บทความวิจัย

แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม

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

ชาติชาย ชัยเกษม

ศูนย์ไซเบอร์ทหาร

127 กองบัญชาการกองทัพไทย อาคาร 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

Chartchai Chaigasem

Royal Thai Armed Forces Cyber Center

127 Royal Thai Armed Forces Headquarter, Building 7, Changwattana Road Laksi, Bangkok 10210

E-mail: chartchaichaigasem@gmail.com

วันที่รับบทความ : 8 กุมภาพันธ์ 2565

วันที่แก้ไขบทความ : 15 กุมภาพันธ์ 2565

วันที่ตอบรับบทความ : 11 มีนาคม 2565

บทคัดย่อ

ภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันได้ทวีความรุนแรงและมีความซับซ้อนมากขึ้นอย่างต่อเนื่อง ที่ส่งผลกระทบตั้งแต่ในระดับบุคคล ระดับองค์กรทั้งภาครัฐฯ และภาคเอกชน ระดับประเทศและระดับโลก ทั้งนี้ หัวใจของการรับมือกับเหตุการณ์การถูกโจมตีทางไซเบอร์ในระดับองค์กรขนาดใหญ่ที่มีการนำเอาระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ระบบควบคุมการทำงานของเครื่องจากหรือกลไกขนาดใหญ่ด้วยระบบเครือข่ายคอมพิวเตอร์ (Operational Technology: OT) และระบบอินเทอร์เน็ตสรรพสิ่ง (Internet of Things: IOT) ที่มีมูลค่าสูงมาใช้ในการทำให้การปฏิบัติงานขององค์กรเกิดความมีประสิทธิภาพและมีความสะดวกสบายมากยิ่งขึ้น

ทั้งนี้ มีความสับสนกันอย่างมากสำหรับแนวทางในการจัดตั้ง และการดำเนินการของศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศหรือศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) ว่าควรจะมีลักษณะของการดำเนินการเช่นไร จะเป็นเหมือนกับการจัดตั้ง CSOC ขององค์กรขนาดใหญ่ทั่วไปหรือจะมีลักษณะพิเศษเป็นอย่างไร ซึ่งหลายประเทศและรวมทั้งประเทศไทยยังมีการดำเนินการที่ไม่ค่อยจะถูกต้องนัก ดังนั้นงานวิจัยฉบับนี้จึงมีความตั้งใจจะค้นหาปัญหาที่เกิดขึ้น วิธีการที่ควรจะนำมาเป็นตัวเลือกในการดำเนินการสำหรับ NCOC และแนวทางที่จะเสนอแนะให้ประเทศไทยดำเนินการจัดตั้ง NCOC ที่เป็นรูปธรรมและมีประสิทธิภาพ

คำสำคัญ : ภัยคุกคามทางไซเบอร์, ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศ, ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

Abstract

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.

Keywords: Cybersecurity Threat, National Cybersecurity Operations Center, Cyber Security Operations Center

บทนำ

ประเทศไทยได้มีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ที่เป็นทั้งหน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น 8 กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม โดย พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้กำหนดให้ทุกหน่วยงานที่ถือว่าเป็นสาธารณูปโภคสำคัญของประเทศจะต้องมีการกลไกและการบริหารจัดการที่นำไปสู่การแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานของตน และอาจส่งผลกระทบต่อประเทศในภาพรวม

การตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ อาจสามารถดำเนินการได้ใน 2 รูปแบบหลัก ๆ ได้แก่ การตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) และแบบแยกการ (Decentralize)โดยที่แต่ละแบบนั้นจะมีข้อดีและข้อเสียที่แตกต่างกันไป

ผู้วิจัยได้นำเสนอแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ที่จะต้องเป็นกลไกหลักในระดับประเทศในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ ทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ ซึ่งภายหลังจากการออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 แล้ว ประเทศไทยได้มีการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ขึ้น แต่หัวใจของการดำเนินการและรับมือกับภัยคุกคามทางไซเบอร์คือ Cyber Security Operations Center หรือ CSOC ที่จะเป็นส่วนงานของการทำหน้าที่ Identify, Protect, Detect, Response และ Recover ต่อภัยคุกคามทางไซเบอร์ให้กับองค์กร ที่นำเอาระบบเครือข่ายเทคโนโลยีสารสนเทศมาใช้บริหารจัดการทางธุรกิจหรือการปฏิบัติงาน แต่การที่ดำเนินการด้าน CSOC ของสกมช. ในระดับประเทศหรือ NCOC นั้น ยังไม่มีการออกแบบหรือวางแนวทางในการดำเนินการอย่างชัดเจน ดังนั้นงานวิจัยฉบับนี้จึงมุ่งเน้นและมีความต้องการที่จะศึกษาถึงปัญหาและรูปแบบของการดำเนินการของ NCOC ในระดับประเทศ ที่จะนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศ ตลอดจนศึกษาแนวทางการทำงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในรูปแบบต่าง ๆ ที่ใช้กันอยู่ในระดับนานาชาติ และในท้ายที่สุดจะนำเสนอรูปแบบและแนวทาง ในการจัดตั้งศูนย์เฝ้าระวังและแก้ไขปัญหาทางไซเบอร์แห่งชาติหรือศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ในระดับประเทศ สำหรับประเทศไทยที่สามารถปฏิบัติงานได้จริงอย่างเป็นรูปธรรมและมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center : NCOC) ของประเทศไทยในห้วงที่ผ่านมา
2. เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและ ข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) ที่เป็นแบบรวมการและแยกการ
3. เพื่อเสนอแนวทางในการจัดตั้งและดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1. ได้ทราบความเป็นมาและปัญหาในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

2. ได้ทราบความเหมือน ความต่าง และข้อดีข้อเสียการดำเนินงานของศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติในแบบรวมการและแยกการ

3. ได้แนวทางในการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์แห่งชาติได้ในอนาคต

4. งานวิจัยฉบับนี้จะเป็นแนวทางให้กับหน่วยงานที่ถือเป็นสาธารณูปโภคพื้นฐานสำคัญของประเทศได้เข้าใจถึงปัญหาในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเป็นแนวทางในการดำเนินการจัดตั้งหน่วยงานของตนเพื่อการรับมือกับภัยคุกคามทางไซเบอร์

5. งานวิจัยฉบับนี้จะเป็นแนวทางให้กับ สกมช. ในการนำไปใช้ในการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์แห่งชาติได้ในอนาคต

6. งานวิจัยฉบับนี้จะทำให้ผู้ที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนผู้ที่สนใจสามารถเข้าใจถึงแนวทางในการบริหารจัดการและการปฏิบัติการทางไซเบอร์ในระดับประเทศ มีความเข้าใจระบบการบริหารจัดการด้านไซเบอร์ในระดับประเทศที่เป็นไปในทิศทางเดียวกันและจะนำไปสู่การทำงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ในระดับประเทศร่วมกันได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

การทบทวนวรรณกรรม

การทบทวนวรรณกรรมในการวิจัยครั้งนี้ ผู้วิจัยได้ศึกษาทฤษฎีที่เกี่ยวข้องกับแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ ได้มีการนำทฤษฎีและแนวคิดที่เกี่ยวข้องมาใช้เพื่อเป็นแนวทางในการศึกษา ดังนี้

1. เทคโนโลยี ในปัจจุบัน ศึกษา เทคโนโลยีสารสนเทศ (Information Technology: IT) เทคโนโลยีเชิงปฏิบัติการ (Operational Technology: OT) และเทคโนโลยี (Internet of Things : IoT)

2. พื้นฐานการรักษาความปลอดภัย และภัยคุกคามทางไซเบอร์เพื่อศึกษารูปแบบ ประเภทและความรุนแรงของการโจมตีทางไซเบอร์ในปัจจุบัน

3. ยุทธศาสตร์ชาติ และกฎหมายที่เกี่ยวข้องกับไซเบอร์เกี่ยวกับการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ซึ่งจำเป็นต้องศึกษายุทธศาสตร์ชาติ พ.ร.บ. คอมพิวเตอร์ฯ พ.ศ. 2562 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรฐานการรักษาความปลอดภัยทางไซเบอร์และการจัดตั้งหน่วยพื้นฐานสำคัญทางสารสนเทศ (CII) ตลอดจนการรับมือภัยคุกคามระดับประเทศ

อย่างไรก็ตามผู้วิจัยได้ศึกษาแนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติแต่ละแบบ ทั้งเอกสารและงานวิจัยที่เกี่ยวข้อง ตลอดจนศึกษาข้อมูลเพิ่มเติม ตั้งแต่อดีตจนถึงปัจจุบันจนสามารถวิเคราะห์ถึงจุดเด่น และจุดด้อยของการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ซึ่งสามารถเลือกรูปแบบได้ 2 รูปแบบ ได้แก่ การจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ แบบรวมการ (Centralize) และแบบแยกการ (Decentralize) และได้ศึกษาปัจจัยที่ส่งผลต่อปัญหาในการจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ทั้งทางด้านบุคลากร (People) ด้านกระบวนการบริหารจัดการ (Processes) และด้านเทคโนโลยี (Technologies) ร่วมด้วย

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้มุ่งเน้นศึกษาถึงทฤษฎีและหลักการในการดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เอกสารงานวิจัยที่เกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ ยุทธศาสตร์ด้านไซเบอร์ กฎหมายต่าง ๆ ที่เกี่ยวข้องในการปฏิบัติงานของเจ้าหน้าที่ ข้อมูลพื้นฐานที่เกี่ยวกับศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์และศูนย์ปฏิบัติการร่วมทางไซเบอร์ โครงสร้างการจัด ระเบียบปฏิบัติ เพื่อนำข้อมูลที่รวบรวมได้ มาออกแบบสำหรับเป็นแนวทางในการดำเนินการตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับประเทศ

2. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

กลุ่มตัวอย่าง การเลือกกลุ่มตัวอย่าง (Sampling) โดยเลือกกลุ่มตัวอย่างประเภทการเลือกกลุ่มตัวอย่างที่เป็นตัวแทน (Typing Cases Sampling) เป็นลักษณะการเลือกแบบเจาะจง (Purposive Sampling) เฉพาะบุคคลที่เป็นผู้เชี่ยวชาญ และผู้มีประสบการณ์ในด้านการบริหารจัดการหรือรับมือภัยคุกคามทางไซเบอร์มาแล้วเท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน 5-8 ท่าน และสรรหาผู้เข้าร่วมในการสนทนากลุ่มอีกจำนวนประมาณ 5-10 ท่าน จากกลุ่มประชากรที่เกี่ยวข้องในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ได้กำหนดให้มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ไว้จำนวน 8 ประเภท

3. ขอบเขตเวลา

ทำการศึกษาในช่วงตั้งแต่เดือนธันวาคม 2563 ถึง พฤษภาคม 2564

วิธีดำเนินการวิจัย

งานวิจัยเรื่อง “แนวทางการตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม” จะเป็นการดำเนินการในลักษณะของการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยกระบวนการศึกษาทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องกับเรื่องที่ศึกษา เพื่อให้ได้กรอบแนวคิดในการวิจัยที่เกิดจากกระบวนการวิเคราะห์และสังเคราะห์

1. การเก็บรวบรวมข้อมูล

1.1 การดำเนินวิจัยจากเอกสารต่าง ๆ ที่เกี่ยวข้อง (Documentary Research)

เพื่อให้ทราบถึงแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้องในเรื่องของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) ในหลากหลายรูปแบบ ตลอดจนวิเคราะห์หาข้อเด่นและข้อด้อยของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ทั้งที่เป็นแบบรวมการและแบบแยกการ

1.2 การสัมภาษณ์เชิงลึก (In-Depth Interview)

จะเป็นการดำเนินการสัมภาษณ์กลุ่มเป้าหมายทั้งบุคคลที่เป็นผู้เชี่ยวชาญและมีประสบการณ์ด้านการรับมือภัยคุกคามทางไซเบอร์จริง ๆ เท่านั้น เพื่อใช้ในการเก็บข้อมูลสัมภาษณ์เชิงลึก จำนวน 5-8 ท่าน จากตัวแทนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยเป็นการสัมภาษณ์แบบกึ่งโครงสร้าง หรือการสัมภาษณ์แบบชี้นำ (Guided Interview) กล่าวคือเป็นการสัมภาษณ์ที่มีการใช้คำสำคัญ (Keywords) มาประกอบในการสัมภาษณ์มีการร่างข้อคำถามที่มีลักษณะปลายเปิดพร้อมกับลักษณะของข้อคำถามที่มีความยืดหยุ่น พร้อมที่จะมีการปรับเปลี่ยนถ้อยคำของข้อคำถามให้มีความสอดคล้องกับผู้ให้สัมภาษณ์แต่ละคนในแต่ละสถานการณ์ได้ตอบข้อคำถามอันทำให้ได้มาซึ่งข้อมูลที่มีความหลากหลายในมิติต่าง ๆ และข้อเท็จจริงในทางปฏิบัติที่มีทั้งมิติของความลึกและมิติของความกว้างในเรื่องที่เกี่ยวข้องกับงานวิจัย เพื่อใช้เป็นข้อมูลในการวิเคราะห์และศึกษาปัจจัยสำคัญทำให้สามารถนำข้อมูลที่ได้มาวิเคราะห์หาแนวทาง และรูปแบบของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพต่อไป

1.3 การสนทนากลุ่มเฉพาะ (Focus Group Discussion)

ในการสนทนากลุ่มที่ผู้วิจัยจะทำการรวบรวมข้อมูลจากการสนทนากับกลุ่มผู้ให้ข้อมูลในประเด็นปัญหา โดยผู้วิจัยได้ออกแบบโครงสร้างของข้อคำถามเพื่อนำไปใช้ในการประชุมสนทนากลุ่มซึ่งการใช้กระบวนการการเลือกกลุ่มแบบเจาะจงในการสำรวจข้อมูล จำนวน 5-8 ท่านจากตัวแทนศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย ศูนย์ไซเบอร์กองทัพบก ศูนย์ไซเบอร์กองทัพอากาศ ศูนย์ไซเบอร์กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ ศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ตลอดจนหน่วยงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายนอกกระทรวงกลาโหม เพื่อประมวลแนวคิดและสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cybersecurity Operations Center: NCOC) เพื่อนำไป

สู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ เพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคต

1.4 การสังเกตการณ์ (Observation)

จะเป็นการใช้ข้อมูลของการสังเกตจากตัวนักวิจัยเองที่เป็นผู้มีความรู้และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับกองทัพไทย ในระดับประเทศ และในระดับนานาชาติ มานานกว่า 7 ปี ตลอดจนเป็นผู้มีส่วนร่วมในการร่างกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และเป็นผู้ร่วมจัดตั้ง สกมช. ตั้งแต่เริ่มต้นจนถึงปัจจุบัน

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

2. วิธีการประมวลผลและการวิเคราะห์ข้อมูล

เป็นการวิเคราะห์ข้อมูลในงานเชิงคุณภาพ ซึ่งจะใช้วิธีการวิเคราะห์ข้อมูลเชิงเนื้อหา (Content Analysis) ที่ได้จากกระบวนการสัมภาษณ์และกระบวนการกลุ่มย่อย (Focus Group)

2.1 จัดระเบียบข้อมูล (Data) ในรูปของบันทึกเป็นคำพูด นำมาถอดเทป และพิมพ์บันทึกสรุปใจความการสนทนากลุ่ม

2.2 พัฒนาข้อมูลไปสู่มโนทัศน์ (Concept) โดยการนำเสนอและแสดงข้อมูลเชิงพรรณนาซึ่งมาจากการกลั่นความคิดและหาความสัมพันธ์เชื่อมโยงของข้อมูลที่ถูกต้องและตรงประเด็นตามกรอบความคิด

2.3 จัดมโนทัศน์เข้าสู่หมวดหมู่ (Categories) โดยสรุปข้อมูลเป็นหมวดหมู่เพื่อจำแนกให้อยู่ในขอบเขตและครอบคลุมในประเด็นที่กำหนด เพื่อตอบวัตถุประสงค์ของการวิจัย

2.4 จัดทำข้อเสนอเชิงทฤษฎี (Proposal) ที่ได้จากการจัดกระบวนการกลุ่ม

2.5 ภายหลังจากการเก็บรวบรวมข้อมูลทั้ง 4 วิธีการ ได้แก่ การดำเนินการวิจัยจากเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In-Depth Interview) การสนทนากลุ่มเฉพาะ (Focus Group Discussion) และการสังเกตการณ์ (Observation) เพื่อให้ทราบถึงแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้องในเรื่องของการดำเนินการ ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติในหลากหลายรูปแบบ จะมีการนำเอาข้อมูลที่ได้จากการเก็บรวบรวมข้อมูลไปวิเคราะห์หาจุดเด่นและจุดด้อยของการจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ ทั้งที่เป็นแบบรวมการ และแบบแยกการ และประมวลแนวคิดและสรุปแนวทางที่เหมาะสมในการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ นำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ ในระดับประเทศที่เป็นรูปธรรมและมีประสิทธิภาพ และเพื่อใช้เป็นแนวทางในการปฏิบัติของ สกมช. ต่อไปในอนาคต

ผลการวิจัย

การนำเสนอผลการวิจัยในครั้งนี้ ผู้วิจัยนำเสนอผลการวิจัยโดยยึดวัตถุประสงค์การวิจัยเป็นหลัก จำนวน 3 วัตถุประสงค์การวิจัย ดังนี้

1. ตอบวัตถุประสงค์การวิจัย ข้อที่ 1 เพื่อศึกษาถึงความเป็นมาและปัญหาในการดำเนินการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center: NCOC) ของประเทศไทยในห้วงที่ผ่านมา ซึ่งสามารถพบปัญหาและข้อจำกัดดังต่อไปนี้

1.1 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) ยิ่งมีจำนวนน้อยมาก จึงเกิดการแย่งชิงบุคลากรกลุ่มดังกล่าวจากทั้งภายในและภายนอกประเทศ โดยมีการเสนอค่าตอบแทนและสวัสดิการที่ค่อนข้างสูง เพื่อชักจูงให้ไปร่วมงานกับบริษัทหรือองค์กรที่ให้ค่าตอบแทนที่สูงกว่า ซึ่งการที่หน่วยงานของภาครัฐให้ค่าตอบแทนแก่บุคลากรทางไซเบอร์ที่ค่อนข้างน้อย เมื่อเปรียบเทียบกับบริษัทเอกชนหรือบริษัทของต่างประเทศ ส่งผลให้บุคลากรกลุ่มดังกล่าวที่อยู่ในหน่วยงานส่วนภาครัฐเริ่มทยอยลาออก เพื่อไปรับค่าตอบแทนที่สูงกว่าเป็นจำนวนมาก ดังนั้นการสร้างและผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงถือเป็นความเร่งด่วนในลำดับแรก ๆ ที่จำเป็นต่อการพัฒนาและแก้ไขปัญหาการดำเนินงานด้านไซเบอร์ในระดับประเทศของประเทศไทย ซึ่งมีความจำเป็นที่จะต้องมีการสร้างโรงเรียนหรือสถาบันทางการศึกษาที่จะสามารถผลิตบุคลากรทางไซเบอร์ให้กับหน่วยงานและองค์กรต่าง ๆ ในประเทศไทย ที่มีแนวโน้มที่จะนำเทคโนโลยีดิจิทัลมาใช้เพื่อการพัฒนาธุรกิจหรือการดำเนินกิจการขององค์กรมากยิ่งขึ้นเรื่อย ๆ ดังนั้นการผลิตบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงถือได้ว่ามีความจำเป็นอย่างมาก และจำเป็นที่จะต้องมีการวางแผนในระยะยาว เนื่องจากการสร้างและผลิตบุคลากรด้านไซเบอร์ให้มีความเชี่ยวชาญและมีขีดความสามารถสูงนั้น จำเป็นต้องใช้เวลาในการผลิตและฝึกฝนทักษะฝีมือในห้วงเวลาที่นานพอสมควร และไม่ใช่บุคลากรทุกคนสามารถพัฒนาตัวเองให้เป็นผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้เสมอไป เนื่องจากการดำเนินการพัฒนาขีดความสามารถของบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในขั้นกลางและขั้นสูงนั้น มีความยากลำบากเป็นอย่างมาก ซึ่งจะต้องอาศัยผู้ที่มีความตั้งใจจริงและมีความอดทนสูงมากเท่านั้นที่จะไปถึงเป้าหมายดังกล่าวได้

1.2 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

1.3 เทคโนโลยี (Technology)

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

นั้น เป็นสิ่งที่ไม่น่าจะกระทำ เนื่องจากในความเป็นจริงแล้ว ระบบ SIEM นั้นเป็นระบบที่เหมาะสมกับการวิเคราะห์เฉพาะข้อมูลจราจรในลักษณะของ Log files ของหน่วยงานขนาดไม่ใหญ่มาก (SME) เพียงหน่วยงานเดียวหรือมีข้อมูลไม่มากจนเกินไปเท่านั้นซึ่งถ้าต้องการนำเทคโนโลยีอย่างระบบ SIEM มาใช้ อาจจะต้องมีการแยกระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ออกเป็นหน่วยงานย่อย ๆ หลาย ๆ หน่วยงาน ที่จำเป็นต้องแยกระบบ SIEM ออกเป็นหลาย ๆ ระบบ เพื่อให้เกิดประสิทธิภาพของการเฝ้าระวังตรวจจับและแก้ไขปัญหาให้ได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ทั้งนี้ ระบบการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ในปัจจุบันนั้นมีหลากหลายรูปแบบที่สามารถดำเนินการได้จากการวิเคราะห์จาก Raw Traffics, Meta Data, Net Flows เป็นต้น

2. ตอบวัตถุประสงค์การวิจัย ข้อที่ 2 เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดี และข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center: NCOC) แบบรวมการ (Centralize) และแบบแยกการ (Decentralize)

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

การจัดตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติแบบรวมการ (Centralize) นั้น มีความจำเป็นที่จะต้องมีการดำเนินการให้เกิดการส่งข้อมูลการจราจรทางคอมพิวเตอร์ในรูปแบบต่าง ๆ จากทุก ๆ หน่วยงานที่มีระบบการป้องกันเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ไปยังศูนย์กลางเฝ้าระวังภัยคุกคามทางไซเบอร์เพียงที่เดียว โดยการจัดตั้งและปฏิบัติงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) ถือว่าเป็นแนวคิดที่ดีที่มีความพยายามที่จะทำให้เกิดการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศขึ้น ซึ่งมีความจำเป็นที่จะต้องมีระบบที่สามารถวิเคราะห์ข้อมูลการจราจรทางคอมพิวเตอร์ในลักษณะต่าง ๆ ที่มีจำนวนมากได้อย่างมีประสิทธิภาพ และยังจะต้องมีบุคลากรที่เชี่ยวชาญสูงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในจำนวนที่มากพอต่อการวิเคราะห์ข้อมูลการจราจรในรูปแบบต่าง ๆ ที่ถูกส่งมาจากองค์กรหลายองค์กรที่มีความหลากหลายของระบบเครือข่ายสารสนเทศ และวัตถุประสงค์ของการดำเนินธุรกิจขององค์กร เพื่อที่จะดำเนินการแก้ไขปัญหาการถูกบุกรุกทางไซเบอร์ได้อย่างทันท่วงที ซึ่งข้อด้อยของการจัดตั้ง NCOC แบบรวมการ นั้น อาจมาจากการที่หน่วยงานแต่ละหน่วยงานที่ส่งข้อมูลในรูปแบบต่าง ๆ มายังศูนย์เฝ้าระวังในส่วนการ ในลักษณะที่มีข้อมูลที่มีรูปแบบและความสำคัญของข้อมูลที่แตกต่างกัน ดังนั้นการวิเคราะห์ข้อมูลที่มีรูปแบบและมีความสำคัญที่แตกต่างกันเป็นจำนวนมาก จึงเป็นความยากอย่างมากของผู้วิเคราะห์ซึ่งต้องมีความรู้ที่หลากหลายข้าม Sectors ต่าง ๆ ของ CII ซึ่งถือว่า มีความเป็นไปได้ยากมากที่ผู้วิเคราะห์จะมีความสามารถในการวิเคราะห์ได้ตรงว่าเกิดความผิดปกติหรือไม่อย่างไรขึ้นกับระบบต่าง ๆ ซึ่งจะส่งผลให้การวิเคราะห์ข้อมูลต่าง ๆ ได้ผลไม่ตรงตามความเป็นจริงของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น และไม่สามารถแก้ไขปัญหาของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้อย่างทันเวลาที่จำเป็น และในปัจจุบันยังไม่มีเทคโนโลยีหรืออุปกรณ์ชนิดใด ที่จะสามารถวิเคราะห์ภัยคุกคามทางไซเบอร์จากจำนวนข้อมูลประเภทที่เป็นลักษณะของ Logfiles จำนวนมหาศาลได้อย่างแม่นยำ

2.2 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) อาจทำหน้าที่เป็นเพียงแค่

หน่วยงานในการกระจายหรือแชร์ข้อมูลด้านไซเบอร์ที่สำคัญร่วมกันเท่านั้น ซึ่งการดำเนินการในลักษณะนี้อาจสามารถแก้ปัญหาและรับมือภัยคุกคามทางไซเบอร์ได้จริงอย่างมีประสิทธิภาพในเชิงลึกได้มากกว่า แต่อาจจะต้องใช้เวลาในการสร้างศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ขององค์กรหรือหน่วยงานย่อย ๆ ที่มีความสำคัญ ที่เมื่อถูกโจมตีหรือถูกบุกรุกทางไซเบอร์แล้วจะส่งผลกระทบในภาพรวมต่อประเทศเป็นวงกว้างให้มีความพร้อมทั้ง ด้านบุคลากรทางไซเบอร์ ระบบการบริหารจัดการและระบบเทคโนโลยีต่าง ๆ ที่จะเลือกมาใช้ในการดำเนินการ ซึ่งปัญหาใหญ่มักจะอยู่ที่การขาดแคลนบุคลากรด้านไซเบอร์ที่จะมาเป็นผู้ควบคุมระบบต่าง ๆ ให้สามารถดำเนินการได้จริงอย่างมีประสิทธิภาพ

3. ตอบวัตถุประสงค์การวิจัย ข้อที่ 3 เพื่อเสนอแนะแนวทางในการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (National Cyberspace Operations Center : NCOC) ของประเทศไทยที่สามารถปฏิบัติงานได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ

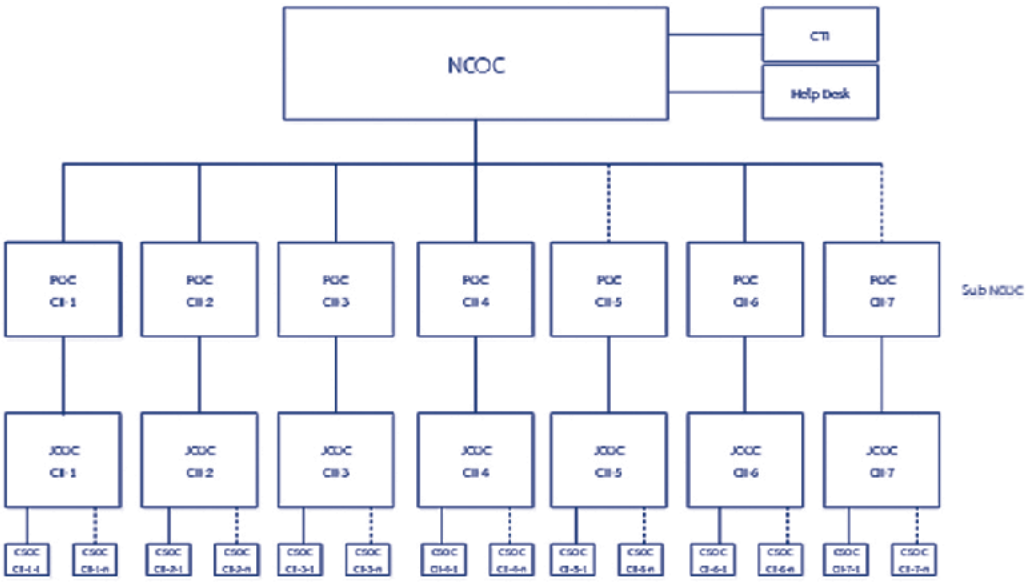
จากผลการวิจัยของตอบวัตถุประสงค์การวิจัย ข้อที่ 2 เพื่อศึกษาและวิเคราะห์เปรียบเทียบความเหมือนและความต่าง ตลอดจนข้อดีและข้อเสียของการดำเนินงานของศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ที่เป็นแบบรวมการและแบบแยกการ พบว่าแนวทางการตั้งศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) แบบรวมการ (Centralize) ซึ่งเป็นกลไกหลักในระดับประเทศของประเทศไทยในห้วงที่ผ่านมา ในการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศทั้งก่อน ระหว่าง และหลังการเกิดเหตุการณ์ทางไซเบอร์ (Cybersecurity Incidents) แต่ไม่สามารถนำไปสู่การเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยได้อย่างเป็นรูปธรรมอย่างแท้จริง ซึ่งอาจเป็นเพราะการใช้ระบบการเฝ้าระวังและตรวจจับด้วยระบบ SIEM ที่มีความไม่เหมาะสม ตลอดจนบุคลากรที่จะมีความสามารถที่เพียงพอในการวิเคราะห์ Log files ที่ถูกจัดส่งมาจากหลากหลายหน่วยงานที่มีความหลากหลายทั้งทางด้านรูปแบบเครือข่ายของการให้บริการทางสารสนเทศ และแตกต่างกันของวัตถุประสงค์ในการดำเนินการทางธุรกิจนั้น แทบเป็นไปไม่ได้เลยที่จะมีใครสามารถวิเคราะห์เหตุการณ์ทางไซเบอร์ที่เกิดขึ้นข้ามไปหลาย ๆ Sectors ได้อย่างถูกต้องและแม่นยำ

ทั้งนี้ ภายหลังจากการออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 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

สรุป

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. การรักษาความมั่นคงปลอดภัย

รูปที่ 1 แนวทางการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยหรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทั้ง 8 ประเภท



ไซเบอร์ พ.ศ.2562 ออกเป็น 8 ประเภท เพื่อนำไปสู่การแก้ไขปัญหาสถานการณ์วิกฤตทางไซเบอร์ในระดับประเทศที่เป็นรูปธรรม ควรมีการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการทางไซเบอร์แห่งชาติ (NCOC) ในแบบแยกการ (Decentralize) ที่จะเป็นรูปแบบการจัดตั้งที่เหมาะสมที่สุดสำหรับประเทศไทยในสถานการณ์ปัจจุบัน เพื่อให้สามารถปฏิบัติภารกิจในการบริหารจัดการ ตลอดจนเฝ้าระวัง ตรวจจับ และแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ให้กับประเทศไทยได้อย่างแท้จริงและมีประสิทธิภาพ

จากรูปที่ 1 แสดงแนวทางการจัดตั้งศูนย์บริหารจัดการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย หรือศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (NCOC) ที่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่แบ่งออกเป็น 8 ประเภท ในแบบแยกการ (Decentralize) ซึ่งแต่ละหน่วยงานที่มีความพร้อมทั้งงบประมาณ และกำลังพลที่เป็นบุคลากรทางไซเบอร์ที่เพียงพอ สามารถจัดตั้งศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วยตนเอง หรือถ้าไม่พร้อม อาจจะต้องมีหน่วยที่ตั้ง JCOC กลางของกลุ่มงานตาม CII ที่มีการดำเนินงาน หรือการให้การบริการในรูปแบบเดียวกัน หรือในลักษณะที่คล้ายกัน เช่น การตั้ง JCOC ของกลุ่มงานธนาคาร โดยธนาคารต่าง ๆ อาจส่ง Logfiles เข้ามายัง CSOC ของธนาคารของตนเอง และส่ง Meta Data มาให้กับ JCOC เพื่อเป็นการช่วยกันในการเฝ้าระวังและตรวจจับปัญหาเหตุการณ์ทางไซเบอร์ร่วมกัน หรือถือได้ว่าเป็นการ Back Up การเฝ้าระวัง และแก้ไขภัยคุกคามทางไซเบอร์อีกชั้นหนึ่งในห้วงเวลาเดียวกัน

การตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของหน่วยงานที่ถูกจัดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) (Joint Cyberspace Operations: JCOC) ของประเทศเพื่อร่วมในการแก้ปัญหาในกรณีที่ศูนย์เฝ้าระวังและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (CSOC) ของหน่วยงานใดหน่วยงานหนึ่ง ไม่สามารถแก้ปัญหาได้เอง หน่วยงานดังกล่าวจะส่งต่อปัญหาภัยคุกคามทางไซเบอร์ไปให้กับ JCOC และ JCOC จะทำหน้าที่ให้การบูรณาการให้เกิดการร่วมกันแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ ในลักษณะของการช่วยเหลือซึ่งกันและกันภายในหน่วยงานที่อยู่ใน

Sector เดียวกันของ JCOC นั้น ๆ และภายหลังจากที่ทาง JCOC สามารถร่วมแก้ปัญหาเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นได้แล้วจะมีการส่งข้อมูลการโจมตีในรูปแบบของข้อมูลข่าวกรองทางไซเบอร์ (CTI) ไปยัง POC ของหน่วย CII ที่ทำงานอยู่กับ NCOC เพื่อให้ NCOC ทำหน้าที่เป็นหน่วยงานกลางด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ ที่จะทำหน้าที่ในการบูรณาการให้เกิดการปฏิบัติงานร่วมกันในระดับประเทศ หรือข้าม Sector โดย NCOC จะดำเนินการแชร์ข้อมูล CTI ให้กับ JCOC ของ Sectors อื่น ๆ เพื่อจะทำให้ JCOC ของแต่ละ Sector นำข้อมูล CTI ที่ได้รับไปแชร์ต่อให้กับ CSOC ใน Sector ของตนเองไม่ให้ถูกโจมตีทางไซเบอร์ในลักษณะเดียวกันได้อีกต่อไป ซึ่งเป็นรูปแบบของการดำเนินการในลักษณะของการช่วยเหลือและพึ่งพาอาศัยกันรับมือและแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ร่วมกันทั้งประเทศ

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

บรรณานุกรม

จินดา สระสมบูรณ์. (2558). ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย.วารสารรัฐฐาภิรักษ์,57(2), 57-69.

พนิดา พาณิชกุล. (2553). จริยธรรมทางเทคโนโลยีสารสนเทศ.เค ที พี คอมพ์แอนด์ คอนซัล.

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. (2564). แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (1) ประเด็นความมั่นคง (พ.ศ.2561–2580). http://nscr.nesdb.go.th/wp-content/uploads/2019/04/01-%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A1%E0%B8%B1%E0%B9%88%E0%B8%99%E0%B8%84%E0%B8%87.pdf

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

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560. (2560, 24 มกราคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 10ก. หน้า 24-35.

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม.วารสารสถาบันวิชาการป้องกันประเทศ,6(3),19 – 29.

สำนักงานปลัดกระทรวงคมนาคมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. (2562). แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงคมนาคม พ.ศ. 2562-2566.https://complain.mot.go.th/prproject/files_upload/publishonweb/MOT_CyberSecurityActiojnPlan.pdf

อรรคเดช ประทีปอุษานนท์.(2560). แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์. วารสารสถาบันวิชาการป้องกันประเทศ,8(3), 11-23.