การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ ให้กับกำลังพลกองทัพบก

เอกสารวิจัยส่วนบุคคล

โดย

พันเอก สุวิทย์ วิจิตรกาญจน์

รองเสนาธิการกองพลทหารราบที่ 2 รักษาพระองค์

วิทยาลัยการทัพบก

กันยายน 2566

เอกสารวิจัยเรื่อง การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก

โดย พันเอก สุวิทย์ วิจิตรกาญจน์

อาจารย์ที่ปรึกษา พันเอก ชยุตรา ไผ่ล้อม

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2566 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ **ดี**

พลตรี **ผู้บัญชาการวิทยาลัยการทัพบก**

(ฉกาจ ขันตี)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก **ประธานกรรมการ**

(ชนะชัย พลเตชา)

พันเอก **ผู้ทรงคุณวุฒิที่ปรึกษา**

(ชวินโรจน์ พรเกตุบุญลือ)

พันเอก **กรรมการ**

(ชยุตรา ไผ่ล้อม)

พันเอกหญิง **กรรมการ**

(ธนิตา วงษ์จินดา)

บทคัดย่อ

ผู้วิจัย พันเอก สุวิทย์ วิจิตรกาญจน์

เรื่อง การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก

วันที่ 6 กันยายน 2566 **จำนวนคำ :** 7,677 **จำนวนหน้า :** 24

คำสำคัญ ภัยคุกคาม, ไซเบอร์, กองทัพบก

ชั้นความลับ ไม่มีชั้นความลับ

ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามที่ใกล้ตัวทุกคนในยุคปัจจุบัน การสร้างความตระหนักรู้ถึงความเสียหายต่อตนเองและหน่วยงานจากภัยคุกคามดังกล่าวจึงมีความจำเป็นอย่างมากเพื่อป้องกันไม่ให้เกิดขึ้นกับกำลังพลและหน่วยงานของกองทัพบก ปัจจุบันกองทัพบกยังไม่มีหลักสูตรการให้ความรู้แก่กำลังพลของกองทัพบกแต่เป็นการส่งเสริมให้กำลังพลหาข้อมูลจากหน่วยงานต่างๆ ของรัฐ เช่น ระบบ E-Learning แต่ถ้ามีการใช้เครื่องมือของกองทัพบกที่มีอยู่เป็นแหล่งข้อมูลในการเรียนรู้ให้กับกำลังพลย่อมจะเกิดประโยชน์เป็นอย่างมาก การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อหาแนวทางในการสร้างการเรียนรู้ให้กับกำลังพลของกองทัพบกด้วยตัวเอง โดยศึกษาปัญหาอุปสรรคที่มีผลต่อการเรียนรู้ของกำลังพล เพื่อนำไปพัฒนาแนวทางการเรียนรู้ด้วยตัวเองให้มีประสิทธิภาพมากขึ้น ผลการวิจัยพบว่า เนื้อหาความรู้ที่สร้างความเข้าใจได้ง่าย สื่อการสอนประเภทต่างๆ รวมถึงปัจจัยต่างๆ เช่น ระดับการศึกษา ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และประสบการณ์การทำงานที่เกี่ยวข้องกับไซเบอร์มีผลต่อการเรียนรู้ด้วยตัวเองของกำลังพลของกองทัพบก การส่งเสริมให้มีการเสริมทักษะความรู้ด้านภัยคุกคามไซเบอร์ในหลักสูตรบังคับของกองทัพบกเป็นแนวทางในการสร้างความตระหนักรู้เพิ่มเติมให้กับกำลังพล นอกเหนือจากการให้กำลังพลไปศึกษาด้วยตัวเองหรือจากหน่วยงานอื่นเพื่อเป็นการสร้างความพร้อมในตระหนักรู้และการป้องกันภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบกต่อไป

ABSTRACT

AUTHOR: COLONEL SUWIT VIJITKARN

TITLE: Strengthening Knowledge on Cyber Threats for Royal Thai Army Personnel

DATE: 6 September, 2023 **WORD COUNT :** 7,677 **PAGES :** 24

KEY TERMS: Threat, Cyber, Royal Thai Army

CLASSIFICATION: Unclassified

Cyber threats are imminent threats to everyone in the present. Realization of its destruction to individuals and organization is crucial in order to prevent personnel and the army from it. Nowadays, the Royal Thai Army (RTA) has not created any academic course for personnel but only encourages them to conduct self-learning from any governmental services such as E-Learning websites. However, it would be useful if all materials of the RTA have been used properly to be a source of information for all personnel. In this research, the main propose is to figure out of self-learning guidelines for RTA personnel by studying of problems and obstacles of process of factors effecting to develop more effective self-learning. The findings demonstrated the content facilitating understanding, types of educational materials, knowledge regarding to cyber security and working experiences relevant to cyber that effects on self-learning. The knowledge improvement on cyber threat in the RTA obligatory course would promote realization to all personnel besides self-learning from the existing materials from the army and other government services in order to build realization on and prevention from cyber threat for all RTA personnel.

กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคลฉบับนี้ สำเร็จลุล่วงได้ด้วยความอนุเคราะห์จาก พันเอก ชยุตรา ไผ่ล้อม ผู้ช่วยอาจารย์อำนวยการ ส่วนวิชาความมั่นคงแห่งชาติและยุทธศาสตร์ วิทยาลัยการทัพบก อาจารย์ที่ปรึกษา ที่กรุณาให้คำปรึกษารวมทั้งปรับปรุงแก้ไขข้อบกพร่องต่างๆ ด้วยความเอาใจใส่อย่างดียิ่ง และ พันเอก ชวินโรจน์ พรเกตุบุญลือ หัวหน้าแผนกเทคนิคการปฏิบัติการไซเบอร์ กองปฏิบัติการไซเบอร์ศูนย์ไซเบอร์กองทัพบก ผู้ทรงคุณวุฒิที่ปรึกษา และผู้บังคับบัญชาที่กรุณามอบโอกาสให้ได้เข้ารับการศึกษาในวิทยาลัยการทัพบกและได้ให้แนวคิดในการศึกษา ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณ พลตรี ฉกาจ ขันตี ผู้บัญชาการวิทยาลัยการทัพบก ที่กรุณาอนุมัติให้ผู้วิจัยทำวิจัยเรื่องนี้ ผู้ที่เกี่ยวข้อง พันเอก ชนะชัย พลเตชา ประธานคณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล พันเอก หญิง ธนิตา วงษ์จินดา กรรมการและเลขานุการคณะกรรมการ ที่กรุณาให้ข้อเสนอแนะอันเป็นประโยชน์อย่างยิ่งต่องานวิจัยฉบับนี้

สุดท้ายนี้ ขอขอบคุณเพื่อนนักศึกษาหลักสูตรหลักประจำวิทยาลัยการทัพบก ชุดที่ 68 ที่ให้ความช่วยเหลือและเป็นกำลังใจให้กับผู้วิจัยในทุกขั้นตอนของการดำเนินการวิจัย ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิจัยฉบับนี้ จะเป็นแนวทางและเป็นประโยชน์ต่อการสร้างความรู้ภัยคุกคามไซเบอร์ให้กับกำลังพลของกองทัพบกต่อไป

สารบัญ

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ปัจจุบันภัยคุกคามในโลกไซเบอร์ได้มีวิวัฒนาการหลากหลายรูปแบบและสร้างผลกระทบความมั่นคงของชาติ โดยในปี 2565 มีสถิติการก่ออาชญากรรมทางไซเบอร์ในประเทศไทย จำนวน 119,528 คดี และเพิ่มจำนวนอีกในอนาคต แนวโน้มการขยายตัวของอาชญากรรมไซเบอร์ที่กระทำโดยองค์กรอาชญากรรม ซึ่งมีความเชื่อมโยงกับการใช้อินเทอร์เน็ตของประชาชนทั่วโลกที่มากขึ้นในช่วงการระบาดของโรคโควิด-19 มุ่งเน้นแสวงประโยชน์จากสถานการณ์โรคโควิด-19 ได้สรุปตัวอย่างอาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมมีแนวโน้มเป็นผู้กระทำการสูงขึ้น 4 ประเภท ได้แก่ (1) การฉ้อโกงทางอินเทอร์เน็ตผ่านวิธีการฟิชชิ่งและสแกมมิ่ง (2) การใช้ไวรัสเรียกค่าไถ่ (3) การแทรกซึมตลาดการค้าทางออนไลน์ และ (4) การละเมิดสิทธิมนุษยชนโดยอาศัยช่องทางอินเทอร์เน็ต เช่น การค้ามนุษย์ และการแสวงประโยชน์ทางเพศ [1] โดยในประเทศไทยมีสถิติการโจมตีทางไซเบอร์ ในปี 2565 (1 ตุลาคม 2564 - 30 กันยายน 2565) ประเทศไทยถูกคุกคาม 511 เหตุการณ์ โดยหน่วยงานด้านการศึกษาและด้านสาธารณสุข เสี่ยงถูกโจมตีทางไซเบอร์สูงสุด โดยมีรูปแบบในการโจมตีดังนี้ การโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บไซต์และหลอกเอาข้อมูลจำนวน 367 ครั้ง Ransomware มัลแวร์เรียกค่าไถ่ที่มีความสามารถเข้ารหัสลับข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อได้ จำนวน 21 ครั้ง และ Emotet Malware เป็นมัลแวร์ที่มีความสามารถในการขโมยข้อมูลทางการเงิน เช่น รหัสผ่านบัญชีธนาคารออนไลน์ จำนวน 9 ครั้ง ซึ่งตามที่กล่าวมาทำให้เห็นว่าภัยคุกคามทางไซเบอร์ในปัจจุบันมีระดับความรุนแรงและมีแนวโน้มเพิ่มมากขึ้น

ยุทธศาสตร์ชาติด้านความมั่นคงมีเป้าหมายการพัฒนาที่สำคัญคือ ประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัยและมีความสงบเรียบร้อยในทุกระดับตั้งแต่ระดับชาติ สังคม ชุมชน มุ่งเน้นการพัฒนาคน เครื่องมือ เทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่

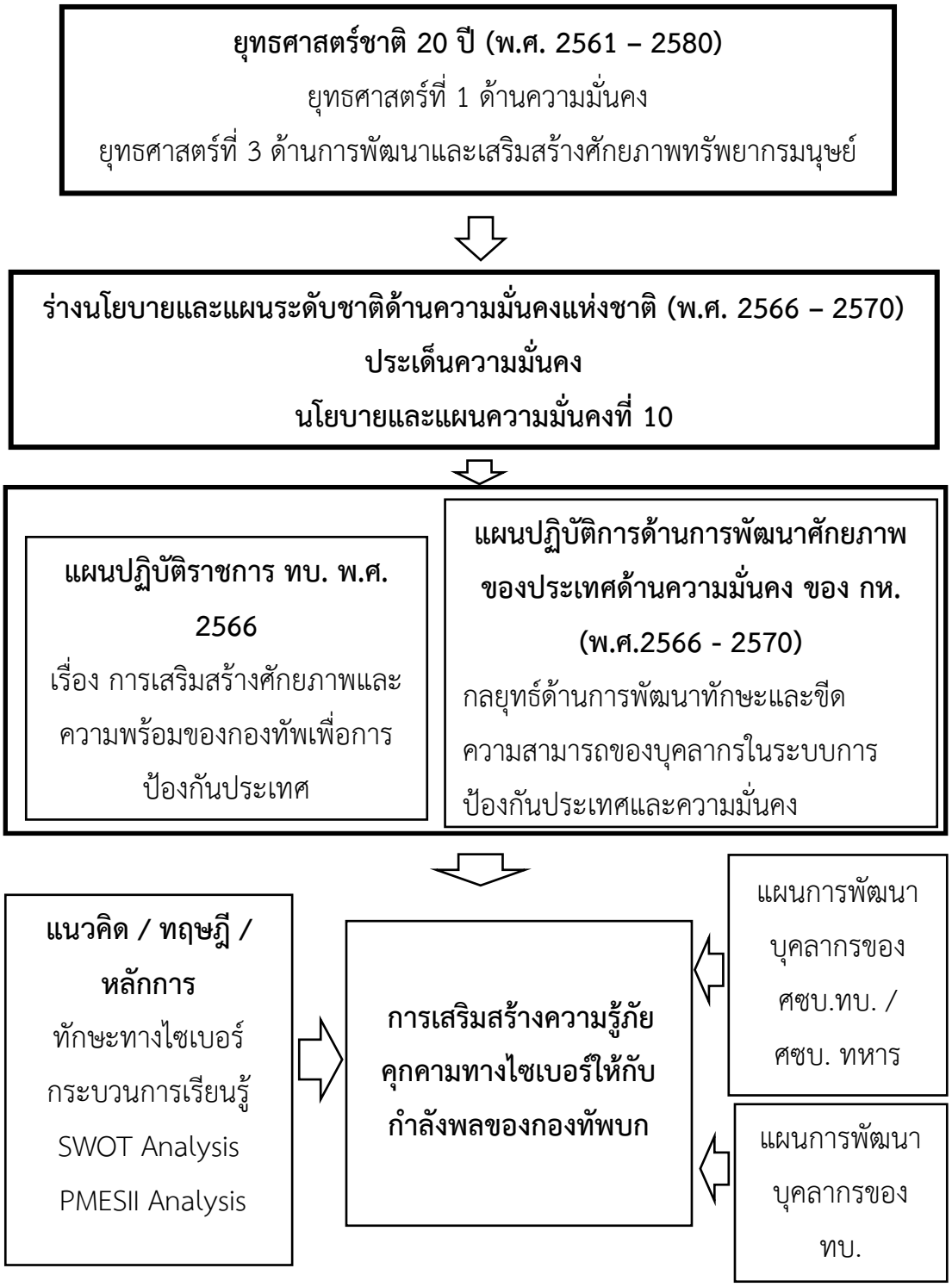
ให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบและสามารถแก้ไขปัญหาและภัยคุกคามในอนาคตได้ทันท่วงทีก่อนที่จะลุกลามต่อไป รวมทั้งป้องกันไม่ให้ส่งผลกระทบต่อการบริหาร การสร้างการเข้าถึงและใช้ประโยชน์จากข้อมูลหลากหลายจากแหล่งข้อมูลที่เชื่อถือได้ มีการป้องกันที่ครอบคลุมความปลอดภัยไซเบอร์ [2] จากนโยบายและแผนความมั่นคงแห่งชาติ มุ่งเน้นให้ประเทศไทยพัฒนาศักยภาพการป้องกันเพื่อรองรับภัยคุกคามทางไซเบอร์ โดยการยกระดับมาตรฐานรักษาความมั่นคงปลอดภัยทางไซเบอร์ ลดการก่ออาชญากรรมทางไซเบอร์ และพัฒนาการสอบสวนทางไซเบอร์[3] แผนปฏิบัติราชการของกระทรวงกลาโหม [4] และนโยบายของกองทัพบก [5] ได้เน้นการพัฒนาศักยภาพของกำลังพลของกองทัพบกด้านความรู้และเทคโนโลยีด้านไซเบอร์ ให้มีความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในอนาคต

ดังนั้นผู้วิจัยจึงทำการศึกษาเรื่อง แนวทางการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบก เนื่องจากภัยคุกคามไซเบอร์ในปัจจุบันที่มีแนวโน้มสูงขึ้นที่จะสร้างปัญหาให้กับกองทัพบกทั้งทางด้านกำลังพลและงานการป้องกันประเทศหากกำลังพลของกองทัพบกไม่มีความเท่าทันภัยคุกคามไซเบอร์ในปัจจุบัน รวมถึงวิธีการเข้าถึงแหล่งให้ความรู้ด้านภัยไซเบอร์ด้วยเครื่องมือของกองทัพบกที่มีอยู่ในปัจจุบัน เพื่อเป็นแนวทางการการป้องกันตนเองและหน่วยงาน รวมถึงการช่วยเหลือในกรณีตกเป็นเหยื่อจากภัยไซเบอร์ในปัจจุบัน เพื่อเสริมสร้างของกองทัพบกมีความพร้อมที่จะปฏิบัติหน้าที่ในการป้องกันอธิปไตยของชาติต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาแนวทางการป้องกันภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก
2. เพื่อศึกษาถึงปัจจัยที่มีผลต่อการศึกษาด้วยตนเอง
3. เพื่อหาแนวทางการใช้เครื่องมือของกองทัพบกในการเป็นคลังความรู้ให้กำลังพลค้นคว้าหาข้อมูลภัยคุกคามทางไซเบอร์

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดวิจัย

การศึกษาแนวทางการเสริมสร้างความรู้ภัยคุกคามไซเบอร์ให้กับกำลังพลของกองทัพบก จะสอดคล้องกับแผนปฏิบัติราชการของกองทัพบก พ.ศ. 2565 เรื่องการเสริมสร้างศักยภาพและความพร้อมของกองทัพเพื่อการป้องกันประเทศ โดยใช้เป็นกรอบแนวทางในการจัดทำ ซึ่งจะเชื่อมโยงกับแผนปฏิบัติการด้านความมั่นคงของกระทรวงกลาโหม พ.ศ. 2566 - 2570 ในกลยุทธ์ด้านการพัฒนาทักษะและขีดความสามารถของบุคลากรในระบบการป้องกันประเทศและความมั่นคง รวมถึงแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ด้านความมั่นคง นโยบายและแผนความมั่นคงที่ 10 การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ เพื่อสนับสนุนยุทธศาสตร์ชาติ 20 ปี ประเด็นที่ 1 ด้านความมั่นคง และประเด็นที่ 3 ด้านพัฒนาและเสริมสร้างทรัพยากรมนุษย์

วิธีการศึกษา

1. รูปแบบการวิจัย

การวิจัยนี้ใช้รูปแบบการวิจัยเชิงยุทธศาสตร์โดยรูปแบบการวิจัยเอกสาร (Documentary Research) ตามแนวทางที่วิทยาลัยการทัพบกกำหนด

2. ขอบเขตการศึกษา

ศึกษานโยบาย แผนการปฏิบัติงานของศูนย์ไซเบอร์กองทัพบกเพื่อให้เข้าใจภาพรวมแนวทางการเตรียมความพร้อมในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัย ไซเบอร์ของกรมกำลังพลทหารบก และศึกษาสภาวะแวดล้อมที่มีผลต่อการพัฒนาศักยภาพบุคลากร

3. การเก็บรวบรวมข้อมูล

เอกสารทางวิชาการด้านไซเบอร์ บทความต่างๆ ด้านความมั่นคงทางไซเบอร์ เอกสารแนวทางการพัฒนาบุคลากรจากองค์กรทางการศึกษาต่างๆ นำผลการวิเคราะห์ที่ได้มาทำการสรุปเพื่อหาภาพรวมแนวทางการพัฒนาความรู้ทางไซเบอร์

4. การวิเคราะห์ข้อมูล

ทำการวิเคราะห์ข้อมูลจากการรวบรวมความรู้ที่จำเป็นต่องานความมั่นคงด้านไซเบอร์ วิเคราะห์ความเหมาะสมของเนื้อหาการเรียนรู้สำหรับกำลังพลของ

หน่วย และวิเคราะห์ปัญหาและอุปสรรคที่มีผลกระทบต่อการพัฒนาความรู้ด้านไซเบอร์สำหรับกำลังพลของกองทัพบก เพื่อรองรับภัยคุกคามความมั่นคงทางไซเบอร์

ประโยชน์ที่ได้รับ

1. ให้ทราบถึงแนวการให้ความรู้ด้านภัยไซเบอร์ให้กับกำลังพลของกองทัพบก
2. ได้แนวทางการกำหนดรูปแบบการให้ความรู้กับกำลังพลของกองทัพบกตามตัวแปรที่มีผลกระทบต่อการเรียนรู้ด้วยตนเอง
3. ทำให้กำลังพลของกองทัพบกสามารถใช้เครื่องมือที่มีอยู่เข้าถึงข้อมูลของภัยคุกคามทางไซเบอร์และข้อมูลด้านอื่นๆ

บทที่ 2
บทวิเคราะห์

การวิจัยเรื่อง การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบก เป็นการสนองตอบต่อแนวความคิดทางยุทธศาสตร์ในด้านความมั่นคงทางไซเบอร์ จากการพัฒนาศักยภาพบุคลากรของกองทัพบกให้มีความตระหนักรู้ในเรื่องภัยคุกคามจากไซเบอร์ โดยมุ่งเน้นการวิเคราะห์แนวทางการเรียนรู้ด้วยตัวเองรวมถึงปัจจัยที่มีผลต่อการเรียนรู้ และแนวทางการใช้เครื่องมือของกองทัพบกในการช่วยเหลือในการเข้าถึงข้อมูลต่างๆ หรือใช้ในการแนะนำแนวทางที่ถูกต้องที่ทำให้กำลังพลของกองทัพบกสามารถเรียนรู้ได้อย่างถูกต้องและง่ายในการเข้าถึง มุ่งไปสู่ความพร้อมของกำลังพลที่พร้อมที่จะทำงานโดยมีความระมัดระวังในภัยคุกคามไซเบอร์ ผู้วิจัยได้ศึกษาหลักการ ทฤษฎี ตลอดจนวรรณกรรมที่เกี่ยวข้อง รวมถึงบทวิเคราะห์ที่สำคัญที่สอดคล้องกับวัตถุประสงค์งานวิจัยในบทที่ 1 โดยมีรายละเอียดดังต่อไปนี้

สภาพแวดล้อมทางยุทธศาสตร์ของภัยคุกคามไซเบอร์ที่มีต่อกำลังพลกองทัพบก

จากการวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ของภัยคุกคามไซเบอร์ที่มีต่อกำลังพลกองทัพบก โดยใช้กรอบ PMESII ประกอบด้วย ด้านการเมือง (Political) ด้านการทหาร (Military) ด้านเศรษฐกิจ (Economic) ด้านสังคม (Social) ด้านข้อมูลข่าวสาร (Information) และด้านโครงสร้างพื้นฐาน (Infrastructure) สรุปผลได้ดังนี้

1. ด้านการเมือง (Political) ระดับโลกมีความขัดแย้งระหว่างประเทศมหาอำนาจซึ่งส่งผลการเมืองระหว่างประเทศ และนำไปสู่อาชญากรรมรูปแบบต่างๆ รวมถึงภัยคุกคามไซเบอร์ดังที่พบว่ามีการก่ออาชญากรรมไซเบอร์ สงครามไซเบอร์และการก่อเหตุรุนแรงโดยใช้เทคโนโลยีเป็นเครื่องมือการเมืองระดับโลกจึงมีผลการดำเนินชีวิตของผู้คนจากภัยคุกคามดังกล่าว ในระดับประเทศในประเทศไทยให้ความสำคัญในเรื่องการรักษาความปลอดภัยไซเบอร์ โดยได้ตรากฎหมาย พระราชบัญญัติความปลอดภัยไซเบอร์ พ.ศ. 2562 และมีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรับผิดชอบในเรื่องภัยคุกคามไซเบอร์ในภาพรวมของประเทศโดยมีการจัดทำหลักสูตรเผยแพร่ความรู้แก่ประชาชนเพื่อ

ป้องกันภัยคุกคามไซเบอร์ในระดับบุคคลแก่ประชาชนและบุคคลากรของหน่วยงานภาครัฐ โดยเผยแพร่ผ่านเว็บไซต์ของ สถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy โดยในประเทศไทยพบว่ามีการโจมตีทางไซเบอร์ในห้วงที่ผ่านมา มีการโจมตีระบบการเงินธนาคารของในประเทศ โดยเฉพาะการโจมตีระบบเว็บไซต์ของภาครัฐโดยการโจมตีดังกล่าวเป็นลักษณะการแสดงเชิงสัญลักษณ์ในการแสดงออกของภาคประชาชน

2. ด้านการทหาร (Military) ในปี พ.ศ. 2566 ผลการจัดอันดับแสนยานุภาพทางการทหารของกองทัพทั่วโลกโดยเว็บไซต์ Global Fire Power 2023 พบว่า ประเทศ 5 อันดับแรกของโลกที่มีคะแนน Power Index สูงสุดได้แก่ สหรัฐอเมริกา รัสเซีย จีน อินเดียและสหราชอาณาจักร สำหรับประเทศไทยจัดอยู่ในอันดับที่ 24 ของโลก ปัจจุบันการปฏิบัติภารกิจทางทหาร ได้นำระบบออนไลน์มาใช้สนับสนุนในหลายรูปแบบ เช่น ระบบปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง Network Centric Operations ระบบสารสนเทศสายงานส่งกำลังบำรุง LOGMIS ระบบสารสนเทศ E-Army รวมถึงแอพพลิเคชั่น Smart Soldier ซึ่งกำลังพลต้องมีความรู้ความเข้าใจเรื่องความปลอดภัยทางไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำข้อมูลสำคัญของกองทัพนำไปเผยแพร่ รวมถึงการก่อกวนแก้ไขข้อมูลทำให้เกิดความผิดพลาดในการตัดสินใจในการปฏิบัติการทางทหาร ซึ่งจะทำให้กองทัพสามารถใช้เครื่องมือและเทคโนโลยีได้อย่างมีประสิทธิภาพ

3. ด้านเศรษฐกิจ (Economic) ปัจจุบันระบบเศรษฐกิจทั่วโลกหันมาใช้เทคโนโลยีกันมากขึ้น โดยมีการเปลี่ยนผ่านไปสู่ระบบดิจิทัลอย่างรวดเร็วเช่น ระบบสกุลเงินดิจิทัล ธุรกรรมการเงินออนไลน์ (E-Banking) การซื้อขายหรือการค้าออนไลน์ (E-Commerce) ซึ่งส่งผลกระทบต่อการใช้ชีวิตประจำวันการจับจ่ายใช้สอยมากขึ้นและมีความเสี่ยงในการถูกหลอกลวงทางไซเบอร์เพิ่มมากขึ้น รวมถึงการก่อกวนทำให้ระบบไม่สามารถทำงานได้ตามปกติ การขโมยข้อมูลเพื่อทำธุรกรรมทางการเงิน โดยจากการกระทำดังกล่าวทำให้ผู้ได้รับผลกระทบได้รับความเสียหายต่อทั้งบุคคลและสังคมในวงกว้าง ในปัจจุบันธุรกิจจำนวนมากโยกย้ายระบบส่วนใหญ่ขึ้นไปบนโลกดิจิทัล ขอบเขตของการโจมตีจึงไม่ใช่แค่ที่ตัวข้อมูล แต่เป็นตัวระบบหลักที่ขับเคลื่อนธุรกิจ ส่งผลให้ความเสียหายที่เกิดขึ้นอาจรุนแรงถึงขั้นทำให้ธุรกิจหยุดชะงัก สร้างความเสี่ยงทางการเงิน หรือสูญเสีย

ความเชื่อมั่นในตัวธุรกิจ โดยยิ่งความเสียหายรุนแรงขึ้นเท่าไร ต้นทุนค่าใช้จ่ายในการกู้คืนระบบก็สูงขึ้นตามไปด้วย

4. ด้านสังคม (Social) กระแสโลกาภิวัตน์ได้นำมาซึ่งการเปลี่ยนวิถีชีวิตของผู้คนในสังคมโดยมีอินเตอร์เน็ตเป็นสื่อกลางที่เชื่อมโยงผู้คนให้มีการแลกเปลี่ยนข้อมูลข่าวสารวัฒนธรรมความเป็นอยู่ ส่งผลให้อินเตอร์เน็ตกลายเป็นสิ่งจำเป็นในชีวิตประจำวัน เกิดสังคมออนไลน์มีการเผยแพร่ความรู้ข่าวสารความบันเทิงในอินเตอร์เน็ต ทำให้ผู้คนเข้าถึงและแลกเปลี่ยนข่าวสารกันได้ตลอดเวลา กลายเป็นวิถีชีวิตรูปแบบใหม่ของผู้คนในยุคปัจจุบัน อย่างไรก็ตามข้อมูลข่าวสารต่างๆ อาจมีทั้งข้อมูลจริงและข้อมูลเท็จ หรือ Fake News ทำให้ประชาชนต้องมีความรู้ในการเท่าทันโลกแห่งข้อมูลข่าวสารและมีการตระหนักรู้ทางการรักษาความปลอดภัยทางไซเบอร์ รวมถึงการนำสื่อออนไลน์ ไปใช้เป็นเครื่องมือในการเผยแพร่แนวคิดที่นิยมการใช้ความรุนแรง หรือการสอนการก่อการร้าย การจัดหาอาวุธและวัสดุที่ใช้ประกอบเป็นอาวุธ รวมทั้งสอนวิธีการทำ การหาสมาชิกเพื่อมาร่วมอุดมการณ์การก่อการร้ายและการสร้างความคิดความเชื่อให้กับเยาวชนในปัจจุบันในลักษณะบิดเบือนเพื่อปลูกฝังความคิดอุดมการณ์ทางการเมืองและการอยู่ร่วมกันในสังคมเพื่อหวังผลต่อการสร้างความวุ่นวายในสังคม

5. ด้านข้อมูลข่าวสาร (Information) ในยุคแห่งข้อมูลข่าวสาร (Information Age) โลกขับเคลื่อนด้วยข้อมูลข่าวสารอยู่ตลอดเวลา ข้อมูลจากเหตุการณ์ในซีกโลกหนึ่งสามารถส่งผลกระทบไปยังอีกซีกโลกหนึ่งได้ภายในเสี้ยววินาที ผลกระทบของข้อมูลจึงเกิดขึ้นทั้งในระดับบุคคล ชุมชน สังคม ประเทศและในระดับโลก ยิ่งปัจจุบันมีความเจริญก้าวหน้าของเทคโนโลยีข้อมูลข่าวสารทำให้เทคโนโลยีดังกล่าวนำมาใช้ในทางที่ผิด เช่นการสร้างข่าวลวงบิดเบือนข้อเท็จจริงเพื่อส่งผลทางการปฏิบัติ ไม่ว่าจะเป็นการปลุกปั่นสร้างความวุ่นวายภายในประเทศ จนไปถึงการจารกรรมหรืออาชญากรรมทางไซเบอร์ในรูปแบบต่างๆ

6. ด้านโครงสร้างพื้นฐาน (Infrastructure) โครงสร้างพื้นฐานด้านอินเตอร์เน็ตทั่วโลกมีความเจริญก้าวหน้าอย่างรวดเร็วจากการสำรวจของ We are social เว็บไซต์ที่รวบรวมสถิติการใช้สื่อโซเชียลของแต่ละประเทศ เผยสถิติการใช้เทคโนโลยีดิจิทัลทั่วโลกผ่านรายงานดิจิทัล 2022 Global Overview ณ เดือนมกราคม 2565 พบผู้ใช้

อินเตอร์เน็ตทั่วโลกร้อยละ 62.5 โดยประเทศไทยติดอันดับใช้อินเตอร์เน็ตต่อประชากรมากถึงร้อยละ 77.8 นับเป็นอันดับที่ 34 ของโลก สะท้อนให้เห็นว่าการพัฒนาโครงสร้างพื้นฐานด้านอินเตอร์เน็ตของไทยมีขีดความสามารถสูง ส่งผลให้ประชาชนเข้าถึงอินเตอร์เน็ตได้ครอบคลุมประชากรส่วนใหญ่ นอกจากนี้ยังสามารถช่วยขับเคลื่อนเศรษฐกิจของประเทศและส่งเสริมการดำเนินการต่างๆ ของหน่วยงานภาครัฐและเอกชนเป็นอย่างดี ในขณะเดียวกันก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์จากในประเทศและนอกประเทศประชาชนจึงควรเตรียมความพร้อมและมีความรู้เท่าทันสามารถแก้ไขปัญหาดังกล่าวได้หากโครงสร้างพื้นฐานถูกโจมตีและหยุดการให้บริการ การโจมตีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ของประเทศไทยได้แก่ระบบให้บริการทางการเงินการธนาคาร สาธารณูปโภค การขนส่งและโลจิสติกส์ บริการสุขภาพ พลังงาน การสื่อสารโทรคมนาคม เป็นภัยคุกคามทางไซเบอร์ที่ก่อให้เกิดผลกระทบที่รุนแรงในวงกว้าง และสามารถสร้าง ความเสียหายที่ร้ายแรงต่อเสถียรภาพทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ ซึ่งอาจทำให้ประเทศ สูญเสียความได้เปรียบในการแข่งขันทางการค้าในตลาดโลก ทำให้ประเทศขาดความเชื่อมั่นในสายตา ประชาคมโลกหรือประชาชนทั่วไป การปฏิบัติงานของประเทศต้องหยุดชะงัก

แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์และ E-Learning

1. ความหมายของภัยคุกคามไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำ หรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง โดยภัยคุกคามทางไซเบอร์ ที่เป็นประเด็นสำคัญมี 2 มิติ ได้แก่ การโจมตีทางไซเบอร์และการครอบงำทางไซเบอร์

การโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง การโจมตีฝ่าย ตรงข้าม โดยมีวัตถุประสงค์เพื่อขัดขวาง ทำลาย หรือควบคุม การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมไปถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของ ฝ่ายตรงข้ามด้วย

การครอบงำทางไซเบอร์ (Cyber Dominance) หมายถึง การ ถูกชี้นำ หรือครอบงำทางความคิดโดยไม่รู้ตัวจากอำนาจของสารสนเทศและสื่อ มัลติมีเดีย รวมถึง การสร้างกระแสเทียมบนสื่อสังคมออนไลน์ เช่น การปั่นกระแส ด้วยแฮชแท็ก (#HashTag) การโพสต์ข่าวลือเทียม (False Rumor) การสร้างข่าวปลอม (Fake News) เป็นต้น ซึ่งส่งผล กระทบต่อความคิดเห็น ความเชื่อและการตอบสนองของประชาชนโดยรวม

2. รูปแบบเบื้องต้นที่พึงระวัง

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ใน การผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบ คอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจ แชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา

Phishing คือ รูปแบบของการหลอกลวงผ่านช่องทางการใช้งาน อินเทอร์เน็ตของผู้ใช้ทั่วไป ซึ่งไม่ใช่การล่อลวงธรรมดาที่เราพบเห็นกันทั่วไป แต่จะเป็นกล ยุทธ์การหลอกที่ใช้วิธีทางจิตวิทยาเข้าร่วมด้วย ส่วนใหญ่แล้วจะมาในรูปแบบของอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ที่จะทำการหลอกให้ผู้ใช้กรอกข้อมูลส่วน บุคคลที่เป็นความลับ ไม่ว่าจะเป็นรหัสผ่าน หมายเลขบัตรประชาชน เลขที่ Passport รวม ไปถึงข้อมูลลับทางการเงิน ทั้งเลขที่บัญชีและรหัสผ่าน หรือจะเป็นการหลอกให้กดยอมรับ และติดตั้งไวรัสตัวร้ายเข้าสู่คอมพิวเตอร์ของตัวเอง

Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็น ภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้ เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

3. แนวทางการรับมือ

ในชีวิตประจำวันของมีในปัจจุบันแต่ละบุคคลมีความจำเป็นที่จะต้องเกี่ยวข้องกับการใช้สื่อออนไลน์ในด้านต่างๆ ดังนี้ การใช้คอมพิวเตอร์ ควรมีการแยกเป็นส่วนบุคคล มีการจัดการ Password ที่ดีรัดกุมและเมื่อไม่ใช้ควรมีการ Log Out มีการอัพเดทระบบ การใช้โปรแกรมแอนตี้ไวรัส การใช้อีเมล์ ควรมีการระมัดระวัง ไม่เปิด E-mail ที่น่าสงสัย ไม่เปิดไฟล์แนบที่น่าสงสัย ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

4. สื่อการสอนที่เหมาะสม

ในปัจจุบันสื่อการสอนที่น่าสนใจในการเรียนรู้ด้วยตัวเองมีหลายรูปแบบ สำหรับผู้วิจัยมีความสนใจในการจัดทำสื่อการสอนดังนี้

4.1 **วีดิทัศน์** เป็นสื่อที่เหมาะสมสำหรับใช้เพื่อการจัดการเรียนรู้ เพราะวิดีทัศน์เป็นสื่อที่ทำให้ผู้เรียนเห็นภาพได้ชัดเจน ซึ่งอาจเป็นภาพนิ่ง หรือภาพเคลื่อนไหว ทำให้ผู้เรียนได้ยินเสียงที่สอดคล้องกับภาพนั้นๆ อีกด้วย วิดีทัศน์สามารถใช้ในการสาธิต เป็นสิ่งที่สามารถช่วยให้ผู้เรียนเห็นสิ่งที่ควรเห็น ผู้สาธิตสามารถจัดเตรียมและจัดทำวิดีทัศน์ได้อย่างถูกต้อง ก่อนที่จะนำไปใช้จริง นอกจากนั้นการใช้วิดีทัศน์สามารถเลือกดูภาพช้า หรือหยุดดูเฉพาะภาพได้การบันทึกภาพวิดีทัศน์สามารถกระทำได้ทั้งในห้องถ่ายภาพ(Studio) และห้องปฏิบัติการซึ่งเราสามารถตัดต่อส่วนที่ต้องการหรือเพิ่มเติมส่วนใหม่ลงไปได้ วิดีทัศน์เป็นสื่อที่สามารถตรวจเช็คภาพได้ทันทีและในขณะที่ถ่ายภาพถ้าไม่พอใจก็สามารถลบทิ้ง และบันทึกใหม่ได้ สำหรับเสียงก็สามารถบันทึกลงในแหล่งบันทึกไปพร้อมๆ กับการบันทึกภาพได้ทันทีในปัจจุบันวิดีทัศน์เข้ามามีบทบาทในชีวิตของเรามากขึ้นด้วยความสามารถทางด้านมัลติมีเดียที่ทำให้การนำเสนองานของเราน่าสนใจประกอบกับเทคโนโลยีในปัจจุบันที่หามาใช้ได้ไม่ยาก พร้อมกับโปรแกรมที่ใช้ในการตัดต่อวิดีทัศน์ก็มีให้เลือกใช้มากมายและก็ไม่ยากเกินไปที่จะเรียนรู้

4.2 E-Book คือหนังสือที่สร้างขึ้นด้วยโปรแกรมคอมพิวเตอร์ เป็นเอกสารในรูปแบบดิจิตัลที่นำเสนอ ข้อมูลในลักษณะข้อความ ภาพนิ่ง ภาพเคลื่อนไหว และ

เสียงต่างๆ ที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์ ที่สามารถเชื่อมโยงข้อมูลที่สัมพันธ์ของเนื้อหาถึงกันได้ผ่านจอคอมพิวเตอร์ ไม่ว่าเนื้อหานั้นจะอยู่ในแฟ้มเดียวกันหรืออยู่คนละแฟ้ม หากเป็นการเชื่อมโยงข้อความที่เป็นตัวอักษรหรือตัวเลข เรียกว่า ข้อความหลายมิติ (Hypertext) และหากข้อมูลนั้นเป็นการเชื่อมโยงลักษณะภาพ เสียง และภาพเคลื่อนไหว เรียกว่าสื่อหลายมิติ (Hypermedia) โดยปกติมักจะเป็นแฟ้มข้อมูลคอมพิวเตอร์ที่ สามารถอ่านเอกสารผ่านทางหน้าจอคอมพิวเตอร์ ตลอดจนมีปฏิสัมพันธ์และโต้ตอบกับผู้อ่านได้ อีกประการหนึ่งที่สำคัญก็คือ หนังสืออิเล็กทรอนิกส์สามารถปรับปรุงข้อมูลให้ทันสมัยได้ตลอดเวลา ซึ่งคุณสมบัติเหล่านี้จะไม่มีในหนังสือธรรมดาทั่วไป

4.3 Podcasts คือการให้ความรู้ในรูปแบบเสียงที่เป็นรูปแบบที่ง่ายที่สุดในการสร้างของผู้สอนเอง เนื่องจากไม่ต้องใช้ตัวหนังสือหรือภาพประกอบเพียงแค่อัดเสียงในการสอน หรือให้ความรู้จากนั้นอัพโหลดขึ้นบนช่องทางออนไลน์ผู้เรียนก็สามารถมาเปิดฟังและเรียนรู้เองได้เลยแต่การอัดเสียงเล่าเนื้อหาการเรียนเพียงอย่างเดียว ก็อาจจะเรียกว่าเป็นการสอนที่ให้ไม่น่าสนใจของผู้เรียน ผู้สอนจึงต้องหาวิธีสอนด้วยเสียงให้มีความน่าติดตาม เช่น ใช้รูปแบบของการพูดคุยหรือสัมภาษณ์ที่สนุกสนานก็จะช่วยให้ผู้เรียนมีสมาธิจดจ่อกับการฟังมากขึ้น หรือเป็นทางเลือกสำหรับคนที่ต้องการใช้การฟังเป็นหลักเพื่อเพิ่มความหลากหลายในการเรียน

จากการศึกษารูปแบบการจัดสื่อการสอนสำหรับสื่อการสอนที่เป็นที่นิยมและควรจะนำไปใช้ประโยชน์ให้กับกำลังพลของกองทัพบกคือการใช้รูปแบบ วิดิทัศน์ และ E-Book โดยสื่อการสอนทั้ง 2 รูปแบบมีความน่าสนใจและใช้การผสมผสานกันในการสร้างความเข้าใจให้กับผู้เรียนได้ครบถ้วนทั้งการอ่านทำความเข้าใจรูปแบบการสอนและการเรียนผ่านระบบวิดีทัศน์

5. E-Learning

การเข้าสู่ยุคของดิจิทัลไม่เพียงแต่มีการนำเทคโนโลยีเข้ามาขับเคลื่อนการใช้ชีวิตของผู้คนเท่านั้น แต่ยังมีการนำไปใช้ประยุกต์ใช้กับการศึกษา โดยพลิกโฉมจากการสอนแบบเดิมให้กลายเป็นรูปแบบที่น่าสนใจมากขึ้น และผู้เรียนเองก็ยังสามารถเข้าถึงการเรียนรู้เหล่านี้ได้อย่างง่ายดาย ผ่านอุปกรณ์ที่เชื่อมต่อกับระบบอินเทอร์เน็ต การเรียนรู้ที่ว่านี้คือ ระบบ E-learning สื่อการเรียนรู้ที่ได้ทำลายกรอบการเรียนรู้แบบเดิมๆ และทำ

ให้กลายเป็นการเรียนรู้เป็นสิ่งที่ไร้พรมแดน E-learning คือ การเรียนรู้ผ่านผ่านตัวกลางที่เป็นสื่อเทคโนโลยีหรือออนไลน์ ที่ช่วยลดข้อจำกัดด้านเวลาและสถานที่เรียน ผู้สอนสามารถนำเสนอไอเดียการเรียนรู้ได้หลากหลายรูปแบบ และทางผู้เรียนสามารถเลือกเรียนในเรื่องที่ตนเองต้องการ E-learning มีรูปแบบดังต่อไปนี้ คอมพิวเตอร์ช่วยสอน,การสอนบนเว็บไซต์,การเรียนออนไลน์และการเรียนทางไกลผ่านดาวเทียม ข้อดีของการเรียนแบบ E-learning ผู้เรียนสามารถเลือกจัดเวลาเรียนด้วยตนเองตามความสะดวกในการเรียนได้เลย สามารถทำให้เข้าถึงข้อมูลได้มากขึ้น ช่วยเสริมทักษะการเรียนรู้ด้วยตนเอง พบว่า คนส่วนใหญ่มีความพึงพอใจ มีการส่งเสริมให้ผู้เรียนได้เข้าถึงข้อมูลต่างๆ ด้วยตนเองได้อย่างสะดวกมากยิ่งขึ้น ถือเป็นการช่วยเสริมทักษะการเรียนรู้ด้วยตนเองได้อีกทางหนึ่ง E-Learning มีประสิทธิภาพในการจัดการเรียนการสอน ทำให้เกิดความน่าสนใจ มีกิจกรรมในการเรียนที่หลากหลาย แสดงให้เห็นว่า การศึกษาผ่านระบบ E-Learning ที่มีสารสนเทศสำหรับการสอน หรือการอบรม ซึ่งใช้การนำเสนอด้วยตัวอักษร ภาพนิ่งผสมผสานกับการใช้ภาพ เคลื่อนไหว วีดิทัศน์และเสียง โดยอาศัยเทคโนโลยีของเว็บ (Web Technology) ในการถ่ายทอดเนื้อหานั้นเป็นสิ่ง กระตุ้นให้ผู้เรียนมีความสนใจในเนื้อหามากขึ้น E-Learning เป็นการเพิ่มช่องทางในการเรียนที่ทันสมัยและสามารถเรียนรู้ได้ตลอดเวลา เป็นการประหยัดเวลาการเรียนในห้องเรียน ช่วยลดระยะเวลาในการเข้าถึงข้อมูล เนื่องจากสามารถเข้าถึงได้หลาก หลายช่องทางมากขึ้น ในสถานที่ใดก็ได้ทุกเวลาโดยไม่ต้องเดินทางไปเข้าห้องเรียน การออกแบบปฏิสัมพันธ์ง่ายต่อการใช้งาน สามารถนำเสนอโดยอาศัยเทคโนโลยีมัลติมีเดีย และเทคโนโลยีเชิงโต้ตอบ โดยเนื้อหาของบทเรียนประกอบด้วย ข้อความ รูปภาพ เสียง วิดีโอ และมัลติมีเดียอื่นๆ มีรูปแบบ การแสดงผลที่เหมาะสมและสวยงาม น่าเรียนรู้ การเพิ่มโอกาสในการเข้าถึงเนื้อหาการเรียน ได้จากอุปกรณ์ต่างๆ

จากข้อมูลดังกล่าวในขั้นต้นสรุปได้ว่า ในการจัดการเรียนการสอนการเรียนรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบกนั้น จำเป็นจะต้องจัดทำหลักสูตรโดยเน้นเนื้อหาและการนำเสนอที่น่าสนใจ เพื่อให้มีผลต่อการเรียนรู้ของกำลังพล รวมถึงการเข้าให้มีลักษณะความเหมาะสม โดยผู้วิจัยมีความคิดเห็นให้จัดการเรียนการสอนในระบบ E-Learning ในการสอนเนื่องจากการเป็นรูปแบบการเรียนการสอนที่มีความ

ทันสมัยและสามารถเรียนได้ทุกเวลาโดยกำลังพลสามารถใช้เวลาว่างในการเรียนและสามารถเรียนได้ในทุกสถานที่

ปัจจัยที่มีผลต่อการเสริมสร้างความรู้ภัยคุกคามไซเบอร์

จากการศึกษาปัจจัยที่มีผลต่อการศึกษาภัยคุกคามด้านไซเบอร์จากบทความวิจัยต่างๆ พบว่า ปัจจัยส่วนใหญ่ที่มีผลต่อการเรียนรู้ขึ้นอยู่กับ ระดับการศึกษาของแต่ละบุคคล ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ประสบการณ์การทำงานที่เกี่ยวข้องกับไซเบอร์จะสร้างความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศเป็นอย่างดี และสิ่งที่สร้างความต้องการในการตระหนักรู้ให้กับผู้เรียนมากที่สุดคือความสำคัญที่มีผลกระทบกับเรื่องงานของตนเองในปัจจุบันเป็นสิ่งเร้าให้เกิดความอยากในการเรียนรู้ ในส่วนของระดับการศึกษาสูงสุดนั้น ถือว่าเป็นองค์ประกอบสำคัญในกระบวนการที่ทำให้เกิดความตระหนักรู้ตามที่ กล่าวเอาไว้ว่า การเกิดความตระหนักรู้เป็นผลลัพธ์จากกระบวนการทางปัญญา ซึ่งหมายถึงหากบุคคลถูกกระตุ้นจากสิ่งเร้าที่ช่วยกระตุ้นบุคคลทำให้เกิดความรู้จนมีความเข้าใจในสิ่งนั้น นำไปสู่การเรียนบังเกิดเป็นความรู้และนำไปสู่ความตระหนักรู้ ดังนั้น ระดับการศึกษาสูงสุดของบุคลากรที่ต่างกัน จึงทำให้เกิดความแตกต่างของความสามารถทางด้านการเรียนรู้และความตระหนักรู้ ดังจะเห็นได้จากการที่บุคลากรที่มีระดับการศึกษาสูงสุด มีค่าเฉลี่ยความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์สูงในทุกด้าน ส่วนของประสบการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ จะเห็นได้ว่าประสบการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์โดยตรง ถือว่าเป็นสิ่งเร้าที่เป็นตัวกระตุ้นทำให้เกิดความตระหนักรู้ เป็นความคิดเห็น ความรู้สึก ความสำนึกถึงความสำคัญ บุคคลจะเกิดความสำนึกหรือความตระหนักรู้ หากบุคคลนั้นมีการรับรู้หรือเคยรับรู้มาก่อนและได้รับสิ่งเร้ามาเป็นตัวกระตุ้น ดังนั้น บุคคลที่เคยมีประสบการ์ตรงจึงมีระดับความตระหนักรู้มากกว่า

ในเรื่องอายุ เพศ ประสบการณ์ในการทำงาน และรายได้ ไม่มีผลต่อการสร้างความตระหนักรู้ในเรื่องภัยคุกคามทางไซเบอร์ เนื่องจากปัจจัยดังกล่าวไม่มีผลต่อสิ่งเร้าในการสร้างความอยากในการเรียนรู้ เนื่องมาจากในปัจจุบัน ประชาชนไม่ว่าจะเป็นเพศใด มีอายุหรือประสบการณ์การทำงาน (อายุงาน) เท่าใด ก็สามารถเข้าถึงและใช้งาน

อินเตอร์เน็ตได้อย่างเท่าเทียมกัน ซึ่งเป็นปัจจัยหนึ่งที่ส่งผลให้เกิดความ ตระหนักรู้คือ ความตระหนักหมายถึง การที่บุคคลเกิดความรู้สึก นึกคิด ความคิดเห็นหรือประสบการณ์ แล้วเกิดความเข้าใจแล้วประเมินสถานการณที่เกี่ยวกับตนเองได้จากสภาวะจิตที่ยอมรับ และเกิดแสดงพฤติกรรมตอบสนองต่อเหตุการณ์ ดังนั้น เพศ อายุ และประสบการณ์การทำงาน จึงไม่ใช่ข้อจำกัดที่จะทำให้โอกาสในการเรียนรู้หรือการสร้างความคุ้นเคยเกี่ยวกับความปลอดภัยในการใช้งานอินเตอร์เน็ต

สรุปปัจจัยที่มีผลกระทบในการเรียนรู้ภัยคุกคามทางไซเบอร์ทำให้เห็นว่า ปัจจัยที่มีผลกระทบในการเรียนรู้เป็นสิ่งจำเป็นในการกำหนดรูปแบบของและวิธีในการจัดเนื้อหาในการสอน หรือจำลองรูปแบบที่จะเกิดขึ้น ให้ผู้เรียนได้มีประสบการณ์ภัยคุกคามทางไซเบอร์เพื่อจะได้มีการเรียนรู้รูปแบบของภัยคุกคามทางไซเบอร์ เพื่อทำให้เกิดการเรียนรู้ที่ดีให้กับผู้เรียนต่อไป

ปัญหาอุปสรรคในการเสริมสร้างความรู้ภัยคุกคามไซเบอร์ให้กับกำลังพลกองทัพบก

จากการวิเคราะห์การดำเนินการของกองทัพบกที่ผ่านมาพบว่า การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบกมีปัญหาอุปสรรคดังต่อไปนี้

1. ขาดหน่วยงานที่รับผิดชอบโดยตรงในการเสริมสร้างให้กำลังพลกองทัพบกมีความรู้ความเข้าใจตระหนักถึงภัยคุกคามทางไซเบอร์สามารถป้องกันผลกระทบที่อาจเกิดขึ้นต่อตนเองหน่วยงานจึงถึงภาพรวมของกองทัพบกได้อย่างมีประสิทธิภาพที่ผ่านมา ศูนย์ประสานงานสารสนเทศศูนย์ปฏิบัติการกองทัพบก (ศปสท.ศปก.ทบ.) เป็นหน่วยงานที่ให้ความสำคัญในเรื่องดังกล่าวเป็นหน่วยงานที่จัดวิทยากรไปอบรมให้ความรู้ตามหน่วยงานต่างๆ แต่ยังไม่สามารถครอบคลุมหน่วยงานของกองทัพบกได้ สำหรับการส่งเสริมให้มีการเรียนรู้ในส่วนของกองทัพบก ได้มีการสั่งการให้กำลังพลของกองทัพบกดำเนินการเรียนรู้ด้วยตนเองผ่านการเรียนรู้ระบบ E-Learning ของสถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy และให้ดำเนินการรายงานผลการเรียนให้กับ กรมกำลังพลทหารบกทราบ ภายในเดือนกันยายน 2566 ให้หน่วยจัดกำลังพลเข้ารับการศึกษาจำนวน 13 บทเรียน (หลักสูตรการเรียนรู้

ทักษะทางด้านดิจิทัล ในมิติการเรียนรู้ที่ 1 และ 2) โดยให้มีกำลังพลเข้ารับการศึกษาอย่างน้อยร้อยละ 50 ของยอดกำลังพลภายในเดือนกันยายน 2566 และมีเป้าหมายให้กำลังพลทั้งกองทัพบก มีการเข้ารับการศึกษาครบทั้งร้อยละ 100 ต่อไปในอนาคต ซึ่งเริ่มกำหนดให้ดำเนินการตั้งแต่ 10 พฤษภาคม 2566 ซึ่งการดำเนินการทั้งกองทัพบกเป็นการสั่งการให้เริ่มดำเนินการในปีงบประมาณ 2566

2. ขาดบุคคลากรที่มีความรู้ความเชี่ยวชาญ ปัจจุบัน ศปสท.ศปก.ทบ. มีบุคคลากรที่มีความรู้ความสามารถในการดำเนินการเรื่องนี้ไม่เพียงพอต่อการดำเนินการในส่วนของ ศซบ.ทบ. นั้นภารกิจส่วนใหญ่จะเป็นการป้องกันระบบสารสนเทศของกองทัพบกเป็นหลัก แต่การแนะนำและจัดทำหลักสูตรในการให้ความรู้กับกำลังพลจะเป็นการสนับสนุนวิทยากรในการไปอบรมแต่ไม่มีหลักสูตรประจำที่ให้กำลังพลไปเข้ารับการศึกษา สำหรับการนำกำลังพลไปศึกษาจะเป็นระดับผู้ปฏิบัติงานในศูนย์ไซเบอร์เพื่อมาพัฒนาระบบในการป้องกันและการวางแผนงานในส่วนของศูนย์ไซเบอร์กองทัพบกเท่านั้น

3. ขาดเครื่องมือ แม้ว่าจะมีความก้าวหน้าเรื่องเทคโนโลยีและนวัตกรรมออนไลน์แต่กองทัพบกยังขาดเครื่องมือสนับสนุนการเสริมสร้างความรู้ภัยคุกคามไซเบอร์ให้กับกำลังพลกองทัพบกปัจจุบัน ในระบบแอพพลิเคชั่น Smart Soldier มีการให้ความรู้เป็นคลิปสั้นๆ จำนวน 18 คลิป แต่ยังไม่ครอบคลุมเนื้อหา แต่แสดงให้เห็นว่าในส่วนของกองทัพบกสามารถนำการเรียนการสอนรวมถึงความรู้ในด้านต่างๆ มาบรรจุในแอพพลิเคชั่น Smart Soldier เพื่อให้กำลังพลสามารถเรียนรู้ได้ในทุกระดับ และสามารถพัฒนาการจัดเป็นคลังความรู้แต่ให้มีการกำหนดการเข้าถึงเพื่อใช้เป็นแหล่งข้อมูลต่างๆ ในทุกๆ ด้านให้กับหน่วยของกองทัพบกในการค้นหาและใช้ประโยชน์ต่อไป

4. ขาดงบประมาณ หน่วยงานที่รับผิดชอบไซเบอร์ไม่ว่าจะเป็น ศซบ.ทบ. และ ศปสท.ศปก.ทบ. ยังไม่มีการจัดทำแผนงบประมาณในการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ที่เป็นลักษณะหลักสูตรการเรียนการสอนที่ชัดเจน

แนวทางการเสริมสร้างความรู้ภัยคุกคามไซเบอร์ให้กับกำลังพลกองทัพบก

จากการวิเคราะห์สภาพแวดล้อมและปัจจัยที่มีผลต่อการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบก รวมถึงปัญหาอุปสรรคและศึกษา

แนวคิดทฤษฎีที่เกี่ยวข้องทำให้สามารถกำหนดแนวทางการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบกได้ดังนี้

1. ด้านบุคลากร กำลังพลกองทัพบกทุกนายควรได้รับการศึกษาอบรมด้านภัยคุกคามไซเบอร์และมีการประเมินผลเป็นระยะ เช่นปีละ 1 ครั้ง เพื่อให้กำลังพลทุกนาย มีความรู้ความเข้าใจเท่าทันต่อการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามทางไซเบอร์ สามารถป้องกันตนเองให้ปลอดภัยจากภัยคุกคามดังกล่าว และรักษาความลับทางราชการในความรับผิดชอบของหน่วยงานตนเองได้อย่างมีประสิทธิภาพ

2. ด้านเครื่องมือ ควรมีการพัฒนาหลักสูตรการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก โดยนำหลักสูตรที่มีความสำคัญจากเว็บไซต์ของสถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัล (TDGA) มาประยุกต์ใช้ให้เหมาะสมกับกลุ่มเป้าหมายซึ่งเป็นกำลังพลของกองทัพบกและใช้แอพพลิเคชั่น Smart Soldier เป็นช่องทางในการเผยแพร่หลักสูตรซึ่งจะเป็นการนำทรัพยากรที่มีอยู่มาใช้ให้เกิดประโยชน์สูงสุด โดยใช้การเรียนการสอนเหมือนกับในระบบ E-learning ของเว็บไซต์ TDGA และนำมาปรับปรุงให้เหมาะสมกับการเรียนการสอนของกองทัพบกทั้งด้านเนื้อหาและมีระบบการประเมินผลให้มีประสิทธิภาพ

3. ด้านงบประมาณ ควรมีการจัดสรรงบประมาณด้านการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้หน่วยงานที่เกี่ยวข้องที่รับผิดชอบของกองทัพบกอย่างเพียงพอและต่อเนื่อง เนื่องจากเป็นภารกิจที่สำคัญและมีการดำเนินการต่อเนื่องโดยเฉพาะกำลังพลที่บรรจุใหม่

4. ด้านการบริหารจัดการ ควรกำหนดหน่วยงานที่รับผิดชอบโดยตรงด้านการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก รวมทั้งจัดสรรทรัพยากรให้เพียงพอทั้งกำลังพลและงบประมาณ สำหรับหน่วยต่างๆ ของกองทัพบกควรมีการบริหารจัดการให้ฝ่ายกำลังพลมารับผิดชอบในดำเนินการในการจัดการให้กำลังพลทุกนายได้รับการดำเนินการ

บทที่ 3
บทอภิปรายผล

ในบทที่ 3 เป็นการอภิปรายผลการวิจัย ซึ่งผู้วิจัยได้นำข้อมูลจากการวิจัยเอกสารต่างๆ ที่เกี่ยวข้องมาใช้ในการอภิปรายผล รายละเอียดมีดังนี้

1. การวิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษามหาวิทยาลัย[6] มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษามหาวิทยาลัยในประเทศไทย โดยได้ทำการเก็บรวบรวมข้อมูลด้วยแบบสอบถามออนไลน์ระหว่างเดือนเมษายนถึงเดือนพฤษภาคม 2565 จากนักศึกษามหาวิทยาลัยในประเทศไทย ระดับอนุปริญญาและระดับปริญญา จำนวนทั้งหมด 422 คน ผลการวิจัยพบว่า ปัจจัยหลักที่ส่งผลต่อการตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษามหาวิทยาลัย ได้แก่ ความรู้ ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ ความปลอดภัยของอุปกรณ์ และการเชื่อมต่อและพฤติกรรมของผู้ใช้งาน ซึ่งสอดคล้องกับงานวิจัยครั้งนี้ที่ได้เสนอให้เห็นถึงปัจจัยที่ส่งผลต่อการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบกเพื่อให้กำลังพลมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ต่อไป

2. การวิจัยเรื่อง การออกแบบและพัฒนาระบบสืบค้นข้อมูลเกี่ยวกับอาชญากรรมทางไซเบอร์[7] ผู้วิจัยได้ออกแบบและพัฒนาระบบสืบค้นข่าวอาชญากรรม โดยรวบรวมข่าวเกี่ยวกับอาชญากรรมทางไซเบอร์ในช่วงปี 2553 - 2557 จากสื่อสิ่งพิมพ์ ข้อความข่าวและคลิปข่าวทำให้การสืบค้นข้อมูลมีประสิทธิภาพมากขึ้น ระบบงานนี้พัฒนาโดยใช้ภาษา PHP และโปรแกรมจัดการฐานข้อมูล MySQL มีผู้ใช้งาน ทั้งหมด 3 กลุ่ม ได้แก่กลุ่มที่ 1 คือ ผู้ใช้งานทั่วไปทำการสืบค้นข้อมูลข่าวอาชญากรรมที่ต้องการ กลุ่มที่ 2 คือ สมาชิกจะคล้ายกับผู้ใช้งานทั่วไป แต่ต่างกันที่สมาชิกสามารถเพิ่มข้อมูลขาวเข้าภายในระบบได้กลุ่มที่ 3 คือ ผู้ดูแลระบบจะทำหน้าที่จัดการทุกอย่างภายในระบบ ตั้งแต่การจัดการข้อมูล ข่าว คลิปข่าว จัดการข้อมูลสมาชิก รวมถึงแก้ไข ยืนยัน ยกเลิก หรือลบข่าวออกจากระบบ ซึ่งจาก การสอบถามผู้ที่ใช้งานระบบดังกล่าวพบว่าข้อมูลและฟังก์ชันต่างๆ สามารถตอบสนองความต้องการ ได้เป็นอย่างดีและมีความพึงพอใจต่อการออกแบบ

และจัดรูปแบบของเว็บไซต์และยังพบอีกว่าระบบนี้เป็นที่สนใจของผู้ที่เคยมีประสบการณ์จากการถูกก่ออาชญากรรมทางไซเบอร์เป็นอย่างมาก งานวิจัยนี้สอดคล้องกับแนวทางการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก กล่าวคือในการพัฒนาหลักสูตรควรนำข้อมูลหรือแหล่งข้อมูลเกี่ยวกับการสืบค้นข้อมูลอาชญากรรมทางไซเบอร์มาบรรจุไว้ในเนื้อหาของหลักสูตรโดยคัดเลือกข้อมูลที่มีความสำคัญและทันสมัยซึ่งจะเป็นประโยชน์ต่อกำลังพลกองทัพบก

3. การวิจัยเรื่อง การประยุกต์ใช้ E-Learning ในกระบวนการเรียนการสอน ของวิทยาลัยเทคโนโลยี บริหารธุรกิจมีนบุรี กรุงเทพ[8] เป็นการจัดการเรียนรู้โดยใช้ระบบ E-Learning เข้ามาเป็นส่วนเสริมใน การเรียนการสอนผ่านทางระบบเครือข่ายอินเทอร์เน็ต ผู้เรียนสามารถเข้าถึงบทเรียนและกิจกรรมต่างๆ ที่ผู้สอนจัดเตรียมไว้ให้ได้จากทุกสถานที่ทุกเวลาที่มีการออนไลน์ ในการนำระบบ E-Learning มาประยุกต์ใช้ในการเรียนการสอนนั้นเพื่อเพิ่มโอกาสในการเข้าถึงเนื้อหาบทเรียน ได้จากอุปกรณ์ ต่างๆ เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ ผ่านทางระบบเครือข่ายอินเทอร์เน็ต และเพื่อลดระยะเวลาในการเรียนในห้องเรียนของผู้เรียน ทำให้ผู้เรียนสามารถใช้เวลาในการทำกิจรรมเสริมการเรียนรู้อื่น ซึ่งการนำระบบ E-learning เข้ามาเป็นส่วนเสริมในกระบวนการเรียนการสอนนั้น จะเกิดประโยชน์เป็นอย่างยิ่ง โดยผู้เรียนมีโอกาสที่จะเข้าถึงเนื้อหาที่หลากหลายมากยิ่งขึ้น ผู้สอนก็สามารถออกแบบการเรียนรู้โดยใช้สื่อมัลติมีเดีย ทั้งในรูปข้อความ ภาพ เสียง และภาพเคลื่อนไหว ทำให้การเรียนการสอนมีความน่าสนใจและสื่อความหมายได้ดีกว่าการเรียนภายในห้องเรียนเพียงอย่างเดียว ซึ่งสอดคล้องกับงานวิจัยในเรื่องการหาแนวทางการสอนความรู้ให้กับกำลังพลของกองทัพบกด้วยระบบ E-Learning จำทำให้การเรียนง่ายต่อการเข้าถึงและสามารถใช้เวลาในการเรียนได้ทุกเวลาได้ในหลายอุปกรณ์ไม่ว่าจะเป็น คอมพิวเตอร์ โทรศัพท์มือถือ ไม่จำเป็นต้องเรียนในห้องเรียน สามารถนำไปบรรจุในแอพพลิเคชั่นของกองทัพบกเช่น Smart soldier ของกองทัพบก เพื่อให้กำลังพลกองทัพบกได้สามารถใช้งานในการเรียนรู้ได้

4. การวิจัยเรื่อง การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลอง การโจมตีด้วยฟิชชิ่ง นำเสนอการศึกษาเพื่อยกระดับความตระหนักรู้ของบุคลากรภายในองค์กรแห่งหนึ่งเกี่ยวกับภัยคุกคาม ความมั่นคง

ปลอดภัยทางไซเบอร์โดยใช้การจำลองการโจมตีด้วยอีเมลฟิชชิ่ง[9] หลังจากที่ได้มีรวบรวมข้อมูลจากบุคลากรจำนวน 482 คน แล้วทำการวิเคราะห์ด้วยสถิติพื้นฐาน พบว่า มีบุคลากรมากกว่า 22.41 % ที่เปิดอ่านอีเมลดังกล่าวและทำการคลิก ลิงก์ที่อยู่ในอีเมล เพื่อยกระดับความตระหนักรู้เกี่ยวกับภัยทางไซเบอร์ซึ่งเป็นเรื่องที่สำคัญ จึงมีการจัดกระบวนการถ่ายทอด ความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากร หลังจากนั้นได้มีการจำลองการโจมตีด้วยฟิชชิ่งอีกครั้งด้วย เนื้อหาในอีเมลที่แตกต่างจากเดิม เมื่อได้รวบรวมข้อมูลจากบุคลากรกลุ่มเดิม แล้วทำการวิเคราะห์อีกครั้ง พบว่า มีบุคลากร น้อยกว่า 7.88 % ที่เปิดอ่านอีเมลดังกล่าวและทำการคลิกลิงก์ที่อยู่ในอีเมล ซึ่งลดลงประมาณ 64.81 % เมื่อเทียบ กับผล การศึกษาในครั้งที่ 1 ทำให้ค่าระดับความความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ของบุคลากรในองค์กรเพิ่มสูงขึ้นเป็น 88.80 % นั่นแสดงว่ากระบวนการถ่ายทอดความรู้ที่ดำเนินการไปสามารถให้ผลลัพธ์ที่ดี ฉะนั้นการศึกษานี้จึงมีคุณค่าสำหรับ นำไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ในองค์การอื่นและกับการโจมตีรูปแบบอื่นได้[9] จากการวิจัยดังกล่าวสอดคล้องการการสร้างความตระหนักรู้ให้กับผู้เรียนในแง่ของการได้รับประสบการณ์ในการถูกโจมตีทางไซเบอร์ในรูปแบบต่างจะสร้างความตระหนักรู้ให้กับผู้เรียนตามที่ได้เป็นอย่างดี และสามารถนำไปสร้างรูปแบบการเรียนในรูปแบบต่างๆ ตามภัยคุกคามที่ปรับเปลี่ยนไปในปัจจุบัน

5. การวิจัยเรื่อง การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[10] มีผลการศึกษาพบว่า แนวทางการพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย 3 ด้าน ได้แก่ ด้านการศึกษา ด้านการฝึกอบรม และด้านการพัฒนา โดยมีปัญหาและอุปสรรคในการพัฒนาทักษะบุคลากร ดังนี้ ด้านงบประมาณได้รับการจัดสรรไม่เพียงพอ หลักสูตรการศึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีจำนวนน้อย ส่งผลให้มีผู้เชี่ยวชาญด้านไซเบอร์น้อย บุคลากรของสำนักงานมีจำนวนน้อย ส่งผลให้บุคลากรไม่มีเวลาในการพัฒนาตนเอง บุคลากรของสำนักงานขาดความรู้ความเข้าใจและอุปกรณ์ที่ใช้ในการปฏิบัติงาน ส่วนแนวทางการแก้ไขปัญหา คือ การสร้างความร่วมมือกับหน่วยงานทั้งภายในและต่างประเทศให้เห็นถึง

ความสำคัญของภัยคุกคามทางไซเบอร์ เพื่อแลกเปลี่ยนบุคลากรและสนับสนุนงบประมาณ ข้อเสนอแนะของงานวิจัย คือ การวางแผนเป้าหมายและวิสัยทัศน์ให้ชัดเจนในการพัฒนาบุคลากร โดยบุคลากรควรจัดสรรเวลาการทำงานให้ดีเพื่อหาเวลาไปพัฒนาตนเอง และควรเพิ่มโอกาสบุคลากรและประชาชนทั่วไปให้เข้าถึงความรู้ทางด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ทางสื่อสังคมออนไลน์ จากการวิจัยดังกล่าวสอดคล้องการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ของกองทัพบกในเรื่องการวางแผนในการปรับปรุงพัฒนาแนวทางการให้ความรู้การวางแผนพัฒนาทั้งระบบให้มีความเหมาะสมและครอบคลุมในทุกด้าน

บทที่ 4
บทสรุป

การศึกษาวิจัยเรื่อง การเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบก มีวัตถุประสงค์ เพื่อศึกษาแนวทางการป้องกันภัยคุกคามทางไซเบอร์ให้กับกำลังพลของกองทัพบก เพื่อศึกษาถึงปัจจัยที่มีผลต่อการศึกษาด้วยตนเองและหาแนวทางการแก้ไข และเพื่อหาแนวทางการใช้เครื่องมือของกองทัพบก คือ แอปพลิเคชัน Smart Soldier ในการเป็นคลังความรู้ให้กำลังพลค้นคว้าหาข้อมูลภัยคุกคามทางไซเบอร์ ผู้วิจัยใช้รูปแบบการวิจัยเชิงยุทธศาสตร์ตามแนวทางที่วิทยาลัยการทัพบกกำหนด โดยใช้วิธีการศึกษาเชิงเอกสาร การรวบรวมข้อมูลจากเอกสารทางวิชาการ เอกสารการวิจัย วิทยานิพนธ์ แนวคิดและทฤษฎีที่เกี่ยวข้อง วิเคราะห์ข้อมูลที่เกี่ยวข้องกับหลักสูตร จุดแข็ง จุดอ่อน โอกาส และอุปสรรค โดยยึดจุดประสงค์สุดท้ายเพื่อพัฒนาแนวทางการให้ความรู้กับกำลังพลกองทัพบกให้สามารถพัฒนาศักยภาพบุคลากรที่พร้อมปฏิบัติหน้าที่ และมีการตระหนักรู้ในภัยคุกคามทางไซเบอร์ ดำเนินการวิจัยในห้วงระหว่างเดือนธันวาคม 2565 – เดือนพฤษภาคม 2566 ผลการวิจัยสรุปได้ดังนี้

สรุปผลการวิจัย

สภาพแวดล้อมด้านการเมือง การทหาร เศรษฐกิจ สังคม ข้อมูลข่าวสาร และโครงสร้างพื้นฐาน มีผลต่อการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์กับกำลังพลกองทัพบก ที่ผ่านมา การดำเนินงานดังกล่าวมีปัญหาอุปสรรค ได้แก่ การขาดหน่วยงานที่รับผิดชอบโดยตรง บุคลากรที่มีความรู้ความเชี่ยวชาญไม่เพียงพอ ไม่มีการวางแผนงบประมาณในการพัฒนาหลักสูตรและขาดเครื่องมือทั้งหลักสูตรและเทคโนโลยีสนับสนุน ดังนั้นผู้วิจัยจึงเสนอแนวทางในการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบกดังนี้

1. ด้านบุคลากร กำลังพลกองทัพบกทุกนายควรได้รับการศึกษาอบรมด้านภัยคุกคามไซเบอร์และมีการประเมินผลเป็นระยะ เช่นปีละ 1 ครั้งเพื่อให้กำลังพลทุกนายมีความรู้ความเข้าใจเท่าทันต่อการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามทาง

ไซเบอร์ สามารถป้องกันตนเองให้ปลอดภัยจากภัยคุกคามดังกล่าวและรักษาความลับทางราชในความรับผิดชอบของหน่วยงานตนเองได้อย่างมีประสิทธิภาพ

2. ด้านเครื่องมือควรมีการพัฒนาหลักสูตรการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก โดยนำหลักสูตรที่มีความสำคัญจากเว็บไซต์ของสถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัล (TDGA) มาประยุกต์ใช้ให้เหมาะสมกับกลุ่มเป้าหมายซึ่งเป็นกำลังพลของกองทัพบกและใช้แอพพลิเคชั่น Smart Soldier เป็นช่องทางในการเผยแพร่หลักสูตรและประเมินผลซึ่งจะเป็นการนำทรัพยากรที่มีอยู่มาใช้ให้เกิดประโยชน์สูงสุด

3. ด้านงบประมาณ ควรมีการจัดสรรงบประมาณด้านการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้หน่วยงานที่เกี่ยวข้องที่รับผิดชอบของกองทัพบกอย่างเพียงพอและต่อเนื่อง เนื่องจากเป็นภารกิจที่สำคัญและมีการดำเนินการต่อเนื่องโดยเฉพาะกำลังพลที่บรรจุใหม่

4. ด้านการบริหารจัดการ ควรกำหนดหน่วยงานที่รับผิดชอบโดยตรงด้านการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลกองทัพบก รวมทั้งจัดสรรทรัพยากรให้เพียงพอทั้งกำลังพลและงบประมาณ สำหรับหน่วยต่างๆ ของกองทัพบกควรมีการบริหารจัดการให้ฝ่ายกำลังพลมารับผิดชอบในดำเนินการในการจัดการให้กำลังพลทุกนายได้รับการดำเนินการ

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะเชิงนโยบาย

1.1 กองทัพบกควรให้ความสำคัญในเรื่องการเสริมสร้างความรู้ภัยคุกคามทางไซเบอร์ให้กับกำลังพลโดยนำแนวทางที่เสนอในการวิจัยครั้งนี้ไปใช้ให้เกิดผลอย่างเป็นรูปธรรมเพื่อมอบหมายหน่วยงานที่รับผิดชอบให้ดำเนินการต่อไป

1.2 ควรมีการประสานงานระหว่างกองทัพบกกับ สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) ในเรื่องการพัฒนาหลักสูตรเพื่อให้มีความเหมาะสมในบริบทของกองทัพบกและมีการปรับปรุงหลักสูตรให้มีความทันสมัยอยู่เสมอ

1.3 ควรมีการบรรจุหลักสูตรด้านภัยคุกคามทางไซเบอร์ในสถาบันการศึกษาของกองทัพบก เช่น วิทยาลัยการทัพบก โรงเรียนเสนาธิการทหารบก โรงเรียนนายร้อยพระจุลจอมเกล้า และโรงเรียนเหล่าสายวิทยาการ ทั้งในการศึกษาของนายทหารสัญญาบัตรและนายทหารประทวน เพื่อสร้างภูมิคุ้มกันให้กับกำลังพลของกองทัพบก

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

2.1 ควรมีการวิจัยพัฒนาหลักสูตรเพื่อกำหนดโครงสร้างหลักสูตรและเนื้อหาให้มีความเหมาะสมสำหรับกลุ่มเป้าหมายกำลังพลกองทัพบกในระดับต่างๆ ตั้งแต่นายทหารสัญญาบัตร นายทหารประทวน และพลทหารกองประจำการ

2.2 ควรมีการวิจัยประเมินผลเพื่อประเมินผลลัพธ์ที่เสนอในการวิจัยครั้งนี้ไปประยุกต์ใช้และปรับปรุงการดำเนินงานให้มีประสิทธิภาพยิ่งขึ้นต่อไป

เอกสารอ้างอิง

1. ฐกฤต แก้วทับทิม. การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์; 2564(2); 163-80.

2. สำนักงานสภาพัฒนาเศรษฐกิจและสังคมแห่งชาติ. ยุทธศาสตร์ชาติ 20 ปี พ.ศ. 2561 - 2580 [อินเทอร์เน็ต]. 2565 [เข้าถึงเมื่อ 25 ธันวาคม 2565]. เข้าถึงได้จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2561/A/082/T_0001.PDF

3. สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. แผนแม่บทภายใต้ยุทธศาสตร์ชาติ พ.ศ. 2561-2580 [อินเทอร์เน็ต]. 2565 [เข้าถึงเมื่อ 25 ธันวาคม 2565]. เข้าถึงได้จาก http://www.nscr.nesdc.go.th/wp-content/uploads/2019/04/01-ความมั่นคง.pdf

4. สำนักนโยบายและแผนกลาโหม. แผนปฏิบัติราชการ ระยะ 5 ปี พ.ศ. 2566 - 2570 ของกระทรวงกลาโหม. 2566.

5. แผนปฏิบัติราชการประจำปีงบประมาณ พ.ศ. 2565 ของกองทัพบก [อินเทอร์เน็ต]. 2565 [เข้าถึงเมื่อ 25 ธันวาคม 2565]. เข้าถึงได้จาก http://kmlo.crma.ac.th/qaedu_crma/wp-content/uploads/2022/04/แผนปฏิบัติ

6. กิติยา วิสิฐพงศ์พันธ์, ชูเกียรติ บุญก่อเกื้อ, กิตติพงศ์ อยู่นิรันดร และนลินภัสร์ บำเพ็ญเพียร. ปัจจัยที่ส่งต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย. วารสารวิชาการวิทยาศาสตร์มหาวิทยาลัยราชภัฏจันเกษม. 2565; 32(1): 33.

7. วีรากร พงศ์พนิตานนท์. การออกแบบและพัฒนาระบบสืบค้นข้อมูลเกี่ยวกับอาชญากรรมทางไซเบอร์ [วิทยานิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยกรุงเทพ; 2557.

8. อนุชา สะเล็ม. การประยุกต์ใช้ E-Learning ในกระบวนการเรียนการสอน วิทยาลัยเทคโนโลยีบริหารธุรกิจมีนบุรีกรุงเทพ [สารนิพนธ์ วิทยาศาสตรมหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยเทคโนโลยีมหานคร; 2560.

9. สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี. การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลองการโจมตีด้วยฟิชชิ่ง. Journal of Science and Technology Thonburi University. 2020; 4(2): 1.

10. วราภรณ์ เพลิดเพลิน. การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [วิทยานิพนธ์ ปริญญารัฐประศาสนศาสตรมหาบัณฑิต]. กรุงเทพฯ: มหาวิทยาลัยรามคำแหง; 2565.

ประวัติย่อผู้วิจัย

ยศ ชื่อ พันเอก สุวิทย์ วิจิตรกาญจน์

วัน เดือน ปีเกิด 23 เมษายน 2520

ประวัติสำเร็จการศึกษา

พ.ศ. 2544	วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ โรงเรียนนายร้อยพระจุลจอมเกล้า
พ.ศ. 2555	โรงเรียนเสนาธิการทหารบก หลักสูตรหลักประจำ ชุดที่ 90

ประวัติการทำงาน

พ.ศ. 2545 - 2554	กองพันทหารราบที่ 2 กรมทหารราบที่ 12 รักษาพระองค์
พ.ศ. 2556 - 2562	กองพลทหารราบที่ 2 รักษาพระองค์
พ.ศ. 2562 - 2563	กองพันทหารราบที่ 2 กรมทหารราบที่ 12 รักษาพระองค์
พ.ศ. 2563 - 2565	กองพันทหารราบที่ 3 กรมทหารราบที่ 12 รักษาพระองค์
พ.ศ. 2565 - 2565	มลฑลทหารบกที่ 12

ตำแหน่งปัจจุบัน

พ.ศ. 2565 - ปัจจุบัน	รองเสนาธิการกองพลทหารราบที่ 2 รักษาพระองค์