใช้ทรัพยากรของระบบเช่น การแอบลักลอบใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตการขัดขวางไม่ให้คอมพิวเตอร์ทำงานได้ตามปกติ การปรับเปลี่ยนข้อมูลหรือสารสนเทศโดยไม่ได้รับอนุญาตเป็นต้น เช่น ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยได้รับอนุญาต โดยภัยคุกคามที่เป็นที่รู้จัก

โดย Known Threats ได้แก่[๘] Viruses, Worms, Trojans, Spyware, Spam, Hoax, Phishing, Rootkits, Cryptors, Miners, Etc.

๒.๑.๑ ไวรัส (Viruses)

โค้ดหรือโปรแกรมคอมพิวเตอร์ที่มุ่งร้ายต่อโปรแกรม/ไฟล์อื่น ๆ โดยจะฝังหรือสำเนาตัวเองไปกับโปรแกรมไฟล์ข้อมูลที่เป็นเป้าหมาย เมื่อโปรแกรม/ไฟล์นั้นถูกรัน โค้ดไวรัสจะเริ่มทำงานตามคำสั่งที่บรรจุอยู่ในโค้ด[๙] เช่น สั่งให้ลบไฟล์หรือแก้ไขค่าบางอย่างของไฟล์ หรือให้แสดงจอภาพเป็นสีฟ้า เป็นต้น

๒.๑.๒ เวิร์ม (Worms)

เวิร์ม เป็นโปรแกรมมุ่งร้ายที่สามารถสำเนาหรือทำซ้ำตัวเองไปยังคอมพิวเตอร์เครื่องอื่นได้โดยไม่ต้องอาศัยพาหนะแต่อาศัยการเดินทางผ่านเครือข่าย ซึ่งเข้ามาตามช่องโหว่ของระบบปฏิบัติการ ไฟล์ข้อมูล หรือ อีเมล์ ต่าง ๆ โดยจะเน้นการโจมตีระบบเครือข่ายมากกว่าการสร้างความเสียหายให้กับไฟล์

๒.๑.๓ ม้าโทรจัน (Trojans Horse)

ม้าโทรจัน เป็นโปรแกรมที่ไม่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นได้ แต่ใช้วิธีการแฝงตัวอยู่ในลักษณะของไฟล์หรือโปรแกรม เพื่อหลอกล่อให้ผู้ใช้เปิดไฟล์หรือดาวน์โหลดมาใช้งาน จากนั้นโทรจันจะทำงานที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์ นอกจากนี้โทรจันจะติดตั้ง Bot ลงในเครื่องเพื่อเปิดช่องโหว่ของระบบปฏิบัติการให้ผู้บุกรุกเข้ามาควบคุมการทำงานของเครื่อง

๒.๑.๔ สปายแวร์ (Spyware)

สปายแวร์ เป็นโปรแกรมที่ไม่สามารถสำเนาตัวเองไปยังระบบเครือข่ายได้ แต่ใช้วิธีการแฝงตัวในรูปแบบต่าง ๆ เพื่อหลอกลวงให้ผู้ใช้ดาวน์โหลดไปติดตั้งเช่นเดียวกับโทรจัน หรืออาศัยช่องโหว่ของเว็บบราวเซอร์เพื่อลักลอบเข้ามาติดตั้งตัวเองลงในเครื่องคอมพิวเตอร์ สปายแวร์จะเข้าไปเปลี่ยนแปลงค่าต่าง ๆ ของเว็บบราวเซอร์โดยการติดตั้งหน้าต่างโฆษณาสินค้า หรือทำให้เครื่องทำงานได้ช้าลง

๒.๑.๕ Spam

Spam เป็นการใช้อีเมล์เพื่อการโฆษณาหรือประชาสัมพันธ์สินค้าและบริการต่าง ๆ ซึ่งอาจสร้างความรำคาญให้แก่ผู้ใช้ได้ ซึ่งบางครั้งอาจแนบไวรัสและเวิร์มมากับอีเมล์ด้วย ดังนั้นไม่ควรเปิดอ่านอีเมล์ถ้าไม่ทราบแหล่งที่มาที่ชัดเจนของอีเมล์

---

[๘] Kaspersky. “Types of known threats.” (Online). Available : https://support.kaspersky.com/614#block10, 2019.

[๙] พนิดา พาณิชกุล. “จริยธรรมทางเทคโนโลยีสารสนเทศ.” (กรุงเทพมหานคร : เค ที พี คอมพ์ แอนด์ คอนซัล, 2019). หน้า 45 – 47.

๒.๑.๖ Hoax

Hoax เป็นการสร้างความสับสนให้กับผู้ใช้ด้วยข่าวไวรัสหลอกลวงที่ถูกส่งต่อ ๆ กันมาในรูปของอีเมล์

๒.๑.๗ Phishing

การหลอกลวงรูปแบบหนึ่งผ่านการส่งอีเมล์ โดยหลักการของ Phishing คือใช้การส่งอีเมล์ไปหาบุคคลเป้าหมาย ซึ่งเนื้อหาของอีเมล์จะเป็นการหลอกลวงในสิ่งที่เป้าหมายมีความคุ้นเคย เช่น หลอกเอาข้อมูลล็อกอินและรหัสผ่านเข้าสู่ระบบบัตรเครดิต หรืออินเทอร์เน็ตแบงค์กิ้ง หรือ PayPal หรือ Facebook

๒.๑.๘ Rootkits

โปรแกรมซ่อนอยู่ภายในเครื่องคอมพิวเตอร์ โดยถูกออกแบบมาให้ฝังตัวในระบบคอมพิวเตอร์ที่สามารถเปิดให้ผู้บุกรุกเข้ามาควบคุมคอมพิวเตอร์เราได้

๒.๑.๙ ภัยคุกคามในลักษณะอื่น ๆ อีกมากมาย ซึ่งอาจจะใช้หลักการของ Mitre ATT & CK Framework ซึ่งเป็นองค์ความรู้และวิธีการที่จะสามารถใช้ในการทำความเข้าใจเทคนิคการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ ของแฮกเกอร์หรือผู้ไม่หวังดี

๒.๒ ภัยคุกคามทางไซเบอร์ที่ยังไม่เป็นที่รู้จัก (Unknown Threats) หรือ Advanced Persistent Threat (APT)

ภัยคุกคามที่ยังไม่เป็นที่รู้จัก ถือเป็นภัยคุกคามประเภท Malicious Code ที่เป็นอันตรายซึ่งระบบ Anti - Virus ไม่สามารถตรวจจับได้ โดยภัยคุกคามดังกล่าวใช้ช่องโหว่ในการโจมตีถือเป็นภัยคุกคามต่อเนื่องขั้นสูง หรือ เป็นการโจมตีแบบกำหนดเป้าหมายซึ่งออกแบบมาโดยมีจุดประสงค์ เพื่อเจาะแนวป้องกันของเหยื่อ เป็นการโจมตีที่ไม่สามารถป้องกันได้ เพราะเป็นการโจมตีที่ไม่เคยพบเห็นมาก่อน วิธีป้องกันที่ดีที่สุดคงเป็น User Behavior Analytics หรือ Machine Learning ที่เรียนรู้พฤติกรรมของการใช้งาน ถ้าพบเห็นสิ่งที่ผิดปกติให้ทำการแจ้งเตือนหรือกักกันสิ่งเหล่านั้นออกจากระบบ [๑๐]

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) กล่าวว่า APT หรือ Advanced Persistent Threat ถือเป็นประเภทหนึ่งของอาชญากรรมทางคอมพิวเตอร์ โดยมีเป้าหมายเพื่อโจมตีหน่วยงานต่าง ๆ ที่มีข้อมูลสำคัญ ซึ่งเป็นการโจมตีระบบเครือข่ายรูปแบบหนึ่งที่แฮกเกอร์ จะเลือกเป้าหมายเพียงรายเดียว เช่น หน่วยงานทางทหารหรือหน่วยงานทางด้านการรักษาความมั่นคงปลอดภัยของประเทศ หน่วยงานทางการเมือง หรือองค์กรธุรกิจขนาดใหญ่ ซึ่งรูปแบบการโจมตีแบบ APT ส่วนใหญ่ผู้ดำเนินการมักจะเป็นกลุ่มบุคคลมากกว่าเป็นการดำเนินการของบุคคลใดบุคคลหนึ่ง

---

[๑๐] Techtalkthai. “Tag Archives: unknown threats.” (Online). Available : https://www.techtalkthai.com/ tag/unknown-threats/, 2559.

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้สรุปความหมายของ APT ไว้ดังนี้ [๑๑]

Advanced : ผู้ที่โจมตี เป็นบุคคลที่มีความสามารถ และมีทรัพยากรที่พร้อมสำหรับการโจมตี โดยวิธีการโจมตีจะใช้เครื่องมือและเทคนิคหลายอย่างด้วยกัน เริ่มตั้งแต่การใช้ความรู้ทางคอมพิวเตอร์ขั้นสูงเพื่อเจาะระบบ ไปจนถึงการใช้เทคนิคพื้นฐาน เช่น Social Engineering ซึ่งเป็นการโจมตีโดยอาศัยหลักจิตวิทยาเพื่อหลอกลวงคนให้เปิดเผยข้อมูลสำคัญ

Persistent : การโจมตีแบบค่อยเป็นค่อยไปและสม่ำเสมอ เนื่องจากผู้โจมตีต้องแฝงเข้าไปอยู่ในระบบโดยไม่ให้เป้าหมายรู้ตัว เพื่อสร้างความเสียหายหรือรวบรวมข้อมูลที่ต้องการให้ได้มากที่สุด

Threat : จัดเป็นภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารเทคนิคการป้องกัน APT

๒.๓ แนวคิดด้านภัยคุกคามที่เกี่ยวข้องกับความมั่นคงแห่งชาติ

การที่ประเทศชาติจะมีความมั่นคงและปลอดภัยจากอันตรายทั้งปวงได้นั้น จะต้องปราศจากสิ่งที่เรียกว่า ภัยคุกคาม (Threats) โดยภัยคุกคามคือการกระทำที่เป็นอันตรายหรือสั่นคลอนต่อความมั่นคงของชาติในทุก ๆ ด้าน ทั้งภัยคุกคามที่เกิดจากภายในและภายนอกตลอดจนภัยคุกคามทางไซเบอร์ ซึ่งในปัจจุบันภัยคุกคามมีการพัฒนารูปแบบใหม่ ๆ ต่างจากอดีตเป็นอย่างมาก ไม่ว่าจะเป็น Advanced Persistent Threats, Advanced Targeted Attacks, Advanced Malware, Unknown Malware หรือ Zero - Day Attack ทำให้องค์กรส่วนใหญ่เริ่มรับมือกับภัยคุกคามเหล่านี้ได้ยากขึ้นเรื่อย ๆ ถึงแม้ว่าแต่ละองค์กรจะมีอุปกรณ์สำหรับป้องกันภัยคุกคามหลากหลายประเภท ไม่ว่าจะเป็น Firewall, IPS, Anti - virus และอื่น ๆ แต่เมื่ออุปกรณ์เหล่านั้นต้องมาเจอกับภัยคุกคามรูปแบบใหม่ ๆ การที่ต่างฝ่ายต่างทำงาน ไม่มีการแชร์ข้อมูลระหว่างกันทำให้เป็นเรื่องยากที่จะระบุและตรวจจับภัยคุกคามขั้นสูงเหล่านั้นได้อย่างถูกต้องและแม่นยำ โดยประเภทของภัยคุกคามทางไซเบอร์สามารถจำแนกตามข้อมูลเชิงสถิติเกี่ยวกับเหตุภัยคุกคามที่ ไทยเซิร์ต ได้รับแจ้งเป็น ๙ ประเภท ตามที่ได้กำหนดโดย The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่าย ความร่วมมือของหน่วยงาน CSIRT โดย eCSIRT [๑๒]

๒.๓.๑ เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) คือ ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เช่น ลามก อนาจาร หมิ่นประมาท

---

[๑๑] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “ความหมาย APT.” (Online). Available : https://www.thaicert.or.th/papers/technical/ 2011 /pa2011te002.html, ๒๕๕๔.

[๑๒] ThaiCERT. “สถิติภัยคุกคาม.” (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2015.html.

๒.๓.๒ โปรแกรมไม่พึงประสงค์ (Malicious Code) คือ ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เช่น Virus, Worm, Trojan หรือ Spyware ต่าง ๆ

๒.๓.๓ การรวบรวมข้อมูลของระบบ (Information Gathering) คือภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน

๒.๓.๔ การบุกรุกเข้าระบบ (Intrusion Attempts) คือภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ

๒.๓.๕ การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) คือ ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

๒.๓.๖ การโจมตี สภาพความพร้อมการใช้งานของระบบ (Availability) คือภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบเพื่อทำให้บริการต่าง ๆ ของระบบทำให้ไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่าง ๆ

๒.๓.๗ การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) คือภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

๒.๓.๘ การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) คือภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) ซึ่งเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง

๒.๓.๙ ภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) ภัยคุกคามประเภทอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น

๓. หลักพื้นฐานการรักษาความปลอดภัยทางไซเบอร์

เทคโนโลยีสารสนเทศและอินเทอร์เน็ตสร้างคุณประโยชน์ต่อมนุษย์มากมายมหาศาล ทั้งในส่วนของภาคธุรกิจ รัฐบาล สถาบันการศึกษา หรือแม้กระทั่งบุคคลทั่วไป โดยเทคโนโลยีสารสนเทศช่วยให้ผู้ใช้คอมพิวเตอร์สามารถจัดเก็บข้อมูลและประมวลผลเป็นสารสนเทศที่ต้องการในเวลาอันรวดเร็ว ส่วนเทคโนโลยีอินเทอร์เน็ตช่วยให้ผู้ใช้ทั่วโลกเชื่อมโยงถึงกันได้ โดยองค์กรธุรกิจในปัจจุบันได้ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศมากยิ่งขึ้น เนื่องจากอาชญากรรมคอมพิวเตอร์มีจำนวนเพิ่มมากขึ้นตลอดจนรูปแบบการก่ออาชญากรรมหรือรูปแบบ

การโจมตีมีมากขึ้นด้วย องค์กรจึงตระหนักถึงความเสี่ยงต่อการถูกโจมตีที่อาจเกิดขึ้นได้จึงได้หามาตรการป้องกันและรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและไซเบอร์ไว้ เพื่อให้ส่งผลกระทบต่อความเสียหายขององค์กรน้อยที่สุด

๓.๑ หลักพื้นฐานการรักษาความปลอดภัยทางไซเบอร์ ตามหลักการ CIA

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) [๑๓] คือกระบวนการตลอดจนการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ๓ ประการ ได้แก่ [๑๔]

๓.๑.๑ การรักษาความลับของข้อมูล (Confidentiality)

เป็นการป้องกันข้อมูล โดยไม่ให้ผู้ไม่มีสิทธิ์ได้มีโอกาสเข้าไปดำเนินการใด ๆ กับข้อมูล ให้บุคคลผู้มีสิทธิเท่านั้นเข้าถึงเรียกดูข้อมูลได้ ต้องมีการควบคุมการเข้าถึงข้อมูลเป็นความลับ ต้องไม่เปิดเผยกับผู้ไม่มีสิทธิ์ กลไกและวิธีในการรักษาความลับของข้อมูลวิธีหนึ่งที่ถูกนำมาใช้อย่างแพร่หลาย คือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการดำเนินการให้ข้อมูลถูกเปลี่ยนไปอยู่ในรูปแบบที่ไม่สามารถอ่านออกหรือเข้าใจได้โดยบุคคลทั่วไป และการจะอ่านหรือนำข้อมูลเหล่านี้ไปใช้ได้นั้น จะต้องดำเนินการถอดรหัส (Decryption) โดยใช้กุญแจ (Key) หรือรหัสผ่าน (Password) ที่ใช้สำหรับการเข้ารหัส เพื่อทำการถอดรหัสข้อมูลก่อนได้ โดยหากปราศจากกุญแจ หรือเกิดการสูญหายเจ้าของข้อมูลก็อาจจะไม่สามารถใช้ข้อมูลนี้ได้อีกต่อไป

๓.๑.๒ การรักษาความคงสภาพของข้อมูล (Integrity)

ความสมบูรณ์ของข้อมูลคือ ความครบถ้วน มั่นคง ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน กลไกและวิธี ในด้านการรักษาความสมบูรณ์ของข้อมูล ประกอบด้วย ๒ ส่วนคือ

๓.๑.๒.๑ การป้องกัน (Prevention)

การนำมาตรการเกี่ยวกับ การรักษาความปลอดภัยมาใช้ก่อนที่จะมีปัญหาเกิดขึ้น โดยมีวัตถุประสงค์เพื่อการคงสภาพของข้อมูลไว้ให้ดีที่สุด ได้แก่ การพิสูจน์ตัวตน (Authentication) ซึ่งเป็นการกำหนดให้ผู้ที่จะเข้าถึงข้อมูลจะต้องทำการพิสูจน์ตัวตนก่อนว่าเป็นบุคคลที่ได้รับอนุญาตให้เข้าถึงข้อมูลจริง เช่น การกำหนดให้ใช้บัญชีรายชื่อผู้ใช้ (Username หรือ

---

[๑๓] ศิวลีย์ สิริโรจน์บริรักษ์. “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม.” วารสาร สถาบันวิชาการป้องกันประเทศ. ปีที่ ๖(๓),. หน้า 19 – 29.

[๑๔] สฤษดิ์พงษ์ ลิมปิษเฐียร. “ความมั่นคงปลอดภัยด้านสารสนเทศของนักศึกษา.” ประกาศนียบัตรบัณฑิตทางการบริหารการศึกษา, มหาวิทยาลัยสุโขทัยธรรมาธิราช”. ปี ๒๕๕๘.

User Identification หรือ User ID) และรหัสผ่าน (Password) ซึ่งหากผู้ใช้แจ้งรายชื่อผู้ใช้และรหัสผ่านของตนได้ถูกต้อง ระบบจะถือว่า เป็นบุคคลผู้ได้รับสิทธิ์ในการใช้งานได้จริง และจะอนุญาตให้ผู้นั้นสามารถเข้าดำเนินการต่าง ๆ ตามสิทธิ์ที่ได้รับ หรืออีกวิธีหนึ่ง คือ การควบคุมการเข้าถึง (Access Control) ซึ่งเป็นการกำหนดสิทธิ์ในการเข้าถึงและทำงานกับข้อมูล โดยผู้ใช้บางคนอาจไม่มีสิทธิ์ในการเข้าถึงข้อมูลสำคัญขององค์การเลยก็ได้ (No Access) ส่วนผู้ใช้บางคนอาจมีสิทธิ์เพียงการได้เห็นหรืออ่านข้อมูลได้ (Browse) แต่ไม่สามารถดำเนินการอย่างอื่นได้ ในขณะที่บางคนอาจได้รับสิทธิ์จนถึงขั้นสามารถเข้าไปเพิ่มเติม (Insert) แก้ไข (Edit) และปรับเปลี่ยน (Update) ข้อมูลได้

๓.๑.๒.๒ การตรวจจับ (Detection)

การนำมาตรการการรักษาความปลอดภัยมาใช้ เพื่อรักษาความถูกต้องและน่าเชื่อถือของข้อมูล ได้แก่ การตรวจวิเคราะห์เพื่อดูว่า ข้อมูลยังคงสภาพเดิมตามคุณสมบัติที่สำคัญหรือที่คาดหวังไว้อยู่หรือไม่ โดยกลไกดังกล่าวนี้อาจรายงานด้วยว่า ส่วนไหนของข้อมูลหรือแฟ้มข้อมูลมีการแก้ไขไปแล้วบ้าง นอกจากนี้ อาจมีกลไกเพื่อตรวจสอบดูว่า มีความผิดปกติหรือความไม่ถูกต้องปะปนอยู่ในตัวข้อมูลหรือไม่ เช่น ข้อมูลเลขประจำตัวประชาชนของคนไทย จะต้องมีลักษณะเป็นตัวเลข ๑๓ หลัก ดังนั้น หากตรวจจับได้ว่า มีข้อมูลที่มีอยู่ประกอบด้วยตัวเลขไม่ครบ ๑๓ หลักหรือมีตัวอักษรหรืออักขระใด ๆ ปะปนมาในข้อมูล ก็ย่อมแสดงให้เห็นว่า ข้อมูลไม่ถูกต้อง และไม่น่าเชื่อถือเป็นต้น

๓.๑.๓ ความพร้อมใช้งานของข้อมูล (Availability)

ความพร้อมใช้ คือข้อมูลจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่นโดยผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลเหล่านั้นได้เมื่อต้องการ โดยอุปสรรคที่บั่นทอนความพร้อมใช้งานของระบบคอมพิวเตอร์จำแนก ได้ ๒ แบบ คือ การที่ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service) และระบบคอมพิวเตอร์ทำงานด้อยประสิทธิภาพในการทำงาน (Loss of Data Processing Capability)

๓.๒ กรอบแนวคิดการรักษาความปลอดภัยทางไซเบอร์ National Institute of Standard and Technology (NIST) Cyber Security Framework

นำไปใช้ในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย Framework นี้จะเน้นแนวปฏิบัติในเรื่องการบริหารจัดการความเสี่ยง ช่วยป้องกันการรักษาความมั่นคงปลอดภัยให้กับองค์กร และสามารถช่วยให้องค์กรวางแผนในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว โดยแบ่งออกเป็น ๕ ขั้นตอน ดังนี้ [๑๕]

---

[๑๕] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “มาตรฐานและมาตรการ ที่พึงนำไปใช้เป็นกรอบในการทางานเพื่อลดความเสี่ยง.” เอกสารประกอบการประชุม. ๒๕๖๑.

๓.๒.๑ การระบุ (Identify)

เป็นขั้นตอนของการศึกษาและทำความเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยงทางด้านการรักษาความมั่นคงปลอดภัยของไซเบอร์ ที่มีผลกระทบต่อทรัพย์สิน ข้อมูลสารสนเทศ สภาพแวดล้อมทางธุรกิจ การปกครอง การบริหารความเสี่ยง กลยุทธ์ในการบริหารความเสี่ยง

๓.๒.๒ การป้องกัน (Protect)

เป็นขั้นตอนการวางมาตรฐาน ควบคุมเพื่อป้องกันที่เหมาะสมของระบบโครงสร้างพื้นฐานขององค์กร เกี่ยวกับการควบคุมเกี่ยวกับการฝึกอบรมและการให้ความรู้เกี่ยวกับความปลอดภัยของข้อมูลทั้งในส่วนของกระบวนการและการป้องกัน การบำรุงรักษา และวิธีปฏิบัติ

๓.๒.๓ การตรวจจับ (Detect)

เป็นขั้นตอนและกระบวนการต่าง ๆ ในการตรวจจับเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางไซเบอร์ที่คาดว่าจะเกิดขึ้น เช่น การเฝ้าระวังเหตุการณ์ที่ผิดปกติและการติดตามความปลอดภัยอย่างต่อเนื่อง

๓.๒.๔ การตอบสนอง (Respond)

เป็นการกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตอบสนองรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้น รวมถึงการวางแผนการรับมือ การติดต่อสื่อสาร การวิเคราะห์ การลดความเสี่ยง การปรับปรุงการทำงานอย่างสม่ำเสมอ

๓.๒.๕ การคืนสภาพ (Recovery)

เป็นการกำหนดขั้นตอนและวางแผนในการกู้คืนและสามารถให้บริการได้ตามเวลาที่กำหนด เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

๓.๓ มาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001

ISO/IEC 27001 เป็นมาตรฐานที่ถูกกำหนดขึ้นเพื่อใช้เป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ ซึ่งเป็นมาตรฐานเชิงระบบที่เน้นการปฏิบัติ โดยการให้ความสำคัญเกี่ยวกับการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสารสนเทศ (Integrity) และการรักษาสภาพพร้อมใช้งานของระบบ (Availability) ซึ่งสามารถนำไปใช้อ้างอิงเพื่อการประเมินและขอรับการรับรองมาตรฐานต่อไปได้ โดย ISO/IEC 27001 เน้นเรื่องรายละเอียดเชิงเทคนิคมาตรฐานสำหรับการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ ISMS (Information Security Management System) โดย ISO/IEC 27001:2005 ให้รายละเอียดแบบมุ่งเน้นกระบวนการตามหลักการ PDCA (Plan – Do – Check - Act Process focused) สามารถใช้เป็นเกณฑ์เพื่อนำไปใช้งานจริง (Implement) และขอการรับรองได้ สำหรับ ISO/IEC 27001:2013 ไม่ได้มีการระบุแบบมุ่งเน้นกระบวนการตามหลักการ PDCA แต่แบบมุ่งเน้นกระบวนการตามหลักการพัฒนาอย่างต่อเนื่อง

(Continual improvement) ตามที่องค์กรมีอยู่ หรือจะใช้ PDCA ซึ่ง มาตรฐาน ISO/IEC 27001:2013 ประกอบด้วย ๔ ขั้นตอนหลัก ได้แก่ [๑๖]

๓.๓.๑ ขั้นตอนในระยะการวางแผน (Plan)

ประกอบด้วย การระบุบริบทขององค์กร (Context of the Organization) ศึกษาทำความเข้าใจองค์กรและบริบทที่เกี่ยวข้อง ศึกษาและทำความเข้าใจความต้องการและความคาดหวังของกลุ่มผู้ที่ต้องให้ความสำคัญ (ผู้มีส่วนได้ส่วนเสีย) บทบาทผู้นำ (Leadership) ระบุบทบาทผู้นำและพันธะความรับผิดชอบ จัดทำกรอบนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดโครงสร้าง บทบาทความรับผิดชอบ และอำนาจหน้าที่ การวางแผน (Planning) การระบุประเด็นพิจารณาความเสี่ยงและโอกาสในการปรับปรุง กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ กระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และสรุปมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้ในการบริหารความเสี่ยงและดำเนินการ ISMS กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแนวทางเพื่อให้บรรลุตามวัตถุประสงค์ การสนับสนุน (Support) จัดการด้านทรัพยากร จัดการสมรรถนะความสามารถของบุคลากร สร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ สื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดแนวทางการควบคุมเอกสารและจัดทำข้อมูลบันทึก

๓.๓.๒ ขั้นตอนในระยะการนำไปปฏิบัติ (Do)

การปฏิบัติงาน (Operation) ดำเนินการตามกระบวนการและมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและจัดทำรายการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ จัดทำและทบทวนแผนจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการตามแผนและรายงานสถานะผลการดำเนินการ

๓.๓.๓ ขั้นตอนในระยะการตรวจสอบและทบทวน (Check)

การประเมินผลดำเนินการ (Performance Evaluation) ติดตาม วัดผล วิเคราะห์และประเมินผล ดำเนินการตรวจสอบภายใน พิจารณาทบทวนโดยฝ่ายบริหาร

๓.๓.๔ ขั้นตอนในระยะการปรับปรุงต่อเนื่อง (Act)

การปรับปรุง (Improvement) ดำเนินการแก้ไขความไม่สอดคล้องและดำเนินการปรับปรุงอย่างต่อเนื่อง

---

[๑๖] “มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS).” (ออนไลน์). เข้าถึงได้จาก : https://www.iso.org/isoiec-27001-information-security.html, ๒๕๖๓.

๓.๔ เทคนิคการป้องกันการถูกโจมตีแบบ APT

ผู้ดูแลระบบ IT Security ควรศึกษาและพิจารณาเกี่ยวกับเทคนิคต่าง ๆ เพื่อเสริมความแข็งแกร่งให้ระบบขององค์กร เพื่อป้องกันการถูกโจมตีแบบ APT [๑๗]

๓.๔.๑ ออกแบบระบบความมั่นคงปลอดภัยแบบ Defense in - Depth

ระบบรักษาความมั่นคงปลอดภัยแบบหลายชั้นจะทำให้มีโอกาสตรวจจับภัยคุกคามได้มากยิ่งขึ้น

๓.๔.๒ ติดตั้งระบบตรวจจับและเฝ้าระวังที่มีประสิทธิภาพ

การเฝ้าระวังสิ่งต่าง ๆ ที่เกิดขึ้นบนระบบเครือข่ายอย่างใกล้ชิด

๓.๔.๓ ใช้บริการ Threat Intelligence

การช่วยตรวจจับการโจมตีแบบ Zero - day Exploits และ Unknown Malware

๓.๕ แนวทางในการรับมือภัยคุกคามทางไซเบอร์ในรูปแบบอื่น ๆ

ในปัจจุบันภัยคุกคามมีการพัฒนารูปแบบใหม่ ๆ ต่างจากอดีตเป็นอย่างมาก ไม่ว่าจะเป็น Advanced Persistent Threats, Advanced Targeted Attacks, Advanced Malware, Unknown Malware หรือ Zero - Day Attack ทำให้องค์กรส่วนใหญ่เริ่มรับมือกับภัยคุกคามเหล่านี้ได้ยากขึ้นเรื่อย ๆ ถึงแม้ว่าแต่ละองค์กรจะมีอุปกรณ์สำหรับป้องกันภัยคุกคามหลากหลายประเภท ไม่ว่าจะเป็น Firewall, IPS, Anti - Virus และอื่น ๆ แต่เมื่ออุปกรณ์เหล่านั้นต้องเจอกับภัยคุกคามรูปแบบใหม่ ๆ การที่ต่างฝ่ายต่างทำงาน ไม่มีการแชร์ข้อมูลระหว่างกันทำให้เป็นเรื่องยากที่จะระบุและตรวจจับภัยคุกคามขั้นสูงเหล่านั้นได้อย่างถูกต้องและแม่นยำ

๓.๕.๑ การจัดตั้ง ๖ กลุ่มงาน ตามมาตรฐาน SANS

ในการจัดตั้งกลุ่มงานตามมาตรฐาน SANS ได้แบ่งหน่วยงานออกเป็น ๖ กลุ่มงานได้แก่ [๑๘]

๓.๕.๑.๑ การตอบสนองเหตุภัยคุกคามทางไซเบอร์ Incident Response (IR) : Tier 2

๓.๕.๑.๒ การเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ Network Security Monitoring (NSM) : Tier 1

เป็นส่วนงานที่ทำหน้าที่ตรวจสอบข้อมูล เฝ้าระวังเหตุการณ์ที่ไม่ปกติ

---

[๑๗] Techtalkthai. “5 เทคนิคการป้องกัน Advanced Persistent Threats.” (ออนไลน์). เข้าถึงได้จาก : https://www.techtalkthai.com, ๒๕๖๓.

[๑๘] Pescatore, John. “Security Operations Center (SOC) Essential Functions.” (Online). Available : https://www.sans.org/security-resources/posters/security-leadership-poster/135/download, 2020.

๓.๕.๑.๓ การข่าวกรองทางไซเบอร์ Cyber Threat Intelligence

ประกอบด้วยทีมงานที่เป็นนักวิเคราะห์ข้อมูล โดยการแลกเปลี่ยนข้อมูลทั้งบุคคลภายในและภายนอกองค์กร ทำการวิเคราะห์รูปแบบของภัยคุกคามและผลของการตรวจสอบ กำหนดกฎในการกรองข้อมูลข่าวหรือเหตุการณ์ ตลอดจนให้คำแนะนำเกี่ยวกับการปฏิบัติงานให้แก่เจ้าหน้าและเจ้าหน้าที่ดูแลรักษาความปลอดภัย

๓.๕.๑.๔ การตรวจพิสูจน์หลักฐาน ทางดิจิทัล Digital Forensics (DF) : Tier 3

เป็นส่วนงานที่มีภารกิจต่าง ๆ ได้แก่ การตรวจพิสูจน์พยานหลักฐานดิจิทัล และออกรายงานผลการตรวจวิเคราะห์ตามคำร้องขอของหน่วยงานรักษากฎหมาย การให้คำปรึกษาและแนะนำทางวิชาการแก่เจ้าหน้าที่ ซึ่งบางครั้งอาจจะไม่คุ้นเคยกับเทคโนโลยีที่มีการเปลี่ยนแปลงอยู่ตลอดเวลาและพยานหลักฐานดิจิทัลสมัยใหม่ที่มีรูปแบบต่าง ๆ กัน ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์, โน้ตบุ๊ก, แท็บเล็ต, อุปกรณ์บันทึกกล้องวงจรปิด

๓.๕.๑.๕ ระบบควบคุมบังคับบัญชา Command Center : CC

๓.๕.๑.๖ การประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ Self Assessment : SA

๓.๕.๒ การรับมือภัยคุกคามระดับหน่วย

หน่วยงานควรมีการเตรียมความพร้อม เพื่อการปกป้องสินทรัพย์ดิจิทัลและรับมือกับภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพได้แก่ [๑๙]

๓.๕.๒.๑ มีการพัฒนาทักษะการรักษาความปลอดภัยทางไซเบอร์ให้กับบุคลากร ซึ่งการที่บุคลากรมีความรู้เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์จะมีส่วนช่วยให้มีการโจมตีทางไซเบอร์ลดน้อยลง

๓.๕.๒.๒ มีการสำรวจช่องโหว่และข้อบกพร่อง สิ่งที่เปลี่ยนแปลงต่าง ๆ ของหน่วยงานอยู่อย่างต่อเนื่องและสม่ำเสมอ ซึ่งหากตรวจพบให้รีบดำเนินการแก้ไขโดยด่วน

๓.๕.๒.๓ ให้ความสำคัญกับปัญหาภัยคุกคามทางด้านไซเบอร์ ด้วยการจัดสรรงบประมาณอย่างเหมาะสมต่อการพัฒนาการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ให้มีความทันสมัยและเท่าทันกับภัยคุกคามที่เกิดขึ้นในรูปแบบใหม่ ๆ อยู่ตลอดเวลา

๓.๕.๒.๔ คุ้มครองข้อมูลสำคัญของทุกหน่วยงาน ควรมีการสำรองข้อมูลสำคัญและจัดเก็บข้อมูลสำรองไว้แบบออฟไลน์ ตลอดจนควรทดสอบการกู้ข้อมูลกลับมาบ่อย ๆ เพื่อให้มั่นใจว่าข้อมูลจะกลับมาพร้อมใช้งานได้เสมอ แม้จะถูก Ransomware โจมตี

---

[๑๙] ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ. “ภัยคุกคามทางไซเบอร์ (Cyber Security).” ๒๕๕๙.

๓.๕.๒.๕ การจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ต่าง ๆ (Security Operations Center – SOC หรือ Cyber Security Operations Center – CSOC) เพื่อเป็นศูนย์กลางในการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ขององค์กร

กฎหมายและหลักการสำคัญต่าง ๆ ที่เกี่ยวข้อง

๑. ยุทธศาสตร์ชาติ

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) ได้จัดทำยุทธศาสตร์ชาติ ๒๐ ปี ระหว่างปี (พ.ศ. ๒๕๖๑ – ๒๕๘๐) เพื่อใช้เป็นแนวทางในการพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาล และใช้เป็นกรอบในการจัดทำแผนต่าง ๆ เพื่อนำไปสู่การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” เพื่อให้คนไทยมีความสุข ให้ประเทศมีความมั่งคั่ง ยั่งยืน ลดปัญหาความยากจนและความเหลื่อมล้ำทางสังคมให้สอดคล้องและบูรณาการกัน เพื่อนำพาประเทศไทยไปสู่เป้าหมายที่วางไว้ สำหรับยุทธศาสตร์ ๒๐ ปี ประกอบด้วยยุทธศาสตร์หลัก ๖ ด้าน ได้แก่ ด้านความมั่นคง, ด้านความสามารถในการแข่งขัน, การพัฒนาและเสริมสร้างศักยภาพคน, การสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม, การเติบโตบนคุณภาพชีวิตที่เป็นมิตรต่อสิ่งแวดล้อม, การปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ ๒๐ ซึ่งมีประเด็นที่เกี่ยวข้องกับไซเบอร์คือ มีการพัฒนาระบบ กลไก มาตรการและความร่วมมือระหว่างประเทศทุกระดับ และรักษาดุลยภาพความสัมพันธ์กับประเทศมหาอำนาจเพื่อป้องกันและแก้ไขปัญหาความมั่นคงรูปแบบใหม่

แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ.๒๕๖๑ - ๒๕๖๔) กำหนดแผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง และกำหนดแนวทางการพัฒนาในการป้องกันและแก้ไขปัญหาด้านความมั่นคงทางไซเบอร์ โดยมุ่งเน้นการกำหนดกลยุทธและยุทธวิธีในการแก้ไขปัญหาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้ครอบคลุมสภาพปัญหาของภัยคุกคามทางไซเบอร์ ได้แก่ การโจมตีทางไซเบอร์ของกลุ่มแฮกเกอร์ การจารกรรมหรือเปลี่ยนแปลงแก้ไขข้อมูล การโจมตีต่อกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการเผยแพร่ข้อมูลเพื่อความปั่นป่วนอันกระทบต่อประชาชน รวมทั้งอาจส่งผลกระทบต่อความมั่นคง โดยมีการกำหนดแนวคิดการแก้ไขปัญหาที่สำคัญประกอบด้วย

๑.๑ กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันและแก้ไขปัญหาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม

๑.๒ จัดองค์การ โครงสร้าง อำนาจ หน้าที่ ขีดความสามารถในการป้องกันและแก้ไขปัญหาการรักษาความมั่นคงปลอดภัยทางไซเบอร์

---

[๒๐] สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.). “ยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๑ – ๒๕๘๐.” ๒๕๖๐.

๑.๓ กำหนดระบบบริหารจัดการในแต่ละระดับให้ชัดเจน

๑.๔ เสริมสร้างและพัฒนาระบบการรายงานในสถานการณ์ฉุกเฉิน

๑.๕ ยกระดับแนวความคิดในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๖ พัฒนาการป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

๑.๗ สร้างความตระหนักรู้ให้แก่ประชาชนและหน่วยงาน

๑.๘ ปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง

๑.๙ พัฒนาศักยภาพบุคลากรและเทคโนโลยีให้ทันสมัยพร้อมรองรับสถานการณ์ทุกรูปแบบ[๒๑]

๒. พ.ร.บ. คอมพิวเตอร์ พ.ศ.๒๕๖๐ ฉบับที่ ๒

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ มีสาระสำคัญดังนี้ [๒๒]

๒.๑ เข้าถึงระบบ หรือข้อมูลของผู้อื่นโดยมิชอบ

๒.๒ แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย

๒.๓ ส่งข้อมูลหรืออีเมล์ก่อกวนผู้อื่น หรือส่งอีเมล์สแปม

๒.๔ เข้าถึงระบบ หรือข้อมูลทางด้านความมั่นคงโดยมิชอบ

๒.๕ จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด

๒.๖ นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์

๒.๗ ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด

๒.๘ ตัดต่อ เติม หรือดัดแปลงภาพ

๒.๙ เผยแพร่ข้อมูลเกี่ยวกับเยาวชน ต้องกระทำโดยปกปิดไม่ให้ทราบตัวตน

๒.๑๐ เผยแพร่เนื้อหาลามก อนาจาร

๒.๑๑ กด Like `& Share ถือเป็นวิธีหนึ่งในการเผยแพร่ข้อมูล

๒.๑๒ แสดงความคิดเห็นที่ผิด พ.ร.บ. คอมพิวเตอร์

๒.๑๓ ละเมิดลิขสิทธิ์ นำผลงานของผู้อื่นมาเป็นของตนเอง

๓. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ คือ มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ประกอบสาระสำคัญดังนี้ [๒๓]

---

[๒๑] แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (๑) ประเด็นความมั่นคง พ.ศ.๒๕๖๑ - ๒๕๘๐

[๒๒] พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

[๒๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๑ คำนิยาม

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กำหนด

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง” หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง

“ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ

การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

“ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ” หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐ เป็นภัยคุกคามทางไซเบอร์อันกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมาย พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการไซเบอร์

๓.๒ โครงสร้างการบริหารจัดการด้านไซเบอร์ในระดับประเทศของไทย

สำหรับโครงสร้างการบริหารจัดการด้านไซเบอร์ในระดับประเทศของไทยตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบด้วยหน่วยงานดังนี้

๓.๒.๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

มีอำนาจหน้าที่ดังนี้

๓.๒.๑.๑ เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๑.๒ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๑.๓ จัดทำแผนปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๑.๔ กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างและกำหนดมาตรฐานขั้นต่ำเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๑.๕ กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

เป็นคณะกรรมการกำกับดูแลซึ่งเป็นกลุ่มงานผู้ช่วยคณะกรรมการไซเบอร์ มีอำนาจหน้าที่ดังนี้

๓.๒.๒.๑ ติดตามการดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๒.๒ ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

๓.๒.๒.๓ กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ การเผชิญเหตุ และการดำเนินการด้านนิติวิทยาศาสตร์ทางคอมพิวเตอร์

๓.๒.๒.๔ กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๒.๕ กำหนดระดับของภัยคุกคามทางไซเบอร์ (ซึ่งแบ่งเป็น ๓ ระดับ) พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการไซเบอร์

๓.๒.๒.๖ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการไซเบอร์พิจารณาสั่งการในการกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คำนึงถึงหลักการบริหารความเสี่ยงโดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ

๓.๒.๓ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

เป็นหน่วยงานผู้ปฏิบัติงานพื้นฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและต้องรายงานต่อคณะกรรมการไซเบอร์และคณะกรรมการกำกับดูแลเกี่ยวกับการดำเนินงานทั้งหมดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีอำนาจหน้าที่ ดังนี้

๓.๒.๓.๑ รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการไซเบอร์ และคณะกรรมการกำกับดูแล

๓.๒.๓.๒ เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓.๓ ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๓.๔ ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการไซเบอร์

๓.๒.๓.๕ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผล ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๓.๒.๓.๖ ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ตลอดจนแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓.๗ เสริมสร้างความรู้ความเข้าใจ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๓.๘ เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๓.๒.๓.๙ เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

๓.๒.๓.๑๐ ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๒.๔ คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคนเป็นกรรมการ มีอำนาจหน้าที่

๓.๒.๔.๑ กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

๓.๒.๔.๒ ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

๓.๒.๔.๓ อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

๓.๒.๔.๔ ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการ ให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

๓.๒.๔.๕ วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

๓.๒.๔.๖ ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ

๓.๒.๔.๗ ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่ และอำนาจของ กบส. หรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

๓.๓ การจัดกลุ่มหน่วยงานพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งอาจจะเป็นหน่วยงานหรือองค์กร หรือส่วนงานหนึ่ง

ส่วนงานใดของหน่วยงานหรือองค์กรซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน ระบบสารสนเทศที่หน่วยงานซึ่งเป็นโครงสร้างพื้นฐานสำคัญของประเทศใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทาให้ไม่สามารถดำเนินงานหรือให้บริการได้ โดยกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทยแบ่งออกเป็น ๘ กลุ่มได้แก่

๓.๓.๑ กลุ่มความมั่นคง

๓.๓.๒ กลุ่มบริการภาครัฐที่สำคัญ

๓.๓.๓ กลุ่มการเงิน

๓.๓.๔ กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม

๓.๓.๕ กลุ่มการขนส่งและโลจิสติกส์

๓.๓.๖ กลุ่มพลังงานและสาธารณูปโภค

๓.๓.๗ กลุ่มสาธารณสุข

๓.๓.๘ ด้านอื่น ๆ ตามที่คณะกรรมการประกาศเพิ่มเติม[๒๔]

๓.๔ ลักษณะของระดับภัยคุกคามทางไซเบอร์

ทั้งนี้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้แบ่งลักษณะของภัยคุกคามทางไซเบอร์ในระดับประเทศออกเป็น ๓ ระดับ ดังต่อไปนี้

๓.๔.๑ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

๓.๔.๒ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

๓.๔.๓ ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

---

[๒๔] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “การจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย.” เอกสารประกอบการประชุม. ๒๕๖๑.

๓.๔.๓.๑ เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

๓.๔.๓.๒ เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด[๒๕]

๔. มิติสงครามทางไซเบอร์

ในปัจจุบันจะเห็นได้ว่าการพัฒนาทางเทคโนโลยีและการสื่อสารมีความเจริญมากยิ่งขึ้นและกำลังจะเปลี่ยนรูปแบบและวิวัฒนาการของโลกจาก ๔ มิติ ได้แก่ มิติทางพื้นดิน มิติทางพื้นน้ำ มิติทางอากาศ และมิติทางอวกาศ เพิ่มเป็น ๕ มิติ คือโดเมนที่ ๕ หรือที่เรียกกันว่า มิติไซเบอร์/ไซเบอร์โดเมน หรือ โลกไซเบอร์ ซึ่งเป็นมิติที่สามารถสัมผัสด้วยตา เคลื่อนที่ด้วยข้อมูล และข่าวสารจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างรวดเร็ว สามารถไปได้ทุกสถานที่ ทุกเวลา และไร้ขอบเขตจำกัด นอกจากนี้ยังมีความเสมือนจริง สามารถล่องหนไปปรากฏในที่ต่าง ๆ บนโลกไซเบอร์ได้อย่างรวดเร็ว โดยโดเมนที่ ๕ หรือโลกไซเบอร์ในมุมมองของการทหารมองว่า โลกไซเบอร์ คือโดเมนที่ ๕ แห่งการทำสงครามทางด้านการทหาร ถือว่าเป็นโดเมนหนึ่งที่มีความสำคัญในการสู้รบเอาชนะฝ่ายตรงข้าม นอกจากนี้ในด้านการปฏิบัติการข่าวสาร (Information Operations : IO) ทางการทหาร ไม่ว่าในยามปกติและยามสงคราม รวมถึงเมื่อเกิดความขัดแย้งทางการเมืองและทางสังคม นิยมใช้โดเมนที่ ๕ หรือโลกไซเบอร์

---

[๒๕] “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒,” ราชกิจจานุเบกษา เล่มที่ ๑๓๖, ๒๗ พฤษภาคม ๒๕๖๒, หน้า ๔๒ – ๔๓.

ในการเป็นช่องทางในการดำเนินการ เพราะมีการกระจายข้อมูลข่าวสารทั้งในส่วนของ ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว สำหรับการประชาสัมพันธ์ การโฆษณาชวนเชื่อ ฯลฯ ไปในวงกว้าง เพื่อให้เข้าถึงกลุ่มเป้าหมายรวดเร็ว ตลอดจน มีการแชร์ข้อมูลต่อ ๆ กันไป รวมไปถึงมีการแสดงความคิดเห็นต่าง ๆ ทั้งในเชิงบวกและเชิงลบ และมีอิทธิพลต่อความรู้สึกนึกคิด ทัศนคติ และมีผลต่อการตัดสินใจของคนเป็นจำนวนมาก ฉะนั้นโดเมนที่ ๕ หรือโลกไซเบอร์ ถือเป็นปัจจัยสำคัญที่ส่งผลต่อด้านจิตใจ [๒๖]

ในการเตรียมความพร้อมเพื่อปฏิบัติการสงครามไซเบอร์ (Cyber Warfare Operation) สำหรับพื้นที่การรบที่ ๕ ในการปกป้องข้อมูลข่าวสาร บุคคล องค์กร และอธิปไตยของชาติ ต้องดำเนินการในทันที โดยกำหนดหลักนโยบายและแนวปฏิบัติทั้งทางยุทธศาสตร์และยุทธวิธีหรือเทคนิควิธี ที่เป็นปัจจัยสำคัญในการพัฒนาการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้กับกองทัพไทยโดยกองบัญชาการกองทัพไทยเป็นหน่วยงานที่รับผิดชอบในภาพรวมของการปฏิบัติการร่วมทางไซเบอร์ของกองทัพไทย เนื่องจากเป็นยุทธวิธีรูปแบบใหม่ที่มีการนำมาใช้ในการพัฒนากิจการงานด้านการทหาร ทั้งนี้ มีหลายประเทศชั้นนำอย่างสหรัฐ รัสเซีย และจีน ต่างใช้เป็นเครื่องมือในการกระทำกับฝ่ายตรงข้าม เพื่อทำลายระบบต่าง ๆ ไม่ว่าจะเป็นระบบการควบคุมการบังคับบัญชา โครงสร้างพื้นฐานสำคัญของประเทศ (Infrastructure) รวมถึงการได้มาซึ่งข้อมูลข่าวสารสำคัญ (Information Critical) หรือการฝังตัวการโจมตีในรูปแบบใหม่ (Root kit) ที่ใช้หลักการเขียนตรรกะทางโปรแกรม (Logical Programming) แทนกำลังพล และยุทโธปกรณ์ทางทหาร (Armament) [๒๗]

การปฏิบัติการในมิติไซเบอร์ของกองทัพไทยนั้น เป็นการปฏิบัติการทางทหารรูปแบบหนึ่ง เพื่อรับมือกับภัยคุกคามรูปแบบใหม่ ซึ่งมีความสอดคล้องกับหน้าที่ของกองทัพไทย ในการเตรียมกำลังการป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทางทหาร โดยในระดับกระทรวงกลาโหม และกองบัญชาการกองทัพไทยมีหน่วยงานสำคัญที่มีบทบาทในการดำเนินภารกิจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ [๒๘]

๕. การรับมือภัยคุกคามระดับประเทศ

สำหรับการรับมือภัยคุกคามในระดับประเทศนั้น ตามยุทธศาสตร์ชาติด้านความมั่นคงได้กำหนดแผนงาน/โครงการเร่งด่วน (Flagship) ในช่วงระยะ ๕ ปีแรก (พ.ศ. ๒๕๖๑ – ๒๕๖๕) กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมได้จัดทำ (ร่าง) แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหา

---

[๒๖] ฤทธี อินทราวุธ. “โดเมน ที่ ๕ / โลกไซเบอร์ กับ ความมั่นคงของมนุษย์.” (ออนไลน์). เข้าถึงได้จาก : http://rittee1834.blogspot.com/2013/12/blog-post.html. ๒๕๕๖.

[๒๗] จินดา สระสมบูรณ์. “ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย.” วารสารสถาบันวิชาการป้องกันประเทศ. ๘(๓), หน้า ๕๗ - ๖๙.

[๒๘] อรรคเดช ประทีปอุษานนท์. “แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์.” วารสารสถาบันวิชาการป้องกันประเทศ. ๘(๓), หน้า ๑๑ – ๒๓.

ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไว้เพื่อเป็นแนวทางให้หน่วยงานทุกหน่วย นำไปประกอบเพื่อจัดทำแผนปฏิบัติการทางด้านการป้องกันและแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยได้กำหนดกลยุทธ์เพื่อให้บรรลุเป้าหมายไว้ ๙ กลยุทธ์ ดังนี้ [๒๙]

กลยุทธ์ที่ ๑ กำหนดแนวความคิดมาตรการมาตรฐานระบบบริหารจัดการในการป้องกันการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวม รับผิดชอบโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สภาความมั่นคงแห่งชาติ หน่วยงานที่ตั้งใหม่ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งมีแนวทางในการบริหารจัดการ นโยบาย มาตรการมาตรฐานและความร่วมมือทุกภาคส่วนทั้งภายในประเทศและต่างประเทศ โดยได้กำหนดกรอบแนวคิดด้านไซเบอร์ทั้งระบบ และมีการระบุผู้รับผิดชอบแนวทางการติดตามและประเมินผลให้ครอบคลุม การปฏิบัติงานประกอบด้วย การบูรณาการการจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ, การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพการตอบสนองต่อภัยคุกคามไซเบอร์, การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ, การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์, การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์, การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งภาครัฐและเอกชน, การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์, การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ ๒ การจัดองค์กร โครงสร้าง อำนาจหน้าที่ ขีดความสามารถในงานการรักษาความมั่นคงปลอดภัยไซเบอร์ รับผิดโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสภาความมั่นคงแห่งชาติมีแนวทางในการดำเนินงานคือ การจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ซึ่งมีรูปแบบขององค์กร ประกอบด้วย โครงสร้างและอำนาจหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (Cyber Security Agency : CSA) เป็นหน่วยงานราชการอยู่ภายใต้สำนักนายกรัฐมนตรีหรือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือ กปช. (National Cybersecurity Committee : NCSC) ประกอบด้วย นายกรัฐมนตรีเป็นประธาน กรรมการ และมีองค์ประกอบ ๓ คณะ ได้แก่ คณะกรรมการกำกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติคณะกรรมการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการส่งเสริมด้านโครงสร้างพื้นฐานสำคัญทางเทคโนโลยีสารสนเทศแห่งชาติ

---

[๒๙] ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงคมนาคม. “แผนปฏิบัติการป้องกันและแก้ไข ปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงคมนาคม พ.ศ. 2562 – 2566.” ๒๕๖๒.

กลยุทธ์ที่ ๓ กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน รับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สภาความมั่นคงแห่งชาติ และหน่วยงานที่ตั้งใหม่ โดยมีแนวทางการดำเนินงานคือ กำหนดการบริหารจัดการและแนวปฏิบัติร่วมให้เป็นไปตามมาตรฐานสากล เพื่อเตรียมรับมือความเสี่ยงและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ครอบคลุมสภาวะปกติและสภาวะที่เกิดภัยคุกคามไซเบอร์ ประกอบด้วย เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับหน่วยงานบริหารจัดการโดยมีหน่วยงานเป็นผู้ดูแลตนเอง และมี Sector - Based CERT หรือ ThaiCERT เป็นหน่วยงานสนับสนุนเหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับกลุ่มหน่วยงาน (Sector) มีการบริหารจัดการโดยหัวหน้าหน่วยงานกำกับดูแล (Regulator) ตนเอง โดยมี ThaiCERT เป็นหน่วยงานสนับสนุนเพื่อให้ปฏิบัติตามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับเกินกว่า ๑ กลุ่ม (Sector) ให้บริหารจัดการโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมีหน่วยงานความมั่นคงสนับสนุนการดำเนินงาน ต่อเหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบระดับประเทศบริหารจัดการ โดยหน่วยงานด้านความมั่นคงจะต้องสร้างความรับรู้ความเข้าใจกับหน่วยงานภาครัฐหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตลอดจนภาคเอกชนที่มีความเกี่ยวข้องด้านเศรษฐกิจ หรือมีความเกี่ยวข้องหากถูกโจมตีและกระทบต่อความมั่นคงของประเทศให้รับทราบถึงแนวทางปฏิบัติและแนวทางการแก้ไขปัญหา

กลยุทธ์ที่ ๔ ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน รับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สภาความมั่นคงแห่งชาติ หน่วยงานภาครัฐ และหน่วยงานที่ตั้งใหม่ต่าง ๆ ซึ่งมีแนวทางในการดำเนินงานได้แก่ การส่งเสริมพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามไซเบอร์ให้เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามทางไซเบอร์ โดยมีบูรณาการความร่วมมือระหว่างหน่วยงานทหารและพลเรือนที่เกี่ยวข้องทั้งในส่วนของระดับนโยบายและระดับปฏิบัติเพื่อให้การบริหารจัดการ การสั่งการและการรายงานรวมถึงการแจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟูปราบปรามปัญหาภัยคุกคามไซเบอร์

กลยุทธ์ที่ ๕ ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศรับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และทุกกระทรวง ซึ่งมีแนวทางในการดำเนินงาน ได้แก่ การกำหนดให้หน่วยงานทุกหน่วยที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศจะต้องจัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญ สำหรับบริหารจัดการด้วยระบบสารสนเทศและมีแผนรองรับสถานการณ์ฉุกเฉินทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานมีความพร้อม สามารถป้องกันและตอบสนองต่อปัญหาที่เกิดอาจขึ้นได้ และเมื่อเกิดสถานการณ์ที่มีความรุนแรงจนเกินความสามารถของหน่วยงาน สามารถประสานขอรับการสนับสนุนจากหน่วยงานที่กำกับดูแล และ/หรือหน่วยงานกลางที่มีหน้าที่ดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ ตลอดจนต้องฝึกซ้อมรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ เพื่อให้มีความพร้อมทั้งในระดับหน่วยงานและระดับภาคกลุ่ม (Sector) นอกจากนี้ต้องมีการตรวจสอบ

และประเมินระดับความพร้อมของหน่วยงานให้อยู่ในระดับการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐานสากล

กลยุทธ์ที่ ๖ การป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง รับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานที่ตั้งใหม่ต่าง ๆ ซึ่งมีแนวทางในการดำเนินงาน ประกอบด้วย ส่งเสริมวัฒนธรรมการใช้อินเทอร์เน็ตสร้างสรรค์ และรับผิดชอบทั้งในระดับบุคคลและองค์กรมีจิตอาสำนึกต่อผู้อื่นและสังคม โดยต้องเคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์และไม่ละเมิดกฎหมาย, ส่งเสริมการใช้เทคโนโลยีสารสนเทศ และการสื่อสารของประชาชนเพื่อการธำรงไว้ซึ่งชาติศาสนาและพระมหากษัตริย์ ส่งเสริมการมีส่วนร่วมของภาคเอกชนและภาคประชาสังคม ส่งเสริมการผลิตเผยแพร่สื่อที่ปลอดภัยและสร้างสรรค์รวมถึงการป้องกันตรวจสอบสื่อที่เป็นเท็จ ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรม ส่งเสริมการใช้เทคโนโลยีที่ทันสมัยมาสนับสนุนงานสืบสวนและงานข่าว สร้างความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ประสบการณ์และแนวปฏิบัติที่ดีระหว่างหน่วยงานภายในประเทศและหน่วยงานต่างประเทศ ทั้งในระดับภูมิภาคและนานาชาติ มีมาตรการการป้องปรามปราบปรามจับกุม และลงโทษในกลุ่มบุคคลหรือบุคคลที่ไม่ประสงค์ดีต่อความมั่นคงของประเทศซึ่งจะต้องถูกดำเนินการตามกฎหมาย

กลยุทธ์ที่ ๗ การสร้างความตระหนักรู้ให้แก่ประชาชนและหน่วยงาน รับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานที่ตั้งใหม่ต่าง ๆ ซึ่งมีแนวทางการดำเนินงาน ได้แก่ การส่งเสริมให้ประชาชนและทุกหน่วยงานทั่วประเทศ มีความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์ ตลอดจนสร้างวัฒนธรรมการมีคุณธรรมและจริยธรรมในการใช้ไซเบอร์อย่างถูกต้องและสร้างสรรค์มีความรับผิดชอบ และมีจิตสานึกต่อผู้อื่นและสังคม โดยต้องเคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์และไม่ละเมิดกฎหมาย มีดำเนินการโดยอาศัยความร่วมมือระหว่าง หน่วยงานภาครัฐ ภาคเอกชนสถาบันการศึกษา และหน่วยงานที่เกี่ยวข้องในพื้นที่ ในการเผยแพร่ความรู้ประชาสัมพันธ์ข้อมูลข่าวสารและยกระดับความตระหนักรู้อย่างเป็นระบบและต่อเนื่องโดยให้ความสำคัญกับกลุ่มเป้าหมายที่เป็นกลุ่มเสี่ยงต่อภัยไซเบอร์กลุ่มที่ขาดความเข้าใจเทคโนโลยีสมัยใหม่และกลุ่มที่ไม่มีโอกาสเข้าถึงความรู้หรือได้รับการฝึกสอนรวมถึงกลุ่มที่อยู่ห่างไกลความเจริญ

กลยุทธ์ที่ ๘ การปรับปรุงแก้ไขกฎหมาย รับผิดชอบโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สภาความมั่นคงแห่งชาติ และหน่วยงานที่ตั้งใหม่ต่าง ๆ ซึ่งมีแนวทางการดำเนินงาน ได้แก่ การส่งเสริมและสนับสนุน การทบทวนปรับปรุงและพัฒนากฎหมายและมาตรการต่าง ๆ ที่เกี่ยวข้องเพื่อให้ทันต่อความก้าวหน้าและการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล และสอดคล้องกับแนวปฏิบัติและ/หรือกฎหมายสากล โดยจัดให้มีกลไกส่งเสริมการมีส่วนร่วมของตัวแทนทุกภาคส่วนที่เกี่ยวข้องเมื่อมีการปรับปรุงและพัฒนากฎหมาย มาตรฐาน มาตรการต่าง ๆ ส่งเสริมการสร้างกลไกการ บังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น ในการป้องกันและปราบปรามการกระทำความผิดที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

กลยุทธ์ที่ ๙ การพัฒนาศักยภาพบุคลากรและเทคโนโลยี รับผิดชอบโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หน่วยงานด้านความมั่นคง ซึ่งมีแนวทางการดำเนินงาน ได้แก่ การพัฒนาศักยภาพขององค์กรและบุคลากรให้มีทักษะความรู้ เพื่อให้มีความสามารถในการป้องกันตนเองและหน่วยงานในการลดความเสี่ยง และลดความเสียหายจากการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้น ตลอดจนมีพัฒนากำลังคนในทุกระดับ ตั้งแต่การส่งเสริมระดับสถานศึกษา เพื่อการสร้างบุคลากรรองรับความต้องการในอนาคต และยกระดับความพร้อมของประเทศในการรับมือและจัดการกับภาวะความเสี่ยงภัยคุกคามทางไซเบอร์ทั้งในปัจจุบันและอนาคต

งานวิจัยที่เกี่ยวข้อง

จินดา สระสมบูรณ์ ได้ทำการวิจัยเรื่อง ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย Cyber Warfare Operation RTARF โดยการรวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ จากผลการศึกษาทำให้ได้แนวทางในการพัฒนารูปแบบและหลักการปฏิบัติการสงครามไซเบอร์ ด้านการทหาร ทั้งการปฏิบัติเชิงรุกและเชิงรับ สำหรับเตรียมการหรือรองรับภัยคุกคามรูปแบบใหม่ที่อาศัยเครือข่ายในการปฏิบัติ รวมทั้งกำหนดบทบาทและโครงสร้างของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทย ในการปฏิบัติการสงครามไซเบอร์ ซึ่งการปฏิบัติการสงครามไซเบอร์เชิงรุกมีวิธีปฏิบัติประกอบด้วย การหลอกลวงฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามหยุดการให้บริการทางไซเบอร์ การทำลายระบบทางไซเบอร์ฝ่ายตรงข้าม และการเจาะระบบฝ่ายตรงข้าม ส่วนการปฏิบัติการสงครามไซเบอร์เชิงรับ มีวิธีปฏิบัติประกอบด้วย การปกป้องระบบ การทำให้ระบบสามารถระบุตัวตนผู้ใช้งานได้ การกู้คืนหรือการฟื้นคืนระบบ การค้นหาและปิดช่องโหว่ระบบ การปฏิบัติตามข้อกำหนดหรือมาตรฐานทางไซเบอร์ การบำรุงรักษาระบบรวมถึงการปฏิบัติตามข้อกำหนดต่าง ๆ ทางกฎหมายหรือข้อบังคับทางไซเบอร์ โดยมีฝ่ายต่าง ๆ ของศูนย์บัญชาการทางทหาร กองบัญชาการกองทัพไทยที่เกี่ยวข้องกับการปฏิบัติคือ ฝ่ายกำลังพล ฝ่ายการข่าว ฝ่ายยุทธการ ฝ่ายส่งกำลังบำรุง ฝ่ายกิจการพลเรือน และฝ่ายสื่อสาร

ศิวลีย์ สิริโรจน์บริรักษ์ ได้ทำการศึกษาเรื่อง “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” ผลการศึกษาพบว่ากรอบนโยบายยุทธศาสตร์ และการดำเนินงานความมั่นคงไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ. ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีและการสื่อสารของ กห. พ.ศ. ๒๕๕๑ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. ๒๕๕๔ ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e - Defence) แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ ๓ พ.ศ. ๒๕๕๗ – ๒๕๖๑ การจัดตั้งศูนย์บัญชาการไซเบอร์ กห. มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และมาตรฐาน IT BPM

แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานในระดับสากล โดยแบ่งออกเป็น ๒ ส่วน คือ

๑. เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องดำเนินการเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อปัญหา แลเหตุการณ์บุกรุกระบบของหน่วยขึ้นตรงได้อย่างรวดเร็ว ในส่วนของนโยบายและแผน ต้องมีการบรรจุข้อกำหนดในกระบวนการจัดซื้อจัดจ้าง อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้อุปกรณ์มีความปลอดภัยในระดับสากล สำหรับส่วนปฏิบัติการไซเบอร์จะต้องมีหน่วยปฏิบัติการเชิงรับสงครามข้อมูลข่าวสาร และหน่วยปฏิบัติการเชิงรุก สงครามข้อมูลข่าวสาร ส่วนวิจัยและพัฒนาไซเบอร์จะต้องจัดตั้งส่วนงาน Information Warfare System Research เพื่อพัฒนาระบบการรักษาความปลอดภัยของข้อมูลข่าวสารให้มีประสิทธิภาพมากยิ่งขึ้น และต้องบรรจุ อัตราจเรทหารที่มีความเชี่ยวชาญเฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อดำเนินการตรวจสอบตามหลักการ ICT Audit

๒. เชิงปฏิบัติได้แก่ ควรจัดทำหลักสูตร Cyber Training เพื่ออบรมความรู้เกี่ยวกับการใช้งานซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งการให้ทุนการศึกษาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ ควรมีการจัดการองค์ความรู้ด้านไซเบอร์ (Cyber Knowledge Management : KM) ในหน่วยงาน และควรนำ E - Document มาใช้ในการปฏิบัติราชการมากยิ่งขึ้น

ชนินทร เฉลิมทรัพย์ ได้ทำการศึกษาเรื่อง แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ผลการศึกษาพบว่าการศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการ และการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมี องค์กรที่นำเทคนิคการบริหารจัดการมาใช้ ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้น การบูรณาการการบริหารจัดการต้องมีเจ้าภาพที่ชัดเจน โดยบริหารที่ทุกหน่วยงานทำงานแบบมุ่งเน้นผลงานตามยุทธศาสตร์โดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุเป้าหมาย ปัจจัยในการดาเนินงานที่สำคัญที่สุดคือมนุษย์ การศึกษาแนวนโยบายและยุทธศาสตร์ ตลอดจนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่ากระทรวงกลาโหมใช้แนวความคิดในการป้องกันทางไซเบอร์เช่นเดียวกับการศึกษามั่นคงของประเทศ โดยเน้นการป้องกันเชิงรุก การผนึกกาลังป้องกันประเทศและการร่วมมือด้านความมั่นคงทางไซเบอร์ โดยได้จัดตั้งส่วนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เชิงรับและส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security incident Response Team : CSIRT) สำหรับกระทรวงดิจิทัลฯ ได้กำหนดกรอบแนวคิดและนโยบายในระดับชาติกาหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศ กำหนดแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางการรักษาความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure : SOP) รวมทั้งเสนอแนวความคิดในการจัดตั้ง Cyber Security Agency (CSA) หน้าที่เป็นหน่วยงานกลางในการประสานงานและเผชิญเหตุด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Jacobs ได้เสนอแนวคิดในการตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ แบบรวมศูนย์จะเป็นการแก้ไขปัญหาด้านความปลอดภัยในระดับองค์กรได้ดี เนื่องจากมีทีมงานที่ประกอบด้วยนักวิเคราะห์ด้านความปลอดภัยเป็นหลัก เพื่อตรวจจับวิเคราะห์ตอบสนองรายงานและป้องกันเหตุการณ์ นอกจากนี้การที่องค์กรมีศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์แบบรวมศูนย์โดยมีการรักษาความปลอดภัยส่วนกลางคอยให้ความช่วยเหลือในการป้องกันภัยคุกคามแก่หน่วยงาน โดยหน่วยงานมีการป้องกันโดยการระบุตัวตนและการจัดการ ตลอดจนการแก้ไขการโจมตีความปลอดภัยแบบกระจาย อย่างไรก็ตามเป้าหมายสุดท้ายของ SOC คือการป้องกัน ปรับปรุงการรักษาความปลอดภัยขององค์กรโดยการตรวจจับและตอบสนองต่อภัยคุกคามและการโจมตีก่อนที่จะส่งผลกระทบต่อธุรกิจ

กรอบแนวคิดของการวิจัย

แผนภาพที่ ๒ - ๑ กรอบแนวคิดของการวิจัย

ที่มา: ประมวลโดยผู้วิจัย, ๒๕๖๔

จากแผนภาพที่ ๒ - ๑ งานวิจัยเรื่อง เรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The guidance for setting up Thailand National Cybersecurity Operations Center – NCOC – in order to properly solve the critical cybersecurity situation at the national level)” โดยรายละเอียดขั้นตอนในการศึกษาวิจัยในครั้งนี้ประกอบไปด้วย ๖ ขั้นตอนหลัก ดังนี้

๑. ศึกษาปัญหาและที่มา

๒. กำหนดวัตถุประสงค์การวิจัย และตั้งคำถามวิจัย

๓. เก็บรวบรวมข้อมูล จากแหล่งข้อมูล ๔ แบบ ได้แก่ การดำเนินการวิจัยจากเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่มเฉพาะ (Focus Group Discussion) และการสังเกตการณ์ (Observation)

๔. วิเคราะห์ข้อมูล

๕. สรุปผลการศึกษา (ตอบคำถามวิจัย/ วัตถุประสงค์การวิจัย)

๖. สรุป อภิปรายผล และข้อเสนอแนะ

บทที่ ๓
แนวทางการดำเนินการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ

ในการวิจัยเรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The Guidance For Setting Up Thailand National Cybersecurity Operations Center – NCOC – In Order To Properly Solve The Critical Cybersecurity Situation At The National Level)” เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีรายละเอียดของการวิจัยดังต่อไปนี้

๑. ขั้นตอนการดำเนินการวิจัย

๒. ขอบเขตการวิจัย

๓. ประชากรและกลุ่มตัวอย่าง

๔. เครื่องมือที่ใช้ในการรวบรวมข้อมูลสำหรับการวิจัย

๕. การวิเคราะห์ข้อมูล

ขั้นตอนในการดำเนินการวิจัย

๑. ศึกษาปัญหาและที่มา

จากประสบการณ์ของตัวนักวิจัย ซึ่งมีประสบการณ์การทำงานในส่วนของการเฝ้าระวังภัยคุกคามทางไซเบอร์ในระดับกองทัพ หรือแม้แต่ในระดับประเทศก็ตาม การจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) มีอยู่หลายประเภท เช่น การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ ซึ่งการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในประเทศไทยที่มีอยู่ในปัจจุบัน เพื่อแก้ปัญหาหน่วยงานต่าง ๆ ตามโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ยังไม่สามารถปฏิบัติได้จริงอย่างมีประสิทธิภาพ ผู้วิจัยจึงเห็นถึงความสำคัญของแนวทางการตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์แห่งชาติ (NCOC) ที่จะต้องเป็นกลไกหลักในระดับประเทศในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ที่สามารถปฏิบัติได้จริง อย่างมีประสิทธิภาพ

๒. กำหนดวัตถุประสงค์การวิจัย และตั้งคำถามวิจัย

๒.๑ วัตถุประสงค์การวิจัย ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยออกเป็น ๓ ประเด็น เพื่อตอบปัญหาการวิจัย ดังต่อไปนี้

๒.๑.๑ เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒.๑.๒ เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ที่เป็นแบบรวมการและแยกการ

๒.๑.๓ เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๒.๒ คำถามวิจัย เป็นแบบสัมภาษณ์เกี่ยวกับแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม ซึ่งแบบสอบถามสามารถใช้ได้ทั้งเพื่อการจัดเก็บข้อมูลในส่วนของการสัมภาษณ์เชิงลึก (In - Depth Interview) และการสนทนากลุ่ม (Focus Group Discussion) เพื่อตอบปัญหาการวิจัยตามวัตถุประสงค์ที่ได้ตั้งไว้ ดังต่อไปนี้

๒.๒.๑ หน่วยของท่านมีการรับมือภัยคุกคามทางไซเบอร์ยังไง และถ้าไม่สามารถรับมือหรือแก้ปัญหาภัยคุกคามทางไซเบอร์ได้ จะดำเนินการอย่างไรต่อ

๒.๒.๒ ท่านคิดว่าอะไรคืออุปสรรคของการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติของประเทศไทย (NCOC) ทั้งแบบรวมการและแบบแยกการ หรือแบบอื่น ๆ โดยแบ่งตาม บุคลากร กระบวนการ และเทคโนโลยี

๒.๒.๒.๑ บุคลากร (People) ทั้งผู้ปฏิบัติงานและผู้บังคับบัญชา

๒.๒.๒.๒ กระบวนการ (Process) และงบประมาณ (Budget)

๒.๒.๒.๓ เทคโนโลยี (Technology)

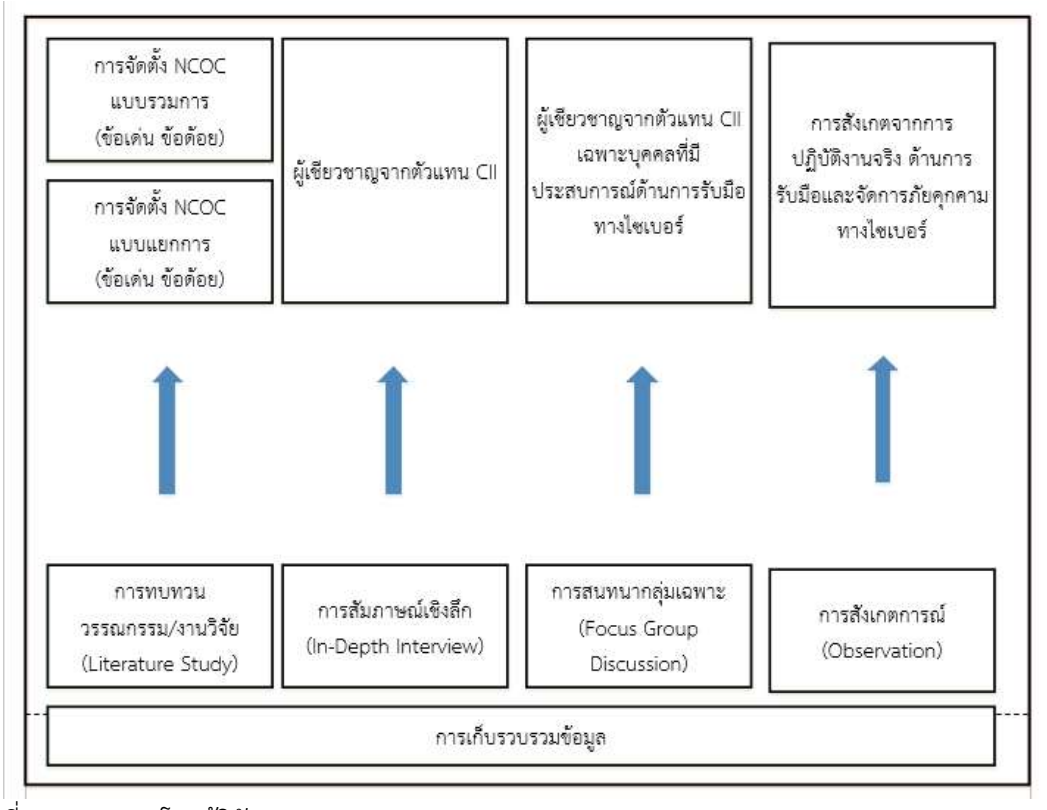
๒.๒.๓ ท่านคิดว่า การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) มีกี่แบบ แต่ละแบบมีข้อเด่น ข้อด้อย ยังไง

๒.๒.๔ ท่านคิดว่า แนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติของประเทศไทย (NCOC) ที่มีประสิทธิภาพ ควรเป็นอย่างไร

๓. เก็บรวบรวมข้อมูล

เก็บรวบรวมข้อมูลวิจัยในครั้งนี้จากแหล่งข้อมูล ๔ แบบ ดังแผนภาพที่ ๓ - ๑

แผนภาพที่ ๓ - ๑ เก็บรวบรวมข้อมูลวิจัย



ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

๓.๑ การวิจัยเอกสาร (Documentary Research)

การวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยกระบวนวิธีการวิจัยเอกสาร (Documentary Research) ในครั้งนี้ ผู้วิจัยได้ดำเนินการศึกษาและวิเคราะห์ข้อมูลจากเอกสารหรือวิจัยเอกสาร (Documentary Research) โดยการทบทวนแนวความคิด ทฤษฎี องค์ความรู้ วรรณกรรม และงานวิจัยที่เกี่ยวข้องกับแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม ข้อดี ข้อเสีย ของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) แต่ละแบบที่เคยมีมา เพื่อนำผลที่ได้มาออกแบบกรอบแนวคิดการวิจัย ในการตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ นำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม และสามารถนำไปใช้งานได้จริง

๓.๒ การสัมภาษณ์เชิงลึก (In - Depth Interview)

การสัมภาษณ์เชิงลึก (In - Depth Interview) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสัมภาษณ์กลุ่มเป้าหมาย เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และมีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์เท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก โดยเป็นการสัมภาษณ์แบบกึ่งโครงสร้าง หรือการสัมภาษณ์แบบชี้นำ (Guided Interview) กล่าวคือเป็นการสัมภาษณ์ที่มีการใช้คำสำคัญ (Keywords) มาประกอบในการสัมภาษณ์ มีการร่างข้อคำถามที่มีลักษณะปลายเปิดพร้อมกับลักษณะของข้อคำถามที่มีความยืดหยุ่น พร้อมที่จะมีการปรับเปลี่ยนถ้อยคำของข้อคำถามให้มีความสอดคล้องกับผู้ให้สัมภาษณ์แต่ละคนในแต่ละสถานการณ์ได้ตอบข้อคำถามอันทำให้ได้มาซึ่งข้อมูลที่มีความหลากหลายในมิติต่าง ๆ และข้อเท็จจริงในทางปฏิบัติที่มีทั้งมิติของความลึกและมิติของความกว้างในเรื่องที่เกี่ยวข้องกับงานวิจัย เพื่อใช้เป็นข้อมูลในการวิเคราะห์และศึกษาปัจจัยสำคัญทำให้สามารถนำข้อมูลที่ได้มาวิเคราะห์หาแนวทาง และรูปแบบของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม ต่อไป

๓.๓ การสนทนากลุ่ม (Focus Group Discussion)

การสนทนากลุ่ม (Focus Group Discussion) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสนทนากลุ่มที่รวบรวมข้อมูลจากการสนทนากับกลุ่มผู้ให้ข้อมูลในประเด็นปัญหาโดยผู้วิจัยได้ออกแบบโครงสร้างของข้อคำถามเพื่อนำไปใช้ในการประชุมสนทนากลุ่มซึ่งการใช้กระบวนการการเลือกกลุ่มแบบเจาะจงในการสำรวจข้อมูล และเพื่อประมวลแนวคิดและสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม เพื่อใช้เป็นแนวทางในการปฏิบัติและเพื่อใช้เป็นแนวทางในการปฏิบัติของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ต่อไปในอนาคต

๓.๔ การสังเกตการณ์ (Observation)

การสังเกตการณ์ (In - Depth Interview and Observation) การสังเกตจากตัวนักวิจัยเองซึ่งเป็นผู้มีความรู้ และประสบการณ์ตรงด้านการบริหารจัดการ และการรับมือกับภัยคุกคามทางไซเบอร์ในระดับกองทัพไทย และในระดับประเทศมาเป็นเวลานานกว่า ๗ ปี และเพื่อหาข้อมูลของปัญหาในการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์แห่งชาติตลอดจนแนวทางในการดำเนินการที่เป็นรูปธรรม และมีประสิทธิภาพ และเพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคตซึ่งสามารถอธิบายขั้นตอนการวิจัยเพิ่มเติม จากกรอบแนวคิดในการวิจัยในหัวข้อต่อไป

๔. วิเคราะห์ข้อมูล

โดยใช้วิธีการวิเคราะห์ข้อมูลเชิงเนื้อหา (Content Analysis) ที่ได้จากกระบวนการดำเนินการวิจัยจากเอกสาร การสัมภาษณ์ การสังเกต และการสนทนากลุ่มเฉพาะ ซึ่งสามารถอธิบายขั้นตอนการวิเคราะห์ข้อมูลเชิงเนื้อหา ได้ดังนี้

๔.๑ จัดระเบียบข้อมูล (Data) ในรูปของบันทึกเป็นคำพูด นำมาถอดเทป และพิมพ์บันทึกสรุปใจความการสนทนากลุ่ม

๔.๒ พัฒนาข้อมูลไปสู่มโนทัศน์ (Concept) โดยการนำเสนอและแสดงข้อมูลเชิงพรรณนาซึ่งมาจากการกลั่นความคิดและหาความสัมพันธ์เชื่อมโยงของข้อมูลที่ถูกต้องและตรงประเด็นตามกรอบความคิด

๔.๓ จัดมโนทัศน์เข้าสู่หมวดหมู่ (Categories) โดยสรุปข้อมูลเป็นหมวดหมู่เพื่อจำแนกให้อยู่ในขอบเขตและครอบคลุมในประเด็นที่กำหนด เพื่อตอบวัตถุประสงค์ของการวิจัย

๔.๔ จัดทำข้อเสนอเชิงทฤษฎี (Proposal) ที่ได้จากการจัดกระบวนการกลุ่ม

๕. สรุปผลการศึกษา (ตอบคำถามวิจัย / วัตถุประสงค์การวิจัย)

การนำเสนอผลการวิจัย ผู้วิจัยนำเสนอผลการวิจัยโดยยึดวัตถุประสงค์การวิจัย จำนวน ๓ ข้อ ดังนี้

๕.๑ ตอบวัตถุประสงค์การวิจัย ข้อที่ ๑ เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๕.๒ ตอบวัตถุประสงค์การวิจัย ข้อที่ ๒ เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) แบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

๕.๓ ตอบวัตถุประสงค์การวิจัย ข้อที่ ๓ เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทยที่สามารถปฏิบัติงาน ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๖. สรุป อภิปรายผล และข้อเสนอแนะ

การอภิปรายผล โดยการนำผลที่ได้จากการเก็บข้อมูลวิจัยการดำเนินการวิจัย เอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่มเฉพาะ (Focus Group Discussion) และการสังเกตการณ์ (Observation) มาสรุป และอภิปรายผล เพื่อสามารถดำเนินการจัดทำข้อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center: NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ตลอดจนข้อเสนอแนะในการทำวิจัยครั้งต่อไป

ขอบเขตของการวิจัย

๑. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้มุ่งเน้นศึกษาถึงทฤษฎีและหลักการในการดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เอกสารงานวิจัยที่เกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ยุทธศาสตร์ด้านไซเบอร์ กฎหมายต่าง ๆ ที่เกี่ยวข้องในการปฏิบัติงานของเจ้าหน้าที่ ข้อมูลพื้นฐานที่เกี่ยวกับศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์และศูนย์ปฏิบัติการร่วมทางไซเบอร์ โครงสร้างการจัดระเบียบปฏิบัติ เพื่อนำข้อมูลที่รวบรวมได้ มาออกแบบสำหรับเป็นแนวทางในการดำเนินการตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับประเทศ

๒. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

กลุ่มตัวอย่าง การเลือกกลุ่มตัวอย่าง (Sampling) โดยเลือกกลุ่มตัวอย่างประเภทการเลือกกลุ่มตัวอย่างที่เป็นตัวแทน (Typing Cases Sampling) เป็นลักษณะการเลือกแบบเจาะจง (Purposive Sampling) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และผู้มีประสบการณ์ในด้านการบริหารจัดการหรือรับมือภัยคุกคามทางไซเบอร์มาแล้วเท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๘ ท่าน และสรรหาผู้เข้าร่วมในการสนทนากลุ่มอีกจำนวนประมาณ ๕ - ๑๐ ท่าน จากกลุ่มประชากรที่เกี่ยวข้องในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่ได้กำหนดให้มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ไว้จำนวน ๘ ประเภท

๓. ขอบเขตเวลา

ทำการศึกษาในช่วงตั้งแต่เดือน ธันวาคม ๒๕๖๓ ถึง พฤษภาคม ๒๕๖๔ ประชากรและกลุ่มตัวอย่าง

กลุ่มตัวอย่าง การเลือกกลุ่มตัวอย่าง (Sampling) โดยเลือกกลุ่มตัวอย่างประเภทการเลือกกลุ่มตัวอย่างที่เป็นตัวแทน (Typing Cases Sampling) เป็นลักษณะการเลือกแบบเจาะจง (Purposive Sampling) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และมีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์เท่านั้น การเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๘ ท่าน และการสนทนากลุ่ม จำนวน ๕-๑๐ ท่าน จากกลุ่มประชากรในการวิจัยได้ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

เครื่องมือที่ใช้ในการรวบรวมข้อมูลสำหรับการวิจัย

๑. การวิจัยจากเอกสาร (Documentary Research)

เป็นการทำการวิจัยจากเอกสารต่าง ๆ ที่เกี่ยวข้องกับหัวข้อการวิจัย เพื่อให้ได้มาซึ่งแนวคิดและทฤษฎีที่เกี่ยวข้องกับการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ตลอดจนหาแนวทางและองค์ความรู้เกี่ยวกับการจัดตั้งและการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC)

๒. การสัมภาษณ์เชิงลึก (In - Depth Interview)

การสัมภาษณ์เชิงลึก (In - Depth Interview) ประกอบด้วยประเด็นคำถามสำคัญ ๔ ข้อ เพื่อตอบปัญหาการวิจัยตามวัตถุประสงค์ที่ได้ตั้งไว้ ดังต่อไปนี้

๒.๑ หน่วยของท่านมีการรับมือภัยคุกคามทางไซเบอร์ยังไง และถ้าไม่สามารถรับมือหรือแก้ปัญหาภัยคุกคามทางไซเบอร์ได้ จะดำเนินการอย่างไรต่อ เพื่อตอบวัตถุประสงค์การวิจัยในหัวข้อของศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒.๒ ท่านคิดว่าอะไรคือปัญหา การจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมการและแบบแยกการ เพื่อตอบปัญหาการวิจัยในหัวข้อของการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ โดยแบ่งตามบุคลากร กระบวนการ และเทคโนโลยี

๒.๒.๑ บุคลากร (People) ทั้ง ผู้ปฏิบัติงาน และผู้บังคับบัญชา

๒.๒.๒ กระบวนการ (Process) และงบประมาณ (Budget)

๒.๒.๓ เทคโนโลยี (Technology)

๒.๓ ท่านคิดว่าทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) มีกี่แบบ แต่ละแบบมีข้อเด่นและข้อด้อยอย่างไร เพื่อตอบวัตถุประสงค์ของการวิจัยในหัวข้อของการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แต่ละแบบที่เคยมีมา

๒.๔ ท่านคิดว่าการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) ควรเป็นยังไง เพื่อตอบวัตถุประสงค์การวิจัยในหัวข้อของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๓. การประชุมสนทนากลุ่มเฉพาะ (Focus Group Discussion)

การประชุมสนทนากลุ่ม (Focus Group Discussion) ประกอบด้วยประเด็นคำถามสำคัญ ๓ ข้อ เพื่อตอบคำถามวิจัยเช่นเดียวกับกระบวนการของการสัมภาษณ์เชิงลึก (In - Depth Interview) แต่จะเน้นการสนทนาเพื่อแสดงความคิดเห็นร่วมกัน และการเล่าประสบการณ์ของผู้เชี่ยวชาญที่มีประสบการณ์ในการรับมือทางไซเบอร์ในระดับหน่วย ตลอดจนระดับประเทศ ได้แก่

๓.๑ หน่วยงานของท่านมีการรับมือภัยคุกคามทางไซเบอร์ยังไง และการส่งเหตุการณ์ภัยคุกคามทางไซเบอร์ต่อเพื่อดำเนินการแก้ไขปัญหา อย่างไร และมีการประสานความร่วมมือกับหน่วยไหนบ้าง เพื่อตอบคำถามวิจัยตามวัตถุประสงค์การวิจัยในหัวข้อของศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติในระดับหน่วยและระดับประเทศ

๓.๒ ท่านคิดว่าปัญหา การจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมการและแบบแยกการ หรือในหน่วยงานของท่านมีอุปสรรคด้านไหนบ้างที่ส่งผลให้การดำเนินงานของการรับมือภัยคุกคามทางไซเบอร์ไม่มีประสิทธิภาพ เพื่อตอบตามวัตถุประสงค์การวิจัยในหัวข้อการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่างตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ

๓.๒.๑ ด้านบุคลากร (People) ทั้ง ผู้ปฏิบัติงาน และผู้บังคับบัญชา

๓.๒.๒ ด้านกระบวนการ (Process) และงบประมาณ (Budget)

๓.๒.๓ ด้านเทคโนโลยี (Technology)

๓.๓ การจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) มีกี่แบบ แต่ละแบบมีจุดเด่น จุดด้อยอะไรบ้าง ประสิทธิภาพ เพื่อตอบปัญหาการวิจัยในหัวข้อการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในกรณีที่ผู้เข้าร่วมประชุมสนทนาเฉพาะกลุ่ม เสนอแนะการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาตินอกเหนือจากแบบรวมการและแบบแยกการ

๓.๔ การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) ที่เป็นรูปธรรม และสามารนำมาปฏิบัติได้จริง ควรเป็นอย่างไร และอุปสรรคเกิดจากอะไร ที่ส่งผลให้ไม่สามารถดำเนินการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ในระดับประเทศได้ เพื่อตอบวัตถุประสงค์ของการวิจัยในหัวข้อการเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๔. การเก็บรวบรวมข้อมูลจากสังเกตุ

มีวิธีดำเนินการเก็บรวบรวมข้อมูล โดยการสังเกตจากตัวนักวิจัยเอง ซึ่งมีความรู้และประสบการณ์ ด้านการจัดการภัยคุกคามทางไซเบอร์ในระดับกองทัพไทยและระดับประเทศ จาก ๒ สถานการณ์ ดังนี้

๔.๑ การสังเกตจากการปฏิบัติงานจริงด้านการรับมือและจัดการภัยคุกคามทางไซเบอร์ของกองบัญชาการกองทัพไทยและกองทัพไทย ซึ่งถือเป็นหน่วยงานที่ถูกกำหนดให้เป็นสาธารณูปโภคพื้นฐานสำคัญของประเทศ

๔.๒ การสังเกตจากการฝึกการปฏิบัติการทางไซเบอร์ประจำปีของกองทัพไทย ซึ่งกองบัญชาการกองทัพไทยได้จัดมาอย่างต่อเนื่องเป็นเวลา ๕ ปี ซึ่งเป็นการฝึกการปฏิบัติการและแก้ไขสถานการณ์ด้านไซเบอร์ทั้งในระดับกองทัพไทย ร่วมกับหน่วยงานที่เกี่ยวข้องที่สำคัญทั้งหมดในระดับประเทศ

การวิเคราะห์ข้อมูล

๑. วิเคราะห์ข้อมูลเชิงคุณภาพ

การวิเคราะห์ข้อมูลวิจัยเรื่อง แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม เป็นการวิเคราะห์ข้อมูลเชิงคุณภาพ โดยการนำข้อมูลเชิงเอกสารที่เกี่ยวข้องกับแนวทางการตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) การสัมภาษณ์เชิงลึก (In - Depth Interview) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และมีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์ และการสังเกตจากตัวนักวิจัย รวมถึงสนทนากลุ่ม (Focus Group Discussion) ซึ่งจากการเก็บข้อมูลทั้ง ๓ ส่วน จะทำให้ได้ข้อมูลในมุมมองของความเป็นมา ปัญหา การเปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสีย ของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ เพื่อให้ได้แนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๒. การอภิปรายผลร่วมกับผู้เชี่ยวชาญ

หลังจากการวิเคราะห์และสังเคราะห์ข้อมูลที่ได้จากการเก็บข้อมูลทั้งจากการทบทวนข้อมูลเชิงเอกสาร การสัมภาษณ์เชิงลึก การสังเกตการณ์แบบมีส่วนร่วม และการสนทนากลุ่ม ผู้วิจัยได้นำข้อมูลที่ได้ไปทำการสัมภาษณ์ผู้เชี่ยวชาญที่มีส่วนเกี่ยวข้องกับบริบทของงานวิจัยนี้อีกครั้ง เพื่อร่วมอภิปรายถึงประเด็นเกี่ยวกับแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ว่าเห็นด้วยกับผลการศึกษาหรือไม่ อย่างไร พร้อมทั้งเสนอแนวทางในการพัฒนานาให้ดียิ่งขึ้น

สรุป

สรุปได้ว่าการศึกษาในบทที่ ๓ นั้น เป็นการศึกษาในรายละเอียดของขั้นตอนการวิจัย เพื่อให้ได้ทิศทางและแนวทางในการดำเนินการวิจัยที่ชัดเจน ก่อนที่จะเริ่มลงมือเก็บรวบรวมข้อมูล เพื่อนำมาใช้ในการวิจัยได้ตรงไปตามวัตถุประสงค์และคำถามวิจัย

บทที่ ๔
วิเคราะห์แนวทางในการจัดตั้งและการปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ

งานวิจัยฉบับนี้จัดทำขึ้นเพื่อศึกษาปัญหาและรูปแบบของการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ในระดับประเทศ ที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ปี พ.ศ. ๒๕๖๒ ตลอดจนศึกษาแนวทางการทำงานของศูนย์ปฏิบัติการทางไซเบอร์ในรูปแบบต่าง ๆ ที่ใช้กันอยู่ในระดับนานาชาติ และในท้ายที่สุดก็จะนำเสนอรูปแบบ ตลอดจนแนวทางในการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อการรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศสำหรับประเทศไทย ให้สามารถปฏิบัติงานได้จริงอย่างเป็นรูปธรรม และมีประสิทธิภาพ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ซึ่งในการวิจัยครั้งนี้ได้กำหนดให้มีวิธีการเก็บข้อมูลใน ๔ รูปแบบ ได้แก่ การวิจัยจากเอกสารและตำราทางทฤษฎีที่เกี่ยวข้อง (Documentary Research) การสัมภาษณ์เชิงลึก (In – Depth Interview) การสนทนากลุ่ม (Focus Group Discussion) และการสังเกตการณ์ (Observation) ซึ่งสามารถสรุปเป็นผลของการวิเคราะห์ภายหลังจากการเก็บข้อมูลทั้ง ๔ รูปแบบได้ ดังนี้

สรุปผลการวิเคราะห์ข้อมูล

๑. ผลการศึกษาจากเอกสารและตำราทางทฤษฎี ตลอดจนงานวิจัยที่เกี่ยวข้องหรือการวิจัยจากเอกสาร (Documentary Research)

การศึกษาจากเอกสารและตำราทางทฤษฎี ตลอดจนงานวิจัยที่เกี่ยวข้อง หรือการวิจัยเอกสาร (Documentary Research) เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ ๑ ศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทย ซึ่งการทบทวนข้อมูลเชิงเอกสารเกี่ยวกับแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในระดับหน่วยงานและในระดับประเทศ ตลอดจนวิเคราะห์จุดเด่นและจุดด้อยของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแต่ละประเภท โดยนำประเด็นคำถามจากตารางแบบสัมภาษณ์ และสนทนากลุ่มเฉพาะ ที่ได้ทำการพัฒนาขึ้นมาเป็นแนวทางในการเก็บข้อมูลและนำข้อมูลที่ได้ไปวิเคราะห์ เพื่อให้เกิดเป็นแนวทางการจัดตั้งศูนย์ปฏิบัติการ

ทางไซเบอร์แห่งชาติ (NCOC) ที่จะสามารถนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ระดับประเทศที่มีประสิทธิภาพ สามารถสรุปได้ ดังนี้

๑.๑ การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ อาจสามารถดำเนินการได้ใน ๒ รูปแบบหลัก ๆ ได้แก่

๑.๑.๑ แนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) แบบรวมการ (Centralize)

การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) โดยที่การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแบบรวมการนั้น มีการดำเนินการให้เกิดการส่งข้อมูลการจราจรมาจำนวนมหาศาลเพื่อเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ไปยังศูนย์กลางเฝ้าระวังภัยคุกคามทางไซเบอร์ ซึ่งในประเทศไทยได้เคยมีการริเริ่มที่จะนำเอาแนวคิดของการจัดตั้ง NCOC แบบรวมการ ซึ่งเป็นการดำเนินการของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (สพธอ. หรือ ETDA) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในอดีต ที่ได้มีการจัดทำโครงการระบบการป้องกันและติดตามรักษาความปลอดภัยทางไซเบอร์ สำหรับองค์กรและหน่วยงานของรัฐที่เรียกว่า ThaiCERT GMS (Government Monitoring System) ซึ่งถือว่าเป็นแนวคิดที่ดีที่มีความพยายามที่จะทำให้เกิดการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศขึ้น ทั้งนี้การดำเนินการในลักษณะดังกล่าว มีความจำเป็นที่จะต้องมีข้อมูลการจราจรทางคอมพิวเตอร์ในลักษณะของ Log files ที่มีจำนวนมากเพียงพอต่อการวิเคราะห์ และระบบตรวจจับภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ตลอดจนมีบุคลากรที่เชี่ยวชาญจำนวนมากเพียงพอในการวิเคราะห์ข้อมูล และดำเนินการแก้ไขปัญหาการถูกบุกรุกทางไซเบอร์ได้อย่างทันท่วงที แต่ข้อด้อยของการตั้ง NCOC แบบรวมการนั้น แต่ละหน่วยงานย่อย ๆ ที่ส่งข้อมูลที่เป็น Log files มายังระบบเฝ้าระวังและตรวจจับแบบรวมการนั้น มีข้อมูลที่สำคัญที่ส่งมาในลักษณะที่แตกต่างกัน มีกระบวนการในการป้องกันข้อมูลที่สำคัญของหน่วยงานของตนเองที่แตกต่างกัน ดังนั้นการส่งข้อมูลจราจรคอมพิวเตอร์หรือ Log files ของระบบต่าง ๆ ไปวิเคราะห์ ตรวจจับภัยคุกคามทางไซเบอร์ ที่จะนำไปสู่การแก้ปัญหาของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น (Cyber Incidents) อาจจะไม่ตรงจุดเท่าที่ควร และในปัจจุบันยังไม่มีอุปกรณ์ใด ๆ ที่จะสามารถวิเคราะห์ภัยคุกคามจากข้อมูลการจราจรคอมพิวเตอร์มหาศาลได้อย่างแม่นยำ เช่น การนำระบบ SIEM (Security Information and Event Management) มาเป็นระบบหลักในการจัดเก็บ และวิเคราะห์ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระบบเครือข่ายสารสนเทศในลักษณะของ Information Technologies (IT) Operational Technologies (OT) หรือระบบ Internet of Things (IOT) ขององค์กร เพื่อนำข้อมูลเหล่านั้นไปใช้ในการแก้ไขและโต้ตอบ การถูกโจมตีหรือการถูกบุกรุกทางไซเบอร์ที่เกิดขึ้นในองค์กรได้อย่างเที่ยงตรงแม่นยำและมีประสิทธิภาพได้นั้น เป็นไปได้น้อยมาก จากปัจจัยต่าง ๆ ที่จะต้องนำมาร่วมในการวิเคราะห์อีกมากมาย ซึ่งในความเป็นจริงแล้วระบบ SIEM นั้น เป็นระบบที่ถูกออกแบบขึ้นมาให้มีความเหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรหรือ Log files ที่ถูกส่งมาจากหน่วยงานที่มีขนาดไม่ใหญ่มากเพียง

หน่วยงานเดียว หรือหน่วยงานระดับเล็ก ๆ ร่วมกันไม่กี่หน่วยงาน ที่จะสามารถนำ Log files ที่ได้รับมาแบบที่มีข้อมูลไม่มากจนเกินไป ที่จะทำให้สามารถวิเคราะห์ภัยคุกคามได้อย่างถูกต้องแม่นยำ และนำไปสู่การแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๑.๑.๒ แนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) แบบแยกการ (Decentralize)

การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ NCOC แบบแยกการ (Decentralize) ซึ่งอาจจะเป็นการดำเนินการโดยให้แต่ละกลุ่มงานที่มีลักษณะของการดำเนินการที่คล้ายกัน ตามลักษณะของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ให้ดำเนินการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของกลุ่ม หรือของหน่วยงานของตนเอง (Joint Cybersecurity Operations Center : JCOC) หรืออาจจะลงลึกถึงหน่วยงานของตนเองที่อาจจะแยกดำเนินการออกไปเองเลยก็ได้ (Cyber Security Operations Center : CSOC) ถ้ามีความพร้อมทั้งด้านงบประมาณ และกำลังพลเชี่ยวชาญด้านไซเบอร์ ส่วนหน่วยกลางใหญ่หรือ NCOC เป็นเพียงแค่การกระจายหรือแชร์ข้อมูลด้านไซเบอร์ที่สำคัญร่วมกันเท่านั้น ซึ่งการดำเนินการในลักษณะนี้อาจสามารถแก้ปัญหาและรับมือภัยคุกคามทางไซเบอร์ในเชิงลึกได้มากกว่า แต่อาจจะต้องใช้เวลาในการสร้างศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (CSOC) ของแต่ละหน่วยงานย่อย ๆ ของแต่ละ Sector ที่จะต้องดำเนินการภายใต้ JCOC ให้มีความพร้อมทั้งด้านบุคลากรทางไซเบอร์ ระบบการบริหารจัดการ และระบบเทคโนโลยีต่าง ๆ ที่จะเลือกมาใช้ในการดำเนินการ ซึ่งปัญหาใหญ่มักจะอยู่ที่การขาดแคลนบุคลากรด้านไซเบอร์ที่จะมาเป็นผู้ควบคุมระบบต่าง ๆ ให้สามารถดำเนินการได้จริงอย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่จะใช้ในการพิจารณาจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ประกอบด้วย ๓ ส่วนหลัก คือ คน (People) ซึ่งถือเป็นปัจจัยที่สำคัญที่สุดที่จะต้องมีบุคลากรที่มีความรู้และประสบการณ์ ที่คอยเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับลูกค้าหรือผู้ใช้งานระบบสารสนเทศรูปแบบต่าง ๆ ของหน่วยงานตลอด ๒๔ ชั่วโมง ตลอดทั้ง ๗ วัน หรือเรียกกว่า ๒๔ × ๗, กระบวนการหรือแนวทางในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร (Process) มีขั้นตอนการทำงานที่ได้มาตรฐาน เริ่มตั้งแต่ การทำความเข้าใจกับระบบของตนเองและภัยคุกคามต่าง ๆ ทางไซเบอร์ ที่จะเกิดขึ้นกับระบบดังกล่าว (Identify) การป้องกัน (Protect) การเฝ้าระวังและตรวจจับ (Detect) การรับมือและแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้น (Response) และการฟื้นฟูระบบให้กลับขึ้นมาใช้ใหม่ได้กรณีที่ไม่สามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้ (Recovery) ตลอดจนต้องมีการปรับปรุงสิ่งต่าง ๆ (Improve) ให้มีความทันสมัยอยู่ตลอดเวลา ให้เท่าทันกับรูปแบบภัยคุกคามใหม่ ๆ และเทคโนโลยีใหม่ ๆ ที่มีการเปลี่ยนแปลงไปอย่างรวดเร็ว และท้ายสุดคือ ปัจจัยด้านเทคโนโลยี (Technology) ซึ่งมีมากมายหลายหลาก ซึ่งจำเป็นจะต้องมีการออกแบบให้เหมาะสมกับองค์กรของแต่ละองค์กร (Enterprise Cybersecurity Architecture) ที่ไม่จำเป็นต้องเหมือนกัน เพราะแต่ละองค์กรมีปัจจัยที่จะสนับสนุนที่ไม่เท่ากันและไม่เหมือนกัน

การตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ แบบแยกการจะสามารถนำไปสู่การแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับองค์กรได้อย่างเป็นรูปธรรมมากกว่า เนื่องจากจะสามารถมองเห็นภัยคุกคามต่าง ๆ ที่เกิดขึ้นในระบบได้อย่างแท้จริง และทีมงานที่ประกอบด้วยส่วนควบคุมบังคับบัญชา (Command Center) ส่วนป้องกัน (Protection) ส่วนเฝ้าระวังตรวจจับ (Cyber Security Operations Center : CSOC) ส่วนรับมือและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ (Incident Response Teams) ส่วนพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Teams) ส่วนงานข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence : CTI) ส่วนดำเนินการก่อนการเกิดเหตุการณ์ทางไซเบอร์ (Proactive Team : Digital Auditing, Penetration Testing Teams) จะเป็นทีมที่มีความเข้าใจกับระบบเครือข่ายของตนเองได้ดี ที่จะสามารถเข้าใจและนำไปสู่การแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระบบของตนเองได้ดีกว่า การดำเนินการแบบรวมการซึ่งจะต้องส่งข้อมูล (Log files) ไปให้คนในส่วนกลางซึ่งไม่มีความเข้าใจในระบบเครือข่ายสารสนเทศขององค์กรเป็นผู้วิเคราะห์ให้

๒. ผลจากการสัมภาษณ์เชิงลึก (In - Depth Interview)

จากผลการวิจัยในส่วนของเก็บข้อมูลการสัมภาษณ์เชิงลึก (In - Depth Interview) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสัมภาษณ์กลุ่มเป้าหมาย ทั้งผู้เชี่ยวชาญ ผู้บริหารและผู้มีประสบการณ์ ที่เกี่ยวข้องเฉพาะกับการรับมือภัยคุกคามทางไซเบอร์ จำนวน ๗ ท่าน ประกอบด้วย

ตารางที่ ๔ - ๑ รายชื่อผู้ให้สัมภาษณ์เชิงลึก (In - Depth Interview)

รายชื่อผู้ให้สัมภาษณ์	**ตำแหน่ง**
พล.ต. นภดล แก้วกำเนิด	ผอ.ศดม.กอ.รมน.
พล.อ.ต. สมพร ร่มพยอม	ผอ.ศซบ.ทอ.
พ.อ. พงศ์พัฒน์ ขันธเขตต์	ฝสธ.ศดม.กอ.รมน.
น.อ. จเด็ด คูหะก้องกิจ	ผอ.กยข.ศซบ.ทหาร
พ.ต.ท. กัมพล พงษ์แสงศรี	รรท. รอง ผกก. กลุ่มงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ บช.สอท.
พ.ต.ท. พรชัย โฆษิตสุรังคกุล	รรท. รอง ผกก. กลุ่มงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ บช.สอท.
พ.ต.ต. จตุพร อรุณฤทษ์ถวิล	ผอ.ส่วนคดีและเทคโนโลยีสารสนเทศ ๑ กรมสอบสวนคดีพิเศษ

๒.๑ แบบคำถามการเก็บข้อมูลเชิงลึก (In - Depth Interview)

เป็นการเก็บข้อมูลเชิงลึก โดยการสัมภาษณ์เฉพาะกลุ่มที่มีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์จริง ๆ เท่านั้น ซึ่งเป็นตัวแทนของโครงสร้างพื้นฐาน (CII) ของประเทศ โดยการนำ

ความคิดเห็นของผู้เข้าร่วมสัมภาษณ์แต่ละท่าน มาสรุปในภาพรวมจากการศึกษาข้อมูลในส่วนนี้ จะสามารถนำไปสู่การสรุปประเด็นสำคัญตามวัตถุประสงค์การวิจัย และจากแบบคำถามการวิจัย ประกอบด้วยประเด็นคำถามสำคัญ ๔ ข้อ เพื่อตอบปัญหาการวิจัยตามวัตถุประสงค์ที่ได้ตั้งไว้ ดังต่อไปนี้

๒.๑.๑ หน่วยงานของท่านมีแนวทางในการรับมือภัยคุกคามทางไซเบอร์อย่างไร และถ้าหากไม่สามารถรับมือหรือแก้ปัญหาภัยคุกคามทางไซเบอร์ได้ หน่วยงานของท่านมีแนวทางที่จะดำเนินการอย่างไรต่อไป เพื่อตอบวัตถุประสงค์การวิจัยในหัวข้อของศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒.๑.๒ ท่านคิดว่าอะไรคือปัญหาของการจัดตั้งศูนย์บริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) ทั้งแบบรวมการและแบบแยกการ เพื่อตอบปัญหาการวิจัยในหัวข้อของการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ โดยแบ่งตามบุคลากร กระบวนการ และเทคโนโลยี

๒.๑.๒.๑ บุคลากร (People) ทั้ง ผู้ปฏิบัติงาน และผู้บังคับบัญชา

๒.๑.๒.๒ กระบวนการ (Process) และงบประมาณ (Budget)

๒.๑.๒.๓ เทคโนโลยี (Technology)

๒.๑.๓ ท่านคิดว่าทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) ควรจะมีกี่แบบ แต่ละแบบมีข้อเด่น ข้อด้อย อย่างไร เพื่อตอบวัตถุประสงค์ของการวิจัยในหัวข้อของการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของ ศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แต่ละแบบที่เคยมีมาในอดีต

๒.๑.๔ ท่านคิดว่าแนวทางในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติเพื่อที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) ได้อย่างแท้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ ควรเป็นอย่างไร เพื่อตอบวัตถุประสงค์การวิจัยในหัวข้อของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

๒.๒ ผลการสัมภาษณ์เชิงลึก (In - Depth Interview)

ผลการสัมภาษณ์เชิงลึก เป็นลักษณะของการนำผลการสัมภาษณ์แต่ละท่านมาดำเนินการวิเคราะห์ผล และสรุปในภาพรวมให้สอดคล้องกับวัตถุประสงค์ของการวิจัย ซึ่งสามารถสรุปได้ดังนี้

๒.๒.๑ ศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ของประเทศไทยในห้วงที่ผ่านมา ซึ่งได้พบปัญหาและข้อจำกัด โดยสามารถแบ่งออกเป็น ๓ ด้าน ได้แก่

๒.๒.๑.๑ ด้านบุคลากร (People) เนื่องจากบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีการขาดแคลนจำนวนมาก โดยเฉพาะบุคลากรที่มีความเชี่ยวชาญ ซึ่งพบว่ามีการถูกดึงตัวบุคลากรกลุ่มดังกล่าว โดยมีการเสนอค่าตอบแทน สวัสดิการสูง เพื่อชักจูงให้การมาร่วมงานด้วย ซึ่งการที่หน่วยงานของภาครัฐให้ค่าตอบแทนที่น้อย ส่งผลให้บุคลากรที่มีความเชี่ยวชาญที่อยู่ในหน่วยงานของภาครัฐทยอยลาออก เพื่อไปรับค่าตอบแทนที่สูงกว่าเป็นจำนวนมาก ส่งผลให้หน่วยงานของภาครัฐเริ่มขาดแคลนบุคลากรกลุ่มนี้ การดำเนินการสร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยการเปิดโรงเรียนสอน เพื่อสร้างบุคคลากรความมั่นคงทางไซเบอร์น่าจะเป็นแนวทางในการแก้ไขปัญหาการขาดแคลนบุคลากรด้านไซเบอร์ได้ดี แต่ในความเป็นจริงแล้วไม่ใช่ทุกคนที่จะสามารถพัฒนาตัวเองเป็นผู้เชี่ยวชาญ และสามารถปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ดีในเวลาอันสั้น จำเป็นต้องใช้ระยะเวลาในการผลิตบุคลากรด้านความปลอดภัยทางไซเบอร์ และผ่านการฝึกฝนในการปฏิบัติการจริง จากนั้นควรจะมีการสอบให้ผ่านการได้รับใบ International Cybersecurity Certification ตามงานในหน้าที่ของตนเองให้สูงขึ้นเรื่อย ๆ

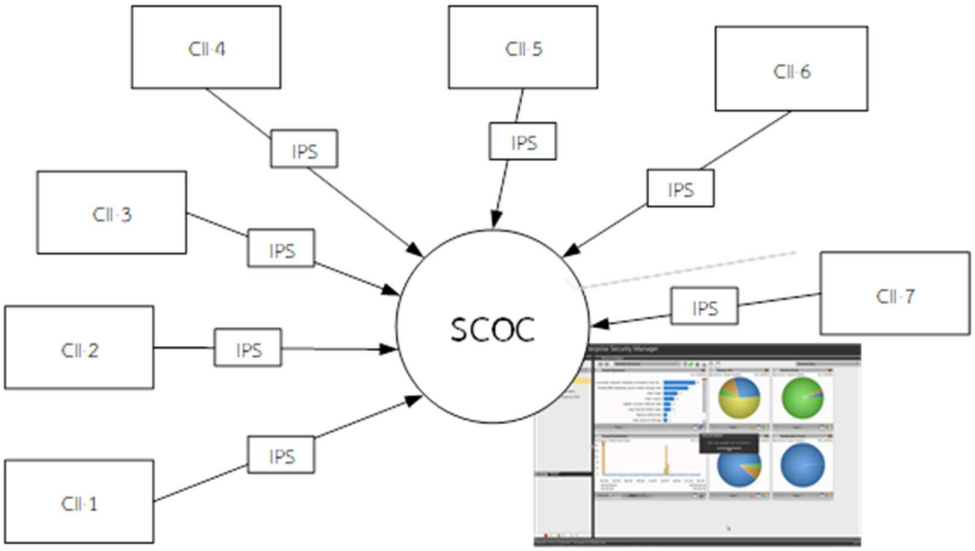
๒.๒.๑.๒ ด้านกระบวนการ (Process) มีความจำเป็นไม่น้อยกว่าด้านบุคลากรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ มีจำนวนหน่วยงานจำนวนมากที่มีการดำเนินงานที่ต่างกัน และจำนวนของข้อมูลการจราจรคอมพิวเตอร์ (Log files) มหาศาล จำเป็นต้องดำเนินการสร้างกระบวนการ และเลือกรูปประเภทของการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ซึ่งต้องมีการประชุมหารือเพื่อออกแบบแนวทางที่จะทำให้เกิดการทำงานที่จะได้ประโยชน์ร่วมกัน ในลักษณะของการพึ่งพาอาศัยกันจากตัวแทนของหลายหน่วยงานจากแต่ละกลุ่มธุรกิจหรือกลุ่มงานที่มีลักษณะของการดำเนินการคล้ายกันในแต่ละกลุ่มสาธารณูปโภคพื้นฐานที่สำคัญของประเทศ (CII) ซึ่งอาจรวมถึงบุคลากรที่มีความเชี่ยวชาญในสายงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อวิเคราะห์หาจุดอ่อน จุดแข็ง และข้อจำกัดในหลากหลายมุมมองของหลาย ๆ Sectors หรือหลาย ๆ กลุ่มงาน ให้ครบทุกมิติ เพื่อลดความเสี่ยงของผลกระทบให้เหลือน้อยที่สุด และมีประโยชน์สูงสุดต่อส่วนรวม หรือส่วนใหญ่ของประเทศ เพื่อที่จะทำให้เกิดความเข้าใจในแนวทางของการดำเนินการ และสามารถใช้อธิบายต่อผู้บริหารระดับสูงขององค์กร หรือแม้แต่ผู้บริหารระดับประเทศ เพื่อการขอรับการสนับสนุนงบประมาณในการลงทุนและการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งการทำอธิบายให้ผู้บริหาระดับสูงเกิดความเข้าใจและให้การสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น ต้องใช้เวลาค่อนข้างนานกว่าปกติ เพราะเรื่องของการรักษาความมั่นคงปลอดภัยจากคุกคามทางไซเบอร์นั้นเป็นเรื่องที่ค่อนข้างจะเข้าใจได้ยาก ซึ่งส่วนใหญ่แล้วผู้บังคับบัญชาหรือผู้บริหารระดับสูงที่ไม่ได้คลุกคลีหรือมีความรู้ในสายงานด้านสารสนเทศหรือการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาก่อน อาจจะต้องใช้เวลาในการทำความเข้าใจกันมากพอสมควร หรือต้องใช้การอธิบายหลาย ๆ ครั้ง จนกว่าจะเข้าใจ

๒.๒.๑.๓ ด้านเทคโนโลยี (Technologies) ทั้งนี้ ปัจจุบันยังไม่มีเทคโนโลยีหรืออุปกรณ์ด้านเทคโนโลยีสารสนเทศใด ๆ ที่สามารถทำหน้าที่วิเคราะห์ภัยคุกคามทางไซเบอร์จากข้อมูลการจราจรคอมพิวเตอร์ (Log files) จำนวนมากได้อย่างแม่นยำ เช่น การนำระบบ SIEM (Security Information and Event Management) ที่เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยทางไซเบอร์จากข้อมูลที่เป็นลักษณะของ Log files จากระบบเครือข่ายสารสนเทศขององค์กรขนาดที่มีขนาดไม่ใหญ่มาก โดยที่จะนำข้อมูลเหล่านั้นไปใช้ในการวิเคราะห์หารูปแบบของการโจมตีทางไซเบอร์จากผู้ไม่หวังดี และหาแนวทางในการแก้ไขปัญหา หรือดำเนินการโต้ตอบตามการสั่งการของผู้บังคับบัญชาหรือผู้บริหารระดับสูงต่อไป ซึ่งในความเป็นจริงแล้วระบบ SIEM นั้นเป็นระบบที่เหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรที่มีจำนวนไม่มากนัก จากองค์กรหรือหน่วยงานเพียงหน่วยงานเดียว หรือหน่วยงานหลายหน่วยที่มีข้อมูลรวมกันแล้วไม่มากจนเกินไปที่จะวิเคราะห์ได้เท่านั้น ซึ่งถ้าต้องการนำเทคโนโลยีอย่างระบบ SIEM มาใช้ในการวิเคราะห์ภัยคุกคามในระดับประเทศหรือหลาย ๆ หน่วยในระดับ Sectors ของหน่วยงานที่เป็นเจ้าของระบบสาธารณูปโภคพื้นฐานสำคัญของประเทศ อาจจะต้องมีการแยกระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ออกเป็นหน่วยย่อย ๆ หรือแบ่งตามกลุ่มที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ในลักษณะเดียวกันเป็นกลุ่มเล็ก ๆ ที่ระบบจะสามารถรับข้อมูล Log files ที่ไม่มากจนเกินไป และสามารถนำข้อมูลของ Log files ดังกล่าวมาตรวจจับ และวิเคราะห์หาภัยคุกคามทางไซเบอร์ได้อย่างถูกต้อง และแม่นยำมากกว่าการส่งข้อมูลการจารจรในลักษณะของ Log files จากหลาย ๆ หน่วยงานไปวิเคราะห์ ณ จุด ๆ เดียวที่ทำหน้าที่ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แบบรวมการ

๒.๒.๒ ศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

ทั้งนี้ การจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการนั้นมีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรในลักษณะของ Log files จากทุก ๆ หน่วยงานที่มีระบบการป้องกัน เฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ไปยังหน่วยงานกลางที่ทำหน้าที่เฝ้าระวังภัยคุกคาม การรักษาความมั่นคงปลอดภัยทางไซเบอร์แบบเป็นศูนย์รวมเพียงที่เดียว ดังแผนภาพที่ ๔ - ๕

แผนภาพที่ ๔ - ๕ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ



ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

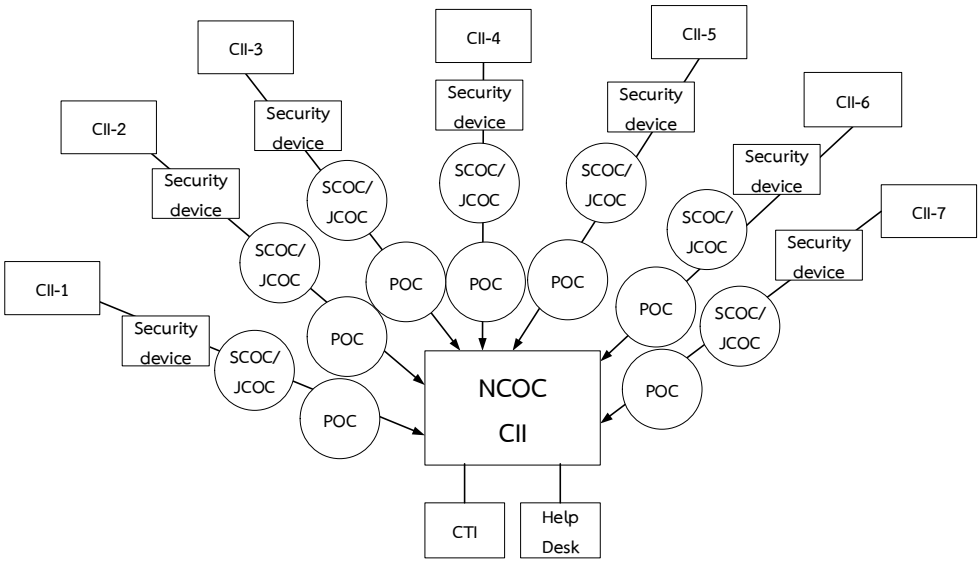
การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) ถือได้ว่าเป็นแนวคิดของความพยายามในการดำเนินการต่อภัยคุกคามทางไซเบอร์ที่ดีแนวทางหนึ่ง ซึ่งมีความพยายามที่จะทำให้เกิดการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศขึ้น โดยมีการออกแบบให้นำข้อมูลการจราจรทางคอมพิวเตอร์ในลักษณะของ Log files จากอุปกรณ์ป้องกันการบุกรุกทางไซเบอร์ หรือ Intrusion Protection System (IPS) จากหลาย ๆ หน่วยงาน ส่งไปยังระบบ SIEM ของหน่วยงานกลางที่ทำหน้าที่เป็นศูนย์กลางในการบริหารจัดการภัยคุกคามทางไซเบอร์ ที่มีระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ แต่ปัญหาคือ ระบบที่จะทำหน้าที่วิเคราะห์และประมวลผลข้อมูลจราจรทางคอมพิวเตอร์ในลักษณะของ Log files จำนวนมหาศาลที่ถูกส่งมาจากหน่วยงานที่มีความหลากหลายทางธุรกิจ หรือการจัดรูปแบบของระบบเครือข่ายสารสนเทศที่นำมาใช้ในเชิงธุรกิจที่แตกต่างกัน ให้สามารถตรวจจับและแจ้งเตือนภัยคุกคามทางไซเบอร์ได้อย่างแม่นยำนั้นมีความเป็นไปได้ยากมาก

ตลอดจนบุคลากรที่มีเชี่ยวชาญและจะทำหน้าที่วิเคราะห์ผลจากการแจ้งเตือนจากระบบ SIEM กลับไปยังต้นทางของ Log files ซึ่งเป็นรูปแบบที่ผู้วิเคราะห์ไม่ได้เชี่ยวชาญในระบบเครือข่ายสารสนเทศของธุรกิจนั้น ๆ ทำให้ไม่สามารถวิเคราะห์ถึงสาเหตุที่แท้จริงที่เกิดขึ้นได้ อาจจะส่งผลต่อการดำเนินการแก้ไขปัญหาการถูกบุกรุกหรือการถูกโจมตีทางไซเบอร์ไม่สามารถดำเนินการได้จริงอย่างทันท่วงที ดังนั้นข้อด้อยของการตั้ง NCOC แบบรวมการ คือหน่วยงานต้นทางที่ส่งข้อมูลการจราจรในลักษณะของ Log file ของแต่ละหน่วยงานจะมีข้อมูลที่มีสำคัญและมีลักษณะของไฟล์ที่แสดงถึงการการดำเนินกิจการต่าง ๆ ของแต่ละองค์กร

หรือหน่วยงานที่แตกต่างกัน ดังนั้นเมื่อมีการส่งข้อมูลจราจรคอมพิวเตอร์ในลักษณะของ Log files ไปวิเคราะห์เพื่อตรวจจับภัยคุกคามทางไซเบอร์ หรือแม้แต่การแก้ปัญหาที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์อาจจะไม่ตรงจุดเท่าที่ควร และในปัจจุบันยังไม่มีอุปกรณ์ที่สามารถวิเคราะห์ภัยคุกคามจากข้อมูลการจราจรคอมพิวเตอร์มหาศาลได้อย่างแม่นยำ เช่น การนำระบบ SIEM (Security Information and Event Management) ที่เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร เพื่อนำข้อมูลเหล่านั้นไปใช้ในการโต้ตอบการโจมตีที่เกิดขึ้น ซึ่งในความเป็นจริงแล้วระบบ SIEM นั้นเป็นระบบที่เหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรเพียงหน่วยเดียวที่เป็นลักษณะของ Small/Medium Enterprise (SME) หรือมีข้อมูลไม่มากจนเกินไป

การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ (Decentralize) มีรูปแบบของสถาปัตยกรรมตาม แผนภาพที่ ๔ – ๖

แผนภาพที่ ๔ - ๖ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ



ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ (Decentralize) เป็นการดำเนินการโดยให้แต่ละกลุ่มที่มีการดำเนินการทางธุรกิจหรือรูปแบบขององค์กรที่คล้ายกัน อาจเป็นไปตามกลุ่มของหน่วยงานโครงสร้างพื้นฐานด้านสาธารณูปโภคสำคัญของประเทศ (CII) ในกลุ่มเดียวกัน ซึ่งจะสามารถดำเนินการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของกลุ่ม (Joint Cybersecurity Operations Center : JCOC) หรือของหน่วยงานของตนเอง (Cyber Security Operations Center : CSOC) หรืออาจจะลงลึกถึงหน่วยงานตนเองที่สามารถแยกดำเนินการได้เอง ซึ่งอาจจะขึ้นอยู่กับว่าหน่วยงานใด มีความพร้อมทั้งด้านงบประมาณและบุคลากรที่มีความเชี่ยวชาญด้านความปลอดภัยการรักษาความมั่นคงปลอดภัย

ทางไซเบอร์ โดยหน่วยงานกลางของประเทศที่ทำหน้าที่เป็น NCOC หรือแต่ละกลุ่มตาม CII ที่มีการจัดตั้ง JCOC อาจทำหน้าที่เป็นเพียงแค่ศูนย์การกระจายหรือแชร์ข้อมูลด้านไซเบอร์ที่สำคัญร่วมกันเท่านั้น ซึ่งการดำเนินการในลักษณะนี้อาจสามารถแก้ปัญหาและรับมือภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพในเชิงลึกได้มากกว่า แต่อาจจะต้องใช้เวลาในการสร้างศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับองค์กรขนาดย่อย ๆ ลงไป (CSOC) ให้มีความพร้อมทั้งด้านบุคลากรด้านระบบการบริหารจัดการ และระบบเทคโนโลยีต่าง ๆ ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่จะมีการเลือกมาใช้ในการดำเนินการ ซึ่งปัญหาใหญ่มักจะอยู่ที่การขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่จะมาเป็นผู้ควบคุมระบบต่าง ๆ ให้สามารถดำเนินการได้จริงอย่างมีประสิทธิภาพ ซึ่งอาจจะต้องเป็นหน้าที่ของรัฐบาลที่จะต้องสนับสนุนให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทำหน้าที่เป็นศูนย์กลางในการผลิตบุคลากรด้านไซเบอร์ให้กับประเทศ หรือส่งเสริมให้สถาบันการศึกษาในระดับอุดมศึกษาให้สามารถผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับประเทศได้ด้วย

๒.๒.๓ เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ซึ่งจากผลการวิจัยของตอบวัตถุประสงค์การวิจัย ข้อที่ ๒ เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการ และแยกการ พบว่าแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์ทั้งแบบรวมการ (Centralize) และแบบแยกการ (Decentralize) สามารถเป็นกลไกหลักในระดับประเทศในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ ทั้งก่อนระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) แต่การที่จะดำเนินการรับมือและแก้ไขปัญหาได้ตรงกับความสามารถของเทคโนโลยีในการเฝ้าระวังตรวจจับ ตลอดจนความสามารถใน การแก้ไขปัญหาได้ในเชิงลึก และการดำเนินการแก้ไขปัญหาในกลุ่ม CII ที่เหมือนกัน การดำเนินการจัดตั้ง NCOC แบบแยกการจะสามารถดำเนินการได้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพมากกว่าแบบรวมการ

๓. ผลจากการสนทนากลุ่ม (Focus Group Discussion)

การสนทนากลุ่ม (Focus Group) ใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสนทนากลุ่มที่รวบรวมข้อมูลจากการสนทนากับกลุ่มผู้ให้ข้อมูลเฉพาะในประเด็นปัญหาที่ต้องการทราบถึงแนวคิดของกลุ่มเป้าหมายที่เป็นเจ้าหน้าที่ผู้เชี่ยวชาญ หรือผู้บริหาร เฉพาะที่มีความรู้ ความสามารถ และมีประสบการณ์ในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จากตัวแทนของหน่วยงานที่เป็นโครงสร้างพื้นฐานด้านสาธารณูปโภคที่สำคัญของประเทศ (Critical Information Infrastructure : CII) จำนวน ๑๐ ท่าน ประกอบด้วย

ตารางที่ ๔ - ๒ รายชื่อผู้เข้าร่วมการสนทนากลุ่ม (Focus Group)

รายชื่อผู้เข้าร่วมการสนทนากลุ่ม	ตำแหน่ง
พล.ต. นภดล แก้วกำเนิด	ผอ.ศดม.กอ.รมน.
พล.อ.ต. สมพร ร่มพยอม	ผอ.ศซบ.ทอ.
พ.อ. พงศ์พัฒน์ ขันธเขตต์	ฝสธ.ศดม.กอ.รมน.
น.อ. จเด็ด คูหะก้องกิจ	ผอ.กยข.ศซบ.ทหาร
พ.ต.ท. กัมพล พงษ์แสงศรี	รรท. รองผกก. กลุ่มงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ บช.สอท.
พ.ต.ท. พรชัย โฆษิตสุรังคกุล	รรท. รองผกก. กลุ่มงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ บช.สอท.
พ.ต.ต. จตุพร อรุณฤทษ์ถวิล	ผอ.ส่วนคดีและเทคโนโลยีสารสนเทศ ๑ กรมสอบสวนคดีพิเศษ
นายทินกฤต ไชยขันธุ์	นักการข่าวชำนาญการ
นายธีรยุทธ ธีรประถัมภ์	นักการข่าวชำนาญการ

ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

ผู้วิจัยได้นำข้อมูลในทุกมิติมาวิเคราะห์จนสามารถกำหนดแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center: NCOC) ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ปี พ.ศ.๒๕๖๒ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม และระดับองค์กรที่ถือว่าเป็นสาธารณูปโภคสำคัญของประเทศ

๓.๑ คำถามการประชุมสนทนากลุ่ม (Focus Group Discussion)

การประชุมสนทนากลุ่ม (Focus Group Discussion) ประกอบด้วยประเด็นคำถามสำคัญ ๔ ข้อ เพื่อตอบคำถามวิจัยเช่นเดียวกับกระบวนการของการสัมภาษณ์เชิงลึก (In - Depth Interview) แต่จะเน้นการสนทนาเพื่อแสดงความคิดเห็นร่วมกัน และการเล่าประสบการณ์ของผู้เชี่ยวชาญที่มีประสบการณ์ในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับหน่วยงานของตนเอง และในระดับประเทศ ได้แก่

๓.๑.๑ หน่วยงานของท่านมีแนวทางในการรับมือภัยคุกคามทางไซเบอร์อย่างไร และการส่งต่อเหตุการณ์ภัยคุกคามทางไซเบอร์กรณีที่หน่วยงานของตนเองไม่สามารถแก้ไขปัญหาทางไซเบอร์ได้ด้วยตนเอง เพื่อดำเนินการแก้ไขปัญหาต่อไปอย่างไร และมีการประสานความร่วมมือกับหน่วยงานใดบ้าง เพื่อตอบคำถามวิจัยตามวัตถุประสงค์การวิจัยในหัวข้อของศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ

๓.๑.๒ ท่านคิดว่าปัญหาของการจัดตั้งหน่วยงานกลางที่จะทำหน้าที่ในการบริหารจัดการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศของประเทศไทย (NCOC) ควรจะเป็นไปในลักษณะของการดำเนินแบบรวมการที่มีหน่วยงานกลางหน่วยงานเดียวทำหน้าที่ให้เกิดการบูรณาการในการดำเนินการทั้งก่อน ระหว่างและหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cyber Incidents) หรือควรจะเป็นการดำเนินการแบบแยกการตามลักษณะของกลุ่มงานสาธารณูปโภคพื้นฐานที่สำคัญของประเทศ หรือแยกการไปตามความพร้อมของแต่ละหน่วยงาน และหน่วยงานของท่านมีอุปสรรคด้านไหนบ้างที่ส่งผลให้การดำเนินงานของการรับมือภัยคุกคามทางไซเบอร์ไม่มีประสิทธิภาพ เพื่อตอบตามวัตถุประสงค์การวิจัยในหัวข้อการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่างตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแยกการ

๓.๑.๒.๑ ด้านบุคลากร (People) ทั้ง ผู้ปฏิบัติงาน และผู้บังคับบัญชาหรือผู้บริหารระดับสูง

๓.๑.๒.๒ ด้านกระบวนการ (Process) และงบประมาณ (Budget)

๓.๑.๒.๓ ด้านเทคโนโลยี (Technology)

๓.๑.๓ ทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) มีกี่แบบ แต่ละแบบมีจุดเด่น จุดด้อยอะไรบ้าง ประสิทธิภาพ เพื่อตอบปัญหาการวิจัยในหัวข้อการศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดี และข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในกรณีที่ผู้เข้าร่วมประชุมสนทนาเฉพาะกลุ่ม อาจมีข้อเสนอแนะการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติในรูปแบบที่นอกเหนือไปจากการดำเนินการแบบรวมการ และการดำเนินการแบบแยกการ

๓.๑.๔ การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ (NCOC) ที่เป็นรูปธรรม และสามารถนำมาปฏิบัติได้จริงอย่างมีประสิทธิภาพควรเป็นอย่างไร และอุปสรรคสำคัญเกิดจากอะไร ที่ส่งผลให้ไม่สามารถดำเนินการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ในระดับประเทศที่สามารถดำเนินการแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นจริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ เพื่อตอบวัตถุประสงค์ของการวิจัยในหัวข้อการเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ โดยมีการพูดคุยและถกแถลงกันถึงปัญหา และข้อเสนอแนะแนวทางในการรับมือภัยคุกคามทางไซเบอร์ในระดับหน่วยและในระดับประเทศ จากผู้มีประสบการณ์ในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และการรับมือกับภัยคุกคามทางไซเบอร์ทั้งในระดับหน่วยงานและในระดับประเทศ ซึ่งผลของการสนทนากลุ่ม (Focus Group Discussion) สามารถสรุปได้ดังนี้

๓.๑.๔.๑ หน่วยที่มีความพร้อมในการเฝ้าระวังภัยคุกคามทางไซเบอร์สามารถเฝ้าระวังภัยคุกคามของหน่วยของตนเอง หรือสามารถช่วยเฝ้าระวังภัยคุกคามหน่วยงานอื่นที่มี

การทำงาน บริการที่คล้ายกัน แต่ไม่ควรเฝ้าระวังภัยคุกคามหน่วยงานที่มีลักษณะของการทำงานหรือให้การบริการที่ไม่เหมือนกัน เนื่องจากไม่มีความรู้เพียงพอในการวิเคราะห์ข้าม Sectors หรือรูปแบบของการดำเนินการทางธุรกิจ ตลอดจนการวางเครือข่ายของการให้การบริการที่ไม่เหมือนกัน เช่น หน่วยงานด้านความมั่นคงฯ ของทหาร ไม่สามารถเฝ้าระวังให้กับระบบเครือข่ายทางเทคโนโลยีสารสนเทศของทางตำรวจได้ เนื่องจากทฤษฎีและรูปแบบของการทำงาน ตลอดจนวิธีคิดในการทำงานอาจมีหลายข้อที่มีวิธีคิดที่แตกต่างกันอย่างสิ้นเชิง เป็นต้น

๓.๑.๔.๒ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๒ ประเทศไทยได้มีการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แต่หัวใจของการดำเนินการและรับมือกับภัยคุกคามทางไซเบอร์ คือ ศูนย์ปฏิบัติการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ซึ่งจำเป็นจะต้องจัดรูปแบบโครงสร้างให้เป็นระดับไล่ลงมา ตั้งแต่ในระดับประเทศที่ควรจัดให้มี NCOC ในระดับสาธารณูปโภคขั้นพื้นฐานด้านสารสนเทศที่สำคัญของประเทศควรจัดให้มี JCOCs แยกเป็น Sectors และในระดับหน่วยงานสำคัญหลาย ๆ หน่วยอาจแยกไปตั้งเป็น CSOC เฉพาะของตนเองตามความสำคัญและความพร้อมของหน่วยงาน ซึ่งจะแบ่งเป็นระดับในการรับมือภัยกับคุกคามทางไซเบอร์แยกกันไป และถ้าไม่สามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ในระดับของตนเองได้ ก็สามารถส่งต่อปัญหาเหตุการณ์ทางไซเบอร์ไปยังส่วนอื่น ๆ ที่มีความสามารถเหนือกว่า หรือดำเนินการให้เกิดการแก้ปัญหาในลักษณะของการพึ่งพาอาศัยกันทั้งใน Sector ของตนเอง หรือข้าม Sector ได้เช่นกัน

๓.๑.๔.๒ การนำระบบ SIEM (Security Information and Event Management) ที่เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยทางไซเบอร์ของระบบเครือข่ายในระดับขององค์กรขนาดเล็กที่เป็นลักษณะของ Small/Medium Enterprise (SME) ไปใช้ในการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ในระดับประเทศหรือหลาย ๆ องค์กรพร้อม ๆ กันนั้นจะไม่สามารถเฝ้าระวังภัยคุกคามได้อย่างแท้จริง เนื่องจากในความเป็นจริงแล้วระบบ SIEM นั้นเป็นระบบที่ถูกออกแบบมาให้มีความเหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรในลักษณะของ Log files ที่ถูกส่งมาจากหน่วยงานที่เป็น SME เพียงหน่วยเดียว หรืออาจจะหลายหน่วยแต่จะต้องมีข้อมูลของ Log files ที่เป็นลักษณะของกลุ่มงานเดียวกันและมีจำนวนไม่มากจนเกินไปเท่านั้น

๓.๑.๔.๓ ปัญหาขององค์กรหรือหน่วยงานต่าง ๆ ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือ หน่วยงานส่วนใหญ่ไม่มีความพร้อม ทั้งด้านของกำลังพลหรือบุคลากรที่มีความรู้ ความสามารถเพียงพอ ต่อการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) จึงจำเป็นต้องหาหน่วยงานที่ช่วยเหลือในการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ให้กับหน่วยงานหรือองค์กรของตนเอง

๓.๑.๔.๔ การวิเคราะห์ภัยคุกคามทางไซเบอร์ อาจช่วยทำได้ด้วยการสร้างระบบ Big Data ด้าน Cyber Threat Intelligence (CTI) ซึ่งจะสามารถช่วยลดปัญหาการขาดแคลนกำลังพลที่มีความเชี่ยวชาญ และประสบการณ์การรับมือทางไซเบอร์

๓.๑.๔.๕ การสร้างโรงเรียนไซเบอร์ เป็นอีกวิธีที่สามารถแก้ปัญหาการขาดแคลนกำลังพลที่สามารถปฏิบัติงานการรับมือภัยคุกคามทางไซเบอร์ได้ในระยะยาว แต่ถ้าต้องการพัฒนากำลังพลแบบเร่งด่วนจำเป็นมีการจัดอบรมกำลังพลดังกล่าวก่อนการปฏิบัติงาน

๓.๑.๔.๖ การจัดตั้งหน่วยงานที่ทำหน้าที่รับผิดชอบด้านงานข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence : CTI) เพื่อจะเป็นองค์ความรู้ให้เท่าทันกับการแก้ปัญหาจากภัยคุกคามทางไซเบอร์ และจะต้องสามารถแจ้งเตือนหน่วยต่าง ๆ ได้ล่วงหน้าก่อนเกิดเหตุการณ์ทางไซเบอร์ โดยข้อมูลและระบบของข่าวกรองทางไซเบอร์ที่สามารถนำมาใช้งานได้จริง จะต้องสามารถแจ้งเตือนได้ตลอด ๒๔ ชม. ซึ่งปัจจุบันศูนย์ไซเบอร์กองทัพอากาศมีจุดอ่อนมากในส่วนของงาน CTIที่อาจจะต้องมีการดำเนินการร่วมกันกับกรมข่าวทหารอากาศในอนาคต เพื่อหาแนวทางในการดำเนินการด้านข่าวกรองทางไซเบอร์ของกองทัพอากาศ ทั้งนี้ หน่วยงานและองค์กรต่าง ๆ ที่รับผิดชอบงานด้านความมั่นคงปลอดภัยทางไซเบอร์ อาจจำเป็นที่จะต้องมีการซื้อข้อมูลข่าวกรองทางไซเบอร์ที่เป็นในรูปแบบการโจมตีที่มีการ Update ข้อมูลตลอด ๒๔ ชั่วโมง เพื่อให้ระบบการป้องกัน เฝ้าระวัง ตรวจจับและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของหน่วยมีข้อมูลข่าวกรองทางไซเบอร์ที่เป็นความรู้ที่เท่าทันกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นอยู่ตลอดเวลา และสามารถป้องกันการโจมตีนั้น ๆ ได้อย่างทันท่วงที

๓.๑.๔.๗ ทุกหน่วยงานจำเป็นต้องดำเนินการทำการประเมินความเสี่ยงทางไซเบอร์ (Cybersecurity Risk Assessment) เพื่อทำความเข้าใจกับระบบงานด้านเครือข่ายเทคโนโลยีสารสนเทศของหน่วยงานตนเอง และศึกษาถึงรูปแบบของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบเครือข่ายสารสนเทศของหน่วยงานตนเอง (Identity) เพื่อจะนำไปสู่การวางแผนและดำเนินการรับมือกับภัยคุกคามทางไซเบอร์ให้เป็นไปตามมาตรฐาน NIST Cybersecurity Framework ซึ่งเป็นมาตรฐานที่หน่วยงานทั่วโลกใช้ในการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งก่อนระหว่างและหลังการเกิดเหตุการณ์ทางไซเบอร์

๓.๑.๔.๘ การจ้างผู้ให้บริการภายนอก หรือบริษัทจากต่างประเทศ หรือการซื้อระบบเกี่ยวกับเฝ้าระวังภัยคุกคามทางไซเบอร์ มีต้นทุนสูงในการจัดหาระบบและการบำรุงรักษา

๓.๑.๔.๙ ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพและมีการใช้งานกันอยู่ในปัจจุบัน จำเป็นจะต้องมีการดำเนินการและให้ความสำคัญกับส่วนงานของ Endpoint Security ที่จำเป็นจะต้องมองเห็นและสามารถแก้ไขปัญหาภัยคุกคามที่เกิดจากบุคคลที่อยู่ในระบบเครือข่ายสารสนเทศของตนเอง ที่เป็นผู้นำเข้าภัยคุกคามทางไซเบอร์จากความประมาทหรือจากความรู้เท่าไม่ถึงการณ์ (Insider Threat) และในอนาคตของระบบของการป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์ จะต้องพัฒนาต่อไปให้เป็นระบบที่สามารถทำงานได้เองโดยอัตโนมัติ (Automation) และก้าวไปสู่ระบบของ Machine Learning ที่ระบบ Automation สามารถใส่ข้อมูล

การเรียนรู้ใหม่ ๆ หรือต่อยอดความรู้เข้าไปใหม่ได้ จนกระทั่งพัฒนาต่อไปให้เป็นระบบปัญญาประดิษฐ์ (Artificial Intelligence : AI) ที่ระบบสามารถเรียนรู้และต่อยอดได้ด้วยตนเอง ไม่ต้องมีใครมาฝึกให้ล่วงหน้า แต่ปัญหาจากการใช้ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เป็นระบบ AI คือ เกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เป็นการแจ้งเตือนจากระบบ แต่เมื่อมนุษย์หรือกำลังพลเข้าไปตรวจสอบในรายละเอียดของการแจ้งเตือนจริง ๆ มักจะพบว่าเป็นเหตุการณ์ที่ใช้งานปกติหรือไม่ใช่ภัยคุกคามทางไซเบอร์ ที่เรียกว่า False Positive เป็นจำนวนมาก ดังนั้น ถึงแม้จะเป็นระบบ AI แต่ก็ยังจำเป็นจะต้องอาศัยมนุษย์หรือกำลังพลที่มีความเชี่ยวชาญเข้าไปดำเนินการวิเคราะห์ให้แน่ใจอยู่ดี

๓.๑.๔.๑๐ การดำเนินการของการเฝ้าระวังภัยคุกคามทางไซเบอร์ จุดที่ต้องเร่งการแก้ปัญหาไม่ใช่เรื่องของงบประมาณ หรือการจัดหายุทโธปกรณ์ที่มีความทันสมัย แต่สิ่งที่ต้องแก้ปัญหาเร่งด่วน คือปัญหาด้านของการขาดแคลนกำลังพล (People) หรือบุคลากรทางไซเบอร์ที่มีความเชี่ยวชาญ หรือมีประสบการณ์ในการป้องกัน เฝ้าระวัง และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ซึ่งการแก้ไขปัญหาด้านนี้ในปัจจุบันส่วนมากจะทำได้ด้วยการฝึกกันเองหรือถ่ายทอดองค์ความรู้กันเองภายในหน่วย จากกำลังพลที่มีประสบการณ์และมีความเชี่ยวชาญ ส่งต่อไปยังกำลังพลที่เข้ามาใหม่และยังไม่มีประสบการณ์ในการทำงานด้านนี้ ซึ่งถือเป็นการแก้ไขปัญหาในระยะสั้นมากกว่า

๓.๑.๔.๑๑ ปัญหาของกำลังพล (People) ที่มีความเชี่ยวชาญทางไซเบอร์ คือการลาออกจากหน่วยงานของราชการ ไปรับเงินเดือนและสวัสดิการที่สูงกว่า ทำให้ยิ่งสร้างกำลังพลด้านไซเบอร์มากเท่าไร เมื่อกำลังพลเหล่านั้นมีประสบการณ์ และมีความชำนาญ ยิ่งเป็นความต้องการของบริษัทเอกชน หรือแม้แต่หน่วยงานราชการด้วยกันเอง ซึ่งการที่จะฝึกให้กำลังพลใหม่ ๆ ที่เข้ามาเกิดความชำนาญในหน้าที่ของตนเองในแต่ละส่วนงานได้ อาจจะต้องใช้ระยะเวลาในการทำงานในสายงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในหน้าที่นั้น ๆ อย่างน้อยสองปีขึ้นไป ดังนั้นการผลิตบุคลากรด้านไซเบอร์ในระดับองค์กรและในระดับประเทศนั้นถือเป็นความเร่งด่วนในลำดับต้น ๆ ของการแก้ไขปัญหาการดำเนินงานด้านไซเบอร์

๓.๑.๔.๑๒ การเฝ้าระวังภัยคุกคามทางไซเบอร์ ปัญหาอีกอีกส่วนหนึ่งเกิดจากการหน่วยต่าง ๆ ไม่ยอมส่งข้อมูลจราจรคอมพิวเตอร์ (Log files) หรือส่งไม่ครบ ส่งมาเพียงแค่บางส่วนเข้ามาให้ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (SCOC) ทำให้การเฝ้าระวังภัยคุกคามทางไซเบอร์ไม่มีประสิทธิภาพ เช่น กองทัพอากาศ มีหน่วยย่อย ๆ ตามต่างจังหวัดจำนวนมาก แต่ไม่ค่อยมีการส่งข้อมูล Log files หรือส่งเพียงบางส่วน เพื่อให้ศูนย์ไซเบอร์ของกองทัพอากาศเฝ้าระวังภัยคุกคามทางไซเบอร์ให้ ซึ่งบางครั้งอาจทราบภายหลังว่าเกิดการโจมตีทางไซเบอร์ที่สำเร็จแล้ว ทำให้ไม่สามารถป้องกันหรือแก้ปัญหาที่เกิดขึ้นได้ทันเวลา

๓.๑.๔.๑๓ การเฝ้าระวังภัยคุกคามทางไซเบอร์จำเป็นต้องดำเนินการวิเคราะห์ให้ทันที ถ้าปล่อยไว้นาน ข้อมูล log files อาจจะถูกลบออกไปจากระบบการจัดเก็บ และไม่สามารถดำเนินการใด ๆ ได้อีกต่อไป

๓.๑.๔.๑๔ การรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น ส่วนใหญ่จะเป็นการดำเนินตามหลักการทำงานของ NIST Cybersecurity Framework โดยจะมีกลไกในการดำเนินการ

หลักอยู่ด้วยกัน ๕ กลุ่ม ได้แก่ การทำความเข้าใจกับระบบเทคโนโลยีสารสนเทศของหน่วยงานตนเอง และเข้าใจรูปแบบของการถูกโจมตีทางไซเบอร์ต่อระบบดังกล่าว (Identify) จากนั้นก็จะเข้าสู่ระบบของการป้องกัน (Protection) การเฝ้าระวังและตรวจจับ (Detection) การแก้ไขปัญหา (Respond) และการกู้คืนให้ระบบกลับมาใช้งานได้อย่างเป็นปกติ กรณีไม่สามารถรับมือกับการถูกโจมตีทางไซเบอร์ได้ (Recovery) และต้องดำเนินการหาบุคคลที่กระทำความผิดได้

๔. ผลจากการสังเกตการณ์ (Observation)

การสังเกตการณ์ (Observation) เป็นการสังเกตจากประสบการณ์โดยตรงของตัวนักวิจัยเอง ซึ่งเป็นผู้มีความรู้และประสบการณ์ตรงด้านจัดการบริหารจัดการ และการรับมือกับภัยคุกคามทางไซเบอร์ในระดับกองทัพไทย และในระดับประเทศมาเป็นเวลาต่อเนื่องกันนานกว่า ๗ ปี และเพื่อหาข้อมูลของปัญหาในการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์แห่งชาติ ตลอดจนแนวทางในการดำเนินการที่เป็นรูปธรรม และมีประสิทธิภาพ และเพื่อใช้เป็นแนวทางในการปฏิบัติของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) สามารถสรุปได้ดังนี้

๔.๑ ปัญหาของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศของประเทศไทยอาจสรุปได้ดังนี้

๔.๑.๑ ประเทศไทยขาดบุคลากรที่มีความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างแท้จริง ส่วนมากแล้วจะมีความรู้กันในลักษณะของการเป็นนักวิชาการมากกว่าการเป็นผู้มีประสบการณ์จริงจากการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๔.๑.๒ ประเทศไทยไม่มีหน่วยงานรองรับงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศอย่างแท้จริงก่อนที่จะมีการออก พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้มีการตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (สกมช.) ซึ่งที่ผ่านมามีสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ทำหน้าที่แทน และไม่มีหน่วยงานใดต้องการเข้ามาทำหน้าที่นี้อย่างแท้จริง ดังนั้นการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานต่าง ๆ ในประเทศไทยก็ดำเนินไปในลักษณะที่ต่างคนต่างทำและต่างคนต่างอยู่ แก้ไขปัญหาเฉพาะหน้าด้วยตนเอง ไม่มีการช่วยเหลือซึ่งกันและกันอย่างแท้จริง

๔.๑.๓ แนวทางการดำเนินการด้านไซเบอร์ที่ผ่านมาของ สพธอ. ที่ดำเนินการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ให้กับหน่วยงานมากกว่า ๒๐๐ องค์กรนั้น ในความเป็นจริงแล้ว ไม่สามารถเห็นถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในองค์กรได้อย่างแท้จริง เพราะปริมาณ Log files ที่ถูกส่งมานั้นเป็นข้อมูลจากระบบ Intrusion Protection System เพียงอย่างเดียว ซึ่งอาจจะไม่เพียงพอต่อการวิเคราะห์ถึงความเป็นไปได้ว่าถูกบุกรุกทางไซเบอร์ และยิ่งไปกว่านั้นการใช้ระบบ SIEM เป็นระบบในการวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์นั้น ถือว่าไม่มีความเหมาะสมเป็นอย่างมาก เนื่องจาก SIEM ถูกออกแบบมาให้เฝ้าระวังภัยคุกคามทางไซเบอร์ต่อหน่วยงานที่เป็นลักษณะของ Small/Medium Enterprise (SME) เท่านั้น

๔.๒ การดำเนินการของศูนย์เฝ้าระวังในการรับมือและแก้ไขปัญหาทางไซเบอร์ในระดับประเทศอาจดำเนินการได้ใน ๒ รูปแบบ ได้แก่การดำเนินการแบบรวมการ (Centralize) และการดำเนินการแบบแยกการ (Decentralize) ซึ่งทั้ง ๒ รูปแบบมีข้อดีและข้อเสียที่ต่างกันดังนี้

๔.๒.๑ การดำเนินการแบบรวมการ

๔.๒.๑.๑ ข้อดี

๑. ดำเนินการง่าย

๒. ใช้คนน้อย

๓. ลงทุนน้อย

๔.๒.๑.๒ ข้อเสีย

๑. ไม่สามารถนำไปสู่การเฝ้าระวัง ตรวจจับและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ได้อย่างแท้จริง เนื่องจากข้อมูลการจราจรในลักษณะของ Log files ที่ถูกส่งมาจากหลาย ๆ หน่วยงานเป็นข้อมูลที่มีลักษณะแตกต่างกัน การจะให้บุคคลที่ไม่มีความรู้เกี่ยวกับองค์กรในส่วนกลางมาวิเคราะห์ถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในองค์กรได้อย่างถูกต้องและแม่นยำนั้นเป็นไปได้ยากมาก

๒. เป็นการลงทุนที่สูญเปล่าเนื่องจากไม่สามารถนำไปสู่การป้องกันเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ได้อย่างแท้จริง

๔.๒.๑.๓ ตัวอย่างของประเทศที่ใช้รูปแบบของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์แบบรวมการ ที่ผู้วิจัยได้รับทราบมาจากเจ้าของผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Vender) จากประเทศมาเลเซีย

๔.๒.๒ การดำเนินการแบบแยกการ

๔.๒.๒.๑ ข้อดี

๑. สามารถนำไปสู่การแก้ไขปัญหาทางไซเบอร์ได้อย่างแท้จริงเป็นรูปธรรมและมีประสิทธิภาพ

๒. มีความสมบูรณ์ของระบบไม่พร้อม แยกกันจัดตั้ง แยกกันพัฒนา

๔.๒.๒.๒ ข้อเสีย

๑. ดำเนินการค่อนข้างยาก

๒. ใช้คนมาก

๓. ลงทุนมากเพราะต้องแยกดำเนินการเป็นส่วน ๆ ให้สามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ได้จริงอย่างมีประสิทธิภาพ

๔.๒.๒.๓ ตัวอย่างของประเทศที่ใช้รูปแบบของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์แบบแยกการ คือประเทศอิสราเอล ซึ่งผู้วิจัยได้เคยเดินทางไปดูงาน ณ ศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ของประเทศอิสราเอล (Israel National Cyber Directorate) มาแล้ว ทั้งนี้ ประเทศอิสราเอลเคยใช้รูปแบบของศูนย์เฝ้าระวังฯ แบบรวมการนานกว่า

๑๐ ปี ก่อนที่จะเปลี่ยนรูปแบบมาเป็นศูนย์เฝ้าระวังฯ แบบแยกการ เนื่องจากพบว่าศูนย์เฝ้าระวังฯ แบบแยกการสามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ได้อย่างไปรูปธรรมและมีประสิทธิภาพมากกว่า

๔.๓ แนวทางในการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาทางไซเบอร์ในระดับประเทศของประเทศไทยควรดำเนินการในลักษณะของการแยกการ โดย สกมช. มีความจำเป็นต้องจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศ (National Cybersecurity Operations Center : NCOC) โดยให้หน่วยงานที่ทำหน้าที่เป็นสาธารณูปโภคพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure : CII) ทั้ง ๘ กลุ่มตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ จำเป็นต้องกำหนดให้มีหน่วยงานที่ทำหน้าที่เป็น Regulator ของแต่ละกลุ่ม และหน่วยงานที่ทำหน้าที่เป็น Regulator ดังกล่าวของแต่ละ Sector จะต้องดำเนินการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของแต่ละ Sector (Joint Cybersecurity Operations Center : JCOC) เพื่อทำหน้าที่ให้เกิดการประสานงานและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ร่วมกันกับหน่วยงานย่อย ๆ ของแต่ละ Sector โดยหน่วยงานย่อย ๆ ของแต่ละ Sector ที่มีความสำคัญจะต้องตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ของหน่วยงานตนเองขึ้นมา เพื่อดูแลระบบงานด้านสารสนเทศของตนเองให้มีความปลอดภัย โดยทั้งหมดจะต้องมีการออกแผนรับมือเหตุการณ์ทางไซเบอร์ในทุกระดับ ตั้งแต่ระดับ CSOC, JCOC ไปจนถึงระดับ NCOC ให้สามารถแก้ไขปัญหาได้เป็นระดับ ๆ ไป ในลักษณะของการพึ่งพาอาศัยและช่วยเหลือกันทั้งประเทศ โดยมี สกมช. และ NCOC เป็นหน่วยงานกลางในการบูรณาการให้เกิดการช่วยเหลือกันทั้งประเทศ

๔.๔ การฝึกแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศนั้น ถือว่าเป็นกลไกสำคัญในการทดสอบทั้งโครงสร้าง และกระบวนการในการทำงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศเป็นอย่างมาก เนื่องจากการฝึกจะเป็นการทดสอบทุกอย่างที่มีอยู่ว่าจะสามารถนำไปสู่การแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศได้จริงหรือไม่

๔.๕ กลไกในการแชร์ข้อมูลข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence : CTI) ในระดับประเทศและระดับนานาชาติ ถือว่ามีความสำคัญเป็นอย่างมาก เพราะ CTI ถือเป็นฐานข้อมูลขององค์ความรู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ที่จะทำให้ทุกองค์กรสามารถใช้รับมือกับภัยคุกคามทางไซเบอร์ได้อย่างเท่าทันกับภัยคุกคามในปัจจุบัน ความหมายคือถ้าองค์กรใดตรวจพบภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ ๆ และแชร์ข้อมูลดังกล่าวให้กับองค์กรอื่น ๆ ทั้งในและต่างประเทศ องค์กรที่ได้รับการแชร์ข้อมูลก็จะสามารถปรับแต่งระบบป้องกันและเฝ้าระวังเหตุการณ์ทางไซเบอร์ ให้ปลอดภัยจากภัยคุกคามในรูปแบบใหม่ ๆ ได้ดียิ่งขึ้น

บทที่ ๕
สรุป อภิปรายผล และข้อเสนอแนะ

การศึกษางานวิจัยเรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม (The guidance for setting up Thailand National Cybersecurity Operations Center – NCOC – in order to properly solve the critical cybersecurity situation at the national level)” เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ ๓ ข้อ ประกอบด้วย

๑. เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒. เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

๓. เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

งานวิจัยฉบับนี้ มุ่งเน้นศึกษาความสำคัญของแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่จะต้องเป็นกลไกหลักในระดับประเทศเพื่อการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) และมีความต้องการที่จะเพื่อศึกษาถึงปัญหาและรูปแบบของการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ (CSOC) ในระดับประเทศ ที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตลอดจนศึกษาแนวทางการทำงานของศูนย์ปฏิบัติการทางไซเบอร์ในรูปแบบต่าง ๆ ที่ใช้กันอยู่ในระดับนานาชาติ

ซึ่งในการดำเนินการวิจัยครั้งนี้ ผู้วิจัยใช้การศึกษาจากการรวบรวมข้อมูลจากเอกสารและตำราทางทฤษฎี ตลอดจนงานวิจัยที่เกี่ยวข้อง (Documentary Research) โดยใช้ข้อมูลทุติยภูมิ (Secondary Data) และรวบรวมข้อมูลปฐมภูมิจากการสัมภาษณ์เชิงลึก (In - Depth Interview) การประชุมสนทนากลุ่ม (Focus Group Discussion) และการสังเกตการณ์ (Observation) ซึ่งเป็นการสังเกตการณ์จากประสบการณ์ตรงจากตัวนักวิจัยเอง ซึ่งเป็นผู้มีความรู้และประสบการณ์ตรงด้านการบริหารจัดการ และการรับมือกับภัยคุกคามทางไซเบอร์ในระดับกองทัพไทย และในระดับประเทศมาเป็นเวลานานกว่า ๗ ปี เพื่อให้ข้อมูลที่ได้มีความเที่ยงตรงและน่าเชื่อถือในการวิเคราะห์

ข้อมูลนั้น ผู้วิจัยใช้การวิเคราะห์ผลจากการสัมภาษณ์เชิงลึก (In - Depth Interview) และการประชุมสนทนากลุ่ม (Focus Group Discussion) เป็นหลัก โดยเมื่อนำข้อมูลที่ได้มาวิเคราะห์และสังเคราะห์ประกอบกับแนวคิดทฤษฎีที่เกี่ยวข้อง จนกระทั่งได้แนวทางการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ ซึ่งในบทที่ ๕ นี้ จะนำเสนอเป็น ๓ ประเด็นหลักคือ สรุปผล อภิปรายผลการวิจัย และข้อเสนอแนะ

สรุป

การนำเสนอผลการวิจัยในครั้งนี้ ผู้วิจัยนำเสนอผลการวิจัยโดยยึดวัตถุประสงค์การวิจัยเป็นหลัก จำนวน ๓ วัตถุประสงค์การวิจัย ดังนี้

๑. ตอบวัตถุประสงค์การวิจัย ข้อที่ ๑ เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทยในห้วงที่ผ่านมา ซึ่งสามารถพบปัญหาและข้อจำกัดดังต่อไปนี้

๑.๑ บุคลากร (People)

เนื่องจากบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยมีจำนวนไม่มากเพียงพอต่อความต้องการของตลาดและหน่วยงานต่าง ๆ ของประเทศไทยในปัจจุบัน และโดยเฉพาะอย่างยิ่งบุคลากรที่มีความเชี่ยวชาญลึกลงไปในแต่ละส่วนงานของการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ไม่ว่าจะเป็นนักวิเคราะห์เหตุการณ์ในศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ (Cyber Security Operations Center : CSOC) หรือ CSOC Analyst นักตรวจประเมินมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Auditor) นักทดสอบเจาะระบบ (Penetration Tester) นักพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Analyst) ผู้เชี่ยวชาญด้านข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence Expert) ยิ่งมีจำนวนน้อยมากจึงเกิดการแย่งชิงบุคลากรกลุ่มดังกล่าวจากทั้งภายในและภายนอกประเทศ โดยมีการเสนอค่าตอบแทนและสวัสดิการที่ค่อนข้างสูง เพื่อชักจูงให้ไปร่วมงานกับบริษัทหรือองค์กรที่ให้ค่าตอบแทนที่สูงกว่า ซึ่งการที่หน่วยงานของภาครัฐให้ค่าตอบแทนแก่บุคลากรทางไซเบอร์ที่ค่อนข้างน้อย เมื่อเปรียบเทียบกับบริษัทเอกชนหรือบริษัทของต่างประเทศ ส่งผลให้บุคลากรกลุ่มดังกล่าวที่อยู่ในหน่วยงานส่วนภาครัฐเริ่มทยอยลาออก เพื่อไปรับค่าตอบแทนที่สูงกว่าเป็นจำนวนมาก ดังนั้นการสร้างและผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงถือเป็นความเร่งด่วนในลำดับแรก ๆ ที่จำเป็นต่อการพัฒนาและแก้ไขปัญหาการดำเนินงานด้านไซเบอร์ในระดับประเทศของประเทศไทย ซึ่งมีความจำเป็นที่จะต้องมีการสร้างโรงเรียนหรือสถาบันทางการศึกษาที่จะสามารถผลิตบุคลากรทางไซเบอร์ให้กับหน่วยงานและองค์กรต่าง ๆ ในประเทศไทย ที่มีแนวโน้มที่จะนำเทคโนโลยีดิจิทัลมาใช้

เพื่อการพัฒนาธุรกิจหรือการดำเนินกิจการขององค์กรมากยิ่งขึ้นเรื่อย ๆ ดังนั้นการผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงถือได้ว่ามีความจำเป็นอย่างมาก และจำเป็นที่จะต้องมีการวางแผนในระยะยาว เนื่องจากการสร้างและผลิตบุคลากรด้านไซเบอร์ให้มีความเชี่ยวชาญและมีขีดความสามารถสูงนั้น จำเป็นต้องใช้เวลาในการผลิตและฝึกฝนทักษะฝีมือในห้วงเวลาที่นานพอสมควร และไม่ใช่บุคลากรทุกคนสามารถพัฒนาตัวเองให้เป็นผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้เสมอไป เนื่องจากการดำเนินการพัฒนาขีดความสามารถของบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในขั้นกลางและขั้นสูงนั้น มีความยากลำบากเป็นอย่างมาก ซึ่งจะต้องอาศัยผู้ที่มีความตั้งใจจริงและมีความอดทนสูงมากเท่านั้นที่จะไปถึงเป้าหมายดังกล่าวได้

๑.๒ กระบวนการ (Process)

การสร้างกระบวนการ (Process) มีความจำเป็นไม่น้อยกว่าด้านการผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทย จะต้องมีจำนวนหน่วยงานอีกเป็นจำนวนมากที่จะต้องดำเนินงานรองรับวงรอบในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย อีกทั้งจำนวนของข้อมูลการจราจรคอมพิวเตอร์ในลักษณะต่าง ๆ ที่จะนำไปสู่การวิเคราะห์ให้เห็นถึงภัยคุกคามทางไซเบอร์ และสามารถใช้ในการแก้ไขปัญหาทางไซเบอร์ให้ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพนั้น จำเป็นต้องมีการสร้างกระบวนการในการดำเนินการที่ชัดเจน อีกทั้งยังจะต้องออกแบบแนวทางของการจัดตั้งและการดำเนินการของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในระดับประเทศที่มีความลงตัวกับทุกส่วนงานที่เกี่ยวข้องของประเทศไทย ซึ่งต้องมีการประชุมหารือกับผู้แทนจากแต่ละส่วนงานของระบบสาธารณูปโภคขั้นพื้นฐานของประเทศและหน่วยงานสำคัญของประเทศที่เกี่ยวข้อง รวมถึงบุคลากรที่มีความเชี่ยวชาญอย่างแท้จริงในสายงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อวิเคราะห์หาจุดเด่น จุดด้อย ข้อจำกัด ในหลากหลายให้ครบทุกด้าน ทุกมิติ เพื่อเป็นการลดความเสี่ยงและผลกระทบของการดำเนินการให้เหลือน้อยที่สุดและมีประโยชน์สูงสุด ตลอดจนการทำความเข้าใจกับผู้บังคับบัญชาและผู้บริหารระดับสูงของประเทศเพื่อให้เกิดความเข้าใจถึงความสำคัญและแนวทางในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ จนสามารถได้รับการสนับสนุนทั้งด้านงบประมาณ หลักการ กฎหมาย และทรัพยากรต่าง ๆ ที่จำเป็นที่จะนำไปสู่การดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยให้มีความเป็นรูปธรรมทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์

๑.๓ เทคโนโลยี (Technology)

ในปัจจุบันยังไม่มีเทคโนโลยี หรืออุปกรณ์รักษาความปลอดภัยทางไซเบอร์ชนิดใดที่สามารถวิเคราะห์ภัยคุกคามทางไซเบอร์จากข้อมูลการจราจรคอมพิวเตอร์ในลักษณะของ Log files จำนวนมหาศาลได้ โดยเฉพาะการนำระบบ SIEM (Security Information and Event Management) ที่เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กรขนาดย่อม (Small/Medium Enterprise : SME) มาใช้ในการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์

แบบรวมการทั้งประเทศนั้น เป็นสิ่งที่ไม่น่าจะกระทำ เนื่องจากในความเป็นจริงแล้วระบบ SIEM นั้น เป็นระบบที่เหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรในลักษณะของ Log files ของหน่วยงานขนาดไม่ใหญ่มาก (SME) เพียงหน่วยงานเดียวหรือมีข้อมูลไม่มากจนเกินไปเท่านั้น ซึ่งถ้าต้องการนำเทคโนโลยีอย่างระบบ SIEM มาใช้ อาจจะต้องมีการแยกระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ออกเป็นหน่วยงานย่อย ๆ หลาย ๆ หน่วยงาน ที่จำเป็นต้องแยกระบบ SIEM ออกเป็นหลาย ๆ ระบบ เพื่อให้เกิดประสิทธิภาพของการเฝ้าระวังตรวจจับและแก้ไขปัญหาให้ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ทั้งนี้ระบบการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ในปัจจุบันนั้นมีหลากหลายรูปแบบที่สามารถดำเนินการได้จากการวิเคราะห์จาก Raw Traffics, Meta Data, Net Flows เป็นต้น

๒. ตอบวัตถุประสงค์การวิจัย ข้อที่ ๒ เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดี และข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center: NCOC) แบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

๒.๑ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) แบบรวมการ (Centralize)

การจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) นั้น มีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรทางคอมพิวเตอร์ในรูปแบบต่าง ๆ จากทุก ๆ หน่วยงานที่มีระบบการป้องกัน เฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ไปยังศูนย์กลางเฝ้าระวังภัยคุกคามทางไซเบอร์เพียงที่เดียว โดยการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) ถือว่าเป็นแนวคิดที่ดีที่มีความพยายามที่จะทำให้เกิดการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศขึ้น ซึ่งมีความจำเป็นที่จะต้องมีระบบที่สามารถวิเคราะห์ข้อมูลการจราจรทางคอมพิวเตอร์ในลักษณะต่าง ๆ ที่มีจำนวนมากได้อย่างมีประสิทธิภาพ และยังจะต้องมีบุคลากรที่เชี่ยวชาญสูงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในจำนวนที่มากพอต่อการวิเคราะห์ข้อมูลการจราจรในรูปแบบต่าง ๆ ที่ถูกส่งมาจากองค์กรหลายองค์กรที่มีความหลากหลายของระบบเครือข่ายสารสนเทศ และวัตถุประสงค์ของการดำเนินธุรกิจขององค์กร เพื่อที่จะดำเนินการแก้ไขปัญหาการถูกบุกรุกทางไซเบอร์ได้อย่างทันท่วงที ซึ่งข้อด้อยของการจัดตั้ง NCOC แบบรวมการ นั้น อาจมาจากการที่หน่วยงานแต่ละหน่วยงานที่ส่งข้อมูลในรูปแบบต่าง ๆ มายังศูนย์เฝ้าระวังในส่วนการ ในลักษณะที่มีข้อมูลที่มีรูปแบบและความสำคัญของข้อมูลที่แตกต่างกัน ดังนั้นการวิเคราะห์ข้อมูลที่มีรูปแบบและมีความสำคัญที่แตกต่างกันเป็นจำนวนมาก จึงเป็นความยากอย่างมากของผู้วิเคราะห์ ซึ่งต้องมีความรู้ที่หลากกลายข้าม Sectors ต่าง ๆ ของ CII ซึ่งถือว่ามีความเป็นไปได้ยากมากที่ผู้วิเคราะห์จะมีความสามารถในการวิเคราะห์ได้ตรงว่าเกิดความผิดปกติหรือไม่อย่างไรขึ้นกับระบบต่าง ๆ ซึ่งจะส่งผลให้การวิเคราะห์ข้อมูลต่าง ๆ ได้ผลไม่ตรงตามความเป็นจริงของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น และไม่สามารถแก้ไขปัญหาของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้อย่างทันเวลา

ที่จำเป็น และในปัจจุบันยังไม่มีเทคโนโลยีหรืออุปกรณ์ชนิดใด ที่จะสามารถวิเคราะห์ภัยคุกคามทางไซเบอร์จากจำนวนข้อมูลประเภทที่เป็นลักษณะของ Log files จำนวนมหาศาลได้อย่างแม่นยำ

๒.๒ การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) แบบแยกการ (Decentralize)

การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ (Decentralize) เป็นการดำเนินการโดยให้แต่ละกลุ่มที่มีการดำเนินการในลักษณะที่คล้ายกัน หรือตามหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ดำเนินการตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ของกลุ่มของหน่วยงานตนเอง (Joint Cybersecurity Operations Center : JCOC) หรืออาจจะลงลึกถึงหน่วยงานตนเองแยกดำเนินการเองไปเลย (Cyber Security Operations Center : CSOC) ถ้ามีความพร้อมทั้งด้านงบประมาณ และกำลังพลที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเพียงพอ ส่วนหน่วยกลางใหญ่ในระดับประเทศหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) อาจทำหน้าที่เป็นเพียงแค่หน่วยงานในการกระจายหรือแชร์ข้อมูลด้านไซเบอร์ที่สำคัญร่วมกันเท่านั้น ซึ่งการดำเนินการในลักษณะนี้อาจสามารถแก้ปัญหาและรับมือภัยคุกคามทางไซเบอร์ได้จริงอย่างมีประสิทธิภาพในเชิงลึกได้มากกว่า แต่อาจจะต้องใช้เวลาในการสร้างศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ขององค์กรหรือหน่วยงานย่อย ๆ ที่มีความสำคัญ ที่เมื่อถูกโจมตีหรือถูกบุกรุกทางไซเบอร์แล้วจะส่งผลกระทบในภาพรวมต่อประเทศเป็นวงกว้าง ให้มีความพร้อมทั้งด้านบุคลากรทางไซเบอร์ ระบบการบริหารจัดการ และระบบเทคโนโลยีต่าง ๆ ที่จะเลือกมาใช้ในการดำเนินการ ซึ่งปัญหาใหญ่มักจะอยู่ที่การขาดแคลนบุคลากรด้านไซเบอร์ที่จะมาเป็นผู้ควบคุมระบบต่าง ๆ ให้สามารถดำเนินการได้จริงอย่างมีประสิทธิภาพ

๓. ตอบวัตถุประสงค์การวิจัย ข้อที่ ๓ เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

จากผลการวิจัยของตอบวัตถุประสงค์การวิจัย ข้อที่ ๒ เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแบบแยกการ พบว่าแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) ซึ่งเป็นกลไกหลักในระดับประเทศของประเทศไทยในห้วงที่ผ่านมา ในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) แต่ไม่สามารถนำไปสู่การเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยได้อย่างเป็นรูปธรรมอย่างแท้จริง ซึ่งอาจเป็นเพราะการใช้ระบบการเฝ้าระวังและตรวจจับด้วยระบบ SIEM ที่มีความไม่เหมาะสม ตลอดจนบุคลากรที่จะมีความสามารถที่เพียงพอในการวิเคราะห์ Log files ที่ถูกจัดส่งมาจากหลากหลายหน่วยงานที่มีความหลากหลายทั้งทางด้านรูปแบบเครือข่ายของการให้บริการ

ทางสารสนเทศ และแตกต่างกันของวัตถุประสงค์ในการดำเนินการทางธุรกิจนั้น แทบเป็นไปไม่ได้เลยที่จะมีใครสามารถวิเคราะห์เหตุการณ์ทางไซเบอร์ที่เกิดขึ้นข้ามไปหลาย ๆ Sectors ได้อย่างถูกต้องและแม่นยำ

ทั้งนี้ ภายหลังจากการออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒ แล้ว ประเทศไทยได้มีการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ขึ้นเพื่อเป็นหน่วยงานหลักในการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ แต่หัวใจของการดำเนินการและรับมือกับภัยคุกคามทางไซเบอร์คือ ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center: CSOC) ที่เป็นส่วนงานของการทำหน้าที่ในการระบุภัยคุกคามทางไซเบอร์ (Identify) การป้องกันภัยคุกคามทางไซเบอร์ (Protect) การตรวจจับภัยคุกคามทางไซเบอร์ (Detect) การรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (Response) ตลอดจนการกู้คืนระบบเมื่อไม่สามารถแก้ไขปัญหาที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ได้ โดยต้องนำระบบที่สำรองไว้กลับขึ้นมาใช้งานให้ได้ตามปกติ (Recovery) ให้กับองค์กรหรือหน่วยงานที่นำระบบเครือข่ายเทคโนโลยีสารสนเทศมาใช้บริหารจัดการทางธุรกิจหรือการปฏิบัติงานขององค์กร แต่การที่ดำเนินการด้าน CSOC ของ สกมช. ในระดับประเทศนั้น ยังไม่มีการออกแบบหรือวางแนวทางในการดำเนินการอย่างชัดเจน ซึ่งจากการศึกษาข้อมูลการวิจัยในครั้งนี้พบว่า การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ (Decentralize) เหมาะสมต่อการนำมาใช้ในระดับประเทศ ในการนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ

อภิปรายผลการวิจัย

จากผลการวิจัยที่ได้สรุปผลจากการเก็บข้อมูลทั้งการวิจัยเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่ม (Focus Group Discussion) และการสังเกตการณ์ (Observation) สามารถสรุปได้ดังนี้

๑. รูปแบบการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ หรือ ศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) สามารถจัดการดำเนินการได้เป็น ๒ รูป ได้แก่

๑.๑ การจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมการ (Centralize) เป็นรูปแบบการจัดตั้งที่ไม่เหมาะกับประเทศไทย เพราะแต่ละหน่วยงานหรือแต่ละกลุ่มงานตามหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) มีการดำเนินงานและการให้บริการต่าง ๆ ในรูปแบบที่แตกต่างกันออกไป และการจะให้มีการส่งข้อมูลในลักษณะของ Log files เข้ามาวิเคราะห์ภัยคุกคามทางไซเบอร์ยังจุด ๆ เดียวนั้น ต้องการอาศัยนักวิเคราะห์ที่มีความชำนาญ และมีศักยภาพสูงในการวิเคราะห์ Log files ดังกล่าว และอีกประการหนึ่งซึ่งถือว่ามีความสำคัญเป็นอย่างมาก ที่ในปัจจุบันยังไม่มีเทคโนโลยีหรืออุปกรณ์ใด ๆ ที่จะใช้เป็นระบบ

เฝ้าระวังภัยคุกคามทางไซเบอร์ ซึ่งจะต้องสามารถรองรับการทำงานในการวิเคราะห์ข้อมูลในลักษณะของ Log files จำนวนมหาศาลได้อย่างถูกต้องและแม่นยำ แต่ก็ถือได้ว่าการจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบรวมการ (Centralize) เป็นรูปแบบหนึ่งที่สามารถใช้ในการจัดตั้ง NCOC ในระดับประเทศได้ถ้าหากสามารถแก้ไขปัญหาตามที่กล่าวมาได้

๑.๒ การจัดตั้งศูนย์บริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) แบบแยกการ (Decentralize) เป็นรูปการจัดตั้งที่เหมาะสมกับประเทศไทยมากที่สุดในปัจจุบัน ซึ่งอาจจะเป็นการดำเนินการโดยให้แต่ละกลุ่มที่มีรูปแบบของการดำเนินการทางธุรกิจหรือกิจการของหน่วยงานที่คล้ายคลึงกัน หรือตามกลุ่มของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยสามารถดำเนินการตั้งศูนย์เฝ้าระวังภัยคุกคามของกลุ่มของหน่วยตนเอง (Joint Cybersecurity Operations Center : JCOC) หรืออาจจะแยกดำเนินการเป็นหน่วยงานเฉพาะไปเลย ด้วยการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ของตนเอง (Cyber Security Operations Center : CSOC) ถ้ามีงบประมาณ และกำลังพลหรือบุคลากรทางไซเบอร์ที่มีความสามารถเพียงพอ โดยอาจจะต้องดำเนินการเฝ้าระวังและแก้ไขปัญหาให้กับหน่วยงานของตนเองให้ได้ก่อน ซึ่งถ้าเกิดปัญหาและแก้ไขปัญหาเองได้ก็สามารถปิด Case ของเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) ที่เกิดขึ้นไปได้เลย แต่ถ้าหากไม่สามารถแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้ด้วยตนเอง ก็จะต้องส่งต่อกระบวนการของการแก้ไขปัญหาไปยังส่วนงานที่อยู่สูงขึ้นไป หรือมีความพร้อมและมีขีดความสามารถในการแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ที่มากกว่า โดยจะใช้การดำเนินการในลักษณะของการพึ่งพาอาศัยกันทั้งใน Sector เดียวกัน หรือข้าม Sector ไป โดยมี สกมช. หรือ NCOC เป็นหน่วยงานกลางในการบูรณาการให้เกิดการช่วยเหลือซึ่งกันและกันในการรับมือกับภัยคุกคามทางไซเบอร์ร่วมกันทั้งประเทศ

๒. อุปสรรคของการดำเนินการเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือการจัดตั้งการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย (NCOC) สามารถแบ่งออกเป็น ๓ ด้าน ได้แก่

๒.๑ ด้านบุคลากร (People) ในปัจจุบันปัญหาหลักของการดำเนินการเฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ หรือการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) และถือว่าเป็นปัญหาสำคัญที่แก้ไขยากที่สุดคือ ปัญหาของการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีความเชี่ยวชาญและมีขีดความสามารถสูงในแต่ละหน้าที่ของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีความจำเป็นต้องวางแผนทั้งในระยะสั้นและระยะยาว โดยในระยะสั้นอาจแก้ไขได้ โดยการถ่ายทอดองค์ความรู้จากหน่วยงานและบุคลากรที่มีประสบการณ์และมีขีดความสามารถสูงไปยังหน่วยงานที่ตั้งใหม่ให้สามารถดำเนินกิจการของตนเองไปได้ในระดับเริ่มต้น แต่แผนการแก้ไขปัญหาการขาดแคลนบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระยะยาวจะต้องมีสถาบันการศึกษาที่จะต้องผลิตบุคลากรทางไซเบอร์เพื่อป้อนให้กับตลาดและหน่วยงานต่าง ๆ ที่มีความต้องการบุคลากรด้านนี้ได้อย่างเพียงพอต่อไปในอนาคต

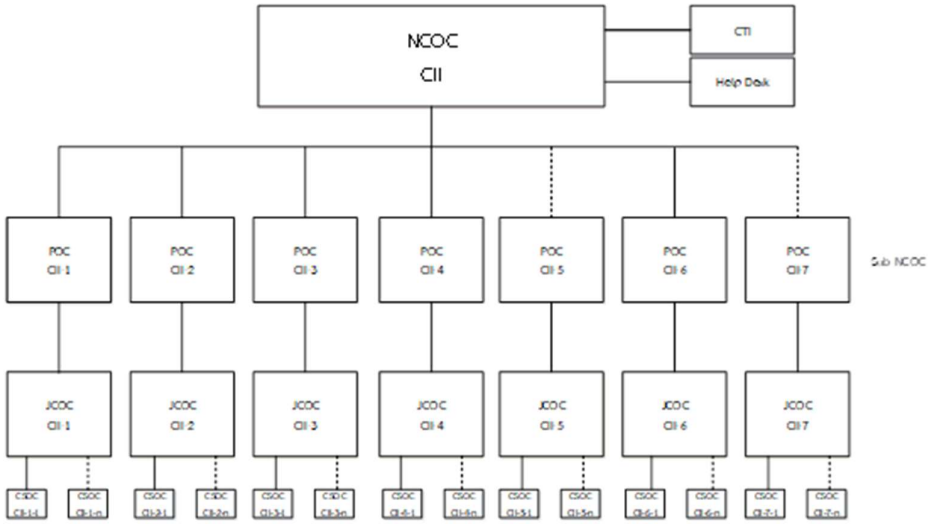
๒.๒ ด้านกระบวนการ (Process) การดำเนินการการเฝ้าระวังภัยคุกคามทางไซเบอร์และการดำเนินการจัดตั้งและการปฏิบัติงานของศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ซึ่งจะต้องมีจำนวนหน่วยงานที่เกี่ยวข้องและจัดตั้งขึ้นใหม่จำนวนมาก ทั้งที่มีการดำเนินงานที่คล้ายกัน และที่มีการดำเนินงานที่แตกต่างกัน ตลอดจนจะมีจำนวนของข้อมูลการจราจรคอมพิวเตอร์ในรูปแบบ ต่าง ๆ ที่มีจำนวนมหาศาลเข้ามาเกี่ยวข้อง ซึ่งจำเป็นต้องมีการสร้างกระบวนการในการดำเนินการที่ชัดเจน และเลือกรูปแบบหรือประเภทของการจัดตั้งศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศที่มีความลงตัวกับประเทศไทย ซึ่งต้องมีการประชุมหารือกับตัวแทนของแต่ละส่วนจากหน่วยงานที่ถือเป็นสาธารณูปโภคสำคัญของประเทศ (CII) และหน่วยงานสำคัญของประเทศที่เกี่ยวข้อง เพื่อการทำเข้าใจที่ตรงกัน และสามารถสื่อสารให้กับผู้บริหารระดับสูงขององค์กรหรือผู้บังคับบัญชาให้เกิดความความเข้าใจ และให้การสนับสนุนต่าง ๆ เพื่อการปฏิบัติงานที่คล่องตัว ไม่ว่าจะเป็นด้านงบประมาณ หรือการให้การสนับสนุนในด้านต่าง ๆ อย่างเพียงพอ เพราะการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องที่ยาก และจำเป็นต้องใช้ระยะเวลาในการทำความเข้าใจอย่างแท้จริง ซึ่งถ้าหากไม่ได้รับการสนับสนุนที่เพียงพอแล้ว ความสำเร็จจะเป็นไปได้ยากมากขึ้นไปอีก

๒.๓ ด้านเทคโนโลยี (Technology) ในปัจจุบันอุปกรณ์ หรือระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ที่มีความเหมาะสมสำหรับการเฝ้าระวัง และวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นลักษณะของ Log files จำนวนมหาศาลได้อย่างถูกต้องและแม่นยำถึงภัยคุกคามทางไซเบอร์นั้นยังไม่มีแต่สามารถนำมาใช้วิเคราะห์และตรวจสอบ Log files ที่มีจำนวนไม่มากนัก หรือเฉพาะกับหน่วยงานจำนวนไม่กี่หน่วยงานเท่านั้น ดังนั้นการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศของประเทศไทย (NCOC) ควรเป็นไปในลักษณะแบบแยกการ (Decentralize) น่าจะเหมาะสมที่สุด

๓. การจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC)

จากผลของการวิจัยที่ได้ศึกษามาทั้งหมดซึ่งประกอบด้วย ผลจากการวิจัยเอกสาร (Documentary Research) ผลจากการสัมภาษณ์เชิงลึก (In - Depth Interview) ผลจากการสนทนากลุ่ม (Focus Group Discussion) และผลจากการสังเกตการณ์ (Observation) พบว่า รูปแบบของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ที่มีการแบ่งประเภทของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ปี พ.ศ.๒๕๖๒ ออกเป็น ๘ ประเภท เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม ควรมีการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในแบบแยกการ (Decentralize) ที่จะเป็นรูปแบบการจัดตั้งที่เหมาะสมที่สุดสำหรับประเทศไทยในสถานการณ์ปัจจุบัน เพื่อให้สามารถปฏิบัติภารกิจในการบริหารจัดการ ตลอดจนเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ให้กับประเทศไทยได้อย่างแท้จริงและมีประสิทธิภาพ

แผนภาพที่ ๕ – ๑ แนวทางการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทั้ง ๘ ประเภท



ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

จากแผนภาพที่ ๕ – ๑ แสดงแนวทางการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัตการทางไซเบอร์แห่งชาติ (NCOC) ที่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่แบ่งออกเป็น ๘ ประเภท ในแบบแยกการ (Decentralize) ซึ่งแต่ละหน่วยงานที่มีความพร้อมทั้งงบประมาณ และกำลังพลที่เป็นบุคลากรทางไซเบอร์ ที่เพียงพอ สามารถจัดตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วยตนเอง หรือถ้าไม่พร้อม อาจจะต้องมีหน่วยที่ตั้ง JCOC กลางของกลุ่มงานตาม CII ที่มีการดำเนินงาน หรือการให้การบริการในรูปแบบเดียวกัน หรือในลักษณะที่คล้ายกัน เช่น การตั้ง JCOC ของกลุ่มงานธนาคาร โดยธนาคารต่าง ๆ อาจส่ง Log files เข้ามายัง CSOC ของธนาคารของตนเอง และส่ง Meta Data มาให้กับ JCOC เพื่อเป็นการช่วยกันในการเฝ้าระวังและตรวจจับปัญหาเหตุการณ์ทางไซเบอร์ร่วมกัน หรือถือได้ว่าเป็นการ Back Up การเฝ้าระวังและแก้ไขภัยคุกคามทางไซเบอร์อีกชั้นหนึ่งในห้วงเวลาเดียวกัน

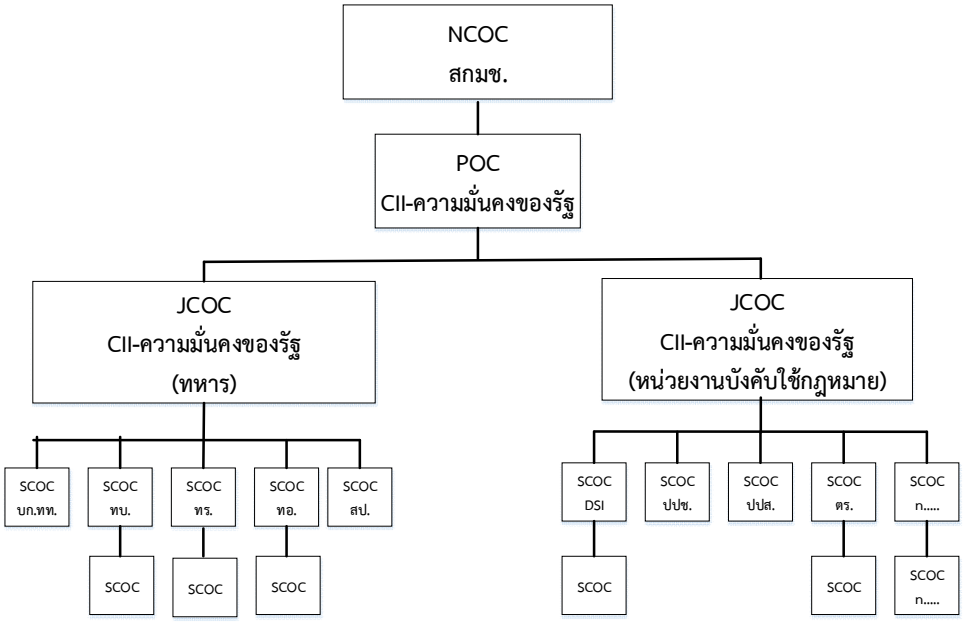
การตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของหน่วยงานที่ถูกจัดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) (Joint Cyberspace Operations : JCOC) ของประเทศ เพื่อร่วมในการแก้ปัญหาในกรณีที่ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วยงานใดหน่วยงานหนึ่ง ไม่สามารถแก้ปัญหาได้เอง หน่วยงานดังกล่าวจะส่งต่อปัญหาภัยคุกคามทางไซเบอร์ไปให้กับ JCOC และ JCOC จะทำหน้าที่ให้การบูรณาการให้เกิดการร่วมกันแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ ในลักษณะของการช่วยเหลือซึ่งกันและกันภายในหน่วยงานที่อยู่ใน Sector เดียวกันของ JCOC นั้น ๆ และภายหลังจากที่ทาง JCOC สามารถร่วมแก้ปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้แล้ว จะมีการส่งข้อมูลการโจมตีในรูปแบบของข้อมูลข่าวกรองทางไซเบอร์ (CTI) ไปยัง POC ของหน่วย CII

ที่ทำงานอยู่กับ NCOC เพื่อให้ NCOC ทำหน้าที่เป็นหน่วยงานกลางด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ที่จะทำหน้าที่ในการบูรณาให้เกิดการปฏิบัติงานร่วมกันในระดับประเทศ หรือข้าม Sector โดย NCOC จะดำเนินการแชร์ข้อมูล CTI ให้กับ JCOC ของ Sectors อื่น ๆ เพื่อจะทำให้ JCOC ของแต่ละ Sector นำข้อมูล CTI ที่ได้รับไปแชร์ต่อให้กับ CSOC ใน Sector ของตนเอง ไม่ให้ถูกโจมตีทางไซเบอร์ในลักษณะเดียวไนได้อีกต่อไป ซึ่งเป็นรูปแบบของการดำเนินการในลักษณะของการช่วยเหลือและพึ่งพาอาศัยกันรับมือและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ร่วมกันทั้งประเทศ

การจัดตั้งศูนย์บริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) นอกจากจะทำหน้าที่เป็นหน่วยงานที่ดำเนินการบูรณาการให้เกิดการแก้ปัญหาเหตุการณ์ทางไซเบอร์ร่วมกันทั้งประเทศแล้ว ยังมีหน้าที่ในการรวบรวมข้องมูลการโจมตีทางไซเบอร์ในรูปแบบข้อมูลข่าวกรองทางไซเบอร์ (CTI) ที่ได้มาจาก POC ของแต่ละหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ตามกลุ่มของ CII ซึ่งในปัจจุบันสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะต้องดำเนินการจัดตั้ง NCOC ของประเทศไทยขึ้นในระยะเวลาอันใกล้นี้ โดยมีหน้าที่ในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อรับมือและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศ (National Cybersecurity Incident Response Plan) ตลอดจนทำหน้าที่ในการประสานงาน และการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประสานงาน และให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ต่าง ๆ ทั้งในประเทศและต่างประเทศ ในส่วนที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการให้เกิดการทำงานร่วมกันทั้งประเทศ และเป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน เป็นต้น

๔. แนวทางการจัดตั้งศูนย์บริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในการปฏิบัติงานร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของหน่วยงานด้านความมั่นคงของรัฐ

แผนภาพที่ ๕ – ๒ ตัวอย่างการจัดตั้ง JCOC ของหน่วยงานด้านความมั่นคงของรัฐ



ที่มา : ประมวลโดยผู้วิจัย, ๒๕๖๔

จากแผนภาพที่ ๕ – ๒ แสดงถึงตัวอย่างของแนวทางในการจัดตั้ง JCOC ของหน่วยความมั่นคงของรัฐ ซึ่งภายในหน่วยความมั่นคงอาจแบ่งออกได้เป็น CII - ความมั่นคงของรัฐ (ทหาร) CII – ความมั่นคงของรัฐ (หน่วยบังคับใช้กฎหมาย) และอื่น ๆ โดยจากกรอบแนวทางการจัดตั้ง JCOC ของหน่วยความมั่นคงของรัฐ (ทหาร) สามารถจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วย ได้แก่ กองบัญชาการกองทัพไทย (บก.ทท.) กองทัพบก (ทบ.) กองทัพเรือ (ทร.) กองทัพอากาศ (ทอ.) และอาจมีศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของสำนักปลัดกลาโหม (สป.) มาขึ้นควบคุมทางยุทธการ เพื่อการแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ร่วมกันทั้งกระทรวงกลาโหม ซึ่งหน่วยงานเหล่านี้มีระดับข้อมูลที่เป็นชั้นความลับ และมีความพร้อมทั้งกำลังพล หรืองบประมาณสนับสนุนที่เพียงพอ เนื่องจากมีการดำเนินการในภารกิจการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสงครามไซเบอร์มานานกว่า ๕ ปีแล้ว จึงสามารถจัดตั้ง CSOC เองได้ และกรณีที่หน่วยงานภายใต้กองทัพไทยหรือกระทรวงกลาโหม มีหน่วยงานย่อย ๆ แยกออกไปยังส่วนต่าง ๆ ห่างไกลออกไป ก็อาจจะสามารถจัดตั้ง CSOC ย่อยออกไปอีกก็ได้ และเช่นเดียวกับหน่วยงานความมั่นคงของรัฐ (หน่วยงานบังคับใช้กฎหมาย) ได้แก่ กรมสอบสวนคดีพิเศษ (DSI) คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ (ป.ป.ช.) สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) สำนักงานตำรวจแห่งชาติ ถ้ามีความพร้อมทั้งด้านกำลังพลที่เป็นบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ และงบประมาณที่เพียงพอ ก็สามารถจัดตั้ง CSOC ของหน่วยเองตน แต่ถ้ายังไม่มีความพร้อมก็อาจจะต้องฝากหรืออาศัยให้หน่วยงานอื่นที่พร้อมกว่า ให้ช่วยดำเนินการวิเคราะห์ภัยคุกคามทางไซเบอร์แทนหน่วยงานของตนเองไปก่อนได้ จนกว่าหน่วยงานของตนเองจะมีความพร้อม

ทั้งนี้ การจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ (JCOC) ของหน่วยความมั่นคงของรัฐ (ทหาร) ซึ่งในปัจจุบันศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ได้ทำหน้าที่เป็น JCOC ของหน่วยความมั่นคงของรัฐ (ทหาร) อยู่แล้ว ซึ่งหน่วยความมั่นคงของรัฐ (บังคับใช้กฎหมาย) อาจจำเป็นที่จะต้องเลือกหน่วยงานที่มีความพร้อมมากที่สุด ให้ทำหน้าที่เป็น JCOC ซึ่งอาจจะเป็นหน่วยงานของสำนักงานตำรวจแห่งชาติหน่วยงานใดหน่วยงานหนึ่งที่มีความพร้อมมากที่สุดเป็นหน่วยดำเนินการในโอกาสต่อไป

ข้อเสนอแนะ

ในการศึกษาวิจัยในครั้งนี้ ผู้วิจัยได้แสดงข้อเสนอแนะสำหรับแนวทางการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ โดยข้อเสนอแนะได้แบ่งออกเป็น ๓ ส่วน ประกอบด้วย ข้อเสนอแนะเชิงนโยบาย การนำผลการวิจัยไปใช้ และแนวทางในการดำเนินการวิจัยในครั้งต่อไป ซึ่งมีรายละเอียดดังต่อไปนี้

๑. ข้อเสนอแนะเชิงนโยบาย

การหาแนวทางของการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ ควรมีการศึกษาวัตถุประสงค์ของการดำเนินการจัดตั้ง ปัญหาอุปสรรค และประโยชน์ที่จะได้รับจากการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์ในแต่ละรูปแบบให้ได้ข้อมูลที่แท้จริงให้มากที่สุด เพื่อที่จะนำไปสู่การลดปัญหาที่อาจจะเกิดขึ้นในอนาคต และการได้รับประโยชน์สูงสุดจากการตัดสินใจถึงรูปแบบของการดำเนินการ ให้สามารถบรรลุวัตถุประสงค์ในการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ซึ่งถือเป็นประเด็นสำคัญที่สุดในการจัดตั้งศูนย์ฯ ดังกล่าวขึ้นมา ซึ่งจะต้องสามารถทำให้เกิดการบูรณาการให้มีการทำงาน แก้ปัญหา ใช้ข้อมูลร่วมกันเพื่อประโยชน์ของประเทศด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือเป็นการดำเนินการร่วมกันของแต่ละกลุ่มงานของ CII เพื่อยกระดับการรักษาความมั่นคงปลอดภัยในระดับของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือการให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่คล้ายกัน ซึ่งตาม พรบ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ ได้แบ่ง CII ออกเป็น ๘ กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม ให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น พร้อมทั้งมีมาตรการในการป้องกันรับมือ และลดความเสี่ยงจากการถูกบุกรุกหรือถูกโจมตีทางไซเบอร์ที่อาจส่งผลกระทบต่อด้านความมั่นคงของรัฐ ด้านเศรษฐกิจ และด้านความสงบเรียบร้อยภายในประเทศได้อย่างทันท่วงที ทั้งนี้ ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ฯ ได้กำหนดให้ทุกหน่วยงานที่ถือว่าเป็นสาธารณูปโภคสำคัญของประเทศ (CII) จะต้องมีการกลไกและการบริหารจัดการที่นำไปสู่การแก้ไขปัญหาภัยคุกคามทางไซเบอร์

ที่อาจเกิดขึ้นกับหน่วยงานของตน และอาจส่งผลกระทบต่อประเทศในภาพรวม ซึ่งหน่วยงานดังกล่าวอาจจำเป็นต้องจัดตั้งกลไกในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้นมาด้วยศักยภาพของหน่วยงานของตนเอง หรือจ้างหน่วยงานเอกชนเข้ามาดำเนินการให้ ซึ่งในทางความมั่นคงปลอดภัยทางไซเบอร์นั้น มีความจำเป็นที่จะต้องดำเนินการใน ๓ ส่วนพร้อม ๆ กันไป ได้แก่ ด้านบุคลากร (People) ด้านกระบวนการบริหารจัดการ (Processes) และด้านเทคโนโลยี (Technologies)

ควรมีการส่งเสริมและเสริมสร้างขีดความสามารถในการปฏิบัติการร่วมในมิติไซเบอร์ของกองทัพไทย เพื่อให้มีความพร้อมและมีขีดความสามารถเพียงพอที่จะรับมือกับสงครามไซเบอร์ ซึ่งเป็นการดำเนินการจากรัฐบาลของประเทศคู่สงคราม (State Actor & State Sponsors) ในอนาคต

๒. การนำผลการวิจัยไปใช้

การวิจัยในครั้งนี้ได้ดำเนินการตามวัตถุประสงค์ของการวิจัยคือ เพื่อหาแนวทางของการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) นำเสนอข้อดี ข้อเสีย ของแต่ละรูปแบบของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ไปใช้ประโยชน์ในการพิจารณาในการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ต่อไปได้ในอนาคต ซึ่งการจะได้ประโยชน์สูงสุดควรนำแนวทางที่ได้นำเสนอในการวิจัยในครั้งนี้ นำไปเป็นแนวทางในการปฏิบัติจริง จากระดับสูงสุดของประเทศ ลงมาแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศเป็นรูปธรรมและมีประสิทธิภาพ ตลอดจนสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งจะทำหน้าที่เป็นหน่วยงานที่ดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ และจะต้องทำหน้าที่เป็นหน่วยงานหลักที่สามารถเป็นทั้งที่ปรึกษา กำกับดูแล แก้ไขปัญหา และสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ในทุกมิติ ก็ควรจะต้องศึกษาและนำงานวิจัยฉบับนี้ไปใช้ประโยชน์ได้ไม่มากก็น้อย

๓. แนวทางในการดำเนินการวิจัยในครั้งต่อไป

๓.๑. การวิจัยครั้งต่อไปควรมีการศึกษาให้ลงลึกแต่ละกลุ่มงานตามหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ที่อาจมีแนวทางในการดำเนินการที่แตกต่างกันได้ เนื่องจากรูปแบบของระบบเครือข่ายสารสนเทศที่มีความต่างกันทั้งด้านรูปแบบ และ Protocol ของระบบที่ใช้งานในแต่ละ CII เพื่อได้แนวทางการดำเนินการที่ชัดเจน และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ และเป็นรูปธรรมมากยิ่งขึ้นไปอีก

๓.๒. การวิจัยในครั้งต่อไปควรจะมีการลงลึกในเรื่องของวิธีการ (Process) ในการดำเนินการทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ในระดับประเทศ ให้ผู้อ่านสามารถนำไปเป็นแนวทางในการปฏิบัติได้เลย อีกทั้งควรมีการนำแนวทางในการปฏิบัติจากประเทศอื่น ๆ ที่ประสบความสำเร็จในการรับมือและบริหารจัดการกับเหตุการณ์ทางไซเบอร์ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพประกอบให้เห็นภาพของการปฏิบัติด้วย

บรรณานุกรม

ภาษาไทย

จินดา สระสมบูรณ์. “ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย”. วารสารสถาบันวิชาการป้องกันประเทศ. ๘(๓), หน้า ๕๗ - ๖๙.

เทคโนโลยีสารสนเทศและการสื่อสาร, กระทรวง. “แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ ๓) ของประเทศไทย พ.ศ.๒๕๕๗ - ๒๕๖๑”. ๒๕๕๗.

พนิดา พาณิชกุล. จริยธรรมทางเทคโนโลยีสารสนเทศ. กรุงเทพมหานคร : เค ที พี คอมพ์ แอนด์ คอนซัล, ปี ๒๕๖๒.

ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ. “ภัยคุกคามทางไซเบอร์ (Cyber Security)”. ๒๕๕๙.

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒”, ราชกิจจานุเบกษา. เล่มที่ ๑๓๖, ๒๗ พฤษภาคม ๒๕๖๒, หน้า ๔๒ – ๔๓.

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

“มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS)”. (Online). Available : https://www.iso.org/isoiec- 27001 - information -security.html, ๒๕๖๓.

“มาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems: ISMS)”. (Online). Available : https://www.iso.org/isoiec-27001-information-security.html, ๒๕๖๓.

วอนชนก ไชยสุนทร. “Internet of Things เมื่อทุกสิ่งเชื่อมต่ออินเทอร์เน็ต. วารสารครุรุศาสตร์อุตสาหกรรม”. (Online). Available : https://ph01.tci-thaijo.org/index.php/JIE/article/view/137017, ๒๕๕๘.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “ความหมาย APT”. (Online). Available : https://www.thaicert.or.th, ๒๕๕๔.

ศิวลีย์ สิริโรจน์บริรักษ์. “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม”. วารสาร สถาบันวิชาการป้องกันประเทศ. ปีที่ ๖(๓),. หน้า ๑๙ – ๒๙.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงคมนาคม. “แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงคมนาคม พ.ศ. 2562 – 2566”. ๒๕๖๒.

เลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, สำนักงาน. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.). “ยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๑ – ๒๕๘๐”. ๒๕๖๐.

คณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ, สำนักงาน, “เทคโนโลยี Internet of Things และนโยบาย Thailand ๔.๐”. ๒๕๖๐.

สฤษดิ์พงษ์ ลิมปิษเฐียร. “ความมั่นคงปลอดภัยด้านสารสนเทศของนักศึกษา”. ประกาศ นียบัตรบัณฑิต ทางการบริหารการศึกษา, มหาวิทยาลัยสุโขทัยธรรมาธิราช”. ๒๕๕๘.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “มาตรฐานและมาตรการ ที่พึงนาไปใช้เป็นกรอบในการทางานเพื่อลดความเสี่ยง”. เอกสารประกอบการประชุม. ๒๕๖๑.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. “การจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย”. เอกสารประกอบการประชุม. ๒๕๖๑.

อรรคเดช ประทีปอุษานนท์. “แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์”. วารสารสถาบันวิชาการป้องกันประเทศ. ปีที่ ๘(๓), หน้า ๑๑ – ๒๓.

ฤทธี อินทราวุธ. “โดเมน ที่ ๕ / โลกไซเบอร์ กับ ความมั่นคงของมนุษย์”. (Online). เข้าถึงได้จาก : http://rittee1834.blogspot.com/2013/12/blog-post.html. ๒๕๕๖.

ThaiCERT. “สถิติภัยคุกคาม”. (Online). Available : https://www.thaicert.or.th/statistics2015.html, ๒๕๕๘.

Techtalkthai. “5 เทคนิคการป้องกัน Advanced Persistent Threats”. (Online). Available : https://www.techtalkthai.com, ๒๕๖๓.

ภาษาต่างประเทศ

Andrew Spender. “Gartner’s Top 10 Strategic Technology Trends for 2558”. (Online). Available : https://ph01.tci-thaijo.org/index.php/JIE/article/view/137017, 2015.

Earl Perkins. “Operational Technology Security – Focus on Securing Industrial Control and Automation Systems.” (Online) Available : https://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security- focus-on-securing-industrial-control-and-automation-systems/, 2014.

FORTINET. “What Is Operational Technology (OT)? Retrieved by 10 September 2020”. (Online). Available : https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security, 2014.

Kaspersky. “Types of known threats”. (Online). Available : https://support.kaspersky.com, 2019.

National Institute of Standards and Technology. “หลักการทำงานของ NIST Cybersecurity Framework”. (Online). Available : https://www.nist.gov/cyberframework, 2020.

Pescatore, John. “Security Operations Center (SOC) Essential Functions”. (Online) Available : https://www.sans.org/security-resources/posters/security-leadership-poster/135 /download, 2020.

Techtalkthai. “Tag Archives: unknown threats”. (Online). Available : https://www.techtalkthai.com/ tag/unknown-threats/, 2016.

ผนวก ก

ภาพบรรยากาศการสัมภาษณ์เชิงลึก (In - Depth Interview)

โดยผู้ทรงคุณวุฒิ

พล.ต. นภดล แก้วกำเนิด

พล.อ.ต. สมพร ร่มพยอม

พ.อ. พงศ์พัฒน์ ขันธเขตต์

น.อ. จเด็ด คูหะก้องกิจ

พ.ต.ท. กัมพล พงษ์แสงศรี

พ.ต.ท. พรชัย โฆษิตสุรังคกุล

พ.ต.ต. จตุพร อรุณฤทษ์ถวิล

ภาพที่ ๑ ผู้เข้าร่วมการสนทนากลุ่ม (Focus Group)
ประชุมเมื่อวันที่ ๒๑ ธันวาคม ๒๕๖๓

ผนวก ข

ภาพบรรยากาศการประชุมสนทนากลุ่ม

(Focus Group Discuccion)

ภาพที่ ๑ ผู้เข้าร่วมการสนทนากลุ่ม (Focus Group Discussion) (๑)
ประชุมเมื่อวันที่ ๒๑ ธันวาคม ๒๕๖๓

ภาพที่ ๓ ผู้เข้าร่วมการสนทนากลุ่ม (Focus Group Discussion) (๒)
ประชุมเมื่อวันที่ ๒๑ ธันวาคม ๒๕๖๓

ภาพที่ ๔ ผู้เข้าร่วมการสนทนากลุ่ม (Focus Group Discussion) (๓)
ประชุมเมื่อวันที่ ๒๑ ธันวาคม ๒๕๖๓

ภาพที่ ๕ เป็นบรรยากาศผู้เข้าร่วมการสนทนากลุ่ม (Focus Group Discussion)
ประชุมเมื่อวันที่ ๒๑ ธันวาคม ๒๕๖๓

ประวัติผู้วิจัย

ยศ ชื่อ/สกุล พล.ต. ชาติชาย ชัยเกษม

วัน/เดือน/ปีเกิด ๒๗ ก.ย. ๒๕๑๐

การศึกษา ป.ตรี - วทบ.ทบ. (ตท.๒๖, จปร.๓๗)

ป.โท - Master of Arts in Strategic and Security Studies,
College of international Security Affair, US National Defense University

ป.เอก - รัฐศาสตรดุษฎีบัณฑิต สาขายุทธศาสตร์และความมั่นคง มหาวิทยาลัยบูรพา

การศึกษาด้านไซเบอร์ - Network penetration and ethical hacking (SANS - 2014)

- Managing of digital forensics unit (Data Expert - 2014)
- Cyber assurance workshop (Risk, security, privacy and resilience in action) (Prof. Edward (Ted) Humphreys - Chair of the ISO/IEC JTC 1/SC27-2015)
- Cyber Threat Intelligence (SANS - 2016)
- SANS training program for CISSP certification (SANS - 2016)
- Managing Security Operations: detection, response, and intelligence (SANS - 2017)
- Military Strategy and Tactics for Cyber Security (Blackhat USA – 2018)

ประกาศนียบัตรด้านไซเบอร์ : - CompTIA Security+

- CompTIA Cyber Security Analyst+
- CompTIA Pentest+
- CompTIA Advanced Security Practitioner+
- CompTIA Certified Technical Trainer+
- CompTIA Security Analytics Professional
- CompTIA Network Security Professional
- CompTIA Network Vulnerability Assessment Professional
- CompTIA Security Analytics Expert
- CompTIA Secure Infrastructure Expert
- Certified Ethical Hacker
- Computer Hacking Forensic Investigation
- Certified EC – Council Instructor

ประวัติการทำงานโดยย่อ

ตำแหน่งสำคัญในอดีต - ผู้บังคับกองพันจู่โจม (พ.ศ.๒๕๔๖ - ๒๕๔๙)

- รองผู้ช่วยทูตทหารและรองผู้ช่วยทูตทหารบก ณ กรุงวอชิงตัน ดีซี ประเทศสหรัฐ (พ.ศ.๒๕๕๐ - ๒๕๕๓)
- ผู้อำนวยการกองสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (พ.ศ.๒๕๕๗ - ๒๕๖๐)

ประสบการณ์ที่สำคัญ - ราชการพิเศษกัมพูชา ๓ ปี

- ราชการพิเศษพม่า ๕ เดือน
- ผู้สังเกตการณ์ทางทหารของสหประชาชาติ (UNMO) ประเทศติมอร์ตะวันออก ๑ ปี
- ผู้บังคับกองพันจู่โจม สนับสนุน ๑ กองร้อยจู่โจมปฏิบัติงานใน ๓ จังหวัดชายแดนภาคใต้ ตั้งแต่ ปี พ.ศ.๒๕๔๗ - ๒๕๔๙
- Team leader for writing 1st Thailand National Military Strategy in 2015
- Team leader for writing 1st Thailand National Military Strategy for Cyberwarfare in 2015
- Team member for writing 1st Thailand Cyber Security Strategy in 2018
- Team member for writhing 1 Thailand Cyber Security Law (Draft)

ตำแหน่งปัจจุบัน - ผู้อำนวยการศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมบทคัดย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอแห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม

ผู้วิจัย พลตรี ชาติชาย ชัยเกษม **หลักสูตร** วปอ. **รุ่นที่** ๖๓

ตำแหน่ง ผู้อำนวยการศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการ กองบัญชาการกองทัพไทย

ความเป็นมาและความสำคัญของปัญหา

ประเทศไทยได้มีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมีวัตถุประสงค์เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น ๘ กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม โดย พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้กำหนดให้ทุกหน่วยงานที่ถือว่าเป็นสาธารณูปโภคสำคัญของประเทศ จะต้องมีการกลไกและการบริหารจัดการที่นำไปสู่การแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานของตน และอาจส่งผลกระทบต่อประเทศในภาพรวม

การตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ อาจสามารถดำเนินการได้ใน ๒ รูปแบบหลัก ๆ ได้แก่ การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) และแบบแยกการ (Decentralize) โดยที่การตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแบบรวมการนั้น มีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรทางคอมพิวเตอร์จากทุก ๆ หน่วยงานที่มีระบบการป้องกัน เฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ไปยังศูนย์กลางเฝ้าระวังภัยคุกคามทางไซเบอร์เพียงที่เดียว ซึ่งในประเทศไทยได้มีการริเริ่มที่จะนำเอาแนวคิดของการจัดตั้ง NCOC แบบรวมการ มาดำเนินการแล้วเช่นกัน ซึ่งถือว่าเป็นเป็นแนวคิดที่ดีที่มีความพยายามทำให้เกิดการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ขึ้นในระดับประเทศ

ผู้วิจัยได้นำเสนอแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ที่จะต้องเป็นกลไกหลักในระดับประเทศในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ ซึ่งภายหลังจากการออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๒ แล้ว ประเทศไทยได้มีการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ขึ้น แต่หัวใจของการดำเนินการและรับมือกับภัยคุกคามทางไซเบอร์คือ Cyber Security Operations Center หรือ CSOC ที่จะเป็นส่วนงานของการทำหน้าที่ Identify, Protect, Detect, Response และ Recovery ต่อภัยคุกคามทางไซเบอร์ให้กับองค์กร ที่นำเอาระบบเครือข่ายเทคโนโลยีสารสนเทศมาใช้บริหารจัดการทางธุรกิจหรือการปฏิบัติงานขององค์กร แต่การที่ดำเนินการด้าน CSOC ของ สกมช. ในระดับประเทศหรือ NCOC นั้น ยังไม่มีการออกแบบหรือวางแนวทางในการดำเนินการอย่างชัดเจนในระดับประเทศ ดังนั้นงานวิจัยฉบับนี้จึงมุ่งเน้นและมีความต้องการที่จะศึกษาถึงปัญหาและรูปแบบของการดำเนินการของ NCOC ในระดับประเทศ ที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ ตลอดจนศึกษาแนวทางการทำงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในรูปแบบต่าง ๆ ที่ใช้กันอยู่ในระดับนานาชาติ และในท้ายที่สุดจะนำเสนอแนวทางในการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาทางไซเบอร์แห่งชาติ หรือศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศได้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและการปฏิบัติงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยในห้วงที่ผ่านมา

๒. เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

๓. เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

ขอบเขตของการวิจัย

การวิจัยเรื่อง แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ มีขอบเขตของการเก็บรวบรวมข้อมูลวิจัยออกเป็น ๔ วิธีการ ได้แก่

๑. การดำเนินการวิจัยจากเอกสาร (Documentary Research) จะเป็นการทำการวิจัยจากเอกสารต่าง ๆ ที่เกี่ยวข้องกับหัวข้อการวิจัย เพื่อให้มาซึ่งแนวคิด และทฤษฎีที่เกี่ยวข้องกับการดำเนินการ

ด้านความมั่นคงปลอดภัยความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ตลอดจนหาแนวทางและองค์ความรู้เกี่ยวกับการจัดตั้งและการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ

๒. การสัมภาษณ์เชิงลึก (In - Depth Interview) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสัมภาษณ์จากกลุ่มเป้าหมาย ซึ่งเป็นบุคคลที่มีความผู้เชี่ยวชาญ และมีประสบการณ์ด้านการบริหารจัดการและการรับมือภัยคุกคามทางไซเบอร์จริง ๆ เท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน ๕ - ๑๐ ท่าน ที่เป็นผู้แทนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ในระดับประเทศ

๓. การสนทนากลุ่ม (Focus Group Discussion) โดยใช้ข้อมูลปฐมภูมิ (Primary Data) จากการสนทนากลุ่มที่รวบรวมข้อมูลจากการสนทนากับกลุ่มผู้ให้ข้อมูลในประเด็นปัญหา กลุ่มเป้าหมาย จำนวน ๕ - ๑๐ ท่าน ที่เป็นผู้แทนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ในระดับประเทศ

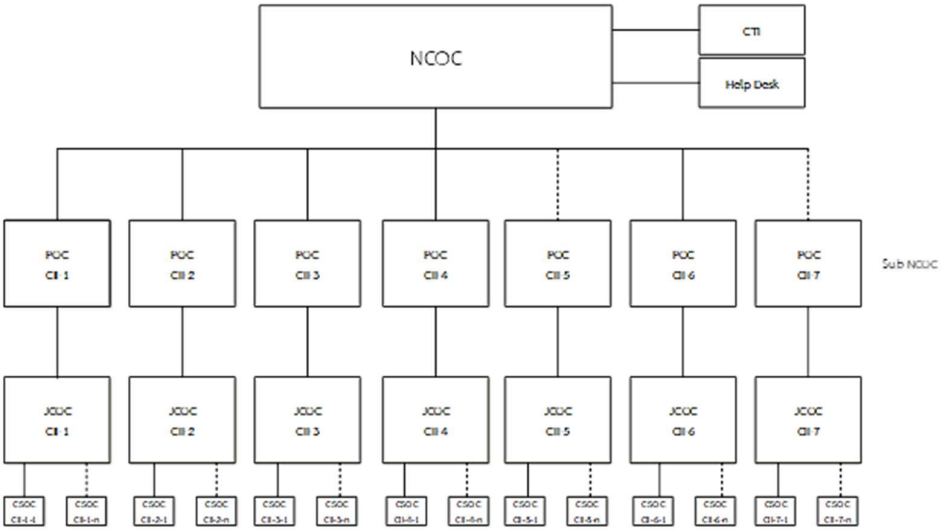
๔. การสังเกตการณ์ (Observation) การสังเกตจากตัวนักวิจัยเองซึ่งเป็นผู้มีความรู้และประสบการณ์ตรงด้านจัดการบริหารจัดการ และการรับมือกับภัยคุกคามทางไซเบอร์ในระดับกองทัพไทยและในระดับประเทศมาเป็นเวลานานกว่า ๘ ปี

วิธีดำเนินการวิจัย

ภายหลังจากการเก็บรวบรวมข้อมูลทั้ง ๔ วิธีการ ได้แก่ การดำเนินการวิจัยจากเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In - Depth Interview) การสนทนากลุ่มเฉพาะ (Focus Group Discussion) และการสังเกตการณ์ (Observation) เพื่อให้ทราบถึงแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้องในเรื่องของการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางในการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติในหลากหลายรูปแบบ จะมีการนำเอาข้อมูลที่ได้จากการเก็บรวบรวมข้อมูลไปวิเคราะห์หาจุดเด่นและจุดด้อยของการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติทั้งที่เป็นแบบรวมการ และแบบแยกการ และประมวลแนวคิดตลอดจนสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ นำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤต ทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ และเพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคต

ผลการวิจัย

การจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) แบบแยกการ (Decentralize) เป็นทางออกที่มีประสิทธิภาพมากที่สุด โดยการตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของแต่ละหน่วยแยกออกจากกัน หรือถ้าหน่วยงานใดไม่มีความพร้อมทั้งด้านงบประมาณและบุลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อาจจะต้องมีการจัดตั้ง CSOC รวมกับหน่วยอื่นที่อยู่ใน CII เดียวกัน โดยมีพฤติกรรมและวัตถุประสงค์ของการรักษาความปลอดภัยของข้อมูลที่คล้ายกัน ดังภาพที่ ๑



ภาพที่ ๑ การดำเนินงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติของประเทศไทยที่สามารถปฏิบัติงาน ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

จากภาพที่ ๑ แสดงแนวทางการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย (NCOC) ที่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่แบ่งออกเป็น ๘ ประเภท ในแบบแยกการ (Decentralize)

การตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของหน่วยงานที่ถูกจัดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Joint Cybersecurity Operations Center: JCOC) ของประเทศ เพื่อร่วมในการแก้ปัญหาในกรณีที่ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วยงานใดหน่วยงานหนึ่ง ไม่สามารถแก้ปัญหาได้เอง หน่วยงานดังกล่าวจะส่งต่อปัญหาภัยคุกคามทางไซเบอร์ไปให้กับ JCOC และจะทำหน้าที่ให้การบูรณาการให้เกิดการร่วมกันแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ ในลักษณะของการช่วยเหลือซึ่งกันและกันภายในหน่วยงานที่อยู่ใน Sector เดียวกันของ JCOC นั้น ๆ และภายหลังจากที่ทาง JCOC สามารถร่วมแก้ปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้แล้ว จะมีการส่งข้อมูลการโจมตีในรูปแบบของข้อมูลข่าวกรองทางไซเบอร์ (CTI) ไปยัง Point of Contact หรือ POC ของหน่วย CII ที่ทำงานอยู่กับ NCOC เพื่อให้ NCOC ทำหน้าที่เป็นหน่วยงานกลางด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ในการแชร์ข้อมูลข่าวกรองทางไซเบอร์ (CTI) ให้กับ Sector อื่น ๆ ต่อไป

การจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย (NCOC) นอกจากจะทำหน้าที่เป็นหน่วยงานที่ดำเนินการบูรณาการให้เกิดการแก้ปัญหาเหตุการณ์ทางไซเบอร์ร่วมกันทั้งประเทศแล้ว ยังมีหน้าที่ในการรวบรวมข้องมูลการโจมตีทางไซเบอร์ในรูปแบบข้อมูลข่าวกรองทางไซเบอร์ (CTI) ที่ได้มาจาก POC ของแต่ละหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ตามกลุ่มของ CII ซึ่งในปัจจุบันสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะต้องดำเนินการจัดตั้ง NCOC ของประเทศไทยขึ้นในระยะเวลาอันใกล้นี้ โดยนอกจากมีหน้าที่ในการบูรณาการให้เกิดการ

เฝ้าระวังและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศแล้ว ยังต้องทำหน้าที่ในการจัดทำแผนการรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ในระดับประเทศ (National Cybersecurity Incident Response Plan) ตลอดจนทำหน้าที่ในการประสานงาน และการบูรณาการให้เกิดการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใน Sectors ต่าง ๆ และยังต้องประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ต่าง ๆ ทั้งในระดับประเทศ และในระดับนานาชาติอีกด้วย

ข้อเสนอแนะ

ในการศึกษาวิจัยในครั้งนี้ ผู้วิจัยได้แสดงข้อเสนอแนะสำหรับแนวทางการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ โดยข้อเสนอแนะได้แบ่งออกเป็น ๓ ส่วน ประกอบด้วย ข้อเสนอแนะเชิงนโยบาย การนำผลการวิจัยไปใช้ และแนวทางในการดำเนินการวิจัยในครั้งต่อไป ซึ่งมีรายละเอียดดังต่อไปนี้

๑. ข้อเสนอแนะเชิงนโยบาย

การหาแนวทางของการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ควรมีการศึกษาวัตถุประสงค์ของการดำเนินการจัดตั้ง ปัญหาอุปสรรค และประโยชน์ที่จะได้รับจากการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์ในแต่ละรูปแบบให้ได้ข้อมูลที่แท้จริงให้มากที่สุด เพื่อที่จะนำไปสู่การลดปัญหาที่อาจจะเกิดขึ้นในอนาคต และการได้รับประโยชน์สูงสุดจากการตัดสินใจถึงรูปแบบของการดำเนินการ ซึ่งในทางความมั่นคงปลอดภัยทางไซเบอร์นั้น มีความจำเป็นที่จะต้องดำเนินการใน ๓ ส่วนพร้อม ๆ กันไป ได้แก่ ด้านบุคลากร (People) ด้านกระบวนการบริหารจัดการ (Processes) และด้านเทคโนโลยี (Technologies)

๒. การนำผลการวิจัยไปใช้

การวิจัยในครั้งนี้ได้ดำเนินการตามวัตถุประสงค์ของการวิจัยคือ เพื่อหาแนวทางของการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) นำเสนอข้อดี ข้อเสีย ของแต่ละรูปแบบของการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ไปใช้ประโยชน์ในการพิจารณาในการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ต่อไปได้ในอนาคต ซึ่งการจะได้ประโยชน์สูงสุดควรนำแนวทางที่ได้นำเสนอในการวิจัยในครั้งนี้ นำไปเป็นแนวทางในการปฏิบัติจริง จากระดับสูงสุดของประเทศ ลงมาแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศเป็นรูปธรรมและมีประสิทธิภาพ

๓. แนวทางในการดำเนินการวิจัยในครั้งต่อไป

การวิจัยครั้งต่อไปควรมีการศึกษาให้ลงลึกแต่ละกลุ่มงานตามหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ที่อาจมีแนวทางในการดำเนินการที่แตกต่างกันได้ เนื่องจากรูปแบบของระบบเครือข่ายสารสนเทศที่มีความต่างกันทั้งด้านรูปแบบ และ Protocol ของระบบที่ใช้งานในแต่ละ CII เพื่อได้แนวทางการดำเนินการที่ชัดเจน และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพและเป็นรูปธรรมมากยิ่งขึ้นไปอีก