แนวทางในการแก้ไขปัญหาจากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

เอกสารวิจัยส่วนบุคคล

โดย

พันเอก เรวัฒ ธรรมจิรเดช
รองผู้บังคับการ กรมทหารราบที่ 13

วิทยาลัยการทัพบก
กันยายน 2567

เอกสารวิจัยเรื่อง แนวทางในการแก้ไขปัญหาจากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

โดย พันเอก เรวัฒ ธรรมจิรเดช

อาจารย์ที่ปรึกษา พันเอกหญิง จิตติมา รวยรื่น

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2567 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ **ดีมาก**

พลตรี (ทนงศักดิ์ มหาวงศ์) **ผู้บัญชาการวิทยาลัยการทัพบก**

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก (ประภาส แก้วศรีงาม) **ประธานกรรมการ**

พันโทหญิง (รชาดา ธรรมจิรเดช) **ผู้ทรงคุณวุฒิที่ปรึกษา**

พันเอกหญิง (กนิษฐา ฐิติวัฒนา) **กรรมการ**

พันเอกหญิง (จิตติมา รวยรื่น) **กรรมการ**

บทคัดย่อ

ผู้วิจัย พันเอก เรวัฒ ธรรมจิรเดช

เรื่อง แนวทางในการแก้ไขปัญหาจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

วันที่ 11 กันยายน 2567 **จำนวนคำ :** 9,626 **จำนวนหน้า :** 29

คำสำคัญ ภัยคุกคามด้านไซเบอร์

ชั้นความลับ ไม่มีชั้นความลับ

งานวิจัยนี้ ดำเนินการเพื่อศึกษารายละเอียดของภัยคุกคามด้านไซเบอร์ ปัญหา และผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัวในค่ายสุรนารี รวมทั้งแนวทางในการแก้ปัญหา โดยทบทวนเอกสารที่เกี่ยวข้องร่วมกับการสัมภาษณ์กำลังพล ครอบครัว และเจ้าหน้าที่ ที่มีบทบาทรับผิดชอบด้านไซเบอร์ของหน่วยในพื้นที่ค่ายสุรนารี แล้วได้นำข้อมูลทั้งหมดมาทำการวิเคราะห์สภาพแวดล้อมภายนอกและภายในโดยใช้ SWOT Analysis, 4M และ 3 แกนหลักขององค์กร พบว่า การเปลี่ยนแปลงด้านเทคโนโลยีอย่างรวดเร็ว เป็นช่องทางให้เหล่าอาชญากรไซเบอร์สามารถเข้าโจมตีต่อกำลังพลและครอบครัวของหน่วยได้ง่าย เนื่องจากทุกหน่วยยังไม่มีการจัดตั้งศูนย์ไซเบอร์และเจ้าหน้าที่ที่มีทักษะและขีดความสามารถในการแก้ไขปัญหาด้านไซเบอร์ได้โดยตรง อีกทั้งยังขาดงบประมาณและกำลังพล พร้อมครอบครัวก็ยังขาดความรู้ความเข้าใจจึงยากต่อการรับมือต่อภัยคุกคามด้านไซเบอร์ สำหรับแนวทางในการแก้ปัญหาที่เหมาะสม ทุกหน่วยควรจัดเจ้าหน้าที่และกำลังพลพร้อมครอบครัว เข้ารับการฝึกอบรมในหลักสูตรที่กองทัพบกกำหนด จัดสรรงบประมาณสนับสนุนให้เพียงพอ ติดตามประเมินผลอย่างต่อเนื่อง เพื่อนำผลการประเมินมาพัฒนาระบบ อีกทั้งภาครัฐควรออกกฎหมายคุ้มครองและป้องกันปราบปรามการกระทำผิดด้านไซเบอร์อย่างเป็นรูปธรรม

ABSTRACT

AUTHOR: Colonel Raywat Thammachiradet

TITLE: Guidelines for Addressing Cyber Threats Impacting the Lives of Personnel and Their Families at Fort Suranaree

DATE: 11 September, 2024 **WORD COUNT:** 9,626 **PAGES:** 29

KEY TERMS Cyber Threats

CLASSIFICATION: Unclassified

This research was conducted to study the details of cyber threats, issues, and their impacts on the lives of personnel and their families at Fort Suranaree, as well as to propose guidelines for solving problems. The study involved reviewing relevant documents and interviewing personnel, families, and officials responsible for cybersecurity at Fort Suranaree. All gathered data were analyzed using SWOT Analysis, the 4M framework, and the organization's 3 core pillars. The findings revealed that rapid technological changes have enabled cybercriminals to easily attack the personnel and their families due to the lack of an established cyber center and skilled staff to directly address cybersecurity issues. There is also a shortage of budget and a lack of knowledge and understanding among personnel and their families, making it difficult to cope with cyber threats. To address these issues, each unit should arrange for personnel and their families to undergo training in courses specified by the Royal Thai Army, allocate sufficient budgetary support, and continuously monitor and evaluate the outcomes to improve the system. Furthermore, the government should enact concrete laws to protect against, prevent, and suppress cybercrimes.

กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคลฉบับนี้ สำเร็จลงได้ด้วยความกรุณาจากคณาจารย์ของวิทยาลัยการทัพบกทุกท่าน ที่ได้ถ่ายทอดความรู้ ประสบการณ์ในการศึกษา ตลอดจนความอนุเคราะห์ช่วยเหลือ ในการดำเนินการจัดทำวิจัย ในครั้งนี้อย่างดียิ่ง โดยเฉพาะ พันโทหญิง รชาดา ธรรมจิรเดช ผู้ทรงคุณวุฒิที่ปรึกษา พันเอกหญิง จิตติมา รวยรื่น อาจารย์ที่ปรึกษา และ พันเอกหญิง นุสรา วรภัทราทร ที่ปรึกษาพิเศษ ที่กรุณาให้คำแนะนำและแนวคิดที่เป็นประโยชน์ในการจัดทำเอกสารวิจัยส่วนบุคคล รวมถึงตรวจสอบต้นฉบับอย่างละเอียด จนทำให้งานวิจัยฉบับนี้สำเร็จลุล่วงและเสร็จสมบูรณ์ ขอขอบพระคุณ พลตรี ทนงศักดิ์ มหาวงศ์ ผู้บัญชาการวิทยาลัยการทัพบก ที่ให้ความกรุณา ตลอดระยะเวลาที่ได้ศึกษา พันเอก ประภาส แก้วศรีงาม ประธานคณะกรรมการสอบเอกสารวิจัยส่วนบุคคล พันเอกหญิง กนิษฐา ฐิติวัฒนา คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล และ อ.ดร. วีระพัฒน์ กฤตธนาทิพย์ อาจารย์ที่ปรึกษาพิเศษประจำกลุ่มวิจัย รวมทั้งท่านผู้บังคับบัญชาทุกระดับ ที่ได้กรุณาให้แนวคิด ข้อเสนอแนะทางวิชาการที่เป็นประโยชน์ยิ่งในการวิจัย ทำให้เอกสารวิจัยส่วนบุคคลฉบับนี้ สำเร็จลงด้วยดี ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของทุกท่าน และขอขอบพระคุณ เป็นอย่างสูงมา ณ ที่นี้

หวังเป็นอย่างยิ่งว่าเอกสารวิจัยส่วนบุคคลฉบับนี้จะเป็นประโยชน์ต่อผู้ที่สนใจและหน่วยงานทางราชการที่เกี่ยวข้องต่อไป

สารบัญ

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ตามแผนระดับ 1 ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580) ได้กำหนดวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาเศรษฐกิจพอเพียง” โดยยุทธศาสตร์ที่ 1 คือ ยุทธศาสตร์ชาติด้านความมั่นคง การป้องกันและการแก้ปัญหาที่มีผลกระทบต่อความมั่นคง[1] และแผนระดับ 2 แผนปฏิรูปประเทศ: ด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ, การป้องกันคุ้มครอง และรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์[2] จนถึงแผนระดับ 3 นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัล การพัฒนาเศรษฐกิจและสังคม (พ.ศ. 2561 - 2580) โดยยุทธศาสตร์ที่ 6: สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล[3] ได้ให้ความสำคัญในการเพ่งเล็งต่อภัยคุกคามด้านไซเบอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม Ministry of Digital Economy and Society จึงได้กำหนดนโยบายและแผนว่าด้วยการรักษาความมั่งคงปลอดภัยไซเบอร์[4] ออกมาดูแลแก้ไขปัญหาในงานด้านนี้โดยเฉพาะและสำหรับยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม (พ.ศ. 2560 - 2579) กำหนดให้กองทัพบกเป็นหน่วยงานหลักด้านความมั่นคง เป็นเครื่องมือของรัฐบาลในการต่อสู้ภัยคุกคามรูปแบบต่างๆ ของชาติ[7] ซึ่งกองทัพบก ได้กำหนดนโยบายการปฏิบัติงานของกองทัพบก ประจำปีงบประมาณ 2567[5] และได้ให้ความสำคัญกับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นในปัจจุบัน โดยเฉพาะภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของคนในชาติ ในทุกเพศ ทุกวัย รวมทั้งกำลังพลพร้อมครอบครัวของกองทัพบก ก็ได้รับผลกระทบโดยตรง จากภัยคุกค้ามด้านไซเบอร์เช่นเดียวกัน จึงจำเป็นที่หน่วยจะต้องพัฒนาแนวทาง[6] และเตรียมความพร้อม สำหรับการเผชิญกับภัยคุกคามรูปแบบใหม่นี้

ภัยคุกคามด้านไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใดๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่าย ที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่ายหรือข้อมูภายใน ได้มีวิวัฒนาการหลากหลายรูปแบบ และทุกการโจมตีนั้น ไม่ได้มีลักษณะตายตัว แม้ว่าจะมีความคล้ายคลึงกันบ้าง แต่ก็จะต้องหาวิธีในการรับมือ ที่แตกต่างกันออกไป ภัยคุกคาม ทางไซเบอร์ที่พบมากที่สุดในปัจจุบันมี 7 ประเภท ได้แก่ มัลแวร์ (Malware), ฟิชชิ่ง (Phishing) , เอสคิวแอล อินเจคชั่น แอ็ทแทค (SQL Injection Attacks), ครอสไซต์ สคริปต์ติ้ง (Cross-Site Scripting (XSS)), ดีไน ออฟ เซอวิส (Denial

of Service (DoS)), แมน อิน เดอะ มิดเดิล แอ็ทแทค (Man-in-the-Middle Attacks), พาสเวิร์ด แอ็ทแทค (Password Attacks) ภัยคุกคามทางไซเบอร์เหล่านี้ มีผลกระทบในชีวิตประจำวันของกำลังพลและครอบครัวของหน่วย ที่สามารถพบเจอกับภัยคุกคามด้านไซเบอร์ได้ ตัวอย่างเช่น เรื่อง ภาพ คลิป คำพูดที่มีความรุนแรง โดยพบเห็นภาพ คลิป คำพูดรุนแรง ถ้อยคำหยาบคาย เรื่องการโฆษณาสินค้า ที่ไม่ได้รับการรับรองความปลอดภัย สินค้าผิดกฎหมาย โดยพบเห็นโฆษณาอวดอ้างสรรพคุณเกินจริง เป็นต้น กำลังพลและครอบครัวต้องศึกษาให้รู้เท่าทันอยู่เสมอ เพราะเทคนิคในการหลอกล่อให้ผู้ใช้คลิก ติดตั้งมัลแวร์ หรือเผลอกรอกข้อมูลตนเองที่แนบเนียนมากยิ่งขึ้น และสำหรับหน่วยในกองทัพบก ผู้บังคับหน่วยจำเป็นต้องหาแนวทางรักษาป้องกันความปลอดภัยของระบบข้อมูล เพื่อรักษาผลประโยชน์สูงสุดให้กับหน่วยของตนเอง กำลังพลพร้อมครอบครัวหน่วยจำเป็นต้องกำหนดแนวทางปฏิบัติด้านความปลอดภัยที่ดี ครอบคลุม พิจารณาทั้ง 3 แกนหลักขององค์กร ได้แก่ คน (People), ขั้นตอน (Process), เทคโนโลยี (Technology) โดยต้องมีการฝึกอบรมเพื่อเตรียมพร้อม ความรู้ความเข้าใจด้านความปลอดภัยทางไซเบอร์ (Cybersecurity) แก่กำลังพลและครอบครัว รวมถึงควบคุมการเข้าถึงสิทธิ์ของผู้ใช้ การเข้ารหัสข้อมูล การกำหนดนโยบายที่เหมาะสมจากประสบการณ์การรับราชการของผู้วิจัย ในห้วงที่เป็นผู้บังคับหน่วย ตั้งแต่ระดับหมวด กองร้อย กองพัน และกรมทหารพราน ได้พบว่ากำลังพลและครอบครัวของหน่วยประสบปัญหาจากภัยคุกคามด้านไซเบอร์หลายราย และมีแนวโน้มเพิ่มมากขึ้นเรื่อยๆ ซึ่งส่งผลกระทบต่อสภาพขวัญกำลังใจ และกระทบต่อเวลาปฏิบัติราชการ ผู้วิจัยจึงมีความสนใจในการทำวิจัยเกี่ยวกับปัญหาจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี เพื่อให้ได้ข้อเสนอถึงแนวทางในการจัดการกับภัยคุกคามทางไซเบอร์ ของกำลังพลและครอบครัว ค่ายสุรนารี อย่างเป็นรูปธรรมต่อไป

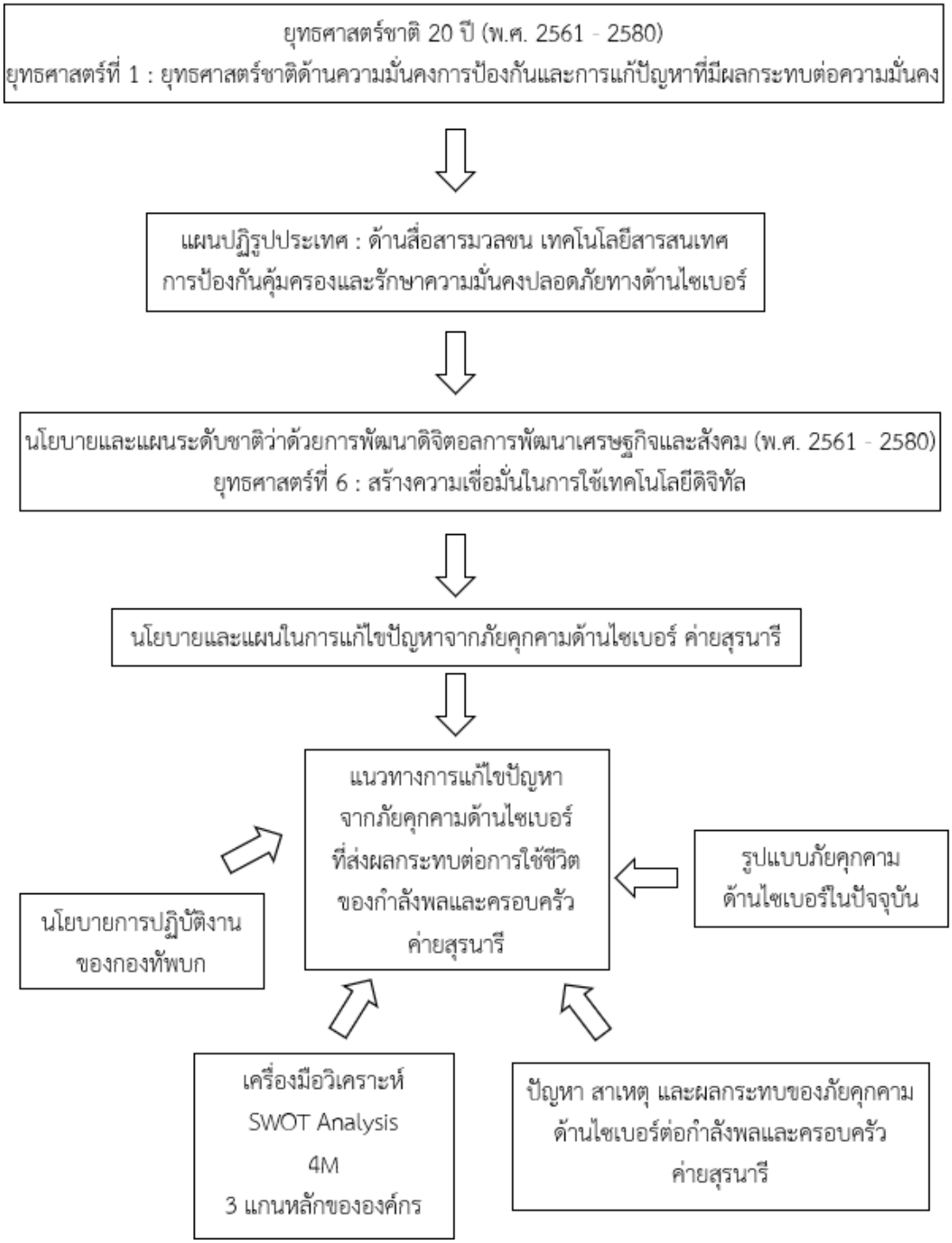
วัตถุประสงค์การวิจัย

1. เพื่อศึกษารายละเอียดของ ภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตในปัจจุบัน

2. เพื่อศึกษาปัญหาและผลกระทบ ที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพล และครอบครัว ค่ายสุรนารี

3. เพื่อหาแนวทาง ในการแก้ปัญหาภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพล และครอบครัว ค่ายสุรนารี

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีการศึกษา

1. รูปแบบการวิจัย การศึกษาในครั้งนี้ ใช้การวิจัยในเชิงยุทธศาสตร์ ตามแนวทางที่วิทยาลัยการทัพบกกำหนด โดยใช้รูปแบบการวิจัยเชิงคุณภาพ และใช้วิธีการวิจัยเชิงเอกสารเป็นแนวทางการวิจัย

2. ขอบเขตการศึกษา การวิจัยนี้ กำหนดขอบเขตการศึกษา เฉพาะกำลังพลและครอบครัว รวมทั้งเจ้าหน้าที่ด้านไซเบอร์ของหน่วยในพื้นที่ ค่ายสุรนารี

3. การเก็บรวบรวมข้อมูล ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลจากเอกสารทางกฎหมาย เอกสารของหน่วยราชการ ที่เกี่ยวข้อง หนังสือ ตำรา เอกสารวิชาการ และข้อมูลที่เผยแพร่จากแหล่งเว็ปไซต์ที่เชื่อถือได้ รวมทั้งผู้วิจัยรวบรวมข้อมูลด้วยตนเอง โดยกำลังพลและครอบครัวในค่ายสุรนารี ตามความสมัครใจ และสัมภาษณ์เจ้าหน้าที่ด้านระบบไซเบอร์ของหน่วยในพื้นที่ค่ายสุรนารี

4. การวิเคราะห์ข้อมูล วิเคราะห์โดยกำหนดกรอบการคิดเชิงยุทธศาสตร์ ตามทฤษฎีการวิเคราะห์ปัจจัยด้วยวิธี SWOT Analysis และแนวความคิดทฤษฎี 4M พร้อมกับ 3 แกนหลักขององค์กร เพื่อหาข้อมูลสรุปและพิจารณาแนวทางในการแก้ไขปัญหาจากภัยคุกคามด้านไซเบอร์ให้มีประสิทธิภาพมากขึ้น

5. ขั้นตอนการดำเนินงาน

ห้วงเวลา / กิจกรรม	ธ.ค. 66	ม.ค. 67	ก.พ. 67	มี.ค. 67	เม.ย. 67	พ.ค. 67	มิ.ย. 67
เลือกเรื่อง และกำหนดหัวข้อการวิจัย	←→						
สอบการนำเสนอโครงร่างเอกสารการวิจัย		←→					
ศึกษาค้นคว้าที่มาของปัญหา		←→	←→				
การวิเคราะห์, สังเคราะห์ข้อมูล				←→			
การสรุปผลการวิจัย					←→		
การนำเสนอผลการวิจัย						←→	
จัดทำรูปเล่ม							←→

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ทราบรายละเอียดของ ภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตในปัจจุบัน

2. ได้ทราบปัญหาและผลกระทบ ที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิต ของกำลังพลและครอบครัว ค่ายสุรนารี

3. ได้แนวทาง ในการแก้ปัญหาภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

บทที่ 2
บทวิเคราะห์

ภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตในปัจจุบัน

1. ภัยคุกคามด้านไซเบอร์ที่พบบ่อยในปัจจุบัน ได้มีวิวัฒนาการหลากหลายรูปแบบ แต่ทุกการโจมตีนั้น ไม่ได้มีลักษณะตายตัว แม้ว่าจะมีความคล้ายคลึงกันบ้าง แต่ก็จะมีวิธีรับมือที่แตกต่างกันออกไป ภัยคุกคามด้านไซเบอร์ที่พบมากที่สุดในปัจจุบันมี 7 ประเภท ดังนี้[4]

1.1 มัลแวร์ (Malware) เป็นภัยคุกคามรุ่นบุกเบิก หรือที่คนส่วนใหญ่จะเรียกกันว่า “ไวรัส” มักแฝงตัวมากับไฟล์ที่เราดาวน์โหลดจากเว็บไซต์ อีเมล หรือจากอุปกรณ์เสริมที่เชื่อมต่อเข้ากับคอมพิวเตอร์ แรนซัมแวร์ ถือว่าเป็นหนึ่งในประเภทของมัลแวร์ ซึ่งหากมีมัลแวร์อยู่ในคอมพิวเตอร์แล้ว ก็จะสามารถสร้างความเสียหายได้มาก ไม่ว่าจะเป็นการทำลายข้อมูล หรือการเข้าควบคุมระบบของบุคคลนั้น

1.2 ฟิชชิ่ง (Phishing) เป็นภัยคุกคามทางอีเมล ที่อาชญากรไซเบอร์ได้พัฒนารูปแบบไปอีกขั้น รูปแบบการโจมตีจะแสร้งมาในรูปแบบของอีเมลจากบุคคลที่สามารถไว้วางใจหรือสั่งการได้

1.3 เอสคิวแอล อินเจคชั่น แอ็ทแทค (SQL Injection Attacks) ระบบ SQL ถูกสร้างมาเพื่อจัดระบบฐานข้อมูลขององค์กร ซึ่งหากอาชญากรไซเบอร์ โจมตีไปยังระบบผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ จะส่งผลกระทบที่มีความเสียหายมากกับระบบเซิร์ฟเวอร์โดยตรง

1.4 ครอส ไซต์ สคริปต์ติ้ง (Cross-Site Scripting (XSS)) ในขณะที่ SQL จะเป็นการโจมตีผ่านเว็บไซต์องค์กร การทำงานของ XSS จะตรงกันข้าม คือ เป็นการโจมตีผู้เข้าใช้บริการเว็บไซต์ โดยอาชญากรไซเบอร์ จะใช้วิธีใส่โค้ดที่เป็นอันตรายลงในช่องทางที่ผู้ใช้งานเว็บไซต์จะต้องเปิดหรือฝังลิงก์ไปยัง จาวาสคริพท์ (JavaScript) ภายในเว็บไซต์ การโจมตีรูปแบบนี้ จะมีผลต่อชื่อเสียง และความน่าเชื่อถือของเว็บไซต์ และองค์กรเป็นอย่างมาก

1.5 ดิไน ออฟ เซอวิส (Denial of Service (DoS)) หรือที่คนบอกว่า “เว็บล่ม” หลายคนเข้าใจว่า การที่เว็บล่มอาจเกิดจากการที่มีคนเข้าใช้บริการเว็บไซต์เยอะเกินกว่าที่ระบบเซิร์ฟเวอร์จะรองรับได้ แต่บางครั้งเกิดจากการโจมตีแบบ DoS ก็เป็นได้

ที่ทำให้การทำงานของเซิร์ฟเวอร์ผิดปกติ อาชญากรไซเบอร์ จะใช้ไอพี (IP) หลากหลายจากทั่วโลกเข้ามาสร้างความหนาแน่นบนเซิร์ฟเวอร์ จนเว็บไซต์ไม่สามารถเข้าใช้งานได้ตามปกติ

1.6 แมน อิน เดอะ มิดเดิล แอ็ทแทค (Man-in-the-Middle Attacks) เป็นการโจมตีแบบแทรกกลางระหว่างการสื่อสารของคอมพิวเตอร์และเซิร์ฟเวอร์ ซึ่งภัยคุกคามนี้จะทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูล โดยที่เราไม่ทันได้รู้ การโจมตีลักษณะนี้จะเข้ามาอ่าน ปลอมแปลง และแก้ไขข้อมูล เพื่อนำไปก่ออาชญากรรมทางไซเบอร์ในอนาคต

1.7 พาสเวิร์ด แอ็ทแทค (Password Attacks) เวลาเข้าใช้ระบบต่างๆ จะมีการเข้าสู่ระบบด้วยรหัสผ่าน ซึ่งจะช่วยสร้างความปลอดภัยได้ในระดับหนึ่ง สิ่งที่ควรจะต้องทำคือ การสร้างรหัสผ่านที่ไม่ซ้ำกันในแต่ละประเภทเว็บไซต์ และแอปพลิเคชั่นที่เราเข้าใช้บริการ เพราะถ้าหากตั้งรหัสผ่านไว้ในแบบเดียวกัน หากโดนขโมยข้อมูลไปส่วนหนึ่งอาจเกิดความเสียหายกับหลายๆบัญชีที่เราใช้บริการอยู่

2. ข้อมูลจาก SCB ไทยพาณิชย์[22] กล่าวว่า การจะอยู่ในโลกออนไลน์ที่เต็มไปด้วยภัยคุกคามทางไซเบอร์ ได้อย่างปลอดภัยนั้น เราควรมาทำความรู้จัก 10 ตัวท็อปรูปแบบการโจมตีในโลกออนไลน์ ดังนี้

2.1 มัลแวร์ หรือ มอลิเวียล ซอฟต์แวร์ (Malware/ Malicious software) เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อรบกวนหรือขโมยข้อมูลจากระบบคอมพิวเตอร์ เครือข่าย หรือ Server โดยแฮกเกอร์มักฝังมัลแวร์ลงไปในอุปกรณ์ เปิดทางเข้าถึงข้อมูลหรือเข้าควบคุมระบบเป้าหมาย

2.2 ฟิชชิ่ง (Phishing) เป็นการหลอกลวงในโลกออนไลน์ที่พบมากที่สุด มีเป้าหมายเพื่อขอข้อมูลสำคัญด้วยวิธีการต่างๆ เช่น อีเมลปลอม ข้อความหลอกลวงผ่าน Messenger หรือเว็ปไซต์ปลอม

2.3 ดีดอส (DDoS) เป็นการโจมตีเป้าหมายด้วยการส่งคำขอเข้าไปจำนวนมาก ด้วยเครื่องคอมพิวเตอร์หลายเครื่องด้วย Botnet ซึ่งในระหว่างการโจมตีนั้น แฮกเกอร์อาจฝังมัลแวร์ เพื่อเข้าระบบหรือข้อมูลสำคัญขององค์กร

2.4 มิทเอ็ม (MitM) เป็นการที่ผู้ประสงค์ร้ายเข้ามาแทรกกลางระหว่างการสนทนา หรือทำธุรกรรมออนไลน์ของคนสองคน และทำหน้าที่เป็นตัวกลางรับส่งข้อมูลโดยที่ทั้งคู่ไม่รู้ตัว โดยทั่วไปการโจมตีแบบ MitM มักจะใช้ช่องโหว่จากเครือข่าย Wifi สาธารณะ และแทรกตัวอยู่ระหว่างผู้ใช้งานกับเครือข่ายต่างๆ เพื่อหลอกเอาข้อมูลสำคัญ แฮกเกอร์หลายรายมักใช้วิธี MitM เพื่อส่งต่อ Malware และ Phishing

2.5 เอสคิวแอล อินเจคชั่น (SQL Injection) เว็ปไซต์ส่วนใหญ่ใช้ SQL Databases เก็บข้อมูลสำคัญ เช่น logins, Passwords และข้อมูลบัญชี เป็นต้น ดังนั้น แฮกเกอร์อาศัยช่องโหว่ของโปรแกรมหรือเว็ปไซต์แอบใส่ SQL เข้าไปทาง input เพื่อหลอก Databases แล้วดึงข้อมูลออกไป

2.6 ซีโร่ เดย์ เอ็กพอท แอนด์ อะแท็ค (Zero-day Exploit & Attack) เป็นการโจมตีระบบด้วยการแอบเข้าไปปล่อย Malware ผ่านช่องโหว่ที่มีอยู่ที่ในซอฟต์แวร์/เครือข่าย/ฮาร์ดแวร์ ที่ผู้พัฒนาหรือเจ้าของซอฟต์แวร์เองก็ไม่รู้ เพื่อโจรกรรมข้อมูลออกไป

2.7 พาสเวิร์ด อะแท็ค (Password Attack) เป็นการโจมตีทางไซเบอร์ด้วยการเดารหัสผ่าน (Password) หรือใช้วิธีการล่อลวงให้เป้าหมายเปิดเผยรหัสผ่าน

2.8 ไดรฟ์ บาย อะแท็ค (Drive-by Attack) การโจมตีนั้นจะแทรกโค้ดที่เป็นอันตรายไปยังเว็บไซต์ที่ถูกต้องทั่วไป ซึ่งอาจอยู่ในรูปแบบเว็บลิงก์ เพียงคลิกเปิดมันขึ้นมาอุปกรณ์ก็จะถูกติดตั้ง Malware โดยไม่รู้ตัว

2.9 ลอท (LoT) เมื่อโลกมีการเชื่อมโยงกันมากขึ้นด้วยอินเทอร์เน็ตทำให้อุปกรณ์ต่างๆ เช่น ลำโพงอัจฉริยะ สมาร์ททีวี หรือแม้แต่กล้องวงจรปิด ตกเป็นเป้าหมายของแฮกเกอร์ เพื่อขโมยข้อมูลจากอุปกรณ์ หรือใช้อุปกรณ์เหล่านั้นเป็น botnet เพื่อใช้โจมตีเป้าหมายแบบ DDoS โดยทั่วไปแล้วอุปกรณ์ LoT ส่วนใหญ่ไม่มีการอัปเดตซอฟต์แวร์แอนตี้ไวรัส ทำให้ติดตั้งมัลแวร์ และควบคุมจากระยะไกลทำได้ง่าย

2.10 ดีเอนเอส สพูฟิง ออ พอยโซนิ่ง (DNS Spoofing or Poisoning) เป็นการปลอมแปลงชื่อเว็บไซต์ หลังเวิร์ด ไว เว็บ (WWW.) เพื่อนำจำนวนคนที่พยายามเข้าเว็บไซต์ที่ถูกต้องส่งต่อไปยังเว็บไซต์ปลอม หน้าตาของเว็บไซต์หลอกจะเหมือนเว็บไซต์ของจริงมาก เพื่อหลอกให้ผู้ใช้งานป้อนข้อมูลส่วนตัวที่สำคัญ แฮกเกอร์มักใช้การโจมตีรูปแบบนี้ เป็นส่วนหนึ่งในการก่อวินาศกรรมองค์กรเป้าหมาย

3. ข้อมูลจากสำนักงานส่งเสริมสุขภาพ[23] ได้แบ่งประเภทของภัยคุกคามทางไซเบอร์ ดังนี้

3.1 Application/Service/ OS configuration problem เกิดจากการ Confi guration แอปพลิเคชัน/การให้บริการ/ระบบปฏิบัติการ ที่ผิดพลาด

3.2 Denial of Service (DoS) ผู้บุกรุกส่งข้อมูล และ packet จำนวนมากไปยังเครือข่าย หรือเครื่องของหน่วยงาน เพื่อให้เครื่องให้บริการหยุดชะงัก

3.3 Fraud เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวง เพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

3.4 Information Gathering ตรวจพบความพยายามของผู้บุกรุกในการค้นหาข้อมูลสำคัญ เพื่อใช้สำหรับการโจมตีเข้าสู่ระบบ

3.5 Information Leak ตรวจพบการรั่วไหลของข้อมูลสำคัญจากช่องทางต่างๆ เช่น Social Media ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัย

3.6 Malware Detected การบุกรุกที่เกิดจากการโจมตีของมัลแวร์ไปยังเครือข่าย และเครื่องให้บริการของหน่วยงาน ได้แก่ Backdoor, Trojan, Virus, Worm และ Botnet

3.7 Server Compromise ตรวจพบว่าเครื่องให้บริการ (Server) ของหน่วยงานถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาตโดยผู้บุกรก เป็นที่เรียบร้อย

3.8 Service Unavaliable การทำให้บริการมีปัญหาหรือเกิดเหตุขัดข้องจนไม่สามารถให้บริการได้

3.9 Suspicious Activity การเชื่อมต่อข้อมูล และ Traffic ที่ผิดปกติและมีความเชื่อมโยงที่จะเป็นการบุกรุกระบบ

3.10 Web Compromise Web Application หรือเว็บไซต์ถูกยึดครองโดยไม่ได้รับอนุญาต

4. ข้อมูลจาก CYBER ELITE[24] ได้รวบรวมเหตุการณ์ Cyber Attack ที่โด่งดังในต่างประเทศ 5 การโจมตี ดังนี้

4.1 อาโนนีเม้าส์ (Anonymous) ได้ประกาศต่อต้านรัสเซียเพื่อช่วยเหลือทางยูเครน ซึ่งมีรายงานว่า อาโนนีเม้าส์ ได้ทำการโจมตีเว็บไซต์รัฐบาลรัสเซีย รวมไปถึงสื่อต่างๆ ด้วยวิธีการดีดอส (DDoS) ทำให้ไม่สามารถเข้าถึงได้

4.2 แล็พซูส (Lapsus$) กลุ่มแฮกเกอร์นี้ ได้ทำการแฮกครั้งยิ่งใหญ่ไปเมื่อต้นปี 2565 โดยได้ทำการขโมยข้อมูลสำคัญต่างๆ ของบริษัทยักษ์ใหญ่อย่าง เอ็นวิเดีย, ซัมซุง และ ยูบิซอฟต์ จากนั้นนำมาเผยแพร่บนอินเทอร์เน็ต ซึ่งกลุ่มแฮกเกอร์นี้จะใช้วิธีฟิชชิ่ง (Phishing) เป็นหลัก

4.3 ข้อมูลชาวอินโดนีเซียที่รั่วไหลกว่า 105 ล้านคน ซึ่งประกอบไปด้วยหมายเลขบัตรประชาชนชาวอินโดนีเซีย ชื่อ นามสกุล วันเกิด รวมไปถึงข้อมูลอื่นๆ ที่สามารถระบุ ตัวบุคคลได้ ผู้ที่อยู่เบื้องหลังเหตุการณ์นี้ใช้ชื่อกลุ่มว่า โบร์ก้า(Bjorka) ซึ่งได้ขายข้อมูลชาวอินโดนีเซีย 105 ล้านคน ในราคา 5,000 ดอลลาร์ ด้วยวิธีฟิชชิ่ง (Phishing)

4.4 การขโมยข้อมูลจากผู้ให้บริการด้านสุขภาพ ของบริษัทชีลเฮวแคร์ กรุ๊ป (Shields Health Care Group) รัฐแมสซาชูเซตส์ เปิดเผยว่ามีการเจาะข้อมูลตลอดเดือนมีนาคม ซึ่งส่งผลกระทบต่อผู้คนประมาณ 2 ล้านคนในสหรัฐอเมริกา ด้วยวิธีซีโร่ เดย์ เอ็กพอท แอนด์ อะแท็ค (Zero-day Exploit & Attack)

4.5 แฮกเกอร์ชาวจีนแฮกข้อมูลโทรคมนาคมและอื่นๆ ได้ทำการขโมยข้อมูลและเอกสารสำคัญจากหลายๆบริษัททั่วโลก รวมไปถึง“บริษัทโทรคมนาคมรายใหญ่” ซึ่งทาง CISA เปิดเผยว่า อาชาญกรไซเบอร์กลุ่มนี้เน้นโจมตีที่ช่องโหว่ และจุดบกพร่องต่างๆ ด้วยวิธี ฟิชชิ่ง (Phishing) แล้วปล่อยมัลแวร์ ลงในอุปกรณ์เครือข่ายรวมไปถึงที่ผลิตภัณฑ์ด้านไซเบอร์ จากบริษัทยักษ์ใหญ่อย่าง ซิสโก้ และ ฟอร์ติเน็ต

จากข้อมูลด้านภัยคุกคามทางไซเบอร์ ทั้งในประเทศและต่างประเทศ เมื่อนำข้อมูลในข้อ 1, 2, 3 และ 4 นำมาวิเคราะห์ พบว่าภัยคุกคามทางไซเบอร์ที่มีความเหมือนกัน คือ มัลแวร์ (Malware), ฟิชชิ่ง (Phishing), เอสคิวแอล อินเจคชั่น (SQL Injection), ดอท หรือ ดีดอท (DoS/DDoS), พาสเวิร์ด อะแท็ค (Password Attack)

5. จากการวิเคราะห์ด้วย 3 แกนหลักยกระดับองค์กร เตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ มีรายละเอียดดังนี้[18]

5.1 **คน (People)** ตามสถิติด้านการโจมตีทางไซเบอร์ พบว่าหนึ่งในสาเหตุหลักเกิดจากความผิดพลาด การตัดสินใจของตัวกำลังพล หรือครอบครัวที่ขาดความรู้ในการเตรียมพร้อมสำหรับรับมือกับภัยคุกคามทางไซเบอร์ ซึ่งหน่วยสามารถป้องกันและลดช่องโหว่ของข้อผิดพลาดนี้ได้ ด้วยวิธี ดังนี้

5.1.1 Awareness Training (อะแวร์เนส เทรนนิ่ง) การฝึกอบรมสำหรับบุคลากร เพื่อเตรียมพร้อมความรู้ความเข้าใจด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กรที่มีส่วนช่วยให้สามารถลดโอกาสที่จะถูกโจมตีทางไซเบอร์ในรูปแบบต่างๆ ได้มากขึ้น

5.1.2 Specialist skill, experience and qualifications ทักษะความรู้และประสบการณ์ ล้วนเป็นสิ่งสำคัญของการทำงานด้านความมั่นคงปลอดภัย ซึ่งประกอบไปด้วย

5.1.2.1 Hard Skills (ฮาร์ด สกิล) ความรู้และทักษะที่เกี่ยวข้องกับการทำงานโดยตรง อาทิเช่น การใช้โปรแกรม การวิเคราะห์ความเสี่ยง ความเข้าใจด้าน IoT และ Cloud security เป็นต้น

5.1.2.2 Soft Skills (ซอฟท์ สกิล) ทักษะด้านต่างๆ ที่จำเป็นในการทำงานร่วมกับผู้อื่น อาทิเช่น บุคลิกภาพภายนอก ทัศนคติ การแก้ไขปัญหาเฉพาะหน้าการสื่อสาร และความฉลาดทางอารมณ์ เป็นต้น

5.1.3 Authorization control (ออเธอริเซชั่น คอนโทรล) การกำหนดสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศ ให้เป็นไปตามความจำเป็นและสอดคล้องกับความต้องการพื้นฐาน ตามที่ได้รับอนุญาต

5.2 **กระบวนการ (Process)** กระบวนการ เป็นแกนหลักสำคัญในการควบคุมการทำงานของคนและการใช้เทคโนโลยี ให้มีประสิทธิภาพสูงสุด โดยองค์กรสามารถนำกระบวนการเหล่านี้ ไปใช้เพื่อพัฒนาองค์กร และป้องกันการโจมตีทางไซเบอร์ได้ ดังนี้

5.2.1 Management system and policies การจัดการความปลอดภัยทางไซเบอร์ และกำหนดนโยบายนั้นเป็นหลักการสำคัญของเทคโนโลยีสารสนเทศที่ทุกองค์กรควรเข้าใจ เพื่อใช้ในการปกป้องและรับมือกับภัยคุกคามทางไซเบอร์

5.2.2 IT governance, risk, and compliance การขับเคลื่อนองค์กรด้วยเทคโนโลยีที่เหมาะสม จำเป็นต้องคำนึงถึงความสำคัญของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และความเสี่ยงด้านภัยคุกคามทางไซเบอร์

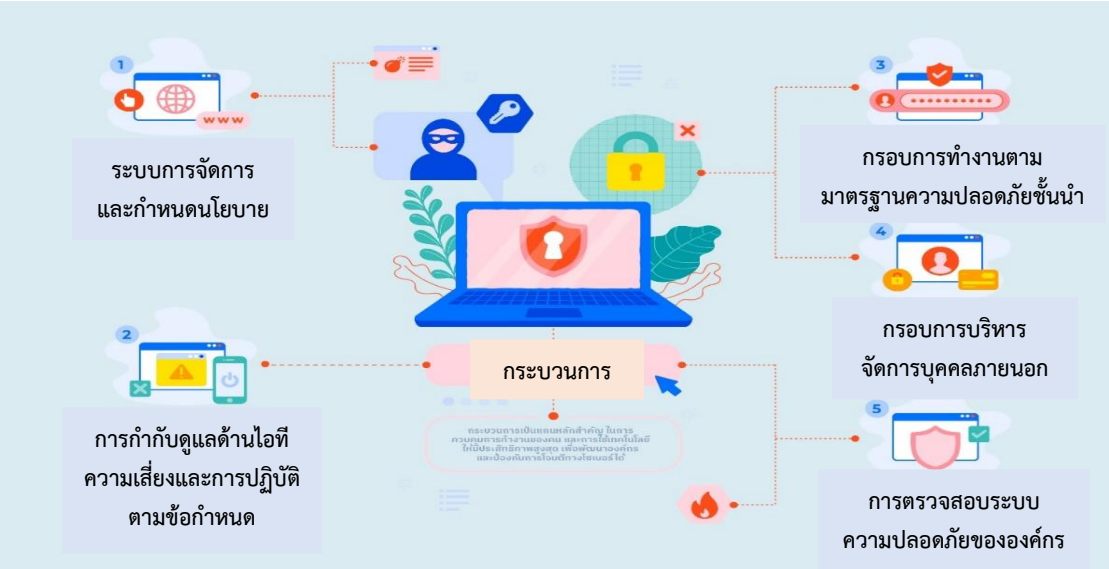
5.2.3 Frameworks by leading security standard หลักการและแนวทางการปฏิบัติ ล้วนเป็นสิ่งจำเป็นที่ทุกองค์กรต้องตระหนักถึง เพื่อช่วยป้องกันความเสียหายที่เกิดจากการโจมตีทางไซเบอร์ อาทิเช่น

5.2.3.1 มาตรฐาน ISO 27001 มาตรฐานสากล สำหรับระบบการจัดการความปลอดภัยของข้อมูล ผ่านการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัย และการนำไปปฏิบัติ โดยระบุแนวทางการดำเนินงานและการบริหารจัดการไว้อย่างชัดเจน

5.2.3.2 NIST หลักการและแนวทางปฏิบัติของการบริหารจัดการความเสี่ยงเพื่อยกระดับความมั่นคง ปลอดภัย ของทุกองค์กร พร้อมทั้งช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับและตอบสนองต่อภัย ได้อย่างรวดเร็วและเป็นระบบ

5.2.4 Third party management องค์กรสามารถนำกรอบการบริหารจัดการบุคคลภายนอก มาปรับใช้ในการกำหนดนโยบาย การรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อควบคุมและป้องกันความเสี่ยง จากการก่ออาชญากรรมทางไซเบอร์

5.2.5 Internal/External audit Internal audit เป็นการตรวจสอบระบบความปลอดภัยขององค์กร เพื่อตรวจสอบว่าระบบทำงานอย่างถูกต้อง และมีความปลอดภัยในการใช้งานจริง ในขณะที่ External audit เป็นการตรวจสอบระบบ โดยมีบริษัทหรือบุคคลภายนอก เป็นผู้ดำเนินการตรวจสอบ เพื่อให้แน่ชัดว่าระบบความปลอดภัยขององค์กร ตรงตามมาตรฐาน ดังตารางภาพที่ 2



ภาพที่ 2 การวิเคราะห์ด้วย 3 แกนหลัก (กระบวนการ)

5.3 **เทคโนโลยี (Technology)** ทุกวันนี้ การโจมตีทางโลกไซเบอร์ได้ทวีความรุนแรงขึ้นอย่างต่อเนื่อง องค์กรจึงจำเป็นต้องเลือกใช้เทคโนโลยีที่เหมาะสมในการรองรับและรับมือกับภัยคุกคามได้อย่างทันถ่วงที ยกตัวอย่างเช่น

5.3.1 Endpoint security, detection and response กระบวนการตรวจสอบและตรวจจับเหตุการณ์ที่น่าสงสัย ที่เกิดขึ้นแบบทันที เพื่อให้องค์กรสามารถเท่าทันต่อภัยคุกคามโดยละเอียด และแจ้งเตือนทันที ในกรณีที่มีการโจมตีผ่านขั้นตอนของการรวบรวมและจัดเก็บข้อมูล การวิเคราะห์และการตอบสนองอย่างรวดเร็ว

5.3.2 Network, infrastructure, and platform security การรักษาความปลอดภัยของระบบอินเทอร์เน็ต โครงสร้างพื้นฐาน และแพลตฟอร์มที่จะช่วยป้องกันการถูกคุกคามจากภายนอก ที่เข้ามาใช้งานโดยไม่ได้รับอนุญาต

5.3.3 Software update/patch ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ถูกเขียนออกมาเพื่อซ่อมแซมหรือแก้ไขจุดบกพร่องของซอฟต์แวร์ก่อนหน้า

5.3.4 Web Application Firewall เครื่องมือสำหรับป้องกันการโจมตีในรูปแบบต่างๆ ภายในองค์กร ซึ่งจะทำการกรองและตรวจสอบที่มาของ HTTP ที่ถูกส่งเข้ามายังเว็บไซต์เพื่อวิเคราะห์ถึงความผิดปกติ หากมีความผิดพลาดเกิดขึ้นก็จะทำการป้องกันเพื่อลดโอกาสการโจมตีทางไซเบอร์

5.3.5 Assessment การใช้เทคโนโลยีในการประเมินความเสี่ยงและช่องโหว่ของการโจมตีทางไซเบอร์ อาทิเช่น

5.3.5.1 VA scan การประเมินช่องโหว่และประเมินความเสี่ยงด้านความปลอดภัยภายในองค์กร ในเชิงลึกเพื่อระบุถึงปัญหาพร้อมทั้งให้แนวทางแก้ไขเพื่อช่วยลดความเสี่ยงที่เกิดขึ้น

5.3.5.2 Pentest การประเมินความเสี่ยงด้วยการทดสอบ เจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ

5.3.6 Identity and access management การบริหารจัดการตัวตนและการเข้าถึง เพื่อใช้ควบคุมสิ่งที่ผู้ใช้สามารถและไม่สามารถเข้าถึงได้ อาทิเช่น อีเมล ฐานข้อมูล ข้อมูล และแอปพลิเคชัน เป็นต้น โดยมีการแทรกแซงน้อยที่สุด เป้าหมายก็คือการจัดการการเข้าถึง เพื่อให้บุคคลที่เหมาะสม สามารถทำงานได้และปฏิเสธบุคคลที่ไม่เหมาะสม เช่น แฮกเกอร์ไม่ให้มีสิทธิ์เข้าถึง

5.3.7 Cloud security Cloud Security ที่จะช่วยเพิ่มความปลอดภัยในการใช้งานระบบคลาวด์ให้ดียิ่งขึ้น โดยมี gateway ที่ปลอดภัย สามารถจัดการกับภัยคุกคามต่างๆ บนคลาวด์ได้อย่างดี

5.3.8 Data security and protection การรักษาความปลอดภัยของข้อมูลและลดความสุ่มเสี่ยงด้านความปลอดภัยของข้อมูล อาทิเช่น การป้องกันการรั่วไหลของการเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต ดังตารางภาพที่ 3

ภาพที่ 3 การวิเคราะห์ด้วย 3 แกนหลัก (เทคโนโลยี)

ปัญหาและผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

ในการวิจัยครั้งนี้ ได้ทำการสัมภาษณ์กำลังพล ครอบครัว และเจ้าหน้าที่ที่มีบทบาทหน้าที่รับผิดชอบด้านไซเบอร์ของหน่วย ในพื้นที่ค่ายสุรนารี จำนวน 11 คน ประกอบไปด้วย กำลังพล 5 คน ครอบครัว 3 คน และเจ้าหน้าที่ด้านไซเบอร์ของหน่วย 3 คน เพื่อนำข้อมูลมาวิเคราะห์ปัญหา และผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ดังนี้

1. ปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์

1.1 ปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ มีการโจมตีหลากหลายรูปแบบ และแต่ละประเภทของภัยคุกคาม จะมีลักษณะการโจมตีเป็นของตัวเอง ถึงแม้อาจจะมีความคล้ายคลึงกันบ้างก็ตาม ซึ่งรูปแบบการโจมตีทั่วไปทางไซเบอร์ มีดังต่อไปนี้[8]

1.1 เนื้อหาที่เป็นภัย (Abusive Content)

1.2 โปรแกรมไม่พึงประสงค์ (Malicious Code)

1.3 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)

1.4 ความพยายามเข้าบุกรุก ระบบ (Intrusion Attempts)

1.5 การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)

1.6 การโจมตี สภาพความพร้อมใช้งานของระบบ (Avai;ability)

1.7 การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Content Security)

1.8 การฉ้อฉล ฉ้อโกง หรือ หลอกลวง เพื่อผลประโยชน์ (Fraud)

1.9 การละเมิดนโยบายขององค์กร (Policy Violation)

1.10 ช่องโหว่ (Vulnerability)

2. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

2.1 ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ส่งผลต่อการใช้ชีวิตของกำลังพล และครอบครัว ในค่ายสุรนารี เป็นอย่างมาก จากการพูดคุย สัมภาษณ์ผ่านทางแอปพลิเคชันไลน์[25 - 29] พบว่า

2.1.1 ในเด็กมักเจอ การฉ้อฉล ฉ้อโกง หรือหลอกลวง ในรูปแบบของการเติมเงินเกมส์ ที่โฆษณาเกินจริง ในเพจเฟสบุ๊ค และในโซเชียลออนไลน์ เมื่อเติมเงินไปแล้วเงินไม่เข้าในเกมส์ แสดงพฤติกรรมก้าวร้าว ทำให้ครอบครัวมีสุขภาพจิตที่ตกต่ำ

2.1.2 พบเนื้อหาที่เป็นภัยคุกคาม จากข้อความมือถือ ที่เข้ามาโดยไม่ทราบแหล่งที่มา บ่อยครั้ง ทำให้ กำลังพล และครอบครัว เกิดความวิตกกังวล

2.1.3 การถูกชี้นำหรือครอบงำทางความคิดโดยไม่รู้ตัว จากอำนาจของสารสนเทศและสื่อมัลติมีเดีย รวมถึงการสร้างกระแสเทียม บนสื่อสังคมออนไลน์ เช่น การปั่นกระแสด้วยแฮชแท็ก การโพสต์ข่าวลือเทียม การสร้างข่าวปลอม ส่งผลกระทบต่อความคิดเห็น ความเชื่อ และการตอบสนองของกำลังพล และครอบครัวโดยรวม

2.1.4 มีการพยายามแฮ็กเข้าสู่ระบบแอฟพลิเคชันต่างๆ ของกำลังพล ครอบครัว และหน่วยงาน ของหน่วยบ่อยครั้ง

2.2 ผลกระทบที่ตามมา คือ กำลังพลและครอบครัว เกิดความหวาดระแวง ความมั่นคงในสถาบันครอบครัวลดลง ส่งผลถึงการปฏิบัติงานให้หน่วยไม่เต็มประสิทธิภาพสูงสุด

วิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์

1. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับโลก

การเปลี่ยนแปลงของสภาวะโลกในปัจจุบัน ไม่ว่าจะเป็น การเมือง เศรษฐกิจ สังคมจิตวิทยา การทหาร วิทยาศาสตร์ เทคโนโลยี การพลังงานทรัพยากรธรรมชาติและสิ่งแวดล้อม มีผลกระทบอย่างสำคัญต่อมนุษย์ ทำให้พฤติกรรมการบริโภคของมนุษย์

เปลี่ยนไปกระตุ้นให้เกิดการเปลี่ยนแปลงของเทคโนโลยี (Digital Disruption) ส่งผลให้มีการสร้างนวัตกรรมและการพัฒนาเทคโนโลยีต่างๆ อย่างรวดเร็วเพื่อตอบสนองความต้องการของผู้คน[10] เกิดเป็นแนวโน้มการเปลี่ยนแปลงของโลกอนาคต ที่เรียกว่า “MegaTrends” สำหรับประเทศไทยที่มีการบรรจุเรื่องของ “Mega Trends” ไว้ในร่างแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 ครอบคลุมระยะเวลา 5 ปี (พ.ศ. 2565 - 2570)[11] Mega Trends คือการเปลี่ยนแปลงขนาดใหญ่ สังคมเศรษฐกิจ การเมืองสิ่งแวดล้อม หรือเทคโนโลยีที่เกิดขึ้นแล้ว สามารถมีอิทธิพลต่อกิจกรรม กระบวนการและการรับรู้ที่หลากหลายอาจยาวนานหลายทศวรรษ สิ่งเหล่านี้เป็นพลังเบื้องหลังที่ขับเคลื่อนการเปลี่ยนแปลงในตลาดโลก และชีวิตประจำวันที่ทั่วโลกนำมาเป็นปัจจัยในการวิเคราะห์คาดการณ์อนาคต เพื่อเป็นแนวทางของการพัฒนาแผนงานในมิติต่างๆ ซึ่งมีอยู่ด้วยกัน 5 ด้าน คือ MegaTrends 1 : Shifting economic power (การเปลี่ยนแปลงอำนาจเศรษฐกิจ) MegaTrends 2 : Resource scarcity (การขาดแคลนทรัพยากร) MegaTrends 3 : Technological breakthrough (ความก้าวหน้าทางเทคโนโลยี) MegaTrends 4 : Social change (การเปลี่ยนแปลงทางสังคม) MegaTrends 5 : Rapid Urbanisation(การขยายตัวของเมืองอย่างรวดเร็ว)[13] ด้วยเหตุนี้ทำให้ภัยคุกคามทางไซเบอร์มีความรุนแรงขึ้นตามการเปลี่ยนแปลงของโลก โดยเฉพาะภัยคุกคามทางไซเบอร์ต่อระบบการเงินของโลก ซึ่งนำไปสู่เสถียรภาพทางการเงินในวงกว้าง ทำให้ประชาคมโลกจะต้องร่วมมือกัน เพื่อหาวิธีป้องกันจากภัยคุกคามทางไซเบอร์[14] การโจมตีที่เป็นอันตรายในอนาคตที่น่าเป็นห่วงที่สุดคือเหตุการณ์ที่ทำลายความสมบูรณ์ของข้อมูลทางการเงิน เช่น บันทึก อัลกอลิทึมและธุรกรรม ผู้มุ่งร้ายที่อยู่เบื้องหลังการโจมตีเหล่านี้ ไม่เพียงแต่รวมถึงอาชญากรที่กล้าหาญมากขึ้นเท่านั้น แต่ยังรวมถึงรัฐและกลุ่มที่ได้รับการสนับสนุนจากรัฐ โดยมีเป้าหมายและแรงจูงใจหลากหลาย เช่นกลุ่ม Cabanak ดังตารางภาพที่ 1

2. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับภูมิภาค

จากการศึกษาสภาวะแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับภูมิภาค พบว่าการเปลี่ยนแปลงไปสู่สังคมดิจิทัล (Digitalization) นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ต และคอมพิวเตอร์เป็นช่องทางในการโจมตี หรือที่เรียกว่า อาชญากรรมไซเบอร์ (Cyber-Crime)[12] แนวโน้มความปลอดภัยทางไซเบอร์ในปี 2567 โดยเฉพาะอย่างยิ่งเมื่อมีการเพิ่มขึ้นของ generative AI และเครื่องมืออัตโนมัติในคลังแสงของอาชญากรไซเบอร์ เนื่องจากปี 2023 ได้รับการขนานนามว่าเป็นปีแห่ง AI โดยเฉพาะภัยคุกคามที่อาจเกิดขึ้นจากการใช้เครื่องมือ AI ที่เพิ่มขึ้น ทั้งจากผู้ใช้ในองค์กรและผู้ไม่ประสงค์ดี ข้อมูลข่าวจากไทยรัฐทีวี[16] ได้นำบทความของคุณ วิทาลี คัมลัก หัวหน้าศูนย์วิจัยของภูมิภาคเอเชียแปซิฟิก ทีมวิจัยและวิเคราะห์ระดับโลกแคสเปอร์สกี้

คาดการณ์ว่าภัยคุกคามทางไซเบอร์ในปีนี้ ชี้ไปประเทศในเอเชียแปซิฟิก มีความเสี่ยงถูกโจมตีด้วยฟิชชิ่ง มากเป็นพิเศษ คุณ วิทาลี คัมลัก กล่าวว่า เศรษฐกิจดิจิทัลของเอเชียแปซิฟิกยังคงเติบโตอย่างทวีคูณ และคาดว่าจะรักษาการเติบโตได้ต่อเนื่องไปอีก 5 ปี เนื่องจากเป็นยุคการเปลี่ยนผ่านสู่ดิจิทัล การตอบรับเทคโนโลยีอย่างการชำระเงินดิจิทัล ซุปเปอร์แอป, อุปกรณ์ IoT, เมืองอัจฉริยะ และปัญญาประดิษฐ์ (AI) สิ่งที่น่าสนใจคือ ในปี 2024 การจารกรรมทางไซเบอร์ยังเป็นเป้าหมายหลักของแฮกเกอร์ โดยมีเหตุผลจากความตึงเครียดทางภูมิรัฐศาสตร์ ทีมวิจัยและวิเคราะห์ระดับโลกของแคสเปอร์สกี้ ประเมินว่าประเทศในเอเชียตะวันออกเฉียงใต้ ซึ่งประกอบไปด้วย สิงคโปร์ ฟิลิปปินส์ ไทย เวียดนาม มาเลเซีย และอินโดนีเซีย ยังมีความเสี่ยงจากการถูกหลอกลวงออนไลน์จากการใช้งานการชำระเงินดิจิทัลของผู้ใช้ออนไลน์ โดยถือเป็นหนึ่งในปัญหาที่มีความสลับซับซ้อนต่อการแก้ไขปัญหา นอกจากนี้การถูกโจมตีด้วยกลโกงและฟิชชิ่งก็เป็นสิ่งที่น่ากังวล เนื่องจากความไม่รู้ด้านเทคนิคทำให้ตกเป็นเหยื่อได้ง่าย

3. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับอาเซียน

อาเซียนเป็นภูมิภาคที่มีจำนวนผู้ใช้อินเทอร์เน็ต ที่เติบโตเร็วที่สุดในโลก ภายในอาเซียนมีประชากรกว่าครึ่งหนึ่งเป็นผู้ใช้สื่อสังคมออนไลน์ (Social Media) จึงทำให้อาเซียนเป็นตลาดสังคมออนไลน์อันดับหนึ่งของโลก และจากการจัดอันดับ 10 ประเทศผู้ใช้เฟซบุ๊ค (Facebook) มากที่สุดในโลก พบว่า ประเทศสมาชิกในอาเซียน ได้แก่ ประเทศอินโดนีเซีย ฟิลิปปินส์ เวียดนาม และไทย เป็นกลุ่มประเทศที่อยู่ในอันดับดังกล่าว[9] สำหรับอาเซียนนั้น อาชญากรรมไซเบอร์ ถือเป็นภัยคุกคามความมั่นคง ที่ถูกกำหนดไว้ให้เป็นส่วนหนึ่งของอาชญากรรมข้ามชาติที่สำคัญ ภายใต้ประชาคมการเมืองและความมั่นคงของอาเซียน โดยความร่วมมือของอาเซียนด้านการจัดการปัญหาอาชญากรรมไซเบอร์[17]สามารถแบ่งได้เป็น 3 ลักษณะ ได้แก่ 1) ความร่วมมือภายในอาเซียนลักษณะของการจัดประชุม 2) ความร่วมมือในระดับพหุภาคี และ 3) การจัดทำตราสารอาเซียน และให้ความสำคัญอย่างมากต่อการส่งเสริมความร่วมมือและการเสริมสร้างขีดความสามารถเพื่อรับมือกับความท้าทายทางไซเบอร์ และอาชญากรรมทางไซเบอร์

4. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับประเทศ

จากการศึกษาสภาวะแวดล้อม ความมั่นคงปลอดภัยทางไซเบอร์ระดับประเทศ สถานการณ์ทางไซเบอร์ที่เกิดขึ้นทางรัฐบาลของประเทศไทย ได้ออกนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์ ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยได้จัดตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปัจจุบันเทคโนโลยีและระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนธุรกิจและองค์กร

ให้มีความก้าวหน้าและรวดเร็ว รวมทั้งการเปลี่ยนแปลงธุรกิจให้เข้าสู่สังคมดิจิทัล (Transformation) ทำให้ธุรกิจและองค์กรเหล่านั้น ต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อธุรกิจและองค์กร เป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อม ในการรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อช่วยเพิ่มความมั่นใจ และมั่นคงต่อผู้ใช้บริการ ทั้งภาครัฐ และภาคประชาชน กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ มีมาตรฐาน และมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือ เพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ มีการร่วมมือและประสานงานกัน กับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญ ไม่สามารถทำงานได้ จนทำให้ประชาชนเดือดร้อน ต่อมาโฆษกกลาโหม แถลงว่าที่ประชุมสภากลาโหมที่มี นาย สุทิน คลังแสง รัฐมนตรีกลาโหม ได้ให้ความสำคัญกับภัยคุกคามด้านไซเบอร์ จึงได้ขยายหน่วย ยกระดับศูนย์ไซเบอร์ทหารเป็นหน่วยบัญชาการไซเบอร์ทหาร

5. จากการวิเคราะห์ด้วย SWOT Analysis จุดแข็ง จุดอ่อน โอกาส และอุปสรรค ซึ่งประกอบด้วยปัจจัยภายในและปัจจัยภายนอก ในภาพรวม มีรายละเอียดดังนี้

5.1 **จุดแข็ง (Strength)** หน่วยมีการจัดการเกี่ยวกับการป้องกันภัยจากภัยคุกคามทางไซเบอร์ มีการฝึกอบรมเจ้าหน้าที่ ให้ทันต่อภัยคุกคามรูปแบบใหม่อยู่เสมอ มีเทคโนโลยีที่เข้ามาช่วยป้องกันภัยจากภัยคุกคามด้านไซเบอร์ และมีโครงสร้างของสายการบังคับบัญชาไปจนถึงระดับสูง ที่รับผิดชอบด้านความมั่นคงทางไซเบอร์

5.2 **จุดอ่อน (Weakness)** หน่วยมีกำลังพลที่ปฏิบัติงานด้านไซเบอร์ไม่เพียงพอ ทำให้ขาดการอบรมให้ความรู้แก่กำลังพลและครอบครัว ในค่ายสุรนารีอย่างต่อเนื่อง และขาดความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์

5.3 **โอกาส (Opportunity)** ปัจจุบันกองทัพบก ได้มีการจัดทำหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ ประจำปีงบประมาณ 2567 ดังนี้[9]

5.3.1 หลักสูตรการปฏิบัติการไซเบอร์ขั้นต้น

5.3.2 หลักสูตรการปฏิบัติการไซเบอร์ขั้นสูง

5.3.3 หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ขั้นต้น

5.3.4 หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ขั้นสูง

5.3.5 หลักสูตรพิเศษเฉพาะทางด้านการรักษาความปลอดภัยไซเบอร์

5.3.6 หลักสูตรหลักการใช้งานเครือข่ายสังคมออนไลน์

5.3.7 หลักสูตรการผลิตสื่อด้านไซเบอร์

การจัดทำแผนการฝึกอบรมหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ สำหรับกำลังพล เพื่อเป็นการเตรียมการจัดการฝึกอบรม และพิจารณากำลังพล เข้ารับการฝึกอบรมในหลักสูตร เป็นการเพิ่มศักยภาพให้กับกำลังพลทำหน้าที่ เสริมสร้างความรู้ความเข้าใจ สร้างความตระหนัก ติดตามกำกับดูแลการปฏิบัติของหน่วย ตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวังแจ้งเตือนภัยคุกคาม การติดตาม สืบค้นและตรวจสอบช่องโหว่ของระบบ รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิทัลได้อย่างมีประสิทธิภาพ ในการพัฒนาศักยภาพของกองทัพบก ภายใต้ยุทธศาสตร์ชาติ ได้แก่ การเสริมสร้างบุคลากรด้านเทคโนโลยีดิจิทัลและไซเบอร์ของกองทัพบก การดำรงขีดความสามารถ การปฏิบัติการด้านไซเบอร์ การเสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์ สำหรับกำลังพลของกองทัพบก ศูนย์ปฏิบัติการรักษาความปลอดภัยไซเบอร์ (CSOC) กองทัพบก จัดตั้งชุดรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ระดับกองทัพบก และระดับกองทัพภาค

5.4 **อุปสรรค (Threat)**

5.4.1 ยังคงมีผู้ที่ยังขาดความเข้าใจเกี่ยวกับข้อกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ในหลายประเด็น

5.4.2 แนวโน้มของภัยคุกคามทางไซเบอร์มีปริมาณ ความซับซ้อนและความรุนแรง เพิ่มมากขึ้นอย่างรวดเร็วตามลำดับ แต่กองทัพบก มีขีดความสามารถในการตรวจพบ และควบคุมได้เพียงบางส่วนเท่านั้น

5.4.3 สังคมไทย ยังมีทัศนคติเกี่ยวกับไซเบอร์ในเชิงลบ ทำให้การปฏิบัติด้านไซเบอร์ของกองทัพบก อาจถูกมองไปในแง่ร้าย เป็นที่หวาดระแวง และไม่ได้รับการสนับสนุน

5.4.4 การโจมตีทางไซเบอร์ที่มีระดับความรุนแรง และกระทบต่อความมั่นคงของชาติในวงกว้างอาจเกิดได้ทุกขณะ โดยรูปแบบการโจมตี อาจส่งผลกระทบต่อโครงสร้างพื้นฐานไซเบอร์ทางกายภาพ หรือการโจมตีในลักษณะ การทำสงครามข้อมูล

ข่าวสาร ซึ่งอาจนำไปสู่เงื่อนไขสนับสนุนให้เกิดหรือยับยั้ง การปฏิบัติการทางทหารของกองทัพบกได้

5.4.5 เทคนิค วิธีการ รูปแบบในการโจมตีทางไซเบอร์ มีการพัฒนาไปอย่างรวดเร็ว และไม่มีทิศทาง ดังนั้น การดำรงสภาพให้มีความพร้อมและเท่าทันต่อเทคโนโลยี อย่างต่อเนื่อง จึงจำเป็นต้องใช้งบประมาณจำนวนมาก และอาจมีมูลค่าสูงกว่ามูลค่าของทรัพย์สินที่จะปกป้อง

6. ปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในตามหลัก 4 M สามารถสรุปแยกเป็นจุดแข็ง และจุดอ่อนได้ดังนี้

6.1 **กำลังพล (Man)**

<u>จุดแข็ง</u> มีกำลังพลที่ปฏิบัติงานด้านไซเบอร์ มีการวางแผน และจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วย ตามยุทธศาสตร์ มีการเสริมสร้างทักษะความรู้ให้กำลังพลด้วยการจัดอบรม อาทิ หลักสูตรการพัฒนาขีดความสามารถ ศักยภาพด้านงานข่าวกรองทางไซเบอร์ จัดอบรมให้ความรู้แก่ครอบครัวของกำลังพล ในค่ายสุรนารี มีการสร้างแรงจูงใจให้กำลังพล เพื่อเสริมสร้างศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากล

<u>จุดอ่อน</u> กำลังพลของหน่วย ยังขาดการบูรณาการ และการพัฒนาขีดความสามารถ ศักยภาพ ด้านงานต่อต้านการก่อการร้ายทางไซเบอร์ ทำให้ไม่สามารถแนะนำครอบครัวของหน่วยได้อย่างเต็มประสิทธิภาพ ซึ่งนับเป็นส่วนสำคัญในการทำความเข้าใจกับ ภัยคุกคามรูปแบบต่างๆ ส่วนใหญ่ยังขาดความรู้ ขาดกำลังพลที่เชี่ยวชาญ ขาดจิตสำนึกด้านการรักษาความปลอดภัยทางไซเบอร์

6.2 **งบประมาณ (Money)**

<u>จุดแข็ง</u> หน่วยมีการจัดสรรงบประมาณ ให้กับฝ่ายงานที่รับผิดชอบงานด้านไซเบอร์ สนับสนุนในการต่อต้านการก่อการร้ายทางไซเบอร์

<u>จุดอ่อน</u> เนื่องจากหน่วยงานมีขนาดเล็ก ในการจัดสรรงบประมาณจึงไม่เพียงพอต่อการพัฒนางานด้านไซเบอร์ บุคลากรในการทำงานขาดการวางแผนการนำเสนอโครงการ เพื่อขอรับการสนับสนุนงบประมาณ ทำให้การพัฒนางานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ ไม่มีความต่อเนื่อง

6.3 **วัสดุอุปกรณ์ (Material)**

จุดแข็ง หน่วยมีเครื่องมือระบบตรวจจับ โปรแกรมป้องกันความเสี่ยงระบบสารสนเทศ และป้องกันการโจมตีทางไซเบอร์ ที่ครอบคลุมเครือข่ายข้อมูลทั้งหมดภายในของหน่วย และมีอุปกรณ์สื่อสารที่สามารถเข้าถึงอินเทอร์เน็ต

จุดอ่อน อุปกรณ์ที่ใช้ในชีวิตประจำวัน อาศัยการใช้งานจากอินเทอร์เน็ต มากขึ้น ทำให้เสี่ยงต่อการเกิดภัยทางไซเบอร์ได้ง่ายขึ้น หน่วยงานมีอุปกรณ์ไม่เพียงพอ และทันสมัย ขาดการบำรุงรักษาอุปกรณ์ ทำให้บางชนิดไม่สามารถใช้งานได้ และบางโปรแกรม ไม่ได้สอดคล้องตามมาตรฐานการรักษาความปลอดภัยสารสนเทศสากล

6.4 **การจัดการ (Management)**

จุดแข็ง หน่วยมีนโยบายและยุทธศาสตร์ เกี่ยวกับการพัฒนางานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ มีการจัดกำลังพลที่รับผิดชอบงานด้านไซเบอร์อย่างชัดเจน

จุดอ่อน บุคลากรผู้ใช้งานระบบคอมพิวเตอร์ ยังขาดจิตสำนึกด้านความรักษาความปลอดภัย ขาดการบูรณาการเกี่ยวกับระบบการบริหารจัดการเครือข่ายเพื่อเสริมความมั่นคงของหน่วย ขาดการประสานงานระหว่างหน่วยงานภายในและภาครัฐขาดการพัฒนาระบบและเทคโนโลยีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางในการแก้ปัญหาภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

จากการวิเคราะห์โดยกำหนดกระบวนการศึกษาทางยุทธศาสตร์ตามทฤษฎีการวิเคราะห์ปัจจัยด้วยวิธี SWOT Analysis และปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในตามหลัก 4M พร้อมกับ 3 แกนหลักขององค์กร พบว่าปัญหาเกิดจาก

1. สภาวะแวดล้อมในระดับโลก มีพฤติกรรมการบริโภคของมนุษย์เปลี่ยนแปลงไป กระตุ้นให้เกิดการเปลี่ยนแปลงของเทคโนโลยี ส่งผลให้มีการสร้างนวัตกรรมและการพัฒนาเทคโนโลยี อย่างรวดเร็ว เพื่อตอบสนองความต้องการของผู้คนทั่วโลก ส่งผลให้สภาวะแวดล้อมในระดับภูมิภาค และระดับประเทศ ปรับตัวเปลี่ยนแปลงเข้าสู่สังคมดิจิทัล นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ตและคอมพิวเตอร์เป็นช่องทางในการโจมตี ของเหล่าอาชญากรไซเบอร์

2. กำลังพลของหน่วย ที่ปฏิบัติงานด้านไซเบอร์ไม่เพียงพอ เนื่องจากเป็นหน่วยงานที่มีขนาดเล็ก ขาดการบูรณาการ ขาดความเข้าใจเกี่ยวกับกฎหมายที่เกี่ยวข้อง

กับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการพัฒนาขีดความสามารถศักยภาพด้านงานต่อต้านการก่อการร้ายทางไซเบอร์ ส่งผลทำให้ไม่สามารถอบรมให้ความรู้แก่กำลังพล และครอบครัว ในค่ายสุรนารี

3. ในการจัดสรรงบประมาณด้านไซเบอร์ ไม่เพียงพอต่อการพัฒนางานด้านไซเบอร์ ทั้งบุคลากร อุปกรณ์ต่อต้านทางไซเบอร์ และแผนงานป้องกัน ขาดความต่อเนื่อง ทำให้ขาดการวางแผนการนำเสนอโครงการ เพื่อขอรับการสนับสนุนงบประมาณ

4. การใช้ชีวิตในปัจจุบันของ กำลังพล และครอบครัว ในค่ายสุรนารี ต้องพึ่งพาอาศัยการใช้งานจากอินเทอร์เน็ต โซเชียลมิเดีย มากขึ้น แนวโน้มของภัยคุกคามทางไซเบอร์ ทั้งปริมาณของภัยคุกคาม ความซับซ้อน และความรุนแรง เพิ่มมากขึ้นอย่างรวดเร็ว เกินขีดความสามารถในการตรวจพบ สามารถควบคุมได้เพียงบางส่วน

5. กำลังพล และครอบครัว ในค่ายสุรนารี ยังขาดความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ การรักษาความปลอดภัย ความผิดพลาดในการตัดสินใจ และยังมีทัศนคติเกี่ยวกับไซเบอร์ในเชิงลบ ทำให้การปฏิบัติด้านไซเบอร์ของหน่วยถูกมองไปในแง่ร้าย เป็นที่หวาดระแวงและไม่ได้รับการสนับสนุน

สำหรับแนวทางในการแก้ไขปัญหาที่เหมาะสม จากภัยคุกคามด้านไซเบอร์ มีดังนี้

1. ส่งกำลังพลที่ปฏิบัติงานด้านไซเบอร์ของหน่วย เข้ารับการฝึกหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ ตามหลักสูตรที่กองทัพบกจัดการฝึก ซึ่งมีอยู่ด้วยกัน 7 หลักสูตร โดยกองทัพบก เป็นผู้สนับสนุนงบประมาณ ในการฝึกอบรมหลักสูตร แก่กำลังพลที่เข้ารับการฝึกในฐานะหน่วยงานหลัก

2. จัดอบรมให้ความรู้เกี่ยวกับการป้องกัน จากภัยคุกคามทางไซเบอร์ ให้แก่กำลังพลและครอบครัวของหน่วย ในค่ายสุรนารี ใช้เวลาในห้วงเย็นหลังเลิกงาน จัดกิจกรรมพบปะ ระหว่างผู้บังคับบัญชาและครอบครัวของกำลังพล ให้ความรู้โดยมีกำลังพลที่ไปฝึก หลักสูตรเพิ่มศักยภาพด้านไซเบอร์ เป็นวิทยากรให้ความรู้

3. จัดตั้งศูนย์ไซเบอร์ระดับหน่วยขึ้น ในรูปแบบของการกระจายข่าวสารภัยคุกคามทางไซเบอร์ ผ่านแอปพลิเคชันไลน์ เฟสบุ๊ค มีเจ้าหน้าที่ ฝ่าย/แผนก การข่าว เป็นผู้รับผิดชอบ โดยมีกำลังพล ที่ไปฝึกหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ เป็นตัวหลัก

4. จัดทำแบบประเมินความเข้าใจ เกี่ยวกับภัยคุกคามทางไซเบอร์ แก่กำลังพลและครอบครัว รายงานให้ผู้บังคับบัญชาทราบทุกครั้ง ที่มีการประชุมประจำเดือน

5. กองทัพบกจัดสรรงบประมาณด้านไซเบอร์ ในการจัดซื้ออุปกรณ์ต่อต้านทางไซเบอร์ ให้แก่หน่วย โดยหน่วยเป็นผู้นำเสนอแผนงานป้องกัน และโครงการขึ้นไปของบประมาณประจำปี จากกองทัพบก เพื่อให้เกิดความต่อเนื่องของการป้องกันภัยคุกคามทางไซเบอร์

6. รัฐออกกฎหมายให้สอดคล้องกับภัยคุกคามด้านไซเบอร์ เพื่อเสริมสร้างความปลอดภัยทางไซเบอร์[19] ที่มีประสิทธิภาพ และสามารถยืดหยุ่นปรับเปลี่ยนกฎหมายให้ทันสมัย ตามทันเทคโนโลยีสอดคล้องกับบรรทัดฐานสากล ส่งเสริมบทบาทของผู้ให้บริการด้านไอที ในการต่อสู้กับภัยคุกคามทางไซเบอร์

บทที่ 3
บทอภิปราย

จากการวิเคราะห์ถึงปัจจัยสภาพแวดล้อมที่เกี่ยวข้องกับ การก่อการร้ายทางไซเบอร์ เป็นการทำสงครามบนโลกดิจิทัล โดยใช้กลยุทธ์ทางเทคโนโลยีดิจิทัลในการทำลายความมั่นคง เพื่อขัดขวางระบบและเครือข่าย ทำให้ระบบเครือข่ายไม่สามารถดำเนินการได้ตามปกติ เกิดปัญหากับระบบโครงสร้างสาธารณูปโภคขั้นพื้นฐาน การโจมตีทางไซเบอร์ยังคงมีแนวโน้มที่สร้างความรุนแรง และความซับซ้อนมากขึ้นตามการเปลี่ยนแปลงของเทคโนโลยีสมัยใหม่ ในรูปแบบที่ไม่สามารถคาดเดาได้

การประเมินความเหมาะสม ความเป็นไปได้ และการยอมรับได้ของหนทางปฏิบัติ

1. ความเหมาะสม

สำหรับปัญหาภัยคุกคามการก่อการร้ายทางไซเบอร์ เป็นปัญหาที่กำลังพลและครอบครัว ค่ายสุรนารี รวมถึงประชาชนส่วนใหญ่ ยังขาดความรู้ความเข้าใจด้านภัยคุกคามทางไซเบอร์ ที่มีแนวโน้มว่าความรุนแรงจะเพิ่มมากขึ้น ตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว ดังนั้นแนวทางในการแก้ไขปัญหา เช่น การส่งกำลังพลที่ปฏิบัติงานด้านไซเบอร์ของหน่วยเข้ารับการฝึกหลักสูตรเพิ่มศักยภาพด้านไซเบอร์, การจัดอบรมให้ความรู้เกี่ยวกับการป้องกันจากภัยคุกคามทางไซเบอร์, การจัดตั้งศูนย์ไซเบอร์ระดับหน่วย, การจัดทำแบบประเมินความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์, การจัดซื้ออุปกรณ์ต่อต้านทางไซเบอร์ให้แก่หน่วย และรัฐออกกฎหมายให้สอดคล้องกับภัยคุกคามด้านไซเบอร์ เพื่อเสริมสร้างความปลอดภัยทางไซเบอร์ ที่มีประสิทธิภาพ

2. ความเป็นไปได้และยอมรับได้

ในการดำเนินการแก้ไขปัญหาจากภัยคุคามทางไซเบอร์ ถือเป็นยุทธศาสตร์ชาติด้านความมั่นคง ที่กระทรวงกลาโหม กำหนดให้กองทัพบก เป็นหน่วยงานหลักด้านความมั่นคง ในการต่อสู้ภัยคุกคามรูปแบบต่างๆ ของชาติ ที่เกิดขึ้นในปัจจุบันและอนาคต เป็นความรับผิดชอบของกองทัพบกโดยตรง จึงมีความเป็นไปได้และยอมรับได้ของหนทางปฏิบัติ ซึ่งสอดคล้องกับงานวิจัยของ พันเอกหญิง สุดารัตน์ สุมงคล[20] ในประเด็น แนวทางการแก้ไขปัญหาการขาดแคลนบุคลากรที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก โดยนำทฤษฎี ที่เกี่ยวกับแรงจูงใจมาใช้ในการกำหนดแนวทาง คือ

การศึกษาหลักสูตรอบรมทางด้านไซเบอร์จากหน่วยภาครัฐและเอกชน หรือมอบทุนการศึกษาทางด้านไซเบอร์ทั้งภายในประเทศและต่างประเทศ เงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์ (พ.ป.ซ.) และการมีโรงเรียนไซเบอร์ และสอดคล้องกับงานวิจัยของ คุณ นราวิชญ์ วิตบรรจง[21] ในประเด็นหลักที่ 3 มาตรการและแนวทางปฏิบัติที่เหมาะสมในการพิจารณาและคัดเลือกบุคคลพลเรือน เข้ารับราชการในกองทัพบก ผลการวิจัยพบว่า นโยบายการพิจารณาและคัดเลือกบุคคลพลเรือนเข้ารับราชการในกองทัพบกด้านการใช้สื่อสังคมออนไลน์และการตรวจสอบรอยเท้าทางดิจิทัลนั้น ควรมีมาตรฐานหรือแนวทางการปฏิบัติที่ชัดเจน รวมทั้งควรมีการเตรียมความพร้อมทั้งในระดับนโยบาย กำลังพลผู้ปฏิบัติ เครื่องมือ และกฎระเบียบข้อบังคับที่เกี่ยวข้อง และเป็นนโยบายที่มีความยุติธรรม โปร่งใส และตรวจสอบได้

ความสอดคล้องของแนวทางการปฏิบัติกับผลงานวิจัยที่เกี่ยวข้อง

พันเอกหญิง สุดารัตน์ สุมงคล[20] ได้ทำการศึกษาเรื่อง แนวทางแก้ไขปัญหาการขาดแคลนบุคลากร ที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก อธิบายว่าปัญหาการขาดแคลนบุคลากร ที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก พบว่า กองทัพบกขาดแคลนบุคลากรที่ปฏิบัติงานด้านไซเบอร์ ตั้งแต่ระดับเบื้องต้นจนถึงระดับความเชี่ยวชาญเฉพาะด้าน รัฐบาลให้ความสำคัญกับการเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ จึงกำหนดให้กระทรวงกลาโหมเป็นหน่วยงานนำ ในการจัดการกับภัยคุกคามด้านไซเบอร์ แต่กองทัพบกยังขาดแคลนกำลังพลที่ปฏิบัติงานด้านไซเบอร์ ในทุกระดับโดยเฉพาะระดับความเชี่ยวชาญพิเศษด้านความมั่นคงปลอดภัยไซเบอร์ จึงได้เสนอแนวทางการแก้ไขปัญหาการขาดแคลนบุคลากรที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก โดยนำทฤษฎีที่เกี่ยวกับแรงจูงใจ มาใช้ในการกำหนดแนวทาง คือ การศึกษาหลักสูตรอบรมทางด้านไซเบอร์จากหน่วยภาครัฐและเอกชน หรือมอบทุนการศึกษาทางด้านไซเบอร์ ทั้งภายในประเทศและต่างประเทศ เงินเพิ่มสำหรับตำแหน่งที่มีเหตุพิเศษของผู้ปฏิบัติงานไซเบอร์ (พ.ป.ซ.) และการจัดตั้งโรงเรียนไซเบอร์

นราวิชญ์ วิตบรรจง[21] การศึกษาวิจัยเรื่อง นโยบายการพิจารณาคัดเลือกบุคคลพลเรือนเข้ารับราชการในกองทัพบกด้วยการใช้สื่อสังคมออนไลน์และรอยเท้าทางดิจิทัล เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยได้ทำการคัดเลือกผู้ให้ข้อมูลสำคัญ จำนวน 11 ท่าน เครื่องมือที่ใช้ในการวิจัยเป็นแบบสัมภาษณ์ เพื่อตอบวัตถุประสงค์ของการวิจัย คือ 1) นโยบายการพิจารณาและคัดเลือกบุคคลพลเรือนเข้ารับราชการในกองทัพบกด้วยการใช้สื่อสังคมออนไลน์ และการตรวจสอบรอยเท้าทางดิจิทัล 2) เพื่อวิเคราะห์ผลกระทบของนโยบาย 3) เพื่อเสนอมาตรการ ระบบการคัดเลือก และแนวทางปฏิบัติ

ที่เหมาะสม ผลการวิจัยพบว่า นโยบายการพิจารณาและคัดเลือกบุคคลพลเรือนเข้ารับราชการในกองทัพบกด้วยการใช้โซเชียลมีเดียและการตรวจสอบรอยเท้าทางดิจิทัล เป็นนโยบายที่สำคัญและมีความจำเป็นในยุคปัจจุบัน ซึ่งกองทัพบกกำหนดขึ้นมาใหม่ให้ทันต่อสถานการณ์ มีการตรวจสอบทัศนคติผ่านการใช้โซเชียลมีเดียของผู้เข้ารับการคัดเลือกมาใช้ในการพิจารณา เป็นนโยบายที่เกี่ยวข้องกับงานด้านทรัพยากรบุคคลของหน่วยงานที่ไม่แตกต่างจากองค์กรทั้งภาครัฐ ภาคเอกชนอื่นๆ นโยบายดังกล่าวส่งผลกระทบทั้งผู้รับการคัดเลือกกองทัพบก และ หน่วยงานที่เกี่ยวข้อง ซึ่งมีผลกระทบทั้งเชิงบวกและเชิงลบทั้งทางตรงและทางอ้อม ทั้งนี้จากการศึกษาพบว่า การนำนโยบายไปสู่การปฏิบัตินั้นควรมีมาตรฐานหรือแนวทางการปฏิบัติที่ชัดเจน มีการเตรียมความพร้อมทั้งในระดับนโยบาย กำลังพลผู้ปฏิบัติ เครื่องมือ และกฎระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อให้เป็นนโยบายที่มีความยุติธรรม โปร่งใส และตรวจสอบได้ โดยเฉพาะอย่างยิ่งที่นโยบายดังกล่าวมีความเกี่ยวข้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA:Personal Data Protection Act) ที่มีผลบังคับใช้ในปัจจุบัน

บทที่ 4
บทสรุป

การศึกษาวิจัยเพื่อหาแนวทางในการป้องกันภัยจาก ภัยคุกคามด้านไซเบอร์ของกำลังพลและครอบครัว ในค่ายสุรนารี การศึกษาในครั้งนี้ ผู้วิจัยได้ใช้การวิจัยในเชิงยุทธศาสตร์ ตามแนวทางที่วิทยาลัยการทัพบก กำหนด โดยใช้รูปแบบการวิจัย เชิงคุณภาพ และใช้วิธีการวิจัยเชิงเอกสาร เป็นแนวทางการวิจัย โดยพิจารณาจากปัจจัยสภาพแวดล้อมที่มีผลต่อแนวทางในการปฏิบัติ แนวคิดและทฤษฎีที่เกี่ยวข้อง นำมาวิเคราะห์ถึงจุดแข็ง จุดอ่อน โอกาส และอุปสรรค โดยยึดจุดประสงค์สุดท้ายเพื่อหาแนวทางในการแก้ปัญหาภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี ผลการวิจัยสรุปได้ดังนี้

สรุปผลการวิจัย

1. สภาพปัญหาหรือปัจจัยที่ส่งผลกระทบจากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ค่ายสุรนารี

1.1 สภาวะแวดล้อมในระดับโลก มีพฤติกรรมการบริโภคของมนุษย์เปลี่ยนแปลงไป กระตุ้นให้เกิดการเปลี่ยนแปลงของเทคโนโลยี ส่งผลให้มีการสร้างนวัตกรรมและการพัฒนาเทคโนโลยีอย่างรวดเร็ว เพื่อตอบสนองความต้องการของผู้คนทั่วโลก ส่งผลให้สภาวะแวดล้อมในระดับภูมิภาคและระดับประเทศปรับตัวเปลี่ยนแปลงเข้าสู่สังคมดิจิทัล นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ตและคอมพิวเตอร์ เป็นช่องทางในการโจมตีของเหล่าอาชญากรไซเบอร์

1.2 กำลังพลของหน่วย ที่ปฏิบัติงานด้านไซเบอร์ไม่เพียงพอ เนื่องจากเป็นหน่วยงานที่มีขนาดเล็ก ขาดการบูรณาการ ขาดความเข้าใจเกี่ยวกับกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการพัฒนาขีดความสามารถศักยภาพด้านงานต่อต้านการก่อการร้ายทางไซเบอร์ ส่งผลทำให้ไม่สามารถอบรมให้ความรู้แก่กำลังพลและครอบครัว ในค่ายสุรนารี

1.3 ในการจัดสรรงบประมาณด้านไซเบอร์ ไม่เพียงพอต่อการพัฒนางานด้านไซเบอร์ ทั้งบุคลากร อุปกรณ์ต่อต้านทางไซเบอร์ และแผนงานป้องกัน ขาดความต่อเนื่อง ทำให้ขาดการวางแผนการนำเสนอโครงการ เพื่อขอรับการสนับสนุนงบประมาณ

1.4 การใช้ชีวิตในปัจจุบัน ของกำลังพลและครอบครัว ในค่ายสุรนารี ยังคงพึ่งพาอาศัยการใช้งานจากอินเทอร์เน็ต โซเชียลมิเดีย มากขึ้น แนวโน้มของภัยคุกคามทางไซเบอร์ ทั้งปริมาณของภัยคุกคาม ความซับซ้อน และความรุนแรง เพิ่มมากขึ้นอย่างรวดเร็ว เกินขีดความสามารถในการตรวจพบ สามารถควบคุมได้เพียงบางส่วน

1.5 กำลังพลและครอบครัว ในค่ายสุรนารี ยังขาดความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ การรักษาความปลอดภัย ความผิดพลาดในการตัดสินใจ และยังมีทัศนคติเกี่ยวกับไซเบอร์ในเชิงลบ ทำให้การปฏิบัติด้านไซเบอร์ของหน่วยถูกมองไปในแง่ร้าย เป็นที่หวาดระแวง และไม่ได้รับการสนับสนุน

2. สำหรับแนวทางในการแก้ไขปัญหาที่เหมาะสม จากภัยคุกคามด้านไซเบอร์ มีดังนี้

2.1 ส่งกำลังพลที่ปฏิบัติงานด้านไซเบอร์ของหน่วย เข้ารับการฝึกหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ ตามหลักสูตรที่กองทัพบกจัดการฝึก ซึ่งมีอยู่ด้วยกัน 7 หลักสูตร โดยกองทัพบกเป็นผู้สนับสนุนงบประมาณในการฝึกอบรมหลักสูตรแก่กำลังพลที่เข้ารับการฝึก ในฐานะหน่วยงานหลัก

2.2 จัดอบรมให้ความรู้เกี่ยวกับการป้องกันจาก ภัยคุกคามทางไซเบอร์ ให้แก่กำลังพล และครอบครัวของหน่วย ในค่ายสุรนารี ใช้เวลาในห้วงเย็น หลังเลิกงาน จัดกิจกรรมพบปะ ระหว่างผู้บังคับบัญชา และครอบครัวของกำลังพล ให้ความรู้ โดยมีกำลังพลที่ไปฝึกหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ เป็นวิทยากรให้ความรู้

2.3 จัดตั้งศูนย์ไซเบอร์ระดับหน่วยขึ้น ในรูปแบบของการกระจายข่าวสารภัยคุกคามทางไซเบอร์ ผ่านแอปพลิเคชันไลน์ เฟสบุ๊คฯลฯ มีเจ้าหน้าที่ ฝ่าย/แผนกการข่าวเป็นผู้รับผิดชอบ โดยมีกำลังพลที่ไปฝึกหลักสูตรฯ ด้านไซเบอร์ เป็นตัวหลัก

2.4 จัดทำแบบประเมินความเข้าใจ เกี่ยวกับภัยคุกคามทางไซเบอร์ แก่กำลังพลและครอบครัว รายงานให้ผู้บังคับบัญชาทราบทุกครั้ง ที่มีการประชุมประจำเดือน

2.5 กองทัพบกจัดสรรงบประมาณด้านไซเบอร์ ในการจัดซื้ออุปกรณ์ต่อต้านทางไซเบอร์ ให้แก่หน่วย โดยหน่วยเป็นผู้นำเสนอแผนงานป้องกันและโครงการขึ้นไปของบประมาณประจำปี จากกองทัพบก เพื่อให้เกิดความต่อเนื่องของการป้องกันภัยคุกคามทางไซเบอร์

2.6 รัฐออกกฎหมายเพื่อเสริมสร้างความปลอดภัยทางไซเบอร์[19] ที่มีประสิทธิภาพ และสามารถยืดหยุ่นปรับเปลี่ยนกฎหมายให้ทันสมัย ตามทันเทคโนโลยี สอดคล้องกับบรรทัดฐานสากล ส่งเสริมบทบาทของผู้ให้บริการด้านไอที ในการต่อสู้กับสื่อเฟสบุ๊คแอบแฝงหรือแพลตฟอร์มต่างๆ ที่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะจากผลการวิจัย

1.1 การสนับสนุนงบประมาณเพิ่มเติมเพื่อให้เพียงพอสำหรับการบรรจุบุคลากร และปรับโครงสร้างและอัตรากำลังพลให้ตรงกับสายงาน และเพียงพอต่อการปฏิบัติงาน

1.2 ควรร่วมมือกับหน่วยงานอื่น ๆ เพื่อขอรับการสนับสนุนงบประมาณ และการสนับสนุนผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มีงบประมาณในการดำเนินการสำหรับใช้จัดหาเครื่องมือ และอุปกรณ์ที่ทันสมัยเพื่อใช้ในการปฏิบัติงานและการพัฒนาทักษะ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรให้มีประสิทธิภาพมากยิ่งขึ้น

1.3 ควรเพิ่มหลักสูตรการเรียนการสอนทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับโรงเรียนทหาร เช่น โรงเรียนนายสิบ โรงเรียนนายร้อย เป็นต้น

1.4 ควรมีการเน้นให้เห็นถึงความสำคัญในการพัฒนาทักษะของตนเอง เพื่อให้บุคลากรเกิดการเรียนรู้เพื่อ พัฒนาตนเองมากขึ้น รวมถึงการสำรวจความต้องการพัฒนาทักษะของบุคลากรเพื่อนำมาใช้ในแผนการพัฒนา บุคลากรตามปีงบประมาณ ซึ่งจะส่งผลให้การพัฒนาทักษะบุคลากรมีประสิทธิภาพและเป็นประโยชน์แก่กองทัพ

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

2.1 ควรมีการวิจัยพัฒนาหลักสูตรเพื่อกำหนดโครงสร้างหลักสูตรและเนื้อหาให้มีความเหมาะสม สำหรับกลุ่มเป้าหมายกำลังพลกองทัพบก ในระดับต่างๆ ตั้งแต่นายทหารสัญญาบัตร นายทหารประทวน และพลทหารกองประจำการ

2.2. ควรมีการวิจัยประเมินผลเพื่อประเมินผลลัพธ์ที่เสนอในการวิจัยครั้งนี้ไปประยุกต์ใช้และปรับปรุงการดำเนินงาน ให้มีประสิทธิภาพยิ่งขึ้นต่อไป

2.3 ควรมีการศึกษาวิจัยการใช้ประโยชน์จากหน่วยกำลังสำรอง (รด.) ในด้านไซเบอร์ ซีคิวริตี้ (Cyber Security) ในห้วงที่กองทัพบกมีการเรียกตัวกำลังสำรองมาทำการฝึกศึกษาด้านทหาร เพราะกำลังสำรองบางนาย มีความสามารถด้านเทคโนโลยีหรือทำงานด้านไซเบอร์อยู่หน่วยงานของรัฐหรือเอกชนบางแห่ง ซึ่งจะเป็นประโยชน์อย่างมาก ในการพัฒนาศูนย์บัญชาการไซเบอร์กองทัพบกต่อไป

เอกสารอ้างอิง

1. ยุทธศาสตร์ชาติ 20 ปี (พ.ศ.2561-2580) ยุทธศาสตร์ที่ 1 : ยุทธศาสตร์ชาติด้านความมั่นคงการป้องกันและการแก้ปัญหาที่มีผลกระทบต่อความมั่นคง

2. แผนปฏิรูปประเทศ : ด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ, การป้องกันคุ้มครองและรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์

3. นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิตอลการพัฒนาเศรษฐกิจและสังคม (พ.ศ.2561 – 2580) ยุทธศาสตร์ที่ 6 : สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

4. นโยบายและแผนว่าด้วยการรักษาความมั่งคงปลอดภัยไซเบอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม Ministry of Digital Economy and Society

5. นโยบายการปฏิบัติงานของกองทัพบก ประจำปีงบประมาณ 2567

   พลเอก เจริญชัย หินเธาว์ ผู้บัญชาการทหารบก

6. การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม. วารสารสถาบันวิชการป้องกันประเทศ

7. ศูนย์ไซเบอร์กองทัพบก http://cyber.rta.mi.th//about.php ฤทธี อินทราวุธ, กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ

8. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ประเภทและตัวอย่างภัยคุกคาม ThaiCERT Annual Report, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ), 2017.

9. ราชกิจจานุเบกษา, พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 เล่ม 136 ตอนที่ 69 ก. หน้าที่ 20 , ราชกิจจานุเบกษา 27 พฤษภาคม 2562.

10. The Crowdstrike global Threat Repoet, Crowdstrike, 2021

11. John J. Brandon. Why ASEAN Needs to Invest More in Cybersecurity. 2018.

12. The Global Cybersecurity Capacity Centre แห่ง University of Oxford, National Cybersecurity Capacity Maturity Model (CMM), [อินเทอร์เน็ต]; [เข้าถึงเมื่อ 10 กุมภาพันธ์ 2567]. เข้าถึงได้จาก https://gcscc.ox.ac.uk/the-cmm

13. Peter Fisk. Magatrends2020-2030. (cited in 2019 December 8) Retrieved from Linkedin : https://www.linkedin.com

14. The Global Cyber Threat to Financial Systems-IMF F&D [Internet]. 2021 [cited in 2024 March 11]. Retrieved from: https://www.imf.org/externa/pubs/ft/fandd/2021/03/ global-cyber-threat-to-financial-systems-maurer.htm

15. European Systemic Risk Board 2020.“Systemic Cyber Risk” Internet]. 2021 [cited in 2024 March 11]. Retrieved from: https://www.esrb.europa.eu/Pub/pdf/reports/esrb.report200219_Systemiccyberrisk-101a09685e.en.pdf

16. ไทยรัฐทีวี. Kaspersky ประเมินภูมิภาคเอเชียแปซิฟิก มีความเสี่ยงถูกโจมตีด้วยฟิชชิ่ง. [อินเทอร์เน็ต] [เข้าถึงเมื่อ 30 มกราคม 2567] สืบค้นจาก https://www.thairath.co.th/news/tech/2759306

17. ลัฐกา เนตรทัศน์. LAW for ASEAN by the office of council of State of thailand [เผยแพร่เมื่อวันที่ 27 ธันวาคม 2561]. สืบค้นจาก https://lawforasean.Krisdika.go.th/File/files/cybersecurity_dec2.pdf

18. TCC-Technology.com : 3 แกนหลัก ยกระดับองค์กร เตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์. [อินเทอร์เน็ต] [เข้าถึงเมื่อ 29 กุมภาพันธ์ 2567]

19. งานวิจัยของ Tech For Good Institute (TFGI) เกี่ยวกับความพร้อมในการรับมือภัยคุกคามไซเบอร์ (Cyber resilience) [อินเทอร์เน็ต] [เข้าถึงเมื่อ 13 มีนาคม 2567]

20. สุดารัตน์ สุมงคล, พันเอกหญิง. แนวทางการแก้ไขปัญหาการขาดแคลนบุคลากรที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก [เอกสารวิจัยส่วนบุคคล]. กรุงเทพฯ: วิทยาลัยการทัพบก;2566.

21. นราวิชญ จิตรบรรจง, ร้อยตรี. นโยบายการพิจารณาคัดเลือกบุคคลพลเรือนเข้ารับราชการในกองทัพบกด้วยการใช้สื่อสังคมออนไลน์และรอยเท้าทางดิจิทัล [เอกสารวิจัยนักศึกษาหลักสูตร รัฐประศาสนศาสตรมหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยรามคำแหง; 2565

22. SCB ไทยพาณิชย์. ล่วงลึก 10 รูปแบบการโจมตีทางไซเบอร์ระดับตัวท็อป. [เข้าถึงเมื่อวันที่ 3 เมษายน 2567]. สืบค้นจาก https://www.scb.co.th/th/personal-banking/fraud-fighter/update-fraud/top-10-cyber-attack.html

23. สำนักงานส่งเสริมสุขภาพ. การแบ่งประเภทภัยคุกคามทางไซเบอร์. [เข้าถึงเมื่อวันที่ 3 เมษายน 2567]. สืบค้นจาก https://hp.anamai.moph.go.th/th/km-research-person/download/?did=204968&id=73905&reload=

24. CYBER ELITE. รวบรวมเหตุการณ์ Cyber Attack ที่โด่งดังในต่างประเทศ 5 การโจมตีการแฮ็กที่ฉาวโฉ่. [เข้าถึงเมื่อวันที่ 4 เมษายน 2567]. สืบค้นจาก https://www.cyberelite.co.th/blog/cyber-attack/

25. สุทน ยศสูงเนิน, พันโท. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี [สัมภาษณ์]. รองผู้บังคับการศูนย์ฝึกนักศึกษาวิชาทหาร มณฑลทหารบกที่ 21; 2 มีนาคม 2567.

26. เฉลิมฉัตร บุญหนุน, ร้อยเอก. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี [สัมภาษณ์]. ครูวิชาการสงครามพิเศษ ศูนย์ฝึกนักศึกษาวิชาทหาร มณฑลทหารบกที่ 21; 9 มีนาคม 2567.

27. ปัญญา ยุระศรี, จ่าสิบเอก. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี [สัมภาษณ์]. เจ้าหน้าที่ฝ่ายยุทธการและการข่าว กองพันทหารราบที่ 2 กรมทหารราบที่ 3; 16 มีนาคม 2567.

28. ทหารกองประจำการ จำนวน 5 นาย. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี [สัมภาษณ์]. ทหารกองประจำการในพื้นที่ค่ายสุรนารี; 1-5 มีนาคม 2567.

29. ครอบครัว จำนวน 3 นาย. ผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ ที่ส่งผลกระทบต่อการใช้ชีวิตของกำลังพลและครอบครัว ในค่ายสุรนารี [สัมภาษณ์]. ภริยาและบุตรของกำลังพล หน่วยในพื้นที่ค่ายสุรนารี; 1-5 มีนาคม 2567.

ประวัติย่อผู้วิจัย

ยศ ชื่อ พันเอก เรวัฒ ธรรมจิรเดช

วัน เดือน ปีเกิด 14 ตุลาคม 2519

ประวัติสำเร็จการศึกษา

พ.ศ. 2537	โรงเรียนอัสสัมชัญ นครราชสีมา
พ.ศ. 2539	โรงเรียนเตรียมทหาร รุ่นที่ 37
พ.ศ. 2544	โรงเรียนนายร้อยพระจุลจอมเกล้า รุ่นที่ 48
พ.ศ. 2554	โรงเรียนเสนาธิการทหารบก หลักสูตรหลักประจำ ชุดที่ 89

ประวัติการทำงาน

พ.ศ. 2545	ผู้บังคับหมวดปืนเล็ก กองร้อยอาวุธเบา กองพันทหารราบที่ 3 กรมทหารราบที่ 13
พ.ศ. 2548	ผู้บังคับหมวด กรมนักเรียนนายร้อย รักษาพระองค์
พ.ศ. 2549	ผู้บังคับกองร้อยทหารราบที่ 103
พ.ศ. 2550	นายทหารยุทธการและการฝึก
พ.ศ. 2551	ผู้บังคับกองร้อยลาดตระเวนระยะไกลที่ 3
พ.ศ. 2555	หัวหน้าฝ่ายกิจการพลเรือน กองพลทหารราบที่ 3
พ.ศ. 2556	หัวหน้าฝ่ายกิจการพลเรือน กองกำลังสุรศักดิ์มนตรี
พ.ศ. 2559	ผู้บังคับกองพันทหารราบที่ 2 กรมทหารราบที่ 13
พ.ศ. 2562	เสนาธิการกรมทหารราบที่ 13
พ.ศ. 2563	ผู้บังคับการ หน่วยเฉพาะกิจ กรมทหารพรานที่ 21
พ.ศ. 2564	ผู้บังคับการ หน่วยเฉพาะกิจ กรมทหารพรานที่ 20

ตำแหน่งปัจจุบัน

พ.ศ. 2565 - ปัจจุบัน	รองผู้บังคับการ กรมทหารราบที่ 13