แนวทางส่งเสริมการตระหนักรู้ให้กับกำลังพลกองทัพบก ในเรื่องการป้องกันอาชญากรรมทางไซเบอร์

เอกสารวิจัยส่วนบุคคล

โดย

พันเอก ภานุพันธ์ อินทรพรหม

ฝ่ายเสนาธิการประจำผู้บังคับบัญชา

สำนักปฏิบัติภารกิจรักษาความมั่นคงภายในกองทัพบก ภาค 1

วิทยาลัยการทัพบก

กันยายน 2568

เอกสารวิจัยเรื่อง แนวทางส่งเสริมการตระหนักรู้ให้กับกำลังพลกองทัพบก ในเรื่องการป้องกันอาชญากรรมทางไซเบอร์

โดย พันเอก ภานุพันธ์ อินทรพรหม

อาจารย์ที่ปรึกษา พันเอกหญิง มนทิรา ยิ้มสมบุญ

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2568 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ ดีมาก

พลตรี (เกียรติชัย โอภาโส) **ผู้บัญชาการวิทยาลัยการทัพบก**

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก (สุเทพ ยั่งยืน) **ประธานกรรมการ**

พันเอก (อนิวรรต เหมนิธิ) **ผู้ทรงคุณวุฒิที่ปรึกษา**

พันเอก (ปราโมท หม่อมศิลา) **กรรมการ**

พันเอกหญิง (มนทิรา ยิ้มสมบุญ) **กรรมการ**

พันเอกหญิง (นวลสมร จรวงษ์) **กรรมการและเลขานุการ**

บทคัดย่อ

ผู้วิจัย พันเอก ภานุพันธ์ อินทรพรหม

เรื่อง แนวทางส่งเสริมการตระหนักรู้ให้กับกำลังพลกองทัพบก ในเรื่องการป้องกันอาชญากรรมทางไซเบอร์

วันที่ 9 กันยายน 2568 **จำนวนคำ :** 12,712 **จำนวนหน้า :** 38

คำสำคัญ การตระหนักรู้ทางไซเบอร์, อาชญากรรมทางไซเบอร์

ชั้นความลับ ไม่มีชั้นความลับ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสถานการณ์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อกำลังพลกองทัพบก รวมถึง ปัจจัยที่ส่งผลต่อการตระหนักรู้ และ แนวทางในการส่งเสริมความรู้ด้านไซเบอร์ โดยอ้างอิงจาก ยุทธศาสตร์ชาติ 20 ปี, นโยบายความมั่นคงแห่งชาติ และแผนปฏิบัติราชการของกองทัพบก เป็นกรอบการศึกษา การวิจัยใช้ กรอบวิเคราะห์เชิงยุทธศาสตร์ (PMESII, SWOT และ TOWS Matrix) เพื่อประเมิน จุดแข็ง จุดอ่อน โอกาส และภัยคุกคาม ที่เกี่ยวข้องกับการรับมืออาชญากรรมทางไซเบอร์ภายในกองทัพ พร้อมทั้งใช้ ทฤษฎีการตระหนักรู้ในตนเอง, ทฤษฎีสามเหลี่ยมอาชญากรรม และทฤษฎีพฤติกรรมกิจวัตร ในการวิเคราะห์พฤติกรรมและแนวทางเสริมสร้างการตระหนักรู้ในหมู่กำลังพล

ผลการวิจัยพบว่า การโจมตีทางไซเบอร์ เช่น ฟิชชิ่ง, มัลแวร์ และการโจมตีขั้นสูง มีแนวโน้มเพิ่มขึ้น เนื่องจาก การขาดการฝึกอบรมที่เพียงพอและพฤติกรรมเสี่ยงของกำลังพล ทั้งนี้ พบว่า การอบรมเชิงปฏิบัติการ และหลักสูตร e-Learning สามารถลดความเสี่ยงจากภัยไซเบอร์ได้อย่างมีนัยสำคัญ

ดังนั้น งานวิจัยนี้เสนอแนวทางเชิงรุก ในการส่งเสริมความตระหนักรู้ด้านไซเบอร์ผ่านการฝึกอบรมที่เหมาะสม, การลงทุนในเทคโนโลยีป้องกันภัยไซเบอร์ และการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงาน เพื่อเพิ่มความพร้อมของกองทัพบกในการรับมือกับ ภัยคุกคามไซเบอร์ในยุคดิจิทัล

ABSTRACT

AUTHOR: Colonel Panuphan Intaraprom

TITLE: Guidelines for Enhancing Cybercrime Prevention Awareness Among Royal Thai Army Personnel

DATE: 9 September, 2025 **WORD COUNT :** 12,712 **PAGES :** 38

KEY TERMS: Cyber Awareness, Cybercrime

CLASSIFICATION: Unclassified

This research examines the state of cybersecurity awareness and the factors influencing cybercrime prevention among Royal Thai Army personnel, in alignment with the 20-Year National Strategy, national security policies, and the Army's strategic action plan. The study employs strategic analytical frameworks (PMESII, SWOT, and TOWS Matrix) to evaluate strengths, weaknesses, opportunities, and threats in cybersecurity within the military structure. Additionally, it incorporates Self-Awareness Theory, Crime Triangle Theory, and Routine Activity Theory to analyze behavioral patterns and mechanisms to enhance cybersecurity awareness among personnel.

Findings reveal that cyber threats-including phishing, malware, and advanced persistent threats (APT)-are increasing due to insufficient training and risky behaviors. The study indicates that hands-on training and e-learning programs significantly reduce cybersecurity risks.

Therefore, this research proposes a proactive strategy to improve cybersecurity awareness through structured training programs, investment in cybersecurity technologies, and inter-agency collaboration, strengthening the Army's preparedness against cyber threats in the digital era.

กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางส่งเสริมการตระหนักรู้ให้กับกำลังพลกองทัพบกในเรื่องการป้องกันอาชญากรรมทางไซเบอร์” ฉบับนี้ สำเร็จลุล่วงได้ด้วยความอนุเคราะห์จาก พันเอกหญิง มนทิรา ยิ้มสมบุญ อาจารย์หัวหน้ากอง ส่วนวิชาความมั่นคงแห่งชาติและยุทธศาสตร์ วิทยาลัยการทัพบก อาจารย์ที่ปรึกษา ที่กรุณาให้คำปรึกษา รวมทั้งปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง และ พันเอก อนิวรรต เหมนิธิ ผู้อำนวยการกองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพบกผู้ทรงคุณวุฒิที่ปรึกษา และผู้บังคับบัญชาที่กรุณามอบโอกาสให้ได้เข้ารับการศึกษาในวิทยาลัยการทัพบกและได้ให้แนวคิดในการศึกษา ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณ พลตรี เกียรติชัย โอภาโส ผู้บัญชาการวิทยาลัยการทัพบก ที่กรุณาอนุมัติให้ผู้วิจัยทำวิจัยเรื่องนี้ ผู้ที่เกี่ยวข้อง พันเอก สุเทพ ยั่งยืน ประธานกรรมการควบคุมเอกสารวิจัยส่วนบุคคล พันเอกหญิง นวลสมร จรวงษ์ กรรมการที่กรุณาให้ข้อเสนอแนะอันเป็นประโยชน์อย่างยิ่งต่องานวิจัยฉบับนี้ สุดท้ายนี้ขอขอบคุณเพื่อนนักศึกษาหลักสูตรหลักประจำวิทยาลัยการทัพบก ชุดที่ 70 ที่ให้ความช่วยเหลือและเป็นกำลังใจให้กับผู้วิจัยในทุกขั้นตอนของการดำเนินการวิจัย

ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิจัยฉบับนี้ จะเป็นแนวทางและเป็นประโยชน์ต่อการส่งเสริมการสร้างความตะหนักในเรื่องรู้อาชญากรรมทางไซเบอร์ให้กับกำลังพลของกองทัพบกต่อไป

สารบัญ

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 - 2580)[1] ด้านความมั่นคงมีเป้าหมายการพัฒนาที่สำคัญ คือ ประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัยและมีความสงบเรียบร้อยในทุกระดับตั้งแต่ระดับชาติ สังคม ชุมชน มุ่งเน้นการพัฒนาคน เครื่องมือเทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ ให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบ และสามารถแก้ไขปัญหาและภัยคุกคามในอนาคตได้ทันท่วงทีก่อนที่จะลุกลามต่อไป รวมทั้งป้องกันไม่ให้ส่งผลกระทบต่อการบริหาร การสร้างการเข้าถึงและ ใช้ประโยชน์จากข้อมูลหลากหลายจากแหล่ง ข้อมูลที่เชื่อถือได้ มีการป้องกันที่ครอบคลุมความปลอดภัยไซเบอร์

จากนโยบายและแผนความมั่นคงแห่งชาติ (พ.ศ. 2566 - 2580)[2] เป็นหนึ่งในแผนระดับที่ 2 รองรับยุทธศาสตร์ชาติด้านความมั่นคง มุ่งเน้นให้ประเทศไทยสามารถเพิ่มการป้องกันการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ โดยการยกระดับมาตรฐานรักษาความมั่นคงปลอดภัยทางไซเบอร์ ลดการก่ออาชญากรรมทางไซเบอร์ และพัฒนาการสอบสวนทางไซเบอร์

แผนปฏิบัติราชการของกระทรวงกลาโหม[3] และนโยบายของกองทัพบก[4] ได้เน้นการพัฒนาศักยภาพของกำลังพลของกองทัพบกด้านความรู้ และเทคโนโลยีด้านไซเบอร์ นำกองทัพสู่ความทันสมัย สมุดปกขาวกองทัพบก พ.ศ. 2567[5] ให้สามารถปฏิบัติการด้านไซเบอร์เชิงรับ และเชิงป้องปราม พัฒนา แอดมิน เครือข่ายของหน่วยให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์เพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ภัยคุกคามในโลกไซเบอร์ได้มีวิวัฒนาการหลากหลายรูปแบบและสร้างผลกระทบต่อความมั่นคงของชาติ โดยตั้งแต่ 1 มีนาคม พ.ศ. 2565 ถึง 30 มิถุนายน พ.ศ. 2567 สำนักงานตำรวจแห่งชาติ มีสถิติการก่ออาชญากรรมทางไซเบอร์ในประเทศไทย จำนวน 575,507 คดี[6] อาชญากรรมทางไซเบอร์เป็นการก่ออาชญากรรมรูปแบบใหม่ในยุคปัจจุบัน ซึ่งรัฐจะต้องปรับตัวให้ทันต่อความเปลี่ยนแปลงของการก่ออาชญากกรรมทั้งในแง่ของรูปแบบในการกระทำความผิดและพื้นที่[7] แนวโน้มการขยายตัวของอาชญากรรมไซเบอร์ที่กระทำโดยองค์กรอาชญากรรม ซึ่งมีความเชื่อมโยงกับการใช้อินเทอร์เน็ตของประชาชนทั่วโลกที่มากขึ้นในช่วงการระบาดของโรคโควิด-19 มุ่งเน้นแสวงประโยชน์จากสถานการณ์

โรคโควิด-19 ได้สรุปตัวอย่างอาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมมีแนวโน้มเป็นผู้กระทำการสูงขึ้น 4 ประเภท ได้แก่ การฉ้อโกงทางอินเทอร์เน็ตผ่านวิธีการฟิชชิ่งและสแกมมิ่ง การใช้ไวรัสเรียกค่าไถ่ การแทรกซึมตลาดการค้าทางออนไลน์ และการละเมิดสิทธิมนุษยชนโดยอาศัยช่องทางอินเทอร์เน็ต เช่น การค้ามนุษย์ และการแสวงประโยชน์ทางเพศ [8] ซึ่งหน่วยงานของกองทัพบกบางหน่วยงานถูกปิดกั้นการแชร์หรือเผยแพร่ข้อมูลในการสื่อสารผ่านสื่อสังคมออนไลน์ของหน่วยที่มียอดผู้เข้าถึงแล้วกว่า 100,000 ราย เนื่องจากแอดมินร่วมภายนอกที่ไม่เข้าใจเงื่อนไข หรือกฎเกณฑ์ต่าง ๆ เท่าที่ควร

ปัญหาภัยคุกคามจากอาชญากรรมทางไซเบอร์มีแนวโน้มสูงขึ้นในอนาคต อันจะสร้างปัญหาให้กับกองทัพบก ทั้งทางด้านกำลังพลและงานการป้องกันประเทศ หากกำลังพลของกองทัพบกไม่มีความตระหนักรู้เรื่องอาชญากรรมทางไซเบอร์ รวมถึงวิธีการเข้าถึงแหล่งในการให้ความรู้ด้านภัยไซเบอร์ด้วยเครื่องมือของกองทัพบกที่มีอยู่ เช่น แอปพลิเคชั่น S.M.A.R.T.SOLDIERS Royal Thai Army และเว็บไซต์ของศูนย์ไซเบอร์กองทัพบกในปัจจุบัน

ดังนั้นผู้วิจัยจึงสนใจที่จะศึกษาแนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก เพื่อเป็นการสร้างความตระหนักรู้ในการป้องกันตนเองและหน่วยงาน รวมถึงการช่วยเหลือในกรณีตกเป็นเหยื่อจากภัยอาชญากรรมทางไซเบอร์ อีกทั้งเสริมสร้างกองทัพบกให้มีความพร้อมที่จะปฏิบัติหน้าที่ในการป้องกันอธิปไตยของชาติต่อไป

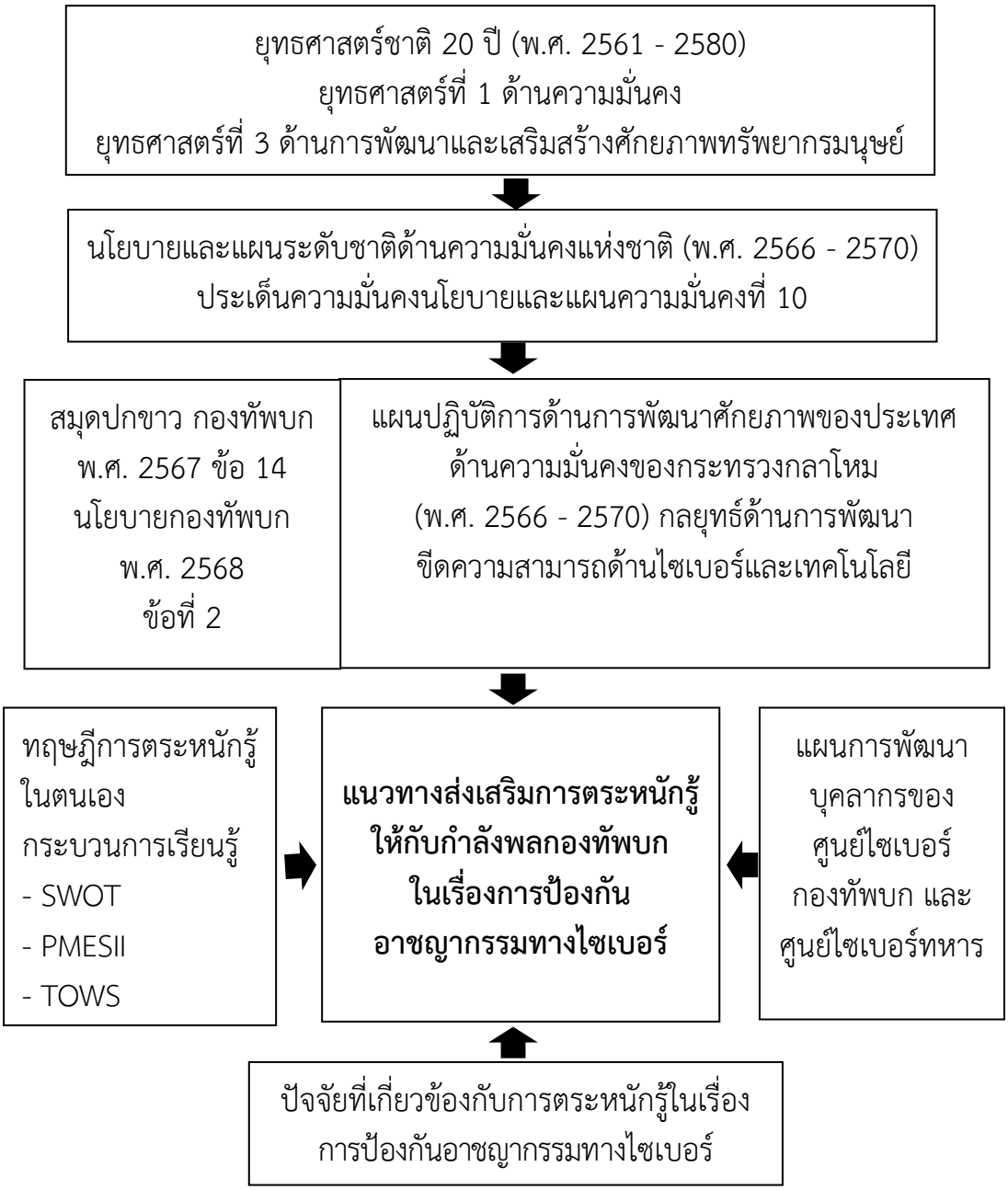
วัตถุประสงค์การวิจัย

1. เพื่อศึกษาสถานการณ์ความรู้เรื่องอาชญากรรมทางไซเบอร์ที่เป็นภัยคุกคามกำลังพลกองทัพบกในปัจจุบัน

2. เพื่อศึกษาปัจจัยที่ส่งผลต่อการตระหนักรู้ในเรื่องอาชญากรรมทางไซเบอร์ของกำลังพลกองทัพบก

3. เพื่อศึกษาแนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีการศึกษา

1. รูปแบบการวิจัย ใช้รูปแบบการวิจัยเชิงยุทธศาสตร์ตามที่วิทยาลัยการทัพบกกำหนดโดยประยุกต์ใช้วิธีการวิจัยเชิงคุณภาพและใช้วิธีการวิจัยเชิงเอกสารเป็นแนวทางในการวิจัย

2. ขอบเขตการศึกษา ศึกษานโยบายแผนการปฏิบัติงานของศูนย์ไซเบอร์กองทัพบกเพื่อให้เข้าใจภาพรวมแนวทางการเตรียมความพร้อมในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของกรมกำลังพลทหารบก และศึกษาสภาวะแวดล้อมที่มีผลต่อการพัฒนาศักยภาพบุคลากร

3. การเก็บรวบรวมข้อมูล เอกสารทางวิชาการด้านอาชญากรรมไซเบอร์ บทความต่าง ๆ ด้านความมั่นคงทางไซเบอร์ เอกสารแนวทางการพัฒนาบุคลากรจากองค์กรทางการศึกษาต่าง ๆ นำผลการวิเคราะห์ที่ได้มาทำการส่งเสริมการตระหนักรู้ถึงอาชญากรรมทางไซเบอร์และการสัมภาษณ์ผู้เกี่ยวข้อง

4. การวิเคราะห์ข้อมูล ทำการวิเคราะห์ข้อมูลจากการรวบรวมความรู้ที่จำเป็นต่องานความมั่นคงด้านไซเบอร์ โดยใช้การวิเคราะห์แบบ PMESII, SWOT, TOWS Matrix และทฤษฎีการตระหนักรู้ในตนเอง แผนการพัฒนาบุคลากรของศูนย์ไซเบอร์กองทัพบกและศูนย์ไซเบอร์ทหาร

5. ขั้นตอนการดำเนินงาน

ห้วงเวลา / กิจกรรม	พ.ย. 67	ธ.ค. 67	ม.ค. 68	ก.พ 68	มี.ค. 68	เม.ย. 68	พ.ค. 68
เลือกเรื่องและกำหนดหัวข้อการวิจัย	←→						
สอบการนำเสนอโครงร่างเอกสารวิจัย		←→					
ศึกษาค้นคว้ารายละเอียดด้านต่าง ๆ		←	→				
การวิเคราะห์, สังเคราะห์ข้อมูล				←→			
การสรุปผลการวิจัย					←→		
การนำเสนอผลการวิจัย						←→	
จัดทำรูปเล่ม							←→

ประโยชน์ที่ได้รับ

1. ทราบถึงสถานการณ์ความรู้เรื่องอาชญากรรมทางไซเบอร์กำลังพลกองทัพบก

2. รับทราบถึงปัจจัยปัญหาการตระหนักรู้ในเรื่องการป้องกันอาชญากรรมทางไซเบอร์ของกำลังพลกองทัพบก

3. แนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก

บทที่ 2
บทแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

แนวความคิดเกี่ยวกับอาชญากรรมทางไซเบอร์

ยุทธศาสตร์ชาติ 20 ปี (ปี 2561-2580) ได้กำหนดให้ “การรักษาความมั่นคงของชาติ” เป็นหนึ่งในเป้าหมายสำคัญ โดยมีการกำหนดให้เสริมสร้างความพร้อมในการป้องกันภัยคุกคามทั้งในรูปแบบทางทหารและในรูปแบบใหม่ๆ เช่น ภัยคุกคามทางไซเบอร์ซึ่งสะท้อนถึงความสำคัญในการเตรียมความพร้อมให้กับกำลังพลกองทัพบกในด้านการตระหนักรู้ภัยคุกคามดังกล่าว[2]

แผนปฏิบัติราชการกระทรวงกลาโหม กำหนดให้มีการพัฒนาศักยภาพในด้านความมั่นคงทางไซเบอร์ โดยให้ความสำคัญกับการเสริมสร้างความรู้ความเข้าใจในวิธีการรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงการเตรียมพร้อมในด้านการป้องกันและการรับมือในกรณีที่เกิดเหตุการณ์ไซเบอร์ขึ้น โดยมีการกำหนดแผนการฝึกอบรมและการพัฒนาหลักสูตรเฉพาะด้านไซเบอร์ในทุกระดับ[3]

สมุดปกขาวของกองทัพบก ได้ระบุถึงความสำคัญของการเสริมสร้างขีดความสามารถด้านการป้องกันภัยคุกคามไซเบอร์ ซึ่งเป็นส่วนสำคัญในการพัฒนาระบบความมั่นคงของกองทัพ รวมถึงการใช้เทคโนโลยีที่ทันสมัยเพื่อพัฒนาการฝึกอบรมและการตรวจสอบความพร้อมของกำลังพลในการรับมือกับภัยคุกคามไซเบอร์[5]

นโยบายกองทัพบก ปี 2568 ได้กำหนดการพัฒนาความพร้อมของกำลังพลในการรับมือกับภัยคุกคามไซเบอร์ โดยมีการปรับปรุงหลักสูตรการฝึกอบรมให้ทันสมัยและสอดคล้องกับสถานการณ์ในปัจจุบันที่การโจมตีทางไซเบอร์มีการพัฒนาอย่างรวดเร็วและซับซ้อนขึ้น รวมถึงการเสริมสร้างการตระหนักรู้ให้กับกำลังพลผ่านการฝึกอบรมและการเรียนรู้ที่ต่อเนื่อง เพื่อให้สามารถป้องกันและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ[4]

กฎหมายและมาตรการทางไซเบอร์ในประเทศไทย ประกอบด้วยกฎหมายหลัก 3 ฉบับ ได้แก่ พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไข พ.ศ. 2560 ควบคุมอาชญากรรมทางไซเบอร์, พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ป้องกันและรับมือภัยคุกคามทางไซเบอร์ โดยมี สำนักคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานหลัก และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำกับดูแล

การเก็บและใช้ข้อมูลส่วนบุคคล ซึ่งการป้องกันและปราบปรามอาชญากรรมไซเบอร์ในไทยมีการปรับปรุงกฎหมายอย่างต่อเนื่อง ปัจจุบันมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ซึ่งแต่ละวันมีผู้ถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก สมควรมีมาตรการเพื่อป้องกันและปราบปรามอาชญากรรมประเภทนี้ให้หมดไปโดยเร็ว อันเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ[12]

ทฤษฎีการตระหนักรู้ในตนเอง (Self-Awareness Theory)

เป็นทฤษฎี ในจิตวิทยาที่เน้นการศึกษาว่าบุคคลรับรู้และมีความเข้าใจในตนเองอย่างไร ในแง่ของความคิด, อารมณ์, พฤติกรรม, และการตอบสนองต่อสิ่งแวดล้อมรอบตัว โดยทั่วไปทฤษฎีนี้มักจะเกี่ยวข้องกับความสามารถในการตรวจสอบและประเมินตนเอง รวมถึงการรู้สึกถึงความสอดคล้องหรือความขัดแย้งระหว่างสิ่งที่บุคคลคิด รู้สึก หรือกระทำกับค่านิยมและความเชื่อของตนเอง มีองค์ประกอบสำคัญ คือการรับรู้และประเมินตัวเอง การเปรียบเทียบกับมาตรฐานภายนอกและภายใน การตอบสนองต่อการตระหนักรู้ผ่านการปรับเปลี่ยนพฤติกรรม การควบคุมอารมณ์ การสะท้อนความคิด และการมองเห็นตัวเองจากมุมมองของผู้อื่น ทั้งหมดนี้ช่วยให้บุคคลพัฒนาความเข้าใจในตัวเองและสามารถตัดสินใจหรือปรับพฤติกรรมในทางที่ดียิ่งขึ้น[13]

อาชญากรรมทางไซเบอร์ (Cybercrime) คือ การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย และ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ อาทิ การโจมตีระบบคอมพิวเตอร์ การทำลาย-แก้ไข-ขโมยข้อมูล การหลอกลวงให้เสียทรัพย์ เป็นต้น การรู้เท่าทันอาชญากรรมทางไซเบอร์ที่เข้ามาเกี่ยวข้องกับชีวิตการทำงานและชีวิตประจำวัน

ผลกระทบของอาชญากรรมทางไซเบอร์ สามารถทำให้เกิดความเสียหายและความไม่สงบในสังคมได้ จากสถิติการก่ออาชญากรรมทางไซเบอร์ (Cybercrime) รูปแบบต่าง ๆ ที่ติดอันดับสูงสุด 3 อันดับแรก ในปี 2565 ได้แก่

1. การหลอกลวงโดยการแอบอ้าง เป็นการหลอกลวงโดยใช้วิธีการแอบอ้างตนเองให้ดูเหมือนเป็นผู้ที่น่าเชื่อถือ เพื่อเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับ ตัวอย่างเช่นการใช้ E-mail, SMS และเว็บไซต์ปลอม เพื่อหลอกให้กรอกข้อมูลส่วนตัวหรือคลิกลิงก์ที่อันตราย

2. การละเมิดข้อมูลส่วนบุคคล เป็นการกระทำที่ทำให้ข้อมูลส่วนบุคคลถูกเข้าถึงโดยไม่ได้รับอนุญาต ถูกเปลี่ยนแปลงแก้ไข ถูกทำให้เสียหาย หรือถูกนำไปเผยแพร่ต่อผู้อื่น ซึ่งอาจเกิดจากภัยคุกคามไซเบอร์ที่เกิดจากการบุกรุก และ/หรือการโจมตีระบบผ่านทางช่องโหว่

3. การลอกลวงซื้อขายสินค้าและบริการ เป็นการใช้เทคนิคการหลอกลวงให้ผู้ซื้อทำธุรกรรมผ่านทางออนไลน์โดยไม่ได้รับสิทธิในการรับสินค้าหรือบริการตามที่ตกลง ตัวอย่างเช่น หลอกให้โอนเงินและไม่ได้รับสินค้า หรือการเลือกซื้อสินค้าแบรนด์เนมแท้แต่ได้ของปลอม[14]

การป้องกันอาชญากรรมทางไซเบอร์ (Cybercrime Prevention) เป็นกระบวนการที่มุ่งเน้นการลดความเสี่ยงและการป้องกันไม่ให้เกิดเหตุการณ์ทางไซเบอร์ที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์ หรือเครือข่ายออนไลน์ต่างๆ โดยการป้องกันอาชญากรรมทางไซเบอร์สามารถทำได้หลายวิธี สามารถแบ่งเป็น 7 ขั้นตอน ได้แก่ การใช้เทคโนโลยีป้องกัน การอบรมและสร้างความตระหนักรู้ การจัดการสิทธิ์การเข้าถึงข้อมูล การปรับปรุงระบบและการอัปเดตซอฟต์แวร์ การใช้มาตรการความปลอดภัยระดับสูง การตอบสนองต่อเหตุการณ์ (Incident Response) และการปฏิบัติตามกฎหมายและข้อบังคับ ซึ่งการป้องกันอาชญากรรมทางไซเบอร์ไม่สามารถทำได้เพียงแค่การใช้เทคโนโลยีหรือเครื่องมือป้องกัน แต่ต้องรวมถึงการให้ความรู้ การฝึกอบรม และการปรับปรุงกระบวนการต่าง ๆ ให้เป็นไปตามมาตรฐานความปลอดภัยที่ดีที่สุด[15]

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) การก่ออาชญากรรมต่อความมั่นคงปลอดภัยทางไซเบอร์ เป็นการทำลายข้อมูล แก้ไขข้อมูลทำลายระบบถอดรหัส ไปจนถึงการโจมตีระบบการสื่อสารของโครงสร้างพื้นฐานบริการสาธารณะ (Critical Infrastructure) เพื่อการก่อวินาศกรรม (Destruction) สหภาพโทรคมนาคมระหว่างประเทศ (ITU Development) โปรแกรมทำลายระบบคอมพิวเตอร์ให้เสียหายที่แอบแฝงมาเป็นไฟล์(Computer Program File) ที่ได้รับมาจากอีเมล์หรือจากเว็บไซต์ที่เรียกว่า Malware (มัลแวร์) ย่อมาจากคำว่า Malicious Software ซึ่งเป็นไฟล์ที่เป็นอันตรายต่อคอมพิวเตอร์ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล Malware แบ่งออกได้หลากหลายประเภท อาทิ Virus Worm Trojan horse Spyware Logic Bomb Botnet Malware Brute Force Attack Spoofing Sniffer[15]

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. ทฤษฎีการตระหนักรู้ในตนเอง (Self-Actualization Theory) ของ Maslow อธิบายว่าการพัฒนาแรงจูงใจในระดับสูงสามารถส่งเสริมพฤติกรรมที่ปลอดภัยในการใช้เทคโนโลยี[11] งานวิจัยของ Compton พบว่าคนที่มีระดับแรงจูงใจสูง มีแนวโน้มที่จะปฏิบัติตามมาตรการรักษาความปลอดภัยทางไซเบอร์มากกว่ากลุ่มที่ขาดแรงจูงใจถึง 35%[16] นอกจากนี้ งานวิจัยของ Smith et al. พบว่าการเสริมสร้างแรงจูงใจผ่านโปรแกรมฝึกอบรมสามารถเพิ่มความตระหนักรู้ทางไซเบอร์ในองค์กรได้ถึง 40%[17]

2. ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) อธิบายว่าอาชญากรรมเกิดขึ้นเมื่อมี “เหยื่อ” “อาชญากร” และ “โอกาส” ที่เอื้ออำนวย สถิติจากสำนักงานตำรวจแห่งชาติ (2567) ระบุว่า 78% ของการโจมตีทางไซเบอร์ในองค์กรเกิดขึ้นจากช่องโหว่ของบุคลากรที่ไม่ได้รับการฝึกอบรมเพียงพอ งานวิจัยของ Williams และ Brown แสดงให้เห็นว่าองค์กรที่มีการใช้มาตรการลดช่องโหว่ด้านพฤติกรรมของบุคลากรสามารถลดการโจมตีไซเบอร์ได้ถึง 60%[18]

3. ทฤษฎีการกระทำที่เป็นกิจวัตร (Routine Activity Theory) ชี้ว่าอาชญากรรมเกิดขึ้นจากพฤติกรรมที่เป็นกิจวัตรของเหยื่อที่เปิดโอกาสให้อาชญากรลงมือ งานวิจัยของ Felson และ Clarke ชี้ว่า 60% ของเหยื่ออาชญากรรมไซเบอร์เป็นผู้ที่ใช้รหัสผ่านเดิมซ้ำในหลายแพลตฟอร์ม[19] ข้อมูลจาก Cybersecurity Report 2023 ระบุว่าผู้ที่เปลี่ยนรหัสผ่านเป็นประจำมีโอกาสถูกโจมตีทางไซเบอร์น้อยลงถึง 45%[20]

4. ทฤษฎีการเลือกอย่างเป็นเหตุเป็นผล (Rational Choice Theory) อธิบายว่าอาชญากรจะก่ออาชญากรรมเมื่อเห็นว่าความเสี่ยงต่ำและผลประโยชน์สูง รายงานของ Clarke และ Cornish ระบุว่า 85% ของอาชญากรไซเบอร์เลือกเป้าหมายที่ไม่มีมาตรการรักษาความปลอดภัยที่เข้มงวด[21] งานวิจัยของ Garcia R, et al. พบว่าการใช้ระบบแจ้งเตือนและตรวจจับพฤติกรรมผิดปกติสามารถลดความเสี่ยงขององค์กรจากการโจมตีไซเบอร์ได้ถึง 50%[22]

5. ทฤษฎีเหตุผลในการเลือกประกอบอาชญากรรม (Rational Choice Theory) ของ Marcus Felson และ Ronald V. Clarke อธิบายว่าการกระทำความผิดเป็นผลจากการเปลี่ยนแปลงทางสังคมและเทคโนโลยีที่รวดเร็ว ซึ่งทำให้เกิดโอกาสในการก่ออาชญากรรมมากขึ้น โดยเฉพาะอย่างยิ่งในกลุ่มที่มีความรู้ความสามารถสูง เช่น ผู้เชี่ยวชาญด้านคอมพิวเตอร์ที่ใช้ทักษะของตนเองในการสร้างโปรแกรมมัลแวร์เพื่อเจาะระบบขององค์กรที่มีช่องโหว่ด้านความปลอดภัย[23] รายงานของ ชรินทร์ทิพย์ ปั้นสุวรรณ พบว่า 70%

ของการโจมตีทางไซเบอร์ที่ประสบความสำเร็จ เกิดขึ้นจากองค์กรที่ไม่มีระบบป้องกันที่แข็งแกร่งเพียงพอ[24]

6. ทฤษฎีการป้องกันและกระตุ้นให้เกิดการกระทำ (Protection Motivation Theory (PMT)) ทฤษฎี PMT ชี้ว่าการรับรู้ถึงความรุนแรงของภัยคุกคาม และการประเมินความเสี่ยงส่วนบุคคล พร้อมกับความมั่นใจในความสามารถในการรับมือ เป็นปัจจัยสำคัญที่ส่งผลต่อพฤติกรรมการป้องกันภัยไซเบอร์[25] งานวิจัยในสาขานี้พบว่าการออกแบบโปรแกรมฝึกอบรมที่ตั้งอยู่บนพื้นฐานของ PMT สามารถเพิ่มการตระหนักรู้และแรงจูงใจให้กับบุคลากร ป้องกันและลดความเสี่ยงจากพฤติกรรมที่ไม่ปลอดภัย ซึ่งสอดคล้องกับผลการทดลองจำลองการโจมตีฟิชชิ่งที่กล่าวถึงข้างต้น โดยมีการเน้นถึงการสื่อสารถึงผลเสียที่อาจเกิดขึ้นและการนำเสนอแนวทางปฏิบัติที่เป็นรูปธรรมในการเสริมสร้างความมั่นใจในการใช้งานเทคโนโลยีอย่างปลอดภัย และยังชี้ให้เห็นว่าการรับรู้ถึงผลกระทบและแรงจูงใจในการปฏิบัติตามมาตรการความปลอดภัยมีผลในการลดโอกาสที่บุคลากรจะตกเป็นเหยื่อของการโจมตีไซเบอร์ โดยเฉพาะในกรณีของการปลอมตัวที่ดำเนินการโดยแก๊งคอลเซนเตอร์ ซึ่งส่งผลให้ความมั่นคงของข้อมูลในหน่วยงานถูกท้าทายอย่างรุนแรง[26]

ปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์[27]

1. การตั้งรหัสผ่าน งานวิจัยของ Alqahtani พบว่าผู้ที่ใช้รหัสผ่านที่ซับซ้อนมีโอกาสถูกแฮ็กบัญชีน้อยกว่าผู้ใช้รหัสผ่านทั่วไปถึง 50%

2. ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การศึกษาโดย Holdsworth & Apeh ระบุว่าองค์กรที่มีการอบรมด้านความมั่นคงไซเบอร์อย่างต่อเนื่อง สามารถลดความเสี่ยงจากการโจมตีทางไซเบอร์ได้ถึง 65%

3. ความปลอดภัยของอุปกรณ์และการเชื่อมต่อ การวิจัยของ Ani et al. พบว่า องค์กรที่มีระบบสำรองข้อมูลบนคลาวด์สามารถลดระยะเวลาการกู้คืนระบบจากการโจมตีทางไซเบอร์ได้ถึง 40%

4. การใช้และดูแลแอปพลิเคชัน งานวิจัยของ Alzubaidi ระบุว่าผู้ใช้ที่อัปเดตระบบปฏิบัติการและซอฟต์แวร์เป็นประจำ สามารถป้องกันการโจมตีจากมัลแวร์ได้มากถึง 80%

5. พฤติกรรมของผู้ใช้งาน งานศึกษาของ Zwilling et al. แสดงให้เห็นว่าผู้ที่มีพฤติกรรมระมัดระวัง เช่น ตรวจสอบ URL ก่อนคลิกลิงก์ มีโอกาสตกเป็นเหยื่อของฟิชชิ่งลดลง 60%

6. การสื่อสารภายในองค์กร นอกจากมาตรการด้านเทคนิคแล้ว การสื่อสารที่ชัดเจนและเป็นระบบภายในองค์กรเพื่อให้ข้อมูลและแนวทางเกี่ยวกับความปลอดภัยในโลกไซเบอร์ เช่น การประชุมเชิงป้องกันภัยไซเบอร์ (Cybersecurity Briefings) และการใช้สื่อสังคมภายในเพื่อแจ้งเหตุการณ์ล่าสุด ยังสามารถช่วยเสริมสร้างการตระหนักรู้และกระตุ้นให้เกิดพฤติกรรมที่ปลอดภัยมากขึ้น[28]

การผสานทฤษฎีต่าง ๆ ทั้ง Self-Actualization, Crime Triangle, Routine Activity, Rational Choice และ Protection Motivation Theory ช่วยให้เข้าใจได้ว่าการตระหนักรู้และพฤติกรรมในการรักษาความปลอดภัยทางไซเบอร์ไม่ได้เป็นเพียงการให้ความรู้ในด้านเทคนิคเท่านั้น แต่ยังต้องคำนึงถึงปัจจัยด้านจิตวิทยา สังคม และวัฒนธรรมที่ส่งผลต่อพฤติกรรมในชีวิตประจำวัน

งานวิจัยที่เกี่ยวข้อง

1. การขาดความตระหนักรู้และเสริมสร้างวัฒนธรรมของบุคลากร งานวิจัยของสุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี ชี้ให้เห็นว่ามีความท้าทายเป็นอย่างมากในการเสริมสร้างความตระหนักรู้ของบุคลากรเกี่ยวกับภัยไซเบอร์[29] ซึ่งเป็นปัจจัยสำคัญที่เพิ่มช่องโหว่ให้กับระบบ การขาดความรู้และทักษะด้านไซเบอร์ส่งผลให้องค์กรไม่สามารถรับมือเหตุการณ์ฉุกเฉินได้อย่างรวดเร็วและมีประสิทธิภาพ

2. การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร จากการศึกษาของ สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี พบว่าการใช้การจำลองการโจมตีฟิชชิ่ง (Phishing Attack Simulation) เป็นวิธีที่มีประสิทธิภาพในการเสริมสร้างการตระหนักรู้เกี่ยวกับภัยไซเบอร์[29] โดยการทดลองกับบุคลากร 482 คน พบว่าก่อนการอบรมมีถึง 22.41% ที่เปิดอีเมลฟิชชิ่งและคลิกลิงก์ หลังจากได้รับการถ่ายทอดความรู้และทำการทดลองซ้ำ จำนวนผู้ที่คลิกลิงก์ลดลงเหลือเพียง 7.88% หรือปรับลดลงถึง 64.81% แสดงให้เห็นว่าการอบรมและการทดลองซ้ำช่วยให้บุคลากรมีความระมัดระวังมากขึ้นงานวิจัยนี้ศึกษาการใช้การจำลองการโจมตีด้วยฟิชชิ่งเพื่อเพิ่มความตระหนักรู้ในองค์กร พบว่าการฝึกอบรมช่วยลดอัตราการคลิกลิงก์ฟิชชิ่งได้อย่างมีนัยสำคัญ

3. รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์ งานวิจัยของกิตติศักดิ์ คุรุนันท์, ทัชชกร แสงทองดี วิเคราะห์ปัญหาอาชญากรรมไซเบอร์ในประเทศไทย รวมถึงกฎหมายที่เกี่ยวข้องและแนวทางการพิสูจน์หลักฐานทางดิจิทัล เพื่อพัฒนามาตรการแก้ไขปัญหาอย่างมีประสิทธิภาพ[30]

4. กรอบกฎหมายของประเทศไทยในการต่อต้านอาชญากรรมคอลเซ็นเตอร์ งานวิจัยของ ภาคิน หวังสถิธรรม ศึกษารูปแบบต่าง ๆ ของกิจกรรมที่ผิดกฎหมายที่เกี่ยวข้องกับคอลเซ็นเตอร์ รวมถึงการฉ้อโกง การขโมยข้อมูลส่วนบุคคล การกรรโชก การฟอกเงิน การค้ามนุษย์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต[31] แสดงให้เห็นว่าอาชญากรรมที่เกี่ยวข้องกับคอลเซ็นเตอร์กลายเป็นความท้าทายระดับโลกที่สำคัญ ซึ่งมีลักษณะที่หลากหลายและซับซ้อน

5. ผลกระทบที่สำคัญต่อเหยื่อและสังคม และกลยุทธ์ที่อาชญากรใช้เพื่ออาศัยประโยชน์จากความก้าวหน้าทางเทคโนโลยี สามารถนำมาใช้เพื่อเป็นแนวทางการรับมือที่มีหลายแง่มุม ซึ่งรวมถึงการปฏิรูปกฎหมาย นวัตกรรมทางเทคโนโลยี และความร่วมมือระหว่างประเทศ ถือเป็นเรื่องจำเป็น เนื่องจากลักษณะที่เปลี่ยนแปลงตลอดเวลาของอาชญากรรมที่เกี่ยวข้องกับคอลเซ็นเตอร์ต้องอาศัยการปรับตัวและความระมัดระวังอย่างต่อเนื่องจากทุกฝ่ายที่เกี่ยวข้อง[31]

6. แนวทางการพัฒนากองทัพไทยด้านความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์แนวทางเสริมสร้างความมั่นคงไซเบอร์ของกองทัพบกไทย โดยเน้นการเพิ่มขีดความสามารถด้านเทคโนโลยีและบุคลากรเพื่อรับมือกับภัยคุกคามที่ซับซ้อน[32]

7. การใช้ AI และ AGI เพื่อพัฒนาความมั่นคงทางไซเบอร์ของกองทัพอากาศไทย ศึกษาการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการวิเคราะห์และป้องกันภัยไซเบอร์ เพื่อเพิ่มความสามารถในการป้องกันภัยไซเบอร์ของกองทัพอากาศไทย โดยใช้การวิเคราะห์ข้อมูลเชิงลึกเพื่อรับมือกับภัยคุกคามที่เกิดขึ้น[33]

งานวิจัยระดับนานาชาติ

1. งานวิจัยของ Smith et al. พบว่าการฝึกอบรมด้านไซเบอร์สามารถลดโอกาสตกเป็นเหยื่อการโจมตีทางไซเบอร์ได้ถึง 40%

2. การศึกษาของ Williams และ Brown แสดงให้เห็นว่าองค์กรที่มีมาตรการรักษาความปลอดภัยที่เข้มงวดสามารถลดการโจมตีทางไซเบอร์ได้ถึง 60%[34] ในบริบทของกำลังพลกองทัพบกมีการพัฒนาโปรแกรมฝึกอบรม เช่น S.M.A.R.T. SOLDIERS Royal Thai Army และการใช้ระบบแจ้งเตือนภัยไซเบอร์เพื่อป้องกันการโจมตีจากภายนอก

3. รายงาน Cybersecurity Report 2023 จาก Global Cybersecurity Institute ย้ำถึงความสำคัญของ การจัดการรหัสผ่าน (Password Management) ในการลดความเสี่ยงจากอาชญากรรมไซเบอร์ การบริหารจัดการรหัสผ่านที่ดี ไม่เพียงช่วยลดโอกาสการโจมตี แต่ยังส่งเสริมวัฒนธรรมความปลอดภัยในองค์กร โดยสนับสนุนการตระหนักรู้ด้านความปลอดภัยไซเบอร์ของกำลังพลกองทัพบก ช่วยลดความเสี่ยงและเพิ่มขีดความสามารถในการป้องกันภัยไซเบอร์ได้อย่างมีประสิทธิภาพ โดยมีประเด็นสำคัญดังนี้

3.1 ความสำคัญของรหัสผ่านที่แข็งแรง การใช้รหัสผ่านที่ซับซ้อนและไม่ซ้ำกันสำหรับแต่ละบัญชีช่วยลดโอกาสที่ผู้โจมตีจะสามารถเข้าถึงข้อมูลสำคัญ ได้รายงานระบุว่าการใช้รหัสผ่านที่ง่ายต่อการคาดเดา เช่น “123456” หรือ “password” ยังคงเป็นช่องโหว่ที่พบได้บ่อยในหลายองค์กร

3.2 การใช้เครื่องมือจัดการรหัสผ่าน (Password Manager) เครื่องมือเหล่านี้ช่วยให้ผู้ใช้สามารถสร้างและจัดเก็บรหัสผ่านที่แข็งแรงได้อย่างปลอดภัย ลดความเสี่ยงจากการใช้รหัสผ่านซ้ำหรือการลืมรหัสผ่าน

3.3 การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) การเพิ่มชั้นความปลอดภัยด้วย MFA ช่วยลดความเสี่ยงจากการที่รหัสผ่านถูกขโมยหรือถูกแฮ็ก โดยเฉพาะในกรณีที่ผู้โจมตีสามารถเข้าถึงรหัสผ่านได้

3.4 ผลกระทบทางเศรษฐกิจ ระบุว่าการละเลยการจัดการรหัสผ่านที่เหมาะสมสามารถนำไปสู่ความเสียหายทางเศรษฐกิจอย่างร้ายแรง เช่น การสูญเสียข้อมูลสำคัญ การโจมตีด้วย Ransomware หรือการละเมิดข้อมูลที่ส่งผลต่อชื่อเสียงขององค์กร

3.5 แนวทางป้องกัน แนะนำให้องค์กรลงทุนในระบบจัดการรหัสผ่านที่ปลอดภัยและให้ความรู้แก่พนักงานเกี่ยวกับการสร้างรหัสผ่านที่แข็งแรง รวมถึงการใช้ MFA เพื่อเพิ่มระดับความปลอดภัย

4. Khan M, Rahman S, Aziz M. ศึกษากลยุทธ์การส่งเสริมความตระหนักรู้ด้านไซเบอร์ในกองทัพบังกลาเทศ โดยใช้การฝึกอบรมและนโยบายองค์กรเพื่อเสริมสร้างความเข้าใจในภัยคุกคามไซเบอร์[35]

5. White J, Thomas P. วิเคราะห์การใช้ไซเบอร์ในยุทธศาสตร์ทางทหารโดยชี้ให้เห็นถึงบทบาทของระบบไซเบอร์ในการสนับสนุนการปฏิบัติการทางทหารและการป้องกันความมั่นคงของชาติ[36]

6. RAND Corporation ศึกษาความเสี่ยงด้านไซเบอร์ของกองทัพอากาศสหรัฐฯ และเสนอแนวทางการพัฒนามาตรการรักษาความปลอดภัยไซเบอร์ตลอดวงจรชีวิตของระบบทางทหาร[37]

7. Military Times รายงานวิเคราะห์ว่ากำลังพลทหารมีแนวโน้มตกเป็นเหยื่อของอาชญากรรมไซเบอร์มากกว่าประชากรทั่วไป เนื่องจากการใช้เทคโนโลยีดิจิทัลและช่องโหว่ด้านความปลอดภัยส่วนบุคคล[38]

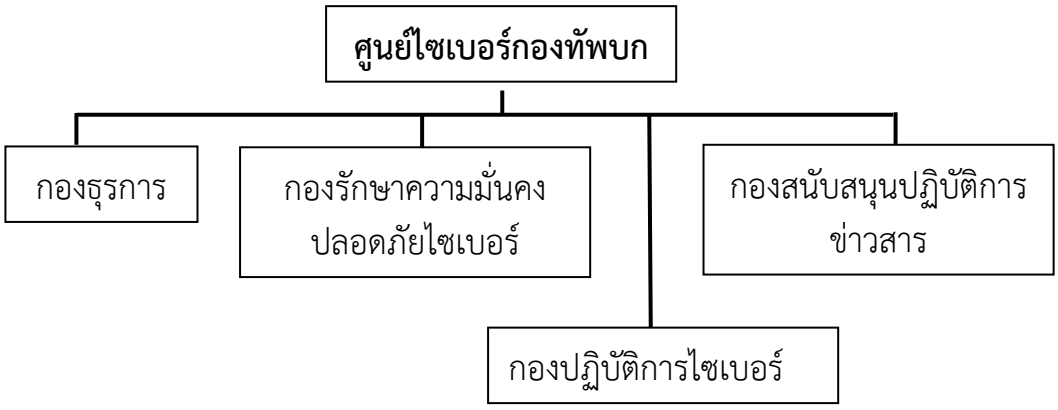
โครงสร้าง/ภารกิจขององค์กรที่ทำการศึกษา

หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย (Military Cyber Center) ดำเนินงานด้านการป้องกันและการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงทางทหารและความมั่นคงของประเทศ โดยมีภารกิจการป้องกันและรักษาความปลอดภัยทางไซเบอร์ การสนับสนุนการปฏิบัติการทางทหาร การติดตามและตรวจสอบภัยคุกคามทางไซเบอร์ การวางแผนและพัฒนานโยบายไซเบอร์ การสนับสนุนงานวิจัยและพัฒนาเทคโนโลยีไซเบอร์ การสร้างความร่วมมือระหว่างหน่วยงาน การสนับสนุนการปฏิบัติการพิเศษ ครอบคลุมทั้งการป้องกันภัยคุกคามทางไซเบอร์ การรักษาความปลอดภัยของข้อมูลและระบบทหาร การตอบสนองต่อเหตุการณ์ที่เกิดขึ้น รวมถึงการพัฒนาเทคโนโลยีและนโยบายเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต

สำหรับกองทัพบกอยู่ระหว่างออกคำสั่งจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเอบร์ (Cyber Security Operation Center: CSOC) แต่ศูนย์ไซเบอร์กองทัพบกทำหน้าที่ CSOC ให้กับ เว็บไซต์ ของหน่วยภายในกองทัพบก Server แม่ข่าย rta.mi.th รวมถึง โรงพยาบาลพระมงกุฎเกล้า อยู่ ณ ปัจจุบัน (ศูนย์ปฏิบัติการ CSOC คือ ศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ มีหน้าที่เฝ้าระวัง ตรวจสอบ วิเคราะห์ และให้คำแนะนำแก่ผู้ดูแลระบบในการรับมือ ป้องกัน การถูกบุกรุกทางไซเบอร์ หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต มายังระบบหรืออุปกรณ์สำคัญขององค์กร ตลอดจนโครงสร้างพื้นฐานด้านความปลอดภัย ซึ่งในศูนย์ CSOC จะต้องมีเจ้าหน้าที่ผู้เชี่ยวชาญในการเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมง เมื่อตรวจพบเหตุการณ์ต้องสงสัย เจ้าหน้าที่จะทำการวิเคราะห์ข้อมูลแวดล้อมของเหตุการณ์ ประเมินระดับความรุนแรงของเหตุกาณ์ พร้อมทั้งให้คำแนะนำเบื้องต้นในการรับมือ จัดการกับปัญหาที่เกิดขึ้น เพื่อลดผลกระทบและลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ รวมถึงการดำเนินธุรกิจ

ศูนย์ไซเบอร์กองทัพบก มีภารกิจหน้าที่ดำเนินการเกี่ยวกับการปฏิบัติด้านไซเบอร์และพัฒนาความพร้อมด้านไซเบอร์ของกองทัพบก มีขีดความสามารถการเฝ้าตรวจแจ้งเตือน กำหนดมาตรการและกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยต่าง ๆ ของกองทัพบก, การติดตาม รวบรวม วิเคราะห์ข่าวสารบนไซเบอร์

เพื่อสนับสนุนการปฏิบัติด้านไซเบอร์และสนับสนุนการปฏิบัติข่าวสารของกองทัพบก, การบริหารจัดการความเสี่ยงด้านสารสนเทศแก่หน่วยต่าง ๆ ของกองทัพบก การอบรมสร้างความตระหนักด้านการรักษาความปลอดภัยไซเบอร์ การตรวจสอบด้านเทคโนโลยีสารสนเทศ การตรวจสอบและประเมินความเสี่ยงทางเทคนิคด้านการรักษาความปลอดภัยสารสนเทศแก่หน่วยต่าง ๆ ของกองทัพบก การทดสอบระบบรักษาความปลอดภัยสารสนเทศ การตรวจสอบและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ การแก้ไขสถานการณ์หรือเหตุการณ์ในภาวะฉุกเฉินทางไซเบอร์ การตอบโต้ภัยคุกคามด้านไซเบอร์ การสำรองและฟื้นฟูระบบไซเบอร์ การวิเคราะห์ข้อมูลการจราจรทางไซเบอร์ รวมทั้งพิสูจน์หลักฐานทางดิจิทัล[39] โดยมีโครงสร้างการจัดหน่วยรายละเอียดตามภาพ



ภาพที่ 2 โครงสร้างการจัดหน่วยศูนย์ไซเบอร์กองทัพบก

ในปัจจุบันกองทัพบกได้อนุมัติให้มีการจัดทำแผนการฝึกหลักสูตรอบรมจำนวน 8 หลักสูตร ได้แก่ หลักสูตรเชิงรุก จำนวน 3 หลักสูตร คือ 1) หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ชั้นสูง 2) หลักสูตรการฝึกจำลองยุทธ์ทางไซเบอร์ และ 3) หลักสูตรพิเศษเฉพาะทางด้านการรักษาความปลอดภัยไซเบอร์, หลักสูตรเชิงรับ จำนวน 3 หลักสูตร คือ 1) หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ชั้นต้น 2) หลักสูตรการผลิตสื่อด้านไซเบอร์ และ 3) หลักสูตรหลักการใช้งานเครือข่ายสังคมออนไลน์ และหลักสูตรสนับสนุนการปฏิบัติการ จำนวน 2 หลักสูตร คือ หลักสูตรการปฏิบัติการไซเบอร์ชั้นต้น และหลักสูตรการปฏิบัติการไซเบอร์ชั้นสูง เพื่อเพิ่มศักยภาพให้กับกำลังพลทำหน้าที่เสริมสร้างความรู้ ความเข้าใจสร้างความตระหนัก ติดตามกำกับดูแลการปฏิบัติของหน่วยตามมาตรการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

บทที่ 3
บทวิเคราะห์

ในบทนี้มีเป้าหมายเพื่อวิเคราะห์สถานการณ์และปัจจัยที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ในกองทัพบก โดยต่อยอดจากข้อมูลและทฤษฎีในบทที่ 2 ที่สรุปว่าอาชญากรรมไซเบอร์ได้กลายเป็นภัยคุกคามที่ซับซ้อนและสำคัญยิ่งต่อกองทัพบก ปัจจัยเสี่ยงสำคัญมาจากพฤติกรรมของบุคลากรที่ขาดการฝึกอบรมและมาตรการป้องกันที่เข้มงวด โดยใช้กรอบการวิเคราะห์เชิงยุทธศาสตร์ เช่น SWOT, TOWS และ PMESII เพื่อประเมินจุดแข็ง จุดอ่อน โอกาส และภัยคุกคาม พร้อมทั้งเชื่อมโยงข้อมูลเพื่อกำหนดแนวทางเชิงรุกและเชิงรับ รวมถึงข้อเสนอแนะเชิงปฏิบัติที่สามารถนำไปใช้ได้จริง การวิเคราะห์นี้จะช่วยกำหนดกลยุทธ์ที่ครอบคลุมและมีประสิทธิภาพในการเสริมสร้างความพร้อมของกำลังพล ตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างเป็นระบบ สอดคล้องกับยุทธศาสตร์ชาติ 20 ปี และแผนปฏิบัติการกองทัพบกในมิติความมั่นคงทางไซเบอร์

ทั้งนี้ ผู้วิจัยได้ศึกษาหลักการ ทฤษฎี ตลอดจนงานวิจัยที่เกี่ยวข้อง รวมถึงบทวิเคราะห์ที่สำคัญที่สอดคล้องกับวัตถุประสงค์งานวิจัยในบทที่ 1 ดังนี้

สถานการณ์ความรู้เรื่องอาชญากรรมทางไซเบอร์ที่เป็นภัยคุกคามกำลังพลกองทัพบกในปัจจุบัน

1. ความรุนแรงของอาชญากรรมทางไซเบอร์ กำลังเป็นภัยคุกคามที่สำคัญต่อกำลังพลของกองทัพบก โดยมีการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตในการโจมตีระบบ ขโมยข้อมูล และฉ้อโกงออนไลน์ ซึ่งแนวโน้มการโจมตีเพิ่มสูงขึ้นหลังการระบาดของโควิด-19 เนื่องจากการขยายตัวของการใช้อินเทอร์เน็ตที่มากขึ้น

1.1 จำนวนคดีและสถิติการโจมตีที่เพิ่มขึ้น งานวิจัยและสถิติจากสำนักงานตำรวจแห่งชาติระบุชัดว่าในช่วงไม่กี่ปีที่ผ่านมา จำนวนคดีอาชญากรรมทางไซเบอร์เพิ่มขึ้นอย่างมีนัยยะ เช่น มีรายงานการรับแจ้งความออนไลน์เกี่ยวกับคดีอาชญากรรมทางเทคโนโลยีจำนวนมาก เพิ่มความกดดันต่อระบบรักษาความปลอดภัยและการสืบสวนจับกุมตอบโต้ภัยไซเบอร์

1.2 ความซับซ้อนและความหลากหลายของรูปแบบการโจมตี อาชญากรรมทางไซเบอร์ในปัจจุบันมีรูปแบบที่หลากหลายมากขึ้น ทั้งการโจมตีด้วยวิธี DDoS, Phishing, Malware และการโจมตีด้วยเทคโนโลยีขั้นสูง เช่น Advanced Persistent

Threats (APT) ซึ่งความซับซ้อนในเทคนิคและวิธีการแต่ละรูปแบบส่งผลให้การป้องกันและการตรวจจับเกิดความยากลำบาก การโจมตีไซเบอร์เหล่านี้มักมีเป้าหมาย ที่เป็นระบบโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบเครือข่าย, ระบบฐานข้อมูลของรัฐบาล และองค์กรที่มีข้อมูลมากมาย

1.3 การขาดความตระหนักรู้และเสริมสร้างวัฒนธรรมของบุคลากร ปัจจัยสำคัญที่เพิ่มช่องโหว่ให้กับระบบ เป็นความท้าทายอย่างมากในการเสริมสร้างความตระหนักรู้ของบุคลากรเกี่ยวกับภัยไซเบอร์ ซึ่งการขาดความรู้และทักษะด้านไซเบอร์ส่งผลให้องค์กรไม่สามารถรับมือเหตุการณ์ฉุกเฉินได้อย่างรวดเร็วและมีประสิทธิภาพ

1.4 ภัยคุกคามจากกลุ่มอาชญากรไซเบอร์และการโจมตีจากต่างประเทศ แนวโน้มของการโจมตีที่มาจากต่างประเทศและกลุ่มอาชญากรไซเบอร์ที่มีความเชี่ยวชาญด้านเทคนิคขั้นสูง ยิ่งทำให้ความรุนแรงของภัยไซเบอร์สูงขึ้น ภัยเหล่านี้มีเป้าหมายเพื่อละเมิดความมั่นคงของชาติและข้อมูลที่เป็นความลับขององค์กรต่าง ๆ ภายในและภายนอกรัฐบาล

1.5 ปรากฏการณ์แก๊งคอลเซนเตอร์ที่กระทบกับกองทัพบก เป็นองค์กรอาชญากรรมที่ใช้ระบบโทรศัพท์หรือการสื่อสารด้วยเสียงเป็นเครื่องมือหลักในการดำเนินกิจกรรมทางอาชญากรรม โดยทั่วไปแล้ว โจรไซเบอร์ในลักษณะนี้จะใช้เทคนิค Social Engineering ในการหลอกลวงข้อมูลและบุคลากร ซึ่งอาจรวมถึงการปลอมตัวเป็นเจ้าหน้าที่ที่มีอำนาจ เช่น เจ้าหน้าที่ของกองทัพบก หรือหน่วยงานรัฐอื่น ๆ เพื่อให้ได้รับความไว้วางใจจากเหยื่อ จากนั้นจึงดำเนินการเรียกเก็บข้อมูลส่วนบุคคล เงินเข้าบัญชีปลอม หรือข้อมูลที่สำคัญทางด้านความมั่นคง

1.5.1 ผลกระทบที่อาจเกิดขึ้นต่อกองทัพบกด้านข้อมูลและความมั่นคง การที่แก๊งคอลเซนเตอร์สามารถปลอมตัวเป็นเจ้าหน้าที่กองทัพหรือตัวแทนหน่วยงานราชการมักจะส่งผลให้เกิดการรั่วไหลของข้อมูลที่อาจมีความลับและสำคัญต่อการปฏิบัติการของกองทัพบก การโจมตีโดยวิธีนี้อาจนำไปสู่การขโมยข้อมูลลับหรือข้อมูลส่วนตัวของบุคลากร ซึ่งส่งผลต่อความมั่นคงและความน่าเชื่อถือในระบบบริหารจัดการความปลอดภัยไซเบอร์ของหน่วยงาน

1.5.2 ผลกระทบที่อาจเกิดขึ้นต่อกองทัพบกด้านการบริหารจัดการและรายงานความปลอดภัย หากแก๊งคอลเซนเตอร์มีความสามารถในการหลอกลวงให้บุคลากรเปิดเผยข้อมูลหรือเชื่อมต่อกับระบบที่ไม่ปลอดภัย ผลลัพธ์ที่ตามมาอาจเป็นการเสื่อมเสียชื่อเสียงของหน่วยงาน ความเข้มแข็งของมาตรการด้านไซเบอร์ที่มีอยู่จะถูกทดสอบอย่างรุนแรง ซึ่งสถิติอาชญากรรมทางไซเบอร์ในประเทศไทยที่มีคดีแจ้งความสูงถึงหลายแสนคดี (สำนักงานตำรวจแห่งชาติ) เป็นหลักฐานยืนยันความกดดันดังกล่าว

1.6 ช่องโหว่และภัยคุกคามในระบบกองทัพบก กองทัพบกกำลังเผชิญกับช่องโหว่ด้านความปลอดภัย โดยเฉพาะจากบุคลากรที่ขาดการฝึกอบรมเพียงพอ สถิติจากสำนักงานตำรวจแห่งชาติ (2567) ระบุว่า 78% ของการโจมตีไซเบอร์ในองค์กรเกิดจากช่องโหว่ของบุคลากรที่ไม่ได้รับการฝึกอบรมเพียงพอ นอกจากนี้ องค์กรที่ไม่มีมาตรการรักษาความปลอดภัยที่เข้มงวดเพียงพอมีความเสี่ยงถูกโจมตีสูง โดยเฉพาะจากอาชญากรที่เลือกเป้าหมายที่มีความเสี่ยงต่ำและผลประโยชน์สูง

1.7 บทบาทของศูนย์ไซเบอร์กองทัพบก (CSOC) กองทัพบกมีศูนย์ไซเบอร์ (CSOC) ที่ทำหน้าที่เฝ้าระวังภัยไซเบอร์และวิเคราะห์ภัยคุกคาม รวมถึงจัดอบรมด้าน ความปลอดภัยไซเบอร์ให้กับกำลังพล โดยมีทั้งหลักสูตรเชิงรับและเชิงรุก รวม 8 หลักสูตร เพื่อเพิ่มขีดความสามารถในการรับมือภัยคุกคาม อย่างไรก็ตาม ศูนย์ CSOC ยังอยู่ระหว่างการจัดตั้งอย่างเป็นทางการ แต่ปัจจุบันศูนย์ไซเบอร์กองทัพบกทำหน้าที่นี้อยู่

1.8 พฤติกรรมเสี่ยงของกำลังพล กำลังพลที่ขาดความตระหนักรู้ด้านปลอดภัยมักมีพฤติกรรมเสี่ยง เช่น การใช้รหัสผ่านซ้ำในหลายแพลตฟอร์ม ซึ่งเพิ่มโอกาสในการตกเป็นเป้าหมายของอาชญากรไซเบอร์ถึง 60%

1.9 มาตรการและผลการฝึกอบรม การฝึกอบรมและสร้างความตระหนักรู้ผ่านการจำลองการโจมตี เช่น ฟิชชิ่ง (Phishing Simulation) ช่วยลดอัตราการตกเป็นเหยื่อได้ถึง 64.81% แสดงให้เห็นว่าการฝึกอบรมมีบทบาทสำคัญในการเสริมสร้างความตระหนักรู้และป้องกันภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

ปัจจัยที่ส่งผลต่อการตระหนักรู้ในเรื่องอาชญากรรมทางไซเบอร์ของกำลังพลกองทัพบก

1. การฝึกอบรมและการพัฒนาความรู้

1.1 หลักสูตรฝึกอบรมเฉพาะทางด้านไซเบอร์ กองทัพบกได้จัดทำหลักสูตรอบรมที่เกี่ยวกับการป้องกันภัยไซเบอร์ เช่น หลักสูตรการปฏิบัติการไซเบอร์ชั้นต้นและขั้นสูง ซึ่งมีวัตถุประสงค์เพื่อเพิ่มพูนความรู้พื้นฐานและความชำนาญในการตรวจจับและตอบโต้ภัยไซเบอร์

1.2 การใช้แพลตฟอร์ม E-Learning กองทัพบกได้นำระบบ e-Learning เข้ามาใช้ในกระบวนการฝึกอบรมเพื่อให้กำลังพลเข้าถึงความรู้ด้านไซเบอร์ได้อย่างทั่วถึงและต่อเนื่อง ยืนยันถึงความสำเร็จในการประยุกต์ใช้ e-Learning ในการฝึกอบรมให้เกิดผลจริง

2. วัฒนธรรมองค์กรด้านความปลอดภัยและพฤติกรรมส่วนบุคคล

2.1 การสร้างวัฒนธรรมความปลอดภัยไซเบอร์ การส่งเสริมวัฒนธรรมองค์กรที่เน้นความปลอดภัยไซเบอร์ เป็นหนึ่งในเป้าหมายหลัก ซึ่งรวมถึงการส่งเสริมให้นำรหัสผ่านที่เข้มงวดและการตรวจสอบข้อมูลอย่างสม่ำเสมอ สนับสนุนแนวคิดที่ว่าการปรับปรุงพฤติกรรมในกิจวัตรประจำวัน จะลดโอกาสในการตกเป็นเหยื่อของอาชญากรรมไซเบอร์

2.2 การมีแรงจูงใจและการส่งเสริมความรู้ในระดับบุคลากร แนวทาง การฝึกอบรมที่เน้นเพิ่มระดับแรงจูงใจได้รับการยืนยันจากงานวิจัยของ Smith et al. (2021) ว่าการสร้างแรงจูงใจช่วยเพิ่มระดับการตระหนักรู้และการปฏิบัติตามมาตรการความปลอดภัยไซเบอร์

3. การใช้เทคโนโลยีและระบบสารสนเทศ

3.1 การใช้เทคโนโลยี AI และ Big Data กองทัพบกได้มีการศึกษาและทดสอบการนำ AI และระบบ Big Data มาใช้ตรวจสอบภัยไซเบอร์ ผลการดำเนินงานแสดงให้เห็นว่าสามารถลดอัตราการโจมตีได้อย่างมีนัยสำคัญ

3.2 การลงทุนในระบบป้องกันภัย ข้อมูลจากเว็บไซต์ของกองทัพบกและนโยบายกองทัพบก ระบุถึงการลงทุนอุปกรณ์เทคโนโลยีต่าง ๆ เช่น ระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection and Prevention Systems: IDPSs) และเครื่องมือเข้ารหัสข้อมูล ซึ่งเป็นปัจจัยที่สำคัญในการลดช่องโหว่ของระบบ

4. การสนับสนุนจากนโยบายและแผนยุทธศาสตร์

4.1 นโยบายและแผนระดับชาติ ยุทธศาสตร์ชาติ 20 ปี, แผนแม่บทภายใต้ยุทธศาสตร์ชาติ, สมุดปกขาวกองทัพบก และนโยบายกองทัพบก ได้วางแนวทางและมาตรการที่ชัดเจนในการพัฒนาความมั่นคงด้านไซเบอร์ ทั้งในด้านการฝึกอบรม การลงทุนในเทคโนโลยีและการประสานงานระหว่างหน่วยงาน

4.2 การสร้างความร่วมมือภายในและภายนอก ความร่วมมือกับมิตรประเทศทั้งในและต่างประเทศ เช่น การแลกเปลี่ยนความรู้กับหน่วยงานไซเบอร์ระดับชาติและนานาชาติ มีผลในการพัฒนาระบบและนวัตกรรมใหม่ ๆ ที่สามารถนำไปใช้ปรับปรุงระบบความปลอดภัยไซเบอร์ได้

5. ปัจจัยที่เป็นอุปสรรคและความท้าทาย

5.1 ความจำกัดด้านงบประมาณและทรัพยากร งานวิจัยจากเอกสารนโยบายและสมุดปกขาวชี้ว่าในบางหน่วยงานยังมีข้อจำกัดด้านงบประมาณและบุคลากรที่เชี่ยวชาญ ซึ่งส่งผลให้การพัฒนาและปรับปรุงระบบความมั่นคงไซเบอร์ไม่สามารถดำเนินการได้อย่างครอบคลุม

5.2 ความซับซ้อนภัยคุกคามที่มาจากแก๊งคอลเซนเตอร์หรือกลุ่มอาชญากรไซเบอร์ ที่ใช้เทคนิคการ Social Engineering มีความซับซ้อนและพัฒนาอย่างรวดเร็ว ทำให้การฝึกอบรมและมาตรการป้องกันสามารถตกเป็นเหยื่อของเทคนิคใหม่ๆ ได้อยู่เสมอ

6. ประสบการณ์และอายุการทำงาน การศึกษาเปรียบเทียบพบว่ากำลังพลที่มีอายุงานมากกว่ามีแนวโน้มให้ความสำคัญเกี่ยวกับความระมัดระวังและตระหนักรู้มากกว่า เช่น

6.1 การตั้งรหัสผ่าน ผู้ที่ใช้รหัสผ่านที่ซับซ้อนมีโอกาสถูกแฮ็กบัญชีน้อยกว่าผู้ใช้รหัสผ่านทั่วไปถึง 50%

6.2 ความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ องค์กรที่มีการอบรมด้านความมั่นคงไซเบอร์อย่างต่อเนื่อง สามารถลดความเสี่ยงจากการโจมตีทางไซเบอร์ได้ถึง 65%

6.3 ความปลอดภัยของอุปกรณ์และการเชื่อมต่อ ระบบสำรองข้อมูลบนคลาวด์สามารถลดระยะเวลาการกู้คืนระบบจากการโจมตีทางไซเบอร์ได้ถึง 40%

6.4 การใช้และดูแลแอปพลิเคชัน ผู้ใช้ที่อัปเดตระบบปฏิบัติการและซอฟต์แวร์เป็นประจำสามารถป้องกันการโจมตีจากมัลแวร์ได้มากถึง 80%

6.5 พฤติกรรมของผู้ใช้งาน ผู้ที่มีพฤติกรรมระมัดระวัง เช่น ตรวจสอบก่อนคลิกลิงก์มีโอกาสตกเป็นเหยื่อของฟิชชิ่งลดลง 60%

การวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ด้วย PMESII Framework และ SWOT Analysis

1. การวิเคราะห์ตามกรอบ PMESII Framework ได้ดังนี้

1.1 การเมือง (Political) นโยบายความมั่นคงแห่งชาติของไทยได้ให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ โดยมีการจัดทำแผนปฏิบัติการที่ชัดเจนภายใต้ยุทธศาสตร์ชาติ 20 ปี ซึ่งถือเป็นปัจจัยสำคัญในการส่งเสริมการตระหนักรู้เรื่อง การป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก การสนับสนุนจาก

ผู้บริหารระดับสูงและความร่วมมือระหว่างหน่วยงานทั้งภาครัฐและเอกชนมีบทบาทสำคัญในการจัดสรรงบประมาณและทรัพยากรเพื่อพัฒนาโครงสร้างพื้นฐานด้านไซเบอร์ รวมถึงการจัดทำหลักสูตรฝึกอบรมที่มีมาตรฐานสากล อย่างไรก็ตาม ความไม่ต่อเนื่องของนโยบายและการเปลี่ยนแปลงทางการเมืองอาจเป็นอุปสรรคต่อการบรรลุเป้าหมายในการสร้างความตระหนักรู้ในระยะยาว

1.2 การทหาร (Military) กองทัพบกมีโครงสร้างการบังคับบัญชาและระเบียบวินัยที่เข้มแข็งเป็นข้อได้เปรียบในการถ่ายทอดความรู้และฝึกอบรมกำลังพลให้มีความตระหนักรู้ด้านการป้องกันภัยไซเบอร์อย่างเป็นระบบ การมีหน่วยไซเบอร์เฉพาะทางและศูนย์เฝ้าระวังภัยไซเบอร์เป็นพื้นฐานสำคัญในการติดตามและวิเคราะห์ภัยคุกคาม รวมถึงการพัฒนาเครือข่ายข้อมูลข่าวกรองที่สามารถแจ้งเตือนภัยล่วงหน้า

1.3 เศรษฐกิจ (Economic) งบประมาณด้านการป้องกันภัยไซเบอร์ของกองทัพบกยังคงมีข้อจำกัด ซึ่งส่งผลต่อการจัดหาเครื่องมือและเทคโนโลยีที่ทันสมัย รวมถึงการฝึกอบรมเชิงลึกให้กับกำลังพล การแสวงหาความร่วมมือกับภาคเอกชนและองค์กรระหว่างประเทศ ในการจัดทำโครงการฝึกอบรมและแลกเปลี่ยนองค์ความรู้เป็นทางเลือกที่สามารถช่วยลดภาระทางการเงินได้ การส่งเสริมความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ยังเป็นปัจจัยที่ช่วยลดความเสี่ยงจากการสูญเสียทางเศรษฐกิจอันเนื่องมาจากการโจมตีทางไซเบอร์

1.4 สังคม (Social) ความตระหนักรู้ของกำลังพลในเรื่องภัยคุกคามทางไซเบอร์ยังคงอยู่ในระดับที่ต้องพัฒนาเพิ่มเติม โดยเฉพาะอย่างยิ่งในกลุ่มผู้ที่ไม่เชี่ยวชาญด้านเทคโนโลยี การจัดทำแคมเปญประชาสัมพันธ์และสื่อการเรียนรู้ที่เข้าถึงง่ายและมีเนื้อหา ที่ตรงประเด็น รวมถึงการส่งเสริมวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยทางข้อมูล เป็นกลยุทธ์ที่สามารถเสริมสร้างความตระหนักรู้ได้อย่างมีประสิทธิภาพ นอกจากนี้ การสร้างความเข้าใจในระดับครอบครัวของกำลังพลเกี่ยวกับภัยคุกคามไซเบอร์ก็เป็นอีกหนึ่งปัจจัยที่ควรให้ความสำคัญ

1.5 ข้อมูลและสารสนเทศ (Information) การใช้ Big Data และ AI ในการวิเคราะห์และเฝ้าระวังภัยคุกคามทางไซเบอร์เป็นปัจจัยสำคัญในการเสริมสร้างการตระหนักรู้และป้องกันการโจมตีได้อย่างมีประสิทธิภาพ การจัดทำฐานข้อมูลภัยคุกคามที่อัปเดตและครอบคลุม รวมถึงการพัฒนาระบบแจ้งเตือนภัยและแพลตฟอร์มการเรียนรู้ออนไลน์ที่สามารถเข้าถึงได้ทุกที่ทุกเวลา จะช่วยให้กำลังพลมีข้อมูลที่ทันสมัยและสามารถตอบสนองต่อสถานการณ์ที่เกิดขึ้นได้อย่างรวดเร็ว อย่างไรก็ตาม ข้อจำกัดด้านความปลอดภัยของข้อมูลและความเป็นส่วนตัวก็เป็นประเด็นที่ต้องคำนึงถึงอย่างรอบคอบ

1.6 โครงสร้างพื้นฐาน (Infrastructure) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของกองทัพบกยังต้องการการพัฒนาเพิ่มเติม โดยเฉพาะในด้านระบบเครือข่ายและการรักษาความปลอดภัยของข้อมูล การจัดทำแผนพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ ที่ครอบคลุมทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ รวมถึงการฝึกอบรมบุคลากรให้มีทักษะ ในการใช้งานและบำรุงรักษาระบบ เป็นปัจจัยที่สำคัญในการเสริมสร้างความตระหนักรู้และขีดความสามารถในการป้องกันภัยคุกคาม นอกจากนี้การลงทุนในเทคโนโลยีป้องกันภัยเชิงรุก เช่น Firewall, Intrusion Detection Systems (IDSs), และการเข้ารหัสข้อมูล

2. การวิเคราะห์ด้วย SWOT Analysis ได้ผลดังนี้

2.1 จุดแข็ง (Strengths) กองทัพบกมีโครงสร้างการบังคับบัญชาที่เข้มแข็งและระเบียบวินัยที่เป็นระบบ ซึ่งเป็นรากฐานสำคัญในการถ่ายทอดความรู้และฝึกอบรมกำลังพลให้มีความตระหนักรู้ด้านการป้องกันอาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ นโยบายด้านความมั่นคงของรัฐที่ให้ความสำคัญกับการป้องกันภัยไซเบอร์ยังเป็นปัจจัยที่เอื้อต่อการจัดสรรงบประมาณและทรัพยากรเพื่อพัฒนาโครงการฝึกอบรมและสื่อการเรียนรู้ที่ทันสมัย รวมถึงการมีศูนย์ไซเบอร์ของกองทัพที่ทำหน้าที่เป็นหน่วยงานหลักในการเฝ้าระวังและวิเคราะห์ภัยคุกคาม ซึ่งสามารถใช้เป็นฐานข้อมูลและแหล่งเรียนรู้สำหรับกำลังพลในการเสริมสร้างความตระหนักรู้ได้อย่างต่อเนื่อง

2.2 จุดอ่อน (Weaknesses) ข้อจำกัดด้านทักษะทางเทคนิคและความรู้เฉพาะทางของกำลังพลส่วนใหญ่ยังเป็นอุปสรรคสำคัญในการรับรู้และป้องกันภัยคุกคามทางไซเบอร์ ได้อย่างทันท่วงที การฝึกอบรมที่มีอยู่นั้นยังคงเน้นไปที่ทฤษฎีมากกว่าการปฏิบัติจริง ทำให้ขาดความเข้าใจในสถานการณ์ที่ซับซ้อน นอกจากนี้การขาดระบบการประเมินผลและติดตามความก้าวหน้าในการเรียนรู้ของกำลังพล รวมถึงข้อจำกัดด้านงบประมาณและทรัพยากรที่ไม่เพียงพอต่อการจัดหาเครื่องมือที่ทันสมัย ก็เป็นปัจจัยที่ทำให้การส่งเสริมความตระหนักรู้ยังไม่เป็นไปตามเป้าหมายที่กำหนด

2.3 โอกาส (Opportunities) การเติบโตของเทคโนโลยีสารสนเทศและความร่วมมือระหว่างประเทศในด้านความมั่นคงทางไซเบอร์ถือเป็นโอกาสที่ดีในการยกระดับความรู้และทักษะของกำลังพล การเข้าร่วมโครงการฝึกอบรมและสัมมนาระดับนานาชาติ รวมถึงการแลกเปลี่ยนข้อมูลกับพันธมิตรต่างประเทศ จะช่วยให้กำลังพลได้รับข้อมูลที่ทันสมัยและเทคนิคการป้องกันภัยไซเบอร์ที่มีประสิทธิภาพ นอกจากนี้การพัฒนาแพลตฟอร์มการเรียนรู้ออนไลน์และสื่อดิจิทัลที่เข้าถึงง่ายยังเป็นโอกาสในการกระจายความรู้และฝึกฝนทักษะให้กับกำลังพลในทุกระดับ

2.4 อุปสรรค (Threats) ภัยคุกคามทางไซเบอร์มีการพัฒนาและเปลี่ยนแปลงอย่างรวดเร็ว รวมถึงเทคนิคการโจมตีที่ซับซ้อนและยากต่อการตรวจจับ เช่น การโจมตีแบบ Phishing และ Advanced Persistent Threats (APTs) ทำให้การสร้างความตระหนักรู้ต้องอาศัยการอัปเดตข้อมูลและการฝึกอบรมที่ต่อเนื่อง ข้อจำกัดด้านงบประมาณและการขาดการสนับสนุนจากหน่วยงานที่เกี่ยวข้องในการปรับปรุงโครงสร้างพื้นฐานทางเทคโนโลยี ยิ่งเพิ่มความเสี่ยงต่อการถูกโจมตี นอกจากนี้ ความเข้าใจที่ยังไม่เพียงพอของกำลังพลบางส่วนเกี่ยวกับความสำคัญของการป้องกันข้อมูลและความปลอดภัยทางไซเบอร์ยังเป็นอุปสรรคที่ต้องเร่งแก้ไข

จากผลการวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ด้วย PMESII และ SWOT Analysis ดังกล่าวจึงสามารถนำข้อมูลมาดำเนินการสร้างกลยุทธ์ด้วย TOWS Matrix ดังนี้

แนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก

นำ TOWS Matrix มาวิเคราะห์เพื่อหากลยุทธ์และแนวทางการส่งเสริมการตระหนักรู้ได้ดังนี้

1. กลยุทธ์เชิงรุก (SO Strategies) ใช้จุดแข็งเพื่อคว้าโอกาส กลยุทธ์เชิงรุกมุ่งเน้นการใช้ทรัพยากรและความได้เปรียบเชิงโครงสร้างของกองทัพบกเพื่อพัฒนาและส่งเสริมการตระหนักรู้ด้านอาชญากรรมทางไซเบอร์ โดยมีแนวทางดังนี้

1.1 การพัฒนาเครือข่ายความร่วมมือระหว่างประเทศและภาคส่วนที่เกี่ยวข้อง การรับมือกับอาชญากรรมทางไซเบอร์ไม่สามารถดำเนินการโดยลำพังได้ กองทัพบกจึงต้องใช้จุดแข็งของโครงสร้างการบังคับบัญชาและศูนย์เฝ้าระวังไซเบอร์ (S) ควบคู่กับโอกาสจากความร่วมมือทางยุทธศาสตร์กับประเทศพันธมิตร (O) เช่น สหรัฐอเมริกา ญี่ปุ่น และอาเซียน ในการจัดทำ MOU ด้านการฝึกอบรมและแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ โดยใช้จุดแข็งด้านนโยบายความมั่นคงที่มีอยู่เป็นพื้นฐานเพื่อจัดทำแพลตฟอร์มแลกเปลี่ยนข้อมูลภัยคุกคามในระดับสากล การสร้างโครงการฝึกอบรมร่วมและการแบ่งปันแนวปฏิบัติที่ดีที่สุด (Best Practices) ระหว่างหน่วยงานด้านความมั่นคงของประเทศต่าง ๆ จะช่วยเพิ่มขีดความสามารถในการรับมือกับภัยคุกคามที่มีความซับซ้อนนอกจากนี้ การร่วมมือกับภาคเอกชนและสถาบันวิจัยสามารถนำไปสู่การพัฒนาศูนย์ข้อมูล Big Data และ AI สำหรับการวิเคราะห์ภัยคุกคาม ซึ่งช่วยให้กำลังพลสามารถเข้าถึงข้อมูลความเสี่ยงทางไซเบอร์แบบเรียลไทม์ระหว่างหน่วยงานรัฐและกองทัพ

1.2 การลงทุนในเทคโนโลยีป้องกันภัยเชิงรุก สามารถใช้จุดแข็งด้านโครงสร้างพื้นฐานทางเทคโนโลยีที่ทันสมัย เช่น ศูนย์ปฏิบัติการด้านไซเบอร์ (Cyber Operations Center) และระบบ Cloud Computing ในการจัดทำโปรแกรมฝึกอบรมที่มีประสิทธิภาพ โดยอาศัยโอกาสจากการสนับสนุนงบประมาณด้านความมั่นคงทางไซเบอร์ที่เพิ่มขึ้นตามยุทธศาสตร์ชาติ 20 ปี ซึ่งกองทัพบกสามารถใช้งบประมาณที่ได้รับการสนับสนุนจากแผนยุทธศาสตร์ชาติ (O) ในการพัฒนาระบบป้องกันภัยไซเบอร์อัจฉริยะ (AI-based Threat Detection, Zero Trust Security Systems, และ Cyber Threat Intelligence Platform) เพื่อตรวจจับและป้องกันการโจมตีที่ซับซ้อนล่วงหน้า อีกทั้งยังควรจัดตั้ง Cyber Range หรือ สนามฝึกจำลองภัยคุกคามไซเบอร์ เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถฝึกซ้อมการรับมือกับการโจมตีที่สมจริง

1.3 การรุกเชิงข้อมูลและการสื่อสาร การใช้ฐานข้อมูลข่าวกรองไซเบอร์เพื่อเฝ้าติดตามแนวโน้มภัยคุกคาม (T) จะช่วยให้สามารถพัฒนา Intranet-Based Threat Sharing System เพื่อส่งข้อมูลภัยคุกคามล่าสุดไปยังหน่วยงานภายในกองทัพได้อย่างรวดเร็ว

1.4 พัฒนาหลักสูตรฝึกอบรมเฉพาะทาง

1.4.1 ยกระดับความรู้และทักษะด้านความปลอดภัยไซเบอร์ให้กับกำลังพล โดยเฉพาะในส่วนที่ใช้ระบบออนไลน์ทางทหาร

1.4.2 จัดทำหลักสูตรการอบรมแบบ E-Learning และ Cyber Range ที่ครอบคลุมประเด็นการป้องกันภัยคุกคามทางไซเบอร์แบบเชิงรุก เช่น การวิเคราะห์ Malware การตอบสนองต่อภัยคุกคาม กฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์และมาตรการป้องกันที่สอดคล้องกับกฎหมายระหว่างประเทศ โดยใช้ทรัพยากรทางการศึกษาของกองทัพบกที่มีอยู่ให้กับกำลังพล

2. กลยุทธ์เชิงป้องกัน (ST Strategies) เตรียมพร้อมรับมือกับการเปลี่ยนแปลงทางเทคโนโลยีและสภาพแวดล้อมด้านความมั่นคง โดยมีแนวทางดังนี้

2.1 การจัดทำมาตรการป้องกันแบบครอบคลุม เพื่อแก้ไขข้อจำกัดด้านงบประมาณและบุคลากรที่เชี่ยวชาญ (W) กองทัพบกสามารถใช้ความร่วมมือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (O) เพื่อเข้าถึง โครงการฝึกอบรมด้านไซเบอร์ระดับนานาชาติที่ไม่มีค่าใช้จ่าย นอกจากนี้ควรพัฒนาระบบ Data Encryption และ Access Control ที่เข้มงวดมากขึ้น รวมถึง Multi-Factor Authentication (MFA) เพื่อลดความเสี่ยงจากการบุกรุกทางไซเบอร์ รวมถึงการใช้ AI และระบบ Threat

Intelligence ที่มีอยู่ในกองทัพบกในการตรวจจับพฤติกรรมที่ผิดปกติและป้องกันการโจมตีแบบ APT (Advanced Persistent Threat) โดยเฉพาะจากประเทศคู่แข่งและกลุ่มแฮกเกอร์ที่มีศักยภาพสูง

2.2 การเสริมสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ กองทัพบกควรจัดทำ โครงการอบรมเชิงปฏิบัติการ ที่ให้ความสำคัญกับสถานการณ์ภัยคุกคามที่เกิดขึ้นจริง เช่น Capture the Flag (CTF) และ Cyber Drill และการจัดตั้งทีม CERT (Computer Emergency Response Team) ทีมเฉพาะกิจด้านไซเบอร์ที่มีความสามารถในการรับมือและตอบสนอง ต่อเหตุการณ์ไซเบอร์แบบเรียลไทม์ โดยอาศัยจุดแข็งด้านทรัพยากรบุคคลที่มีความเชี่ยวชาญทางเทคนิค

2.3 การประเมินความเสี่ยงและการทดสอบเจาะระบบ (Penetration Testing) จัดทำการทดสอบเจาะระบบและการประเมินความเสี่ยงไซเบอร์เป็นระยะเพื่อตรวจสอบช่องโหว่และปิดจุดอ่อน โดยใช้ทีมงานด้าน IT Security ของกองทัพบกที่มีอยู่เป็นแกนหลักในการดำเนินงาน

3. กลยุทธ์เชิงรับ (WT Strategy) บริหารจัดการทรัพยากรอย่างมีประสิทธิภาพท่ามกลางข้อจำกัด โดยมีแนวทางดังนี้

3.1 การเสริมสร้างความมั่นคงของระบบสารสนเทศ การนำมาตรฐาน ISO/IEC 27001 และ NIST Cybersecurity Framework มาใช้ จะช่วยให้กองทัพสามารถบริหารความเสี่ยงทางไซเบอร์ได้อย่างมีระบบ วางแผนรับมือกับเหตุการณ์ที่อาจเกิดขึ้นจากการโจมตีไซเบอร์ เช่น การสำรองข้อมูลและ Disaster Recovery Plan โดยใช้การบริหารความเสี่ยงเป็นเครื่องมือหลัก

3.2 การประเมินและแก้ไขช่องโหว่ด้านบุคลากร จัดทำแบบสอบถามการประเมินทัศนคติของกำลังพลด้านความปลอดภัยไซเบอร์ และจัดอบรมเพื่อปิดช่องโหว่ด้านบุคลากร ทุกระดับที่ขาดความเข้าใจในเรื่องอาชญากรรมทางไซเบอร์

3.3 การพัฒนาโครงสร้างพื้นฐานและเทคโนโลยีป้องกันภัยล่วงหน้า

3.3.1 กองทัพควรลงทุนใน Cloud Security, AI-driven Security Operations Center (SOC), และ Security Information and Event Management (SIEM) เพื่อตรวจจับและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ

3.3.2 ลงทุนในเทคโนโลยีป้องกันการโจมตีแบบ DDoS และการกรองข้อมูลที่เป็นอันตราย

3.3.3 พัฒนาศูนย์ข้อมูลสำรอง (Backup Data Center) เพื่อรับมือกับเหตุการณ์ฉุกเฉิน

4. กลยุทธ์เชิงแก้ไข (WO Strategy) มุ่งปรับปรุงการจัดการหลักสูตรและระบบการประเมินผล โดยมีแนวทางดังนี้

4.1 การพัฒนาทักษะกำลังพลด้านไซเบอร์

4.1.1 ควรจัดทำโครงการ Upskill และ Reskill ให้กับกำลังพล โดยอาศัยโอกาสจากการสนับสนุนงบประมาณการฝึกอบรมจากยุทธศาสตร์ชาติ เพื่อเพิ่มขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์

4.1.2 สร้างหลักสูตร Smart Soldier ที่มีเนื้อหาเกี่ยวกับการป้องกันภัยไซเบอร์และการรับมือเหตุการณ์แฮ็กเกอร์เจาะระบบ และจัดทำการฝึกซ้อมสถานการณ์ (Cyber Drill) เป็นประจำเพื่อเตรียมความพร้อมและประเมินศักยภาพการตอบสนองต่อภัยคุกคาม

4.1.3 เสริมสร้างความรู้และตระหนักรู้ทางไซเบอร์ให้กับกำลังพลและครอบครัวจัดทำคอร์สออนไลน์และเวิร์กช็อปเกี่ยวกับการรับมือกับ Fake News และ Social Engineering ผลักดันการใช้สื่อออนไลน์อย่างปลอดภัยในหน่วยงานทหาร โดยจัดทำแนวทางปฏิบัติ (Guideline) ที่ชัดเจน

4.2 การปรับปรุงระบบการบริหารจัดการความรู้ (Knowledge management)

4.2.1 พัฒนาระบบ KM และฐานข้อมูลภัยคุกคามไซเบอร์เพื่อให้กำลังพลเข้าถึงข้อมูลและแนวทางการรับมือได้สะดวกยิ่งขึ้น โดยใช้ประโยชน์จากโอกาสด้านเทคโนโลยีสารสนเทศที่กำลังเติบโต

4.2.2 พัฒนาระบบป้องกันและตรวจจับภัยคุกคามในธุรกรรมออนไลน์ (Threat Detection Systems) และจัดทำคู่มือป้องกันการหลอกลวงทางไซเบอร์ให้กับกำลังพล

4.2.3 ส่งเสริมความร่วมมือระหว่างกองทัพและสถาบันการเงินในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

4.3 การปรับปรุงกฎหมายและระเบียบด้านไซเบอร์ สนับสนุนการแก้ไขและปรับปรุงกฎหมายไซเบอร์ รวมถึงมาตรการป้องกันและลงโทษ เพื่อให้สอดคล้องกับมาตรฐานสากลและรองรับภัยคุกคามรูปแบบใหม่

4.4 การจัดตั้งทีมตอบสนองต่อเหตุการณ์ภัยคุกคาม (Cyber Incident Response Team (CIRT)) CIRT ควรมีแนวทางปฏิบัติที่ชัดเจนสำหรับการตอบสนองต่อเหตุการณ์ เช่น การกักกันภัยคุกคาม การกู้คืนข้อมูล และการสื่อสารภายในหน่วยงาน

4.5 การวิเคราะห์หลังเหตุการณ์และการเรียนรู้จากภัยคุกคาม การใช้ Root Cause Analysis (RCA) และการจัดทำ Lessons Learned Report จะช่วยให้กองทัพสามารถปรับปรุงมาตรการป้องกันให้มีประสิทธิภาพมากขึ้น

จากการวิเคราะห์ TOWS Matrix ในขั้นต้น ทำให้ได้แนวทางการส่งเสริมการตระหนักรู้ในการป้องกันอาชญากรรมทางไซเบอร์ ซึ่งผู้วิจัยเลือกกลยุทธ์เชิงรุก มาเป็นแนวทางพัฒนาเสริมสร้างการป้องกันและเน้นการบูรณาการทรัพยากร บุคลากร และเทคโนโลยี เนื่องจากเป็นกลยุทธ์ที่ดีที่สุด คุ้มค่า และเป็นไปได้มากที่สุด สามารถบูรณาการจุดแข็งของกองทัพบก เช่น โครงสร้างการบังคับบัญชาและศูนย์ไซเบอร์ เข้ากับโอกาสจากนโยบายชาติและความร่วมมือระหว่างประเทศ เพื่อพัฒนาการตระหนักรู้และป้องกันภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพและรวดเร็ว กลยุทธ์นี้ไม่เพียงตอบโจทย์ความจำเป็นเร่งด่วนในการรับมือภัยคุกคามที่เพิ่มขึ้น แต่ยังสอดคล้องกับทิศทางการพัฒนาความมั่นคงไซเบอร์ของกองทัพบกในระยะยาว ทำให้เป็นทางเลือกที่เหมาะสมที่สุดในบริบทปัจจุบัน โดยมีเหตุผลสนับสนุนกลยุทธ์เชิงรุก (SO Strategies) ดังนี้

1. กลยุทธ์เชิงรุกมุ่งเน้นการใช้ทรัพยากรที่มีอยู่แล้วของกองทัพบก เช่น โครงสร้างการบังคับบัญชาที่เข้มแข็ง (Strengths) และศูนย์ไซเบอร์ที่มีบทบาทในการเฝ้าระวังและวิเคราะห์ภัยคุกคาม เพื่อพัฒนาการตระหนักรู้และป้องกันภัยคุกคามไซเบอร์โดยไม่จำเป็นต้องลงทุนใหม่ในระดับสูง ตัวอย่างเช่น การพัฒนาหลักสูตรฝึกอบรมผ่านระบบ e-Learning และ Cyber Range สามารถใช้โครงสร้างพื้นฐานเทคโนโลยีที่มีอยู่ให้เกิดประโยชน์สูงสุด อีกทั้งการร่วมมือกับภาครัฐและเอกชน รวมถึงพันธมิตรระหว่างประเทศ (Opportunities) เช่น การทำ MOU กับสหรัฐอเมริกา ญี่ปุ่น หรือประเทศในอาเซียน ช่วยลดภาระงบประมาณในการจัดหาเทคโนโลยีใหม่หรือจัดการฝึกอบรมขนาดใหญ่ วิธีนี้ยังช่วยให้กองทัพบกสามารถเข้าถึงทรัพยากรและความรู้จากภายนอกได้โดยไม่ต้องแบกรับค่าใช้จ่ายทั้งหมดด้วยตนเอง

2. กองทัพบกมีจุดแข็งในด้านโครงสร้างการบังคับบัญชาที่เข้มแข็งและระเบียบวินัย รวมถึงหน่วยไซเบอร์เฉพาะทาง เช่น ศูนย์ปฏิบัติการด้านไซเบอร์ (CSOC) ซึ่งสามารถเริ่มดำเนินการตามกลยุทธ์ได้ทันที โดยไม่ต้องรอการจัดตั้งโครงสร้างใหม่ทั้งหมด นอกจากนี้ บุคลากรที่มีความรู้พื้นฐานด้านไซเบอร์อยู่แล้วสามารถถูกยกระดับ

ทักษะผ่านการฝึกอบรมเชิงรุกได้อย่างรวดเร็ว อีกทั้งยังได้รับการสนับสนุนจากนโยบายตามยุทธศาสตร์ชาติ 20 ปี และนโยบายกองทัพบก ปี 2568 เน้นการพัฒนาความมั่นคงทางไซเบอร์เป็นลำดับต้น ๆ ซึ่งหมายถึงมีทั้งงบประมาณและการสนับสนุนจากผู้บริหารระดับสูงอย่างเพียงพอ การที่กลยุทธ์นี้สอดคล้องกับนโยบายดังกล่าวทำให้การผลักดันและการอนุมัติโครงการต่าง ๆ มีโอกาสสำเร็จสูง

3. โครงสร้างการบังคับบัญชาของกองทัพบกที่เข้มแข็ง ช่วยให้การถ่ายทอดความรู้และการฝึกอบรมเป็นไปอย่างมีประสิทธิภาพและครอบคลุมกำลังพลทุกระดับ ตัวอย่างเช่น การจัดฝึกซ้อมสถานการณ์จำลอง (Cyber Drills) หรือการพัฒนา Intranet-Based Threat Sharing System สามารถกระจายข้อมูลภัยคุกคามได้อย่างรวดเร็วผ่านช่องทางที่มีอยู่แล้ว รวมถึงการเติบโตของเทคโนโลยีสารสนเทศ เช่น AI และ Big Data และความร่วมมือระหว่างประเทศ เปิดโอกาสให้กองทัพบกเข้าถึงข้อมูลและเทคนิคการป้องกันที่ทันสมัย เช่น การใช้ AI-based Threat Detection หรือการแลกเปลี่ยน Best Practices กับมิตรประเทศ ซึ่งช่วยยกระดับขีดความสามารถในการรับมือภัยคุกคามได้อย่างมีประสิทธิภาพ

4. การฝึกอบรมเชิงรุก เช่น การจำลองการโจมตีแบบ Phishing หรือการใช้เทคโนโลยีป้องกันภัย เช่น Firewall และ Intrusion Detection Systems (IDSs) ช่วยลดความเสี่ยงจากการโจมตีไซเบอร์ได้ทันที ข้อมูลในเอกสารระบุว่าการฝึกอบรมแบบ Phishing Simulation ลดอัตราการตกเป็นเหยื่อได้ถึง 64.81% ซึ่งแสดงถึงประสิทธิภาพที่วัดผลได้ และตอบสนองต่อภัยคุกคาม ด้วยการจัดตั้ง Cyber Range เพื่อฝึกซ้อมสถานการณ์สมจริง และการพัฒนาระบบแจ้งเตือนภัยผ่านฐานข้อมูลข่าวกรอง ช่วยให้กำลังพลสามารถรับมือกับภัยคุกคามได้อย่างรวดเร็วและแม่นยำ โดยเฉพาะในสถานการณ์ภัยคุกคามต่าง ๆ เช่น การโจมตีแบบ APTs หรือแก๊งคอลเซ็นเตอร์ ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่องในปัจจุบัน

จากการวิเคราะห์โดยใช้เครื่องมือ TOWS Matrix ในกลุ่มกลยุทธ์เชิงรุก (SO Strategies) ซึ่งมุ่งเน้นการใช้จุดแข็งภายในของกองทัพบกควบคู่กับโอกาสจากปัจจัยภายนอก สามารถเสนอแนวทางการส่งเสริมความตระหนักรู้ด้านอาชญากรรมทางไซเบอร์สำหรับกำลังพลได้อย่างเป็นระบบ โดยมีแนวทางสำคัญดังนี้

1. กองทัพบกควรพัฒนาเครือข่ายความร่วมมือกับประเทศมิตรประเทศและหน่วยงานที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ เช่น สหรัฐอเมริกา ญี่ปุ่น และกลุ่มประเทศอาเซียน โดยจัดทำบันทึกข้อตกลงความร่วมมือ (MOU) ด้านการฝึกอบรม การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ และการแบ่งปันแนวปฏิบัติที่ดี

ร่วมกัน เพื่อยกระดับขีดความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามอย่างมีประสิทธิภาพ นอกจากนี้ ควรเปิดกว้างในการทำงานร่วมกับภาคเอกชนและสถาบันวิจัย เพื่อร่วมพัฒนาระบบ Big Data และปัญญาประดิษฐ์ (AI) ที่ใช้ในการวิเคราะห์ข้อมูลภัยคุกคามแบบเรียลไทม์

2. ควรเพิ่มการลงทุนในเทคโนโลยีที่ใช้ป้องกันภัยไซเบอร์ล่วงหน้า โดยใช้จุดแข็งของศูนย์ปฏิบัติการไซเบอร์ (Cyber Operations Center) และระบบ Cloud Computing ที่มีอยู่เดิม ร่วมกับการใช้งบประมาณที่ได้รับการสนับสนุนตามแผนยุทธศาสตร์ชาติ 20 ปี เพื่อพัฒนาระบบป้องกันภัยอัจฉริยะ เช่น ระบบตรวจจับภัยคุกคามโดยใช้ AI ระบบรักษาความปลอดภัยแบบ Zero Trust และแพลตฟอร์มข่าวกรองภัยคุกคามไซเบอร์ รวมถึงการจัดตั้งสนามฝึกจำลองสถานการณ์ภัยไซเบอร์ (Cyber Range) เพื่อให้กำลังพลสามารถฝึกซ้อมรับมือกับภัยคุกคามเสมือนจริงได้อย่างมีประสิทธิภาพ

3. ควรส่งเสริมการใช้ข้อมูลข่าวกรองไซเบอร์อย่างเป็นระบบ โดยจัดทำระบบส่งต่อข้อมูลภัยคุกคามภายในองค์กรผ่านเครือข่าย Intranet ของกองทัพ เพื่อให้หน่วยงานต่าง ๆ สามารถเข้าถึงข้อมูลภัยคุกคามล่าสุดได้อย่างรวดเร็วและทั่วถึง ช่วยเพิ่มความตระหนักรู้และความพร้อมในการป้องกันภัย

4. ควรพัฒนาหลักสูตรการฝึกอบรมเฉพาะทางที่เหมาะสมกับบริบทของกองทัพ โดยเฉพาะในหน่วยที่ใช้ระบบออนไลน์ทางทหารอย่างเข้มข้น อาทิ การจัดทำหลักสูตรแบบ e-Learning และการฝึกผ่าน Cyber Range ที่ครอบคลุมทั้งด้านเทคนิค เช่น การวิเคราะห์มัลแวร์ การตอบสนองต่อเหตุการณ์ไซเบอร์ รวมถึงด้านกฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ทั้งในประเทศและระดับสากล โดยใช้ทรัพยากรทางการศึกษาที่กองทัพมีอยู่ให้เกิดประโยชน์สูงสุด

เพื่อให้การดำเนินงานสามารถประเมินผลและพัฒนาอย่างต่อเนื่องได้ ผู้วิจัยขอเสนอให้มีการจัดทำ

1. โครงการนำร่องการอบรมแบบไฮบริดในระดับกรมหรือระดับเทียบเท่า โดยจัดการฝึกอบรมทั้งในรูปแบบออนไลน์และพบหน้า (On-site) ควบคู่กัน เพื่อให้สามารถเข้าถึงได้อย่างทั่วถึง และเปิดโอกาสให้กำลังพลจากหลากหลายพื้นที่สามารถเข้าร่วมได้ตามความเหมาะสมของบริบทการปฏิบัติงาน

2. กำหนดตัวชี้วัดหลักด้านความตระหนักรู้ไซเบอร์ (Cybersecurity Awareness KPIs) สำหรับแทรกไว้ในสายงานปกติ เช่น สัดส่วนการเข้าร่วมอบรม ความรู้

ก่อน-หลัง อบรม ระดับความสามารถในการตอบสนองต่อสถานการณ์จำลอง รวมถึงพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้สามารถติดตามและประเมินผลการดำเนินงานได้อย่างเป็นรูปธรรม และนำไปสู่การวางแผนพัฒนาระยะยาวในภาพรวมของกองทัพบกต่อไป

บทที่ 4
บทอภิปรายผล

การอภิปรายผลการวิเคราะห์ในบทที่ 3 โดยเน้นการเชื่อมโยงผลลัพธ์กับแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง (เช่น Crime Triangle Theory, Protection Motivation Theory, Self-Actualization Theory และ Routine Activity Theory) พร้อมทั้งประเมินความสอดคล้องของเป้าหมายของยุทธศาสตร์ชาติ 20 ปี สมุดปกขาวกองทัพบก พ.ศ. 2567 และนโยบายกองทัพบก พ.ศ. 2568 เพื่อยืนยันความน่าเชื่อถือของแนวทางวิจัยและเสนอข้อเสนอแนะที่เหมาะสมสำหรับการพัฒนาในอนาคต

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสถานการณ์ความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ที่เป็นภัยคุกคามต่อกำลังพลกองทัพบก ปัจจัยที่ส่งผลต่อการตระหนักรู้ และแนวทางการส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ โดยผลการวิเคราะห์แสดงให้เห็นว่าอาชญากรรมทางไซเบอร์เป็นภัยคุกคามที่มีความซับซ้อนและทวีความรุนแรงมากขึ้น ซึ่งส่งผลกระทบต่อความมั่นคงและการปฏิบัติงานของกองทัพบก

สถานการณ์ความรู้เรื่องอาชญากรรมทางไซเบอร์ที่เป็นภัยคุกคามต่อกำลังพลกองทัพบกในปัจจุบัน

ผลการวิจัยพบว่าภัยคุกคามทางไซเบอร์ เช่น การโจมตีแบบฟิชชิ่ง (Phishing), การใช้มัลแวร์ (Malware), และการโจมตีแบบต่อเนื่องขั้นสูง (Advanced Persistent Threats: APTs) มีแนวโน้มเพิ่มสูงขึ้น โดยเฉพาะในช่วงหลังการระบาดของโควิด-19 ซึ่งมีการใช้งานอินเทอร์เน็ตและอุปกรณ์ดิจิทัลเพิ่มมากขึ้น ภัยคุกคามเหล่านี้ไม่เพียงแต่ส่งผลต่อความปลอดภัยของข้อมูล แต่ยังส่งผลกระทบต่อ โครงสร้างการบังคับบัญชาและความน่าเชื่อถือของกองทัพบก การขาดความรู้และทักษะในการรับมือกับภัยคุกคามไซเบอร์ทำให้กำลังพลมีความเสี่ยงสูง ต่อการตกเป็นเหยื่อของการโจมตีไซเบอร์ ซึ่งสอดคล้องกับงานวิจัยต่าง ๆ ดังนี้

1. สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี ที่ระบุว่าการขาดการจำลองสถานการณ์จริงส่งผลให้กำลังพลไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ และเมื่อมีการจัดอบรมเชิงปฏิบัติ อัตราการตกเป็นเหยื่อของการโจมตีลดลงถึง 64.81%[29]

2. ฐกฤต แก้วทับทิม ในช่วงการระบาดของโควิด-19 องค์กรอาชญากรรมไซเบอร์ มีการขยายตัวอย่างรวดเร็ว ส่งผลให้รูปแบบการโจมตี เช่น Phishing, Malware,

และ Advanced Persistent Threats (APTs) มีความซับซ้อนมากขึ้น ส่งผลต่อความมั่นคงของข้อมูลภายในกองทัพ[8]

3. ชรินทร์ทิพย์ ปั้นสุวรรณ องค์กรที่ขาดมาตรการป้องกันและขาดระบบตรวจสอบภัยคุกคามอย่างมีประสิทธิภาพ มีแนวโน้มตกเป็นเป้าหมายของแฮกเกอร์มากขึ้น[24]

4. ภาคิน หวังสถิธรรม การหลอกลวงผ่านโทรศัพท์เป็นภัยไซเบอร์ที่กำลังพลต้องเผชิญซึ่งส่งผลต่อความปลอดภัยของข้อมูลและความมั่นคงทางการทหาร[31]

5. Smith et al. การขาดการฝึกอบรมด้านไซเบอร์ในกองกำลังทางทหารนำไปสู่ความเสี่ยงที่เพิ่มขึ้นต่อการโจมตีแบบฟิชชิ่งและการใช้มัลแวร์[28]

6. RAND Corporation ระบบป้องกันแบบดั้งเดิมไม่เพียงพอในการป้องกันภัยคุกคามที่พัฒนาขึ้นอย่างต่อเนื่อง ทำให้กองกำลังทางทหารต้องปรับใช้ การตรวจจับภัยคุกคามแบบเรียลไทม์ และการวิเคราะห์เชิงคาดการณ์ (Predictive Analysis) เพื่อป้องกันภัยคุกคามไซเบอร์[37]

จากข้อมูลเหล่านี้สามารถสรุปได้ว่า กองทัพบกไทยจำเป็นต้องมีแนวทางในการเพิ่มความรู้และความตระหนักรู้เรื่องภัยไซเบอร์ให้กับกำลังพลเพื่อให้สามารถรับมือกับสถานการณ์ที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ

ปัจจัยที่ส่งผลต่อการตระหนักรู้ในเรื่องอาชญากรรมทางไซเบอร์ของกำลังพลกองทัพบก

จากการวิเคราะห์พบว่าปัจจัยหลักที่ส่งผลต่อการตระหนักรู้ประกอบด้วย การฝึกอบรมและการพัฒนาความรู้ กำลังพลที่ไม่ได้รับการฝึกอบรมอย่างเพียงพอมักขาดความเข้าใจในภัยคุกคามทางไซเบอร์วัฒนธรรมองค์กรด้านความปลอดภัย หน่วยงานที่มีวัฒนธรรมเน้นความปลอดภัยมีแนวโน้มที่บุคลากรจะตระหนักถึงความสำคัญของการป้องกันมากกว่าการใช้เทคโนโลยี การเข้าถึงเครื่องมือป้องกันที่ทันสมัยช่วยเพิ่มความสามารถในการรับมือนโยบายและการสนับสนุนการขาดนโยบายที่ชัดเจนเป็นอุปสรรคต่อการสร้างความตระหนักรู้ ซึ่งสอดคล้องกับงานวิจัยต่าง ๆ ดังนี้

1. กิติยา วิสิฐพงศ์พันธ์ และคณะ พบว่าการส่งเสริมความตระหนักรู้เกี่ยวกับภัยไซเบอร์สามารถทำได้โดย การอบรม, การให้ข้อมูลที่ชัดเจน, และการสร้างแรงจูงใจในองค์กร ซึ่งช่วยลดพฤติกรรมเสี่ยงจากการใช้งานระบบ[27]

2. ปรเมศวร์ กุมารบุญ ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์ พบว่าผู้ใช้งานที่ไม่เข้าใจความเสี่ยงของเทคโนโลยี มักตกเป็นเหยื่อของการโจมตีทางไซเบอร์มากกว่า[15]

3. Smith et al. ระบุว่าการจัดฝึกอบรมเชิงรุกช่วยลดโอกาสในการตกเป็นเหยื่อของภัยไซเบอร์ได้ถึง 40%[17]

4. Measuring Cybersecurity Awareness in a South African Military Sample พบว่าการให้กำลังพลเข้าร่วมหลักสูตรฝึกอบรมเป็นปัจจัยสำคัญในการเพิ่มระดับความตระหนักรู้[28]

5. Military Members are Disproportionately Affected by Cybercrime พบว่ากำลังพลทางทหารที่มีแนวทางปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่ชัดเจนมีอัตราการตกเป็นเหยื่อน้อยลง เนื่องจากสามารถใช้เทคโนโลยีป้องกันได้อย่างมีประสิทธิภาพ[38]

6. RAND Corporation พบว่ากองกำลังทางทหารที่มีแนวทางปฏิบัติและนโยบายที่ชัดเจนเกี่ยวกับการป้องกันภัยไซเบอร์ สามารถลดความเสี่ยงต่อการโจมตีจากภัยไซเบอร์ได้มากกว่าหน่วยงานที่ไม่มีนโยบายเป็นระบบ[37]

จากข้อมูลเหล่านี้สามารถสรุปได้ว่าการเพิ่มความตระหนักรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ในกำลังพลกองทัพบก จำเป็นต้องดำเนินการผ่านหลายปัจจัยร่วมกัน ทั้งการฝึกอบรม วัฒนธรรมองค์กร เทคโนโลยี และนโยบายที่ชัดเจนเพื่อให้เกิดการป้องกันที่มีประสิทธิภาพ

แนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก

ผลการวิเคราะห์ด้วยกรอบ TOWS Matrix ชี้ว่า แนวทางที่มีประสิทธิภาพสูงสุดคือการใช้กลยุทธ์เชิงรุก (SO Strategies) โดยใช้จุดแข็งของกองทัพบก เช่น โครงสร้างการบังคับบัญชาที่ชัดเจนและทรัพยากรที่มีอยู่ เพื่อคว้าโอกาสจากการพัฒนาเทคโนโลยีและความร่วมมือระหว่างหน่วยงาน แนวทางที่เสนอรวมถึงการพัฒนาการฝึกอบรม การสร้างวัฒนธรรมความปลอดภัย และการลงทุนในเทคโนโลยีป้องกันภัย ซึ่งสอดคล้องกับงานวิจัย

1. Smith et al. ระบุว่าการฝึกอบรมด้านไซเบอร์ช่วยลดโอกาสในการตกเป็นเหยื่อของภัยไซเบอร์ได้ถึง 40%[28]

2. Williams & Brown พบว่าการเปลี่ยนแปลงพฤติกรรมของบุคลากรเป็นปัจจัยสำคัญในการลดความเสี่ยงจากภัยไซเบอร์ โดยการฝึกอบรมและส่งเสริมวัฒนธรรมความปลอดภัยสามารถช่วยลดโอกาสตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้ถึง 60%[18]

3. Compton ชี้ให้เห็นว่าการใช้ Self-Actualization Theory สามารถช่วยเพิ่มแรงจูงใจในการปฏิบัติตามมาตรการด้านไซเบอร์ ทำให้บุคลากรมีความตระหนักและเข้าใจถึงผลกระทบของภัยไซเบอร์มากขึ้น[16]

4. Cyber Security: Promote Awareness for Bangladesh Army ยังเน้นถึงประสิทธิภาพของหลักสูตรฝึกอบรมที่ปรับให้เหมาะสมกับบริบททางทหาร เช่น e-Learning และ Cyber Range ที่ช่วยเสริมทักษะเชิงปฏิบัติ[20]

5. Military Cybersecurity: Policy, Practice, and Preparedness พบว่าองค์กรที่มี วัฒนธรรมด้านความปลอดภัยที่แข็งแกร่ง จะช่วยให้กำลังพลมีพฤติกรรมที่สอดคล้องกับแนวทางป้องกันภัยไซเบอร์ [38]

6. RAND Corporation (2022) การป้องกันภัยไซเบอร์ในระดับกองทัพต้องอาศัยความร่วมมือระหว่างภาครัฐและเอกชน เพื่อให้สามารถแลกเปลี่ยนข้อมูลภัยคุกคามและพัฒนามาตรการรับมือที่มีประสิทธิภาพ[37]

การส่งเสริมความตระหนักรู้ด้านไซเบอร์ให้กับกำลังพลกองทัพบกต้องอาศัยกลยุทธ์เชิงรุกที่รวมถึงการฝึกอบรม วัฒนธรรมองค์กร เทคโนโลยี นโยบาย และความร่วมมือระหว่างหน่วยงาน ซึ่งจะช่วยให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ผลการวิจัยนี้มีความสอดคล้องกับทฤษฎี นโยบาย และยุทธศาสตร์ระดับชาติต่าง ๆ ที่เกี่ยวข้องดังนี้

ผลการวิจัยสอดคล้องกับแนวคิดทฤษฎีการตระหนักรู้ในตนเอง โดยพบว่าการฝึกอบรมที่เน้นการสร้างความเข้าใจและแรงจูงใจช่วยให้กำลังพลปรับเปลี่ยนพฤติกรรมการใช้เทคโนโลยีให้ปลอดภัยยิ่งขึ้นที่ระบุว่าการตระหนักรู้ในตนเองเป็นปัจจัยสำคัญที่ช่วยปรับพฤติกรรมให้เหมาะสม และทฤษฎีสามเหลี่ยมอาชญากรรม ที่ชี้ว่า อาชญากรรมเกิดจาก “เหยื่อ”, “ผู้กระทำผิด” และ “โอกาส” ผลการวิจัยยืนยันว่า การลดโอกาส เช่น การเพิ่มการฝึกอบรมและมาตรการป้องกัน สามารถลดความเสี่ยงจากอาชญากรรมทางไซเบอร์ได้

อีกทั้งผลการวิจัยนี้ยังสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี ที่เน้นการเสริมสร้างความมั่นคงและการพัฒนาทรัพยากรมนุษย์ให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์ การวิจัยนี้ตอบสนองต่อเป้าหมายดังกล่าวโดยเสนอแนวทางการพัฒนาความรู้และทักษะของกำลังพล รวมถึงแผนปฏิบัติราชการของกระทรวงกลาโหมและกองทัพบก แผนนี้ให้ความสำคัญกับการพัฒนาศักยภาพด้านความปลอดภัยไซเบอร์ ซึ่งสอดคล้องกับ

ข้อเสนอแนะของการวิจัยในการพัฒนาการฝึกอบรมและเทคโนโลยีป้องกันภัย และสมุดปกขาวเน้นการป้องกันภัยคุกคามไซเบอร์และการใช้เทคโนโลยีทันสมัย ซึ่งสนับสนุนแนวทางการลงทุนในระบบป้องกันและการฝึกอบรมที่ทันสมัยตามที่วิจัยนี้เสนอ

บทที่ 5
บทสรุปและข้อเสนอแนะ

จากการวิจัยในหัวข้อ “แนวทางส่งเสริมการตระหนักรู้เรื่องการป้องกันอาชญากรรมทางไซเบอร์ให้กับกำลังพลกองทัพบก” ผลการวิเคราะห์พบว่าอาชญากรรมทางไซเบอร์เป็นภัยคุกคามที่รุนแรงและมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยช่องโหว่หลักมาจากพฤติกรรมเสี่ยงและการขาดการฝึกอบรมที่เพียงพอของกำลังพลในองค์กร ซึ่งสอดคล้องกับหลักการในทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ที่ระบุว่าการเกิดอาชญากรรมจะขึ้นอยู่กับองค์ประกอบ “เหยื่อ”, “ผู้กระทำความผิด” และ “โอกาส” ที่มีอยู่ในสภาพแวดล้อมไซเบอร์ ความรู้ที่ได้รับจากงานวิจัยและกรอบแนวคิดที่ใช้ (Self-Actualization Theory, Protection Motivation Theory, Routine Activity Theory) ช่วยให้สามารถระบุข้อสรุปและแนวทางแก้ไขปัญหาได้ชัดเจนและเป็นระบบ

สรุปผลการวิจัย

งานวิจัยนี้ได้ดำเนินการศึกษาและวิเคราะห์สถานการณ์ด้านความปลอดภัยไซเบอร์ในกำลังพลกองทัพบกผ่านการประเมินองค์ประกอบและความสัมพันธ์ของปัจจัยที่มีผลต่อการตระหนักรู้และการป้องกันภัยไซเบอร์ ซึ่งได้รับการสนับสนุนจากวรรณกรรมทั้งในระดับทฤษฎีและงานวิจัยภาคสนาม ผลการวิเคราะห์ในบทที่ 3 และการอภิปรายในบทที่ 4 ยืนยันว่า

สถานการณ์ภัยคุกคาม ปัจจัยที่ส่งผลให้เกิดความเสี่ยงในองค์กรมาจากบุคลากรที่ขาดการฝึกอบรมด้านไซเบอร์ พบว่า 78% ของกรณีโจมตีเกิดจากช่องโหว่ที่เกิดจากพฤติกรรมที่ไม่ปลอดภัย เช่น การใช้รหัสผ่านที่ไม่ดีและการไม่ตรวจสอบ URL ก่อนคลิก ซึ่งสอดคล้องกับรายงานของสำนักงานตำรวจแห่งชาติ[6]

ปัจจัยที่มีผลต่อการตระหนักรู้ การฝึกอบรมและการจำลองสถานการณ์ฟิชชิ่ง (Phishing Simulation) ลดความเสี่ยงจากการตกเป็นเหยื่อได้ถึง 64.81% นอกจากนี้การใช้แรงจูงใจตาม Self-Actualization Theory ยังช่วยเพิ่มระดับการตระหนักรู้ได้ถึง 40%

แนวทางส่งเสริมการตระหนักรู้ การจัดทำหลักสูตรฝึกอบรมเชิงรับและเชิงรุกโดยมีบทบาทของศูนย์ไซเบอร์กองทัพบก (CSOC) รวมถึงการใช้ระบบ Intrusion Detection

Systems (IDSs) และการฝึกอบรมซ้ำอย่างต่อเนื่อง สามารถเพิ่มขีดความสามารถในการป้องกันภัยไซเบอร์ในระดับองค์กรได้อย่างมีประสิทธิภาพ

การเชื่อมโยงกับยุทธศาสตร์ชาติและนโยบาย ผลงานวิจัยนี้สอดคล้องกับเป้าหมายที่ระบุไว้ในยุทธศาสตร์ชาติ 20 ปี, สมุดปกขาวกองทัพบก พ.ศ. 2567 และนโยบายกองทัพบก พ.ศ. 2568 เนื่องจากแนวทางที่นำเสนอเน้นการพัฒนากำลังพลและระบบพื้นฐานให้ทันสมัยและมีความยืดหยุ่นเพื่อตอบสนองต่อภัยไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว

ข้อเสนอแนะ

1. พัฒนาหลักสูตรฝึกอบรมและ e-Learning ให้มีความครอบคลุม ออกแบบหลักสูตรเฉพาะทางที่ตอบสนองต่อภัยไซเบอร์ทุกประเภท เช่น DDoS, Phishing, Malware, และ Cyber Forensics ที่เน้นทั้งด้านทฤษฎีและการปฏิบัติจริง และ สนับสนุนการใช้แพลตฟอร์ม e-Learning เพื่อให้กำลังพลในทุกพื้นที่มีการเรียนรู้อย่างต่อเนื่องและสามารถวัดผลการเรียนผ่านการทดสอบสถานการณ์จำลอง

2. เสริมสร้างแคมเปญการตระหนักรู้และฝึกซ้อมสถานการณ์ จัดทำแคมเปญประชาสัมพันธ์ผ่านสื่อหลายช่องทาง (บรรยาย, โปสเตอร์, เว็บไซต์) เพื่อเพิ่มความเข้าใจเกี่ยวกับภัยไซเบอร์ ควบคู่จัดการฝึกซ้อม Cyber Drills อย่างสม่ำเสมอ พื่อให้กำลังพลได้ทดลองรับมือกับเหตุการณ์ในสภาพแวดล้อมที่เสมือนจริง เพื่อเตรียมความพร้อมในการตอบสนองทันที

3. พัฒนาโครงสร้างพื้นฐานด้านไซเบอร์และลงทุนในเทคโนโลยี จัดตั้งและพัฒนาทีม CERT ให้มีความเชี่ยวชาญสูงในการตรวจจับและตอบสนองต่อเหตุการณ์ไซเบอร์ ควบคู่กับการลงทุนในเทคโนโลยีเบ็ดเสร็จ เช่น ระบบ Intrusion Detection and Prevention Systems (IDPSs), ซอฟต์แวร์ป้องกันไวรัสขั้นสูง, การเข้ารหัสข้อมูล และระบบคลาวด์ที่มีมาตรฐานความปลอดภัยสูง ตามนโยบายกองทัพบก พ.ศ. 2568

4. ส่งเสริมความร่วมมือระหว่างประเทศและภาคธุรกิจ สร้างเครือข่ายความร่วมมือกับพันธมิตรทางการทหารในระดับสากลและภาคเอกชน เพื่อแลกเปลี่ยนข้อมูลและแนวทางป้องกันภัยไซเบอร์ รวมถึงร่วมมือกับสถาบันการศึกษาเพื่อพัฒนาเครื่องมือและนวัตกรรมใหม่ ๆ ที่รองรับการป้องกันภัยไซเบอร์ในระดับชาติ

5. การประเมินผลและปรับปรุงแนวทางอย่างต่อเนื่อง จัดทำระบบประเมินทักษะและความรู้ด้วยการใช้ Penetration Testing และ Vulnerability Assessment อย่างต่อเนื่อง ใช้ข้อมูลจาก Post-Incident Analysis มาปรับปรุงและพัฒนาแนวทางการป้องกันให้ทันสมัยและสอดคล้องกับสภาวะแวดล้อมที่เปลี่ยนแปลงอยู่เสมอ

6. สร้างวัฒนธรรมองค์กรด้านความปลอดภัยไซเบอร์ ส่งเสริมให้กำลังพลมีนิสัยการใช้งานรหัสผ่านที่ปลอดภัยและปฏิบัติตามมาตรการความปลอดภัย การสร้างรางวัลหรือโปรโมชั่นสำหรับพนักงานที่ปฏิบัติอย่างครบถ้วนสามารถช่วยกระตุ้นให้เกิดวัฒนธรรมองค์กรที่เข้มแข็ง รวมทั้งตรวจสอบและปรับปรุงการใช้งานระบบอย่างสม่ำเสมอเพื่อรักษามาตรฐานด้านความปลอดภัยในทุกส่วน

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1. ศึกษาความเสี่ยงด้านไซเบอร์ที่เกิดจาก IoT และ 5G ควรมีการวิจัยเชิงลึกเกี่ยวกับ Internet of Things (IoT) และเครือข่าย 5G ที่เริ่มมีบทบาทมากขึ้นในกองทัพบก โดยเฉพาะความเสี่ยงด้าน Zero-Day Exploits และการโจมตีแบบ Distributed Denial of Service (DDoS)

2. วิเคราะห์พฤติกรรมของอาชญากรไซเบอร์ ศึกษาพฤติกรรมและแรงจูงใจของอาชญากรไซเบอร์ตาม ทฤษฎีเหตุผลในการเลือกก่ออาชญากรรม (Rational Choice Theory) เพื่อพัฒนาแนวทางป้องกันที่มีประสิทธิภาพมากขึ้น

3. ประเมินประสิทธิภาพของมาตรการป้องกันที่ใช้ AI วิจัยและประเมินผลการใช้ Artificial Intelligence (AI) ในการตรวจจับและตอบโต้ภัยคุกคาม โดยเปรียบเทียบกับมาตรการแบบเดิมเพื่อหาแนวทางที่เหมาะสมที่สุด

เอกสารอ้างอิง

1. สำนักนายกรัฐมนตรี. ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561 - 2580). ราชกิจจานุเบกษา เล่ม 135, ตอนที่ 82 ก (ลง 13 ตุลาคม 2561).

2. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. เอกสารประกอบ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2566 - 2580): (ฉบับแก้ไขเพิ่มเติม). กรุงเทพฯ: สำนักงาน; 2566.

3. กองทัพบก. แผนปฏิบัติราชการระยะ 5 ปี พ.ศ. 2566 - 2570 [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 22 กุมภาพันธ์ 2568]. เข้าถึงได้จาก: https://shorturl.asia/YRbr4

4. กองทัพบก. นโยบายการปฏิบัติงานกองทัพบก ประจำปี 2568.

5. กองทัพบก. สมุดปกขาวกองทัพบก พ.ศ. 2567 [อินเทอร์เน็ต]. 2567 [เข้าถึงเมื่อ 14 พฤศจิกายน 2567]. เข้าถึงได้จาก: https://shorturl.asia/Yt7Qy

6. สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา. 80 ล้านบาทต่อวัน! คนไทยสูญเงินให้แก๊งคอลเซ็นเตอร์ [อินเทอร์เน็ต]. 2025 [เข้าถึงเมื่อ 30 พฤศจิกายน 2567]. เข้าถึงได้จาก: https://shorturl.asia/LAjPc

7. วารสารสังคมศาสตร์เพื่อการพัฒนาท้องถิ่น, มหาวิทยาลัยราชภัฏมหาสารคาม. วารสารสังคมศาสตร์เพื่อการพัฒนาท้องถิ่น. 2567.

8. ฐกฤต แก้วทับทิม. การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์. 2564;7(1):55-72

9. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. การกระทำที่ถือเป็นความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2540 และที่ปรับปรุงแก้ไข พ.ศ. 2560. [อินเทอร์เน็ต]. 2564 [เข้าถึงเมื่อ 10 พ.ค. 2568]. เข้าถึงได้จาก: https://shorturl.asia/erV0Z

10. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 10 พ.ค. 2568]. เข้าถึงได้จาก: https://shorturl.asia/Fz2vO

11. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 10 พ.ค. 2568]. เข้าถึงได้จาก: https://shorturl.asia/us6kK

12. Thai News Agency. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 [[อินเทอร์เน็ต]. 2025 [เข้าถึงเมื่อ 10 พ.ค. 2568]. เข้าถึงได้จาก: https://shorturl.asia/NEmyR

13. Duval S, Wicklund RA. A Theory of Objective Self-Awareness. New York: Academic Press; 1972.

14. ธิติรัตน์ สมบูรณ์. รู้เท่าทันอาชญากรรมไซเบอร์. วารสารความมั่นคงไซเบอร์. 2566.

15. ปรเมศวร์ กุมารบุญ. ความสัมพันธ์ระหว่างการไร้ตัวตนกับอาชญากรรมไซเบอร์. [วิทยานิพนธ์ปริญญาเอก]. จุฬาลงกรณ์มหาวิทยาลัย; 2563.

16. Compton WC. The myth of self-actualization: What Maslow really said. J Humanist Psychol. 2018;58(1):1-18.

17. Smith A, et al. Enhancing cybersecurity awareness through motivation training programs. Cybersecurity Journal. 2021;6(3):55-70.

18. Williams J, Brown P. Reducing cybercrime risks in organizations through employee behavior modification. Int J Cyber Sec Policy. 2022;9(2):120-135.

19. Felson M, Clarke RV. Opportunity makes the thief: Practical theory for crime prevention. Policing and Society. 1998;5(1):37-55.

20. Cybersecurity Report 2023. The Impact of Password Management on Cybercrime Risks. Global Cybersecurity Institute; 2023.

21. Clarke RV, Cornish DB. Modeling offenders' decisions: A framework for research and policy. Crime Justice. 1985;6:147-185.

22. Garcia R, et al. AI-driven anomaly detection for cybersecurity risk mitigation. J Cyber Risk Manag. 2022;8(4):210-225.

23. Felson M, Clarke RV. Opportunity makes the thief: Practical theory for crime prevention. Policing and Society. 1998;5(1):37-55.

24. ชรินทร์ทิพย์ ปั้นสุวรรณ. แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. [ปริญญาศิลปศาสตรดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา]. จุฬาลงกรณ์มหาวิทยาลัย; 2565.

25. นวลน้อย ตรีรัตน์. ภัยคุกคามทางออนไลน์: ปัญหาและความท้าทาย. รายงานโครงการศึกษาสถานการณ์ภัยคุกคามทางออนไลน์. 2567.

26. Floyd DL, Prentice-Dunn S, Rogers RW. A meta-analysis of research on protection motivation theory. J Appl Soc Psychol. 2000;30(2):407–29.

27. กิติยา วิสิฐพงศ์พันธ์, ชูเกียรติ บุญก่อเกื้อ, กิตติพงศ์ อยู่นิรันดร, นลินภัสร์ บำเพ็ญเพียร. ปัจจัยที่ส่งต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษา. วารสารวิชาการวิทยาศาสตร์มหาวิทยาลัยราชภัฏจันเกษม. 2565.

28. Smith A, et al. Enhancing cybersecurity awareness through motivation training programs. Cybersecurity Journal. 2021;6(3):55-70.

29. สุรชัย ฉัตรเฉลิมพันธุ์, เทอดพงษ์ แดงสี. การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลองการโจมตีด้วยฟิชชิ่ง. Journal of Science and Technology Thonburi University. 2020;4(2):1-10.

30. กิตติศักดิ์ คุรุนันท์, ทัชชกร แสงทองดี. แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย. *วารสารสังคมศาสตร์และการวิจัยสหวิทยาการ.* 2024;1(1):1-14.

31. ภาคิน หวังสถิธรรม. กรอบกฎหมายของประเทศไทยในการรับมือกับอาชญากรรมคอลเซ็นเตอร์. วารสารสังคมศาสตร์และการวิจัยสหวิทยาการ. 2568];1(1):1–15

32. สมชาย ว, บุญเลิศ ป. แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์. วารสารเทคโนโลยีและความมั่นคง. 2022;9(1):55-72.

33. ขจรศักดิ์ ท, ศิริวรรณ จ. การบูรณาการ AI และ AGI เพื่อเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยไซเบอร์ของกองทัพอากาศไทย. วารสารวิทยาการทหาร. 2023;15(3):112-130.

34. Williams J, Brown P. Reducing cybercrime risks in organizations through employee behavior modification. Int J Cyber Sec Policy. 2022;9(2):120-135.

35. Khan M, Rahman S, Aziz M. Cyber security: Promote awareness for Bangladesh Army. *Asian Military Cyber Studies.* 2022;17(1):78-94.

36. White J, Thomas P. Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. *Defense & Security Studies.* 2023;21(5):310-330.

37. RAND Corporation. Improving the cybersecurity of U.S. Air Force military systems. RAND Security Report. 2022;10(1):45-68.

38. Military Times. Military members are disproportionately affected by cybercrime. Mil Times Cyber Review. 2023;8(3):134-150.

39. ศูนย์ไซเบอร์กองทัพบก. ภารกิจและหลักสูตรอบรมด้านความมั่นคงไซเบอร์. 2567.

ประวัติย่อผู้วิจัย

ยศ ชื่อ พันเอก ภานุพันธ์ อินทรพรหม

วัน เดือน ปีเกิด 7 มิถุนายน 2520

ประวัติสำเร็จการศึกษา

พ.ศ. 2540	โรงเรียนเตรียมทหาร รุ่นที่ 38
พ.ศ. 2545	ปริญญาตรีวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมเครื่องกล โรงเรียนนายร้อยพระจุลจอมเกล้า
พ.ศ. 2546	หลักสูตรปฐมนิเทศนายทหารเหล่าปืน รุ่นที่ 18
พ.ศ. 2546	หลักสูตรชั้นนายร้อย เหล่าทหารปืนใหญ่ รุ่นที่ 57
พ.ศ. 2552	หลักสูตรชั้นนายพัน เหล่าทหารปืนใหญ่ รุ่นที่ 59
พ.ศ. 2555	หลักสูตรหลักประจำ โรงเรียนเสนาธิการทหารบก ชุดที่ 90

ประวัติการทำงาน

พ.ศ. 2545	ผู้ตรวจการณ์หน้า กองร้อยปืนใหญ่ กองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2546	รองผู้บังคับกองร้อยปืนใหญ่ กองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2548	ผู้บังคับกองร้อยปืนใหญ่ กองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2551	นายทหารยุทธการและการฝึก กองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2555	นายทหารยุทธการและการฝึก กรมทหารปืนใหญ่ที่ 1 รักษาพระองค์
พ.ศ. 2556	รองผู้บังคับกองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2558	ผู้ช่วยผู้ประสานการยิงสนับสนุน กรมทหารปืนใหญ่ที่ 1 รักษาพระองค์
พ.ศ. 2559	ผู้บังคับกองพันทหารปืนใหญ่ที่ 11 รักษาพระองค์
พ.ศ. 2562	หัวหน้ากองกำลังพล มณฑลทหารบกที่ 11

ตำแหน่งปัจจุบัน

พ.ศ. 2565 - ปัจจุบัน	ฝ่ายเสนาธิการประจำผู้บังคับบัญชา สำนักปฏิบัติภารกิจรักษาความมั่งคงภายใน ภาค 1