การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

เอกสารวิจัยส่วนบุคคล

โดย

พันเอกหญิง สุชาดา บุญวัฒนะ

ประจำ สำนักงานตรวจสอบภายในทหารบก

วิทยาลัยการทัพบก

กันยายน 2566

เอกสารวิจัยเรื่อง การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

โดย พันเอกหญิง สุชาดา บุญวัฒนะ

อาจารย์ที่ปรึกษา พันเอกหญิง นวลสมร จรวงษ์

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2566 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ **ดีมาก**

พลตรี **ผู้บัญชาการวิทยาลัยการทัพบก**
(ฉกาจ ขันตี)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก **ประธานกรรมการ**
(สินสมุทร์ จันทรเนตร)

พลตรี **ผู้ทรงคุณวุฒิที่ปรึกษา**
(กัณห์ สถิตยุทธการ)

พันเอกหญิง **กรรมการ**
(นวลสมร จรวงษ์)

พันเอกหญิง **กรรมการ**
(ณภัค ภัคคะกรณ์)

บทคัดย่อ

ผู้วิจัย พันเอกหญิง สุชาดา บุญวัฒนะ

เรื่อง การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

วันที่ 6 กันยายน 2566 **จำนวนคำ :** 9,402 **จำนวนหน้า :** 28

คำสำคัญ ประสิทธิภาพ, การก่อการร้ายทางไซเบอร์, กรมข่าวทหารบก

ชั้นความลับ ไม่มีชั้นความลับ

การศึกษาวิจัย เรื่อง “การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก” ฉบับนี้ มีวัตถุประสงค์ เพื่อศึกษาสภาพปัญหาที่มีผลต่อการปฏิบัติงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก เพื่อศึกษาขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก และเพื่อกำหนดแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

จากการวิจัย พบว่า ปัจจัยที่มีผลต่อการต่อต้านการก่อการร้ายทางไซเบอร์ คือ นโยบาย แผนงาน โครงสร้างพื้นฐานทางไซเบอร์ของกรมข่าวทหารบก ยังขาดการสื่อสารที่ชัดเจน ทำให้แผนการดำเนินการไม่ต่อเนื่อง ระบบไฟร์วอลล์ ระบบตรวจหาการบุกรุก ซอฟแวร์ป้องกันไวรัส ความทันสมัยของอุปกรณ์ กำลังพลขาดทักษะ ความรู้ ความเชี่ยวชาญในการใช้ระบบ การรู้เท่าทันโลกไซเบอร์ ความต่อเนื่องในการปฏิบัติงาน รวมถึง การถ่ายทอดองค์ความรู้ให้กำลังพล ปัจจุบัน ขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมการข่าวทหารบก มีนโยบาย แผนปฏิบัติงาน ปกป้องโครงสร้างพื้นฐาน แจ้งเตือน ฟื้นฟูความเสียหาย ปกป้องภัยคุกคามทางไซเบอร์รูปแบบต่างๆ และการรู้เท่าทันโลกไซเบอร์ ไม่หลงเชื่อข่าวปลอม ชัวร์ก่อนแชร์ จากผลการวิจัยได้เสนอให้มีแนวทาง การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก ดังต่อไปนี้ ปรับโครงสร้างหน่วย พัฒนาระบบสารสนเทศสนับสนุนการฝึกอบรม และงบประมาณ พร้อมรับมือจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ

ABSTRACT

AUTHOR: Female Colonel Suchada Boonwattha

TITLE: Efficiency Developing Anti-Handling with Cyber Terrorism of Directorate of Intelligence.

DATE: 6 September, 2023 **WORD COUNT :** 9,402 **PAGES :** 28

KEY TERMS: Efficiency, Anti-Handling with Cyber Terrorism, Directorate of Intelligence.

CLASSIFICATION: Unclassified

This research study: Efficiency Developing Anti-Handling with Cyber Terrorism of Directorate of Intelligence. The aim of; to study problems affecting work performance anti-handling with cyber terrorism of directorate of intelligence, to capability in anti-handling with cyber terrorism of directorate of intelligence and to efficiency development guidelines anti-Handling with cyber terrorism of directorate of intelligence program.

The research finding; factors affecting anti-handling with cyber terrorism is policies, plans, cyber infrastructure not communication is the plan discontinuous and firewall system, intrusion detection system, antivirus software, equipment modernization, the personnel have no skills, without knowledge and expertise of system, cyber literacy and continuous in performance, including knowledge transfer to the personnel Current to capability in anti-handling with cyber terrorism of directorate of intelligence there is a policy, operational plan Infrastructure protection, alerting, disaster recovery protects against a wide range of cyber threats and cyber security literacy. Don't believe in fake news be sure before sharing. The results of the research have proposed a guideline development guidelines anti-Handling with cyber terrorism of directorate of intelligence is restructure the unit, information system development, is support training and budget, with all forms of cyber threats.

กิตติกรรมประกาศ

การวิจัยเชิงยุทธศาสตร์ เรื่อง “การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก” ตามแนวทางการศึกษาในหลักสูตรประจำวิทยาลัยการทัพบก ชุดที่ 68 ฉบับนี้ สำเร็จไปได้ด้วยดี ด้วยความกรุณาจาก พันเอก สินสมุทร์ จันทรเนตร ประธานกรรมการควบคุมเอกสารวิจัยส่วนบุคคล และพันเอกหญิง ณภัค ภัคคะกรณ์ กรรมการควบคุมเอกสารวิจัยส่วนบุคคล และผู้ทรงคุณวุฒิทุกท่านที่สละเวลาอันมีค่า ให้คำแนะนำ และกำลังใจ ตลอดจนความคิดเห็น แนะแนวทางการปรับปรุงงานวิจัยให้สมบูรณ์แบบมากยิ่งขึ้น

ขอขอบพระคุณ ผู้บังคับบัญชาทั้งในอดีต และปัจจุบัน ที่ให้ความรู้ คำแนะนำ และสั่งสอนประสบการณ์การทำงานต่างๆ และ ให้โอกาสมาศึกษาในสถาบันวิทยาลัยการทัพบก อันทรงเกียรติแห่งนี้

ขอขอบพระคุณ พลตรี ฉกาจ ขันตี ผู้บัญชาการวิทยาลัยการทัพบก และคณาจารย์วิทยาลัยการทัพบกทุกท่าน ที่ประสิทธิประสาทวิชาความรู้ อบรม สั่งสอน ช่วยเหลือ ให้คำแนะนำ และแบ่งปันประสบการณ์อันมีค่ายิ่งแก่ผู้วิจัยมาโดยตลอด และขอขอบคุณเจ้าของหนังสือ เอกสารทางวิชาการ วารสาร บทความ และงานวิจัยทุกเล่ม ที่ทำให้งานวิจัยนี้มีความสมบูรณ์

ขอขอบพระคุณ พันเอกหญิง นวลสมร จรวงษ์ อาจารย์ที่ปรึกษา และ พลตรี กัณห์ สถิตยุทธการ ผู้ทรงคุณวุฒิที่ปรึกษา ที่กรุณาให้แนวคิดที่เป็นประโยชน์ในการศึกษา และการจัดทำเอกสารวิจัยส่วนบุคคล รวมถึงตรวจสอบต้นฉบับอย่างละเอียด นอกเหนือจากข้อแนะนำทางวิชาการ อันเป็นประโยชน์ในการวิจัยแล้ว ยังได้รับกำลังใจและคำชี้แนะที่เป็นประโยชน์ยิ่ง ตั้งแต่กำหนดหัวข้อวิจัย จนการจัดทำรูปเล่มสมบูรณ์ ให้ลุล่วงและเสร็จสมบูรณ์เป็นอย่างดี

ขอขอบคุณเพื่อนวิทยาลัยการทัพบก ชุดที่ 68 ทุกท่านที่คอยให้กำลังใจ ห่วงใย และช่วยเหลือกันมาตลอดจนจบหลักสูตร รวมไปถึงเจ้าหน้าที่ประจำหลักสูตรที่คอยดูแล เป็นพี่เลี้ยง อำนวยความสะดวกในการศึกษาดูงานทุกท่าน

ประโยชน์อันเกิดจากงานวิจัยฉบับนี้ ผู้วิจัยขอมอบแด่อาจารย์ที่ปรึกษา และเพื่อนๆ ผู้ที่ให้การสนับสนุนในการศึกษา การทำงาน และกำลังใจจนสำเร็จลุล่วงไปได้ด้วยดี

สารบัญ

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

สภาวการณ์ปัจจุบันทั่วโลกเผชิญกับภัยที่เกิดจากการคุกคามทางเทคโนโลยีสารสนเทศและเครือข่ายอินเทอร์เน็ต ช่องทางที่ถูกโจมตีจากภัยคุกคามทางไซเบอร์ไม่ได้เกิดแค่บนเว็บไซต์ หรือโลกออนไลน์เท่านั้น แต่ยังเกิดจากอุปกรณ์และเทคโนโลยีต่างๆ ที่สร้างขึ้นด้วย จึงส่งผลให้เกิดจุดอ่อนหรือช่องโหว่ (Vulnerability) ในการก่อภัยคุกคามทางไซเบอร์มากยิ่งขึ้น นอกจากนี้ รูปแบบการเกิดภัยคุกคามยังเปลี่ยนแปลงไปตามยุคสมัย จากการขยายตัวของภัยคุกคามทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว บ่อยครั้งและรุนแรงมากขึ้น ซึ่งมักสร้างผลกระทบเชิงลบต่อความมั่นคง โดยภัยคุกคามทางไซเบอร์ที่เป็นประเด็นสำคัญมี 2 มิติ คือ มิติที่ 1 การโจมตีทางไซเบอร์ (Cyber Attack) และมิติที่ 2 การครอบงำทางไซเบอร์ (Cyber Dominance)[1] การโจมตีทางไซเบอร์ หรือโจมตีทางเครือข่าย นับเป็นอีกเป้าหมายสำคัญของกลุ่มผู้ก่อการร้ายและผู้ไม่หวังดีที่ใช้เป็นช่องทางสร้างความเสียหายต่อประเทศ นับเป็นภัยคุกคามต่อความมั่นคงของชาติรวมไปถึงอิทธิพลของสื่อประเภทเครือข่ายสังคมออนไลน์ ที่ใช้เป็นเครื่องมือสำคัญของประชาชนภายในประเทศ ในการรวมตัวดำเนินกิจกรรม และเคลื่อนไหวกิจกรรมทางการเมืองด้วยการใช้วิธีการเข้าครอบงำความคิด ทัศนคติของผู้คนผ่านทางสื่อสังคมออนไลน์และเผยแพร่ข่าวสารไปอย่างรวดเร็ว ก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์และภัยคุกคามรูปแบบใหม่ อาทิ การก่อการร้ายสากล อาชญากรรมข้ามชาติ การก่อความไม่สงบในพื้นที่ต่าง ๆ และมีแนวโน้มที่ทวีความรุนแรงขึ้นทุกวัน

จากยุทธศาสตร์ชาติ 20 ปี ประเด็นความมั่นคง (พ.ศ. 2561 – 2580) การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง และการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคง[2] กองทัพบกจึงได้จัดทำแผนปฏิบัติราชการ (พ.ศ. 2566) แผนปฏิบัติราชการ เรื่อง การเสริมสร้างศักยภาพและความพร้อมของกองทัพเพื่อการป้องกันประเทศการสนับสนุนการปฏิบัติภารกิจการรักษาความมั่นคงภายใน มีเป้าหมาย กองทัพบกมีความพร้อมในการเผชิญภัยคุกคามทางทหาร

และภัยคุกคามรูปแบบต่าง ๆ แนวทางการพัฒนาระบบข่าวกรอง เพื่อแจ้งเตือนภัยคุกคามทางทหาร พัฒนาขีดความสามารถด้านไซเบอร์ ด้วยการร่วมมือกับทุกภาคส่วน[3]

กองทัพบกได้ตระหนักถึงภัยอันตรายจากการสื่อสารซึ่งเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตของระบบเครือข่ายคอมพิวเตอร์นับล้าน ๆ เครื่อง โดยได้เริ่มทำการศึกษาและเตรียมความพร้อมให้แก่กำลังพลเพื่อรับมือกับการโจมตีทางไซเบอร์ที่กองทัพบก โดย พลเอก ประยุทธ์จันทร์โอชา อดีตผู้บัญชาการทหารบก ได้มีนโยบายและอนุมัติหลักการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงานให้เป็นไปตามนโยบายของรัฐบาลโดยร่วมมือกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security: NCSC)[4] ในปัจจุบันกองทัพบกได้มุ่งเน้นการปรับเปลี่ยนโครงสร้างขององค์กร (Structure) ทบทวนอัตรากำลัง (Body) กำหนดบทบาทและหน้าที่ (Role and responsibility) ของหน่วยด้านไซเบอร์ เพื่อรับมือ ป้องกัน และลดความเสี่ยงต่อ ภัยคุกคามทางไซเบอร์ (Cyber Threat) ทั้งการโจมตีทางไซเบอร์ (Cyber Attack) และการครอบงำทางไซเบอร์ (Cyber Dominance)[1]

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อใช้เป็นเครื่องมือในการโจมตีก่อให้เกิดความเสียหายได้เทียบเคียงกับสงครามจริงที่มีการใช้อาวุธในการสู้รบ ซึ่งสงครามไซเบอร์เป็นส่วนหนึ่งของสงครามสารสนเทศ (Information Warfare) โดยเฉพาะอย่างยิ่งการโจมตีที่มีเจตนาเกี่ยวกับระบบสารสนเทศ เพื่อวัตถุประสงค์เชิงกลยุทธ์ หรือการทหาร ซึ่งมีการโจมตีหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด เช่น การโจมตีเว็บไซต์ บล็อคเว็บ การโฆษณาชวนเชื่อ (Propaganda) ด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต การเจาะข้อมูลลับ เป็นต้น ดังนั้น การปฏิบัติงานทางทหารมีการใช้เทคโนโลยีสารสนเทศในการค้นหารวบรวม ดักฟัง ขโมยข้อมูลของฝ่ายตรงข้าม เพื่อช่วงชิงความได้เปรียบในเรื่องข้อมูลข่าวสาร ประกอบการตัดสินใจของผู้นำระดับสูง ในทางตรงกันข้าม ปัญหาที่ตามมาจากภัยคุกคามไซเบอร์ และเปลี่ยนมาเป็นสงครามไซเบอร์มีการต่อสู้แบบ การปฏิบัติการข่าวสาร (Information Operations : IO) ด้านความมั่นคงกล่าวถึง ปัญหาภัยคุกคามไซเบอร์ อาชญากรรมไซเบอร์ที่ซับซ้อนขึ้น รูปแบบการก่อสงครามที่ใช้เทคโนโลยีเป็นเครื่องมือ ซึ่งครอบคลุมความมั่นคงปลอดภัยไซเบอร์ในด้านความมีจริยธรรมและการไม่ละเมิดสิทธิส่วนบุคคล และการปกป้องอธิปไตยไซเบอร์เพื่อรักษาผลประโยชน์ของชาติ[6]

จากสถานการณ์ภัยคุกคามไซเบอร์ข้างต้นที่กล่าวมานั้น ผู้วิจัยในฐานะผู้ปฏิบัติหน้าที่ในส่วนงานประสานงานชายแดน ขึ้นตรงกับกรมข่าวทหารบก ได้วิเคราะห์ประเด็นภัยคุกคามทางไซเบอร์ หน่วยงานรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ จึงเล็งเห็นความสำคัญและความจำเป็นของปัญหา ดังนั้นจึงได้ศึกษา การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก เพื่อให้สอดคล้องกับยุทธศาสตร์ชาติและรองรับภัยคุกคามทางไซเบอร์ ต่อต้านการก่อการร้ายทางไซเบอร์ทั้งในปัจจุบันและอนาคตต่อไป

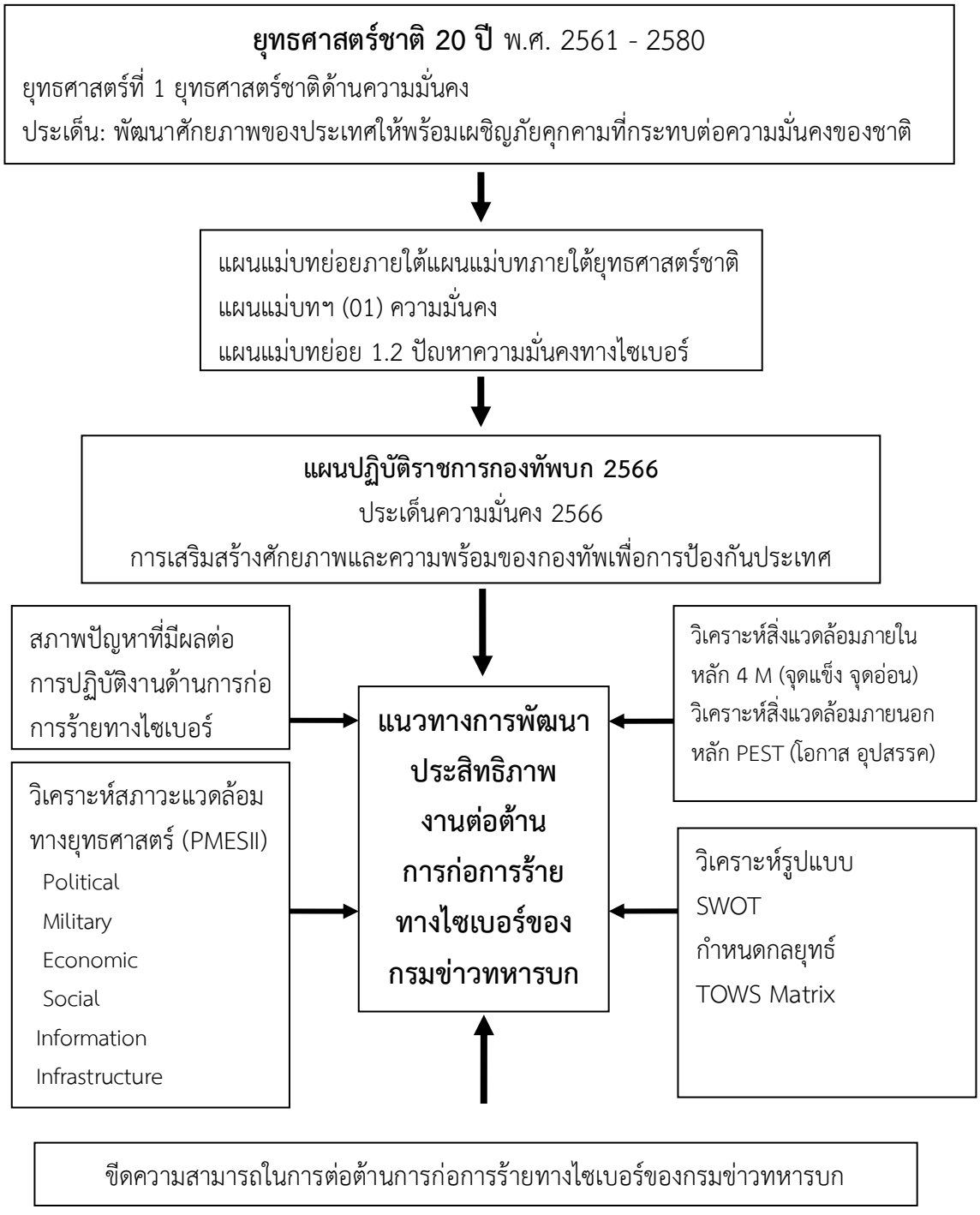
วัตถุประสงค์การวิจัย

1. เพื่อศึกษาสภาพปัญหาที่มีผลต่อการปฏิบัติงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

2. เพื่อศึกษาขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

3. เพื่อกำหนดแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีการศึกษา

1. แนวทางการวิจัย

รูปแบบการวิจัยเชิงยุทธศาสตร์ตามที่วิทยาลัยการทัพบกกำหนด

2. ขอบเขตการศึกษา

ศึกษาสภาพปัญหาความพร้อมของกำลังพล และระบบของหน่วยข่าวกรองไซเบอร์ทางทหารในปัจจุบัน รวมทั้งศึกษา และวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ของโลก ภูมิภาค และในประเทศ ที่ส่งผลต่อแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

3. การเก็บรวบรวมข้อมูล

ข้อมูลการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นด้านความมั่นคง พ.ศ. 2561-2580 และแผนปฏิบัติราชการประจำปีงบประมาณ 2566 ของกองทัพบก แนวคิด ทฤษฎี และหลักการจากหนังสือ บทความ วารสาร และงานวิจัยที่เกี่ยวข้อง

4. การวิเคราะห์ข้อมูล

วิเคราะห์เนื้อหาข้อมูล โดยใช้กรอบการคิดเชิงยุทธศาสตร์ สำหรับวิเคราะห์และสังเคราะห์ข้อมูลจากทางเลือกยุทธศาสตร์ เพื่อหาแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

5. ขั้นตอนการดำเนินงาน

การดำเนินการวิจัยประกอบด้วยกิจกรรม จำนวน 6 ขั้นตอน โดยใช้ระยะเวลาดำเนินการ 6 เดือน ตั้งแต่เดือน ธันวาคม 2565 ซึ่งสามารถนำเสนอเอกสารวิจัยที่สมบูรณ์ได้ภายในเดือนพฤษภาคม 2566

ประโยชน์ที่คาดว่าจะได้รับ

1. ทราบสภาพปัญหาที่มีผลต่อการปฏิบัติงาน แนวทางการติดตาม ตรวจสอบ รวบรวมข้อมูล ความเคลื่อนไหว และเฝ้าระวังภัยคุกคามความมั่นคงทางไซเบอร์ เพื่อแจ้งเตือนป้องกันและระงับยับยั้งภัยคุกคามทางไซเบอร์ของกรมข่าวทหารบกได้

2. ทราบแนวทางการยกระดับขีดสามารถในการปฏิบัติงานของกำลังพลและระบบของเทคโนโลยีข่าวกรองทางไซเบอร์ของกรมข่าวทหารบกได้

3. เสนอแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบกได้

บทที่ 2
บทวิเคราะห์

ปัจจุบันกองทัพบกได้เตรียมความพร้อมสำหรับพัฒนาศักยภาพของกำลังพล เพื่อเตรียมการรองรับกับภัยคุกคามความมั่นคง จากภัยคุกคามในรูปแบบผสมการรับมือกับภัยคุกคามที่มองไม่เห็นบนโลกไซเบอร์ กองทัพบกในฐานะเป็นกำลังหลักด้านความมั่นคงของประเทศ ได้จัดตั้งศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) เป็นหน่วยรับผิดชอบงานด้านไซเบอร์ เป็นหน่วยขึ้นตรงกองทัพบก มีหน้าที่สำคัญในการปกป้องอธิปไตย และความมั่นคงของประเทศ เพื่อการต่อต้านการก่อการร้ายทางไซเบอร์เอาชนะองค์กรและเครือข่ายของผู้ก่อการร้าย กรมข่าวทหารบกมีหน้าที่ วางแผน อำนวยการ ประสานงาน กำกับและดำเนินการเกี่ยวกับงานด้านข่าว ความเคลื่อนไหวของฝ่ายตรงข้าม หรือกลุ่มที่มีแนวโน้มที่จะเป็นภัยคุกคามต่อความมั่นคงของชาติ วิเคราะห์แหล่งข่าว ข้อเท็จจริงของข่าวที่ได้รับเพื่อเตรียมการป้องกันได้ทันท่วงที ดังนั้น งานวิจัยฉบับนี้ จึงมุ่งเน้นในการวิเคราะห์หาแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก เพื่อให้สามารถตอบสนองภารกิจของกองทัพบกได้อย่างมีประสิทธิภาพสูงสุด สอดรับกับแผนปฏิบัติราชการของกองทัพบก และสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี

วิเคราะห์สภาพปัญหาที่มีผลต่อการปฏิบัติงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

กองทัพบกได้เล็งเห็นความสำคัญของการนำเทคโนโลยีสารสนเทศและการสื่อสารมาเสริมสร้างประสิทธิภาพในการบริหาร และการปฏิบัติงานของกองทัพให้เกิดประสิทธิภาพ รวมถึงการพัฒนากำลังพลให้ “ทันโลก ทันงาน ทันข้อมูลข่าวสาร และทันคน” ได้พัฒนาตลอดมาจนก่อตั้งเป็นศูนย์ไซเบอร์กองทัพบก เพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบก และหน่วยที่เกี่ยวข้อง โดยทำหน้าที่ เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ ที่ส่งผลกระทบต่อสถาบัน และความมั่งคงของชาติ การรวบรวมวิเคราะห์ ทิศทาง แนวโน้ม โครงข่ายความสัมพันธ์ของข้อมูล ประเภทสื่อและกลุ่มเป้าหมาย การติดตาม สืบค้น แหล่งที่มาและเป้าหมาย และการกำหนดมาตรการป้องปราม ตอบโต้ สกัดกั้น รวมถึงการประสานการดำเนินการตามกฎหมาย[7]

1. ปัญหาภัยคุกคามทางไซเบอร์ต่อความมั่นคงของชาติ

ภัยคุกคามทางด้านไซเบอร์ทางการทหาร ถือว่าเป็นภัยที่คุกคามความมั่นคงระดับชาติ ซึ่งเชื่อมโยงไปสู่ด้านต่าง ๆ เป็นภัยที่เกิดจากการนำเทคโนโลยีสารสนเทศมาใช้ในทางที่ผิดกฎหมาย รวมทั้งการละเมิดต่อศีลธรรม และความสงบสุขของสังคม เป็นภัยร้ายแรงอีกรูปแบบหนึ่งในด้านการทหาร ซึ่งในปัจจุบันมีหลากหลายรูปแบบ เช่น การสอดแนมข้อมูลผ่านอุปกรณ์ประเภท “IoT” (Internet of Things), การแพร่ระบาดของไวรัสเรียกค่าไถ่ (Ransomware), การโจมตีระบบแม่ข่ายคอมพิวเตอร์ให้ปฏิเสธ หรือหยุดการให้บริการ “DDoS” (Distributed Denial-of-Service) และยุทธการทางข้อมูลข่าวสาร “IO” (Information Operation) การแพร่กระจายข้อมูลข่าวสารที่จัดทำขึ้นอย่างแนบเนียน (Fake News และ Deepfakes) เพื่อหวังผลให้เกิดการตอบสนองต่อข้อมูลข่าวสารในแนวทางที่ต้องการ การโจมตีทางไซเบอร์ในปัจจุบัน ได้แก่ เนื้อหาที่เป็นภัย (Abusive Content) โปรแกรมไม่พึงประสงค์ (Malicious Code) ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ความพยายามบุกรุก เข้าระบบ (Intrusion Attempts) การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) การโจมตี สภาพความพร้อมใช้งานของระบบ (Availability) การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Content Security) การฉ้อฉล ฉ้อโกงหรือ หลอกลวงเพื่อผลประโยชน์ (Fraud) การละเมิดนโยบายขององค์กร (Policy Violation) ช่องโหว่ (Vulnerability)[8] ความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ เนื่องจากการใช้งานผ่านอินเทอร์เน็ต สมาร์ทโฟน และแท็บเล็ต ในการติดต่อสื่อสารระหว่างกันของบุคคล และการติดต่อกันระหว่างหน่วยงานภาครัฐ/เอกชน ทำให้เกิดการเชื่อมโยงแลกเปลี่ยนข้อมูลได้ทุกที่ทุกเวลา ดังนั้น จึงมีช่องโหว่ของโอกาสที่ทำให้เกิดภัยคุกคามทางไซเบอร์ได้ง่ายมากขึ้น ระดับภัยคุกคามไซเบอร์ที่มีผลต่อโครงสร้างพื้นฐานหลักของประเทศไว้ 5 ระดับดังนี้[9]

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติ (National Government) คือ ภัยที่เป็นอันตรายต่อประเทศเป็นการปล่อยข่าวที่ไม่น่าเชื่อถือ การเข้าไปโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ในหน่วยงานของรัฐ หรือการเจาะระบบของโครงสร้างพื้นฐานที่เป็นระบบ การเงินการธนาคาร และระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบประปา ซึ่งให้บริการกับประชาชนในประเทศ

2. ภัยจากการก่อการร้ายสากล (Terrorists) โดยเฉพาะกลุ่มก่อการร้ายต้องการโจมตีต่อประเทศคู่ขัดแย้งทางการเมือง มุ่งทำลายประโยชน์ทางการเมือง เพื่อสร้างความหวาดกลัวไปยังประชาชนในประเทศนั้น ๆ

3. ภัยจากสายลับหรือพวกจารกรรมข้อมูลในภาคอุตสาหกรรม และองค์กรเครือข่ายอาชญากรรม (Industries Spies and Organized Crime Groups) ซึ่งภัยด้านนี้จะกำหนดให้เป็นภัยคุกคามระดับกลางของประเทศ

4. ภัยจากกลุ่มแฮกเกอร์ (Hacktivist) ที่มีอุดมการณ์ซึ่งเกิดจากการรวมกลุ่มของพวกแฮกเกอร์ รวมกันโจมตีเว็บไซต์ของรัฐบาล โดยมีแรงจูงใจจากอุดมการณ์ทางการเมืองหรือความคิดเห็นที่แตกต่างทางการเมือง เพราะกลุ่มแฮกเกอร์เหล่านั้นเห็นว่า รัฐบาลหรือหัวหน้ารัฐบาลในประเทศนั้นๆ ได้ดำเนินนโยบายที่ขัดต่อสิทธิเสรีภาพในการแสดงออกหรือลิดรอนสิทธิเสรีภาพของบุคคล และการปิดกั้นสิทธิเสรีภาพทางการเมืองของประชาชน

5. ภัยจากกลุ่มแฮกเกอร์มือสมัครเล่น (Hackers) โดยกลุ่มแฮกเกอร์จะประชาสัมพันธ์ทางเว็บไซต์ เพื่อรวบรวมพวกมือสมัครเล่นให้รวมกันโจมตีเว็บไซต์ของหน่วยงานภาครัฐ ภาคเอกชน และส่งผลกระทบอย่างกว้างขวางจนสร้างความเสียหายในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติที่ถูกโจมตีได้อย่างมหาศาล

การจัดตั้งศูนย์ไซเบอร์กองทัพบก[10] ได้ดำเนินการภายใต้หลักการบริหารงานเชิงกลยุทธ์ 4 ประการ (POLE) คือ

1. การวางแผนงาน (Planning)

2. การจัดองค์กร (Organizing)

3. การนำไปสู่การปฏิบัติ (Leading)

4. การประเมินผล (Evaluating)

ศูนย์ไซเบอร์กองทัพบก มีแผนการดำเนินงาน และมีการพัฒนาอย่างต่อเนื่อง โดยให้น้ำหนักไปที่มาตรการเชิงรับ คือการพัฒนาระบบป้องกันเครือข่ายข้อมูลของหน่วยงานในกองทัพ ส่วนเชิงรุกสำหรับประเทศไทยยังต้องมีความชัดเจนเกี่ยวกับเรื่องของกฎหมาย แต่อย่างไรก็ตาม ได้มีการเตรียมความพร้อมในเรื่องของการพัฒนาบุคลากร เพื่อเตรียมสำหรับภารกิจที่ท้าทายทางด้านไซเบอร์ กองทัพบกได้กำหนดภารกิจในเรื่องของความมั่นคงของชาติเป็นหลัก โดยให้ความสำคัญ และกำหนดระดับภัยคุกคามทางด้านไซเบอร์ไว้ 4 ประการ

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.)

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันฯ

4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ

นอกเหนือจากภารกิจทั้ง 4 ประการที่กล่าวมา ศูนย์ไซเบอร์กองทัพบกยังได้รณรงค์ปลูกฝังให้ความรู้แก่กำลังพล และประชาชนให้เกิดความตระหนักในเรื่องของการใช้เครื่องมือสื่อสารอย่างฉลาดปลอดภัย ไม่ตกเป็นเหยื่อ/เป็นพาหะ ในการแพร่กระจายความผิดโดยรู้เท่าไม่ถึงการณ์ด้วย

2. การโจมตีทางไซเบอร์

ปัญหาการคุกคามในโลกไซเบอร์มีการโจมตีหลากหลายรูปแบบ และแต่ละประเภทของภัยคุกคามจะมีลักษณะการโจมตีเป็นของตัวเองถึงแม้อาจจะมีความคล้ายคลึงกันบ้างก็ตามซึ่งรูปแบบการโจมตีทั่วไปทางไซเบอร์ มีดังต่อไปนี้[11]

1. เนื้อหาที่เป็นภัย (Abusive Content)

2. โปรแกรมไม่พึงประสงค์ (Malicious Code)

3. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)

4. ความพยายามเข้าบุกรุก ระบบ (Intrusion Attempts)

5. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)

6. การโจมตี สภาพความพร้อมใช้งานของระบบ (Avai;ability)

7. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Content Security)

8. การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (Fraud)

9. การละเมิดนโยบายขององค์กร (Policy Violation)

10. ช่องโหว่ (Vulnerability)

ในทางการทหารนั้น พื้นที่ไซเบอร์ ถูกนิยามว่าเป็นสนามรบแบบใหม่ (New battlefield)ที่มี ความสำคัญเท่ากับพื้นที่บก น้ำ อากาศและอวกาศ[12] ดังนั้น จึงมีการวางยุทธศาสตร์ ยุทธการ และยุทธวิธี ให้สอดคล้องกับสนามรบไซเบอร์ นอกจากนี้เพื่อป้องกันพื้นที่ไซเบอร์ และโครงสร้างพื้นฐานที่สำคัญทางไซเบอร์ หลายประเทศได้มีการพัฒนาอาวุธไซเบอร์ (Cyber weapon) เพื่อใช้ในการโจมตีไซเบอร์ที่มีศักยภาพในการก่อความเสียหายทางกายภาพจริง นอกจากนี้ งานศึกษาร่วมสมัยยังชี้ให้เห็นว่า ปัญญาประดิษฐ์ที่สามารถควบคุมข้อมูลอาจถูกใช้เป็นส่วนหนึ่งในการทำสงครามไซเบอร์ ดังนั้น การคิดเกี่ยวกับความมั่นคงไซเบอร์ จึงต้องพิจารณาถึงความไม่มั่นคงที่เกิดจากการใช้ปัญญาประดิษฐ์ด้วย

(AI-enabled vulnerabilities)[13] ในแง่ระดับความรุนแรง ผู้เชี่ยวชาญอย่างเบร็ท ไมเคิล แห่งวิทยาลัยนาวิกโยธินชั้นสูง (สหรัฐอเมริกา) ก็ให้ความสนใจกับระดับของความขัดแย้งทางไซเบอร์ เขาให้ความเห็นว่า “มิใช่การโจมตีไซเบอร์ทุกกรณี จะถือว่าเข้าข่ายการโจมตีโดยใช้อาวุธ (Armed attacks)”[14] บทความ Cyber War Will Not Take Place โธมัส ริด ได้อธิบายว่า สงครามไซเบอร์ ยังไม่เคยเกิดขึ้นเพราะความขัดแย้งทางไซเบอร์ ไม่ได้มีลักษณะ 3 ประการ ที่เป็นองค์ประกอบของสงคราม ในความหมายแบบ เคลาซ์ วิทซ์ ได้แก่ การใช้ความรุนแรง เพื่อก่อความเสียหายอย่างร้ายแรง (Lethality) การใช้ความรุนแรงดังกล่าว นับเป็นเครื่องมือ ที่ทำให้อีกฝ่ายยอมรับเจตจำนงของผู้ใช้ความรุนแรงและมีแรงจูงใจทางการเมืองที่สื่อสารออกมาอย่างชัดเจน[15] ดังนั้น ในทัศนะของริด การโจมตีไซเบอร์ยังไม่ถึงขั้นทำให้เป้าหมายถึงแก่ชีวิตโดยตรง

3. ปัญหาภัยการครอบงำทางไซเบอร์

การครอบงำทางไซเบอร์ หมายถึง การถูกชี้นำ หรือครอบงำทางความคิด โดยไม่รู้ตัวจากอำนาจของสารสนเทศและสื่อมัลติมีเดีย รวมถึงการสร้างกระแสเทียมบนสื่อสังคมออนไลน์ เช่น การปั่นกระแสด้วยแฮชแท็ก การโพสต์ข่าวลือเทียม การสร้างข่าวปลอม เป็นต้น ซึ่งส่งผลกระทบต่อความคิดเห็น ความเชื่อ และการตอบสนองของประชาชนโดยรวม จากผลการศึกษาข้อมูลจากต่างประเทศทั้ง 17 ประเทศ และประเทศไทย พบว่า แต่ละประเทศประสบปัญหาภัยการครอบงำทางไซเบอร์ที่คล้ายคลึงกัน ซึ่งสามารถสรุปประเภทการครอบงำ และเหตุการณ์ภัยการครอบงำทางไซเบอร์ที่สำคัญทั่วโลก ได้ดังนี้[16] ข่าวปลอม การได้รับข้อมูลที่ไม่ถูกต้อง โฆษณาชวนเชื่อ การล้อเลียน ยั่วยุ เพื่อสร้างกระแส การกลั่นแกล้งบุคคลทางสื่อโซเชียล การชักใย ถ้อยคำสร้างความเกลียดชัง การเผยแพร่ลัทธิและความเชื่อ เป็นต้น

4. รูปแบบของการป้องกันการก่อการร้ายทางไซเบอร์

1. การป้องกันทางกายภาพ (Physical Security)[17] เป็นมาตรการที่ใช้ป้องกันข้อมูล และทรัพย์สินจากภัยคุกคามทางกายภาพ ทั้งโดยเจตนาและไม่เจตนา ด้วยการจำกัดให้เฉพาะผู้ที่มีหน้าที่ในการใช้งานเท่านั้น

2. ระบบไฟร์วอลล์ (Firewall) เป็นระบบป้องกันอันตรายที่มาจากอินเทอร์เน็ต หรือเครือข่ายภายนอก มีหน้าที่ควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกที่ไม่ปลอดภัยกับเครือข่ายภายในองค์กร

3. ระบบการตรวจหาการบุกรุก (Intrusion Detection System) เป็นระบบที่ใช้ตรวจหาการใช้งานเครือข่ายภายในองค์กร ในทางที่ผิดไปจากกฎข้อบังคับ ส่งผลต่อความ

มั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต กลไกระบบตรวจหาการบุกรุกเป็นการวิเคราะห์กิจกรรมต่าง ๆ ที่เกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ ด้วยการตรวจสอบกับข้อกำหนดการใช้งาน และการตรวจสอบจากสถิติการใช้งาน

4. วิทยาการเข้ารหัสข้อมูล (Cryptography) คือกรรมวิธีที่ใช้สำหรับแปลงข้อมูลทั่วไปให้เป็นข้อความที่เข้ารหัส เพื่อส่งไปยังผู้รับ เมื่อผู้รับได้รับก็จะถอดรหัสข้อมูล (Decryption) เพื่อให้ได้ข้อมูลเดิม

5. การใช้ซอฟแวร์ป้องกันไวรัส โดนการติดตั้งโปรแกรมกำจัดไวรัส และตรวจสอบเป็นประจำ ปรับปรุง หรืออัพเดทโปรแกรมกำจัดไวรัส ตรวจสอบอุปกรณ์ บันทึกข้อมูลจากการใช้งานร่วมกับผู้อื่น สังเกตความผิดปกติที่เกิดขึ้นในแต่ละวัน หลีกเลี่ยงการคัดลอกโปรแกรมจากภายนอก[18]

การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก เป็นการพัฒนาประสิทธิภาพการปฏิบัติงานของกำลังพลในหน่วยข่าว ในการเฝ้าระวังภัยคุกคาม และแจ้งเตือนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้เหมาะสมตอบสนองกับผู้ใช้ในงานในทุกระดับ การวิเคราะห์ ตรวจสอบ และการรายงานผลการก่อการร้ายทางไซเบอร์เป็นไปอย่างรวดเร็ว ทำให้ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่ รวมถึงเป็นการลดปริมาณทรัพยากรในหน่วยงาน และสามารถรักษาความลับทางด้านความมั่นคงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

วิเคราะห์ขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

1. ขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

เพื่อเสริมสร้างขีดความสามารถในการรองรับสถานการณ์การก่อการร้ายทางไซเบอร์ ที่อาจจะเกิดขึ้นได้ตลอดเวลา กองทัพบกได้ปฏิบัติตามแผนยุทธศาสตร์ แผนยุทธศาสตร์กองทัพบก ด้านความมั่นคง การป้องกันประเทศที่เกี่ยวข้องกับการป้องกันภัยคุกคามทางไซเบอร์ ด้วยการดำเนินกลยุทธ์ ด้านการจัดเตรียมกำลัง เสริมสร้างพัฒนาให้กองทัพบกมีความพร้อมในการใช้กำลัง เพื่อการป้องกัน ป้องปรามแก้ไขและยุติความขัดแย้ง รวมทั้งความสำคัญต่อความพร้อมของกองทัพในการเผชิญกับภัยคุกคามทางไซเบอร์ระดับประเทศ การวิจัยและพัฒนาวิทยาศาสตร์และเทคโนโลยีเพื่อการทหารและความมั่นคง และอุตสาหกรรมป้องกันประเทศ เพื่อให้เกิดความชัดเจนมากขึ้น

วิเคราะห์ขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก ด้วยแนวความคิดของ National Cybersecurity Capacity Maturity Model (CMM)[19] โครงสร้างของ CMM ได้แบ่งมุมมองการประเมินศักยภาพ และขีดความสามารถในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ ออกเป็น 5 มิติ ดังนี้

มิติที่ 1 เป็นขีดความสามารถในการพัฒนานโยบายและกรอบแนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ การบริหารจัดการในภาวะวิกฤต การปกป้องโครงสร้างพื้นฐานที่สำคัญ การเตือนภัยล่วงหน้า การฟื้นฟูหรือซ่อมแซมความเสียหาย รวมถึงความสามารถในการพัฒนานโยบายความมั่นคงที่มีประสิทธิภาพในการปกป้องและทนทานต่อภัยคุกคาม

มิติที่ 2 Cyber Culture and Society การปรับมุมมองและทัศนคติของประชาชนในเรื่องความเชื่อมั่นในการใช้ชีวิตในโลกไซเบอร์ เป็นการสร้างความเชื่อมั่นของประชาชนการใช้บริการอินเทอร์เน็ต หรือ Online Service ต่างๆ รวมทั้งความเข้าใจของประชาชนในเรื่องความเสี่ยงในการใช้อินเทอร์เน็ต

มิติที่ 3 Cybersecurity Education, Training and Skills การบริหารจัดการเรื่องการสร้างความตระหนักรู้ถึงความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์ ของภาครัฐภาคเอกชน และประชาชนทั่วไป ตลอดจนการอบรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของภาครัฐ ภาคเอกชนและประชาชนทั่วไป

มิติที่ 4 Legal and Regulatory Frameworks การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ถือว่าเป็นอีกมิติที่มีความจำเป็นต้องพัฒนาเพื่อให้เท่าทันการเปลี่ยนแปลงทางดิจิทัล (Digital Transformation) ที่กำลังเกิดขึ้นและส่งผลกระทบต่อการดำเนินชีวิตของประชาชนทั่วโลก

มิติที่ 5 Standards, Organizations, and Technologies การพัฒนามาตรฐานและการปฏิบัติตามมาตรฐานที่เกี่ยวกับการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การควบคุมความมั่นคงปลอดภัยไซเบอร์ การใช้เทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยไซเบอร์ในระดับบุคคล ระดับองค์กร และโครงสร้างพื้นฐานของประเทศ ตลอดจนการพัฒนาเทคโนโลยีเพื่อลดความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

วิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์

เพื่อให้เข้าใจสภาพปัญหา และคาดการณ์สภาวะแวดล้อมทางยุทธศาสตร์ เพื่อนำมาประยุกต์ใช้เป็นแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก ได้ดังนี้

1. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับโลก

การเปลี่ยนแปลงของสภาวะโลกในปัจจุบัน ไม่ว่าจะเป็น การเมือง เศรษฐกิจ สังคมจิตวิทยา การทหาร วิทยาศาสตร์ เทคโนโลยี การพลังงาน ทรัพยากรธรรมชาติและสิ่งแวดล้อม มีผลกระทบอย่างสำคัญต่อมนุษย์ ทำให้พฤติกรรมการบริโภคของมนุษย์เปลี่ยนไป กระตุ้นให้เกิดการเปลี่ยนแปลงของเทคโนโลยี (Digital Disruption) ส่งผลให้มีการสร้างนวัตกรรมและการพัฒนาเทคโนโลยีต่างๆ อย่างรวดเร็วเพื่อตอบสนองความต้องการของผู้คน[19] เกิดเป็นแนวโน้มการเปลี่ยนแปลงของโลกอนาคต ที่เรียกว่า “Mega Trends” ที่ทั่วโลกนำมาเป็นปัจจัยในการวิเคราะห์คาดการณ์อนาคตเพื่อเป็นแนวทางของการพัฒนาแผนงานในมิติต่างๆ รวมทั้งประเทศไทยที่มีการบรรจุเรื่องของ Mega Trends ไว้ในร่างแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 ครอบคลุมระยะเวลา 5 ปี (พ.ศ. 2565-2570)[20]

2. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับภูมิภาค

จากการศึกษาสภาวะแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับภูมิภาค พบว่า การเปลี่ยนแปลงไปสู่สังคมดิจิทัล (Digitalization) ก็นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ต และคอมพิวเตอร์เป็นช่องทางในการโจมตี หรือที่เรียกว่า อาชญากรรมไซเบอร์(Cyber-Crime)[21] อาเซียนเป็นภูมิภาคที่มีจำนวนผู้ใช้อินเทอร์เน็ตเติบโตเร็วที่สุดในโลก ภายในอาเซียนมีประชากรกว่าครึ่งหนึ่งเป็นผู้ใช้สื่อสังคมออนไลน์ (Social Media) จึงทำให้อาเซียนเป็นตลาดสังคมออนไลน์อันดับหนึ่งของโลก และจากการจัดอันดับ 10 ประเทศผู้ใช้เฟซบุ๊ก (Facebook) มากที่สุดในโลก พบว่าประเทศสมาชิกอาเซียน 4 ได้แก่ อินโดนีเซีย ฟิลิปปินส์เวียดนาม และไทยเป็นกลุ่มประเทศที่อยู่ในอันดับดังกล่าว[22] สำหรับอาเซียนนั้น อาชญากรรมไซเบอร์เป็นภัยคุกคามความมั่นคงที่ถูกกำหนดไว้ให้เป็นส่วนหนึ่งของอาชญากรรมข้ามชาติที่สำคัญ ภายใต้ประชาคมการเมืองและความมั่นคงของอาเซียน โดยความร่วมมือของอาเซียนด้านการจัดการปัญหาอาชญากรรมไซเบอร์สามารถแบ่งได้เป็น 3 ลักษณะ ได้แก่ 1) ความร่วมมือภายในอาเซียน ลักษณะของการจัดประชุม 2) ความร่วมมือในระดับพหุภาคี และ 3) การจัดทำตราสาร

อาเซียน และให้ความสำคัญอย่างมากต่อการส่งเสริมความร่วมมือ และการเสริมสร้างขีดความสามารถเพื่อรับมือกับความท้าทายทางไซเบอร์ และอาชญากรรมทางไซเบอร์

3. สภาวะแวดล้อมทางยุทธศาสตร์ในระดับประเทศ

จากการศึกษาสภาวะแวดล้อมความมั่นคงปลอดภัยทางไซเบอร์ระดับประเทศ สถานการณ์ทางไซเบอร์ที่เกิดขึ้นทางรัฐบาลของประเทศไทย ได้ออกนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยได้จัดตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ National Cybersecurity Committee ปัจจุบันเทคโนโลยี และระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนธุรกิจและองค์กรให้มีความก้าวหน้าและรวดเร็ว รวมทั้งการเปลี่ยนแปลงธุรกิจให้เข้าสู่สังคมดิจิทัล (Transformation) ทำให้ธุรกิจและองค์กรเหล่านั้นต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อธุรกิจและองค์กรเป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อช่วยเพิ่มความมั่นใจและมั่นคงต่อผู้ใช้บริการทั้งภาครัฐและภาคประชาชน กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ มีการร่วมมือและประสานงานกันและกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้ประชาชนเดือดร้อน

วิเคราะห์สภาพแวดล้อมการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก ภายใต้กรอบแนวคิด PMESII

การต่อต้านการก่อการร้ายทางไซเบอร์จากโลกไซเบอร์ หรือบนเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันการโจมตีทางไซเบอร์ก่อให้เกิดความเสียหาย และผลกระทบในวงกว้างทางด้านการเมือง เศรษฐกิจ และสังคมจิตวิทยา ซึ่งเป็นกำลังอำนาจแห่งชาติ (National Power) ในด้านความมั่นคงปลอดภัยของประเทศ

ด้านการเมือง (Political) ยุทธศาสตร์การแก้ไขปัญหาการก่อการร้ายทางไซเบอร์ มีการปรับเปลี่ยนเสมอเพื่อให้สอดคล้องกับสภาพแวดล้อม และพัฒนาการของกลุ่มอาชญากรรมทางไซเบอร์ที่มีการเปลี่ยนแปลงยุทธศาสตร์ และยุทธวิธีในการต่อสู้มากขึ้น การโจมตีไซเบอร์เป็นการสร้างความเสียหายต่อพื้นที่ไซเบอร์ที่รองรับการเก็บข้อมูล

และบริหารจัดการข้อมูล การทำธุรกรรมการเงิน และการควบคุมระบบการทำงานของโครงสร้างพื้นฐานภาครัฐ

ด้านการทหาร (Military) กองทัพบกได้ดำเนินการตามมาตรการเชิงรุกเพื่อให้รู้เท่าทันภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ มีการใช้สื่อออนไลน์เพื่อประโยชน์ในงานด้านการข่าว เพื่อป้องการการใช้สื่อเป็นเครื่องมือ ในการเผยแพร่แนวคิดที่นิยม การใช้ความรุนแรง การสอนการก่อการร้าย การจัดหาอาวุธ และวัสดุที่ใช้ประกอบเป็นอาวุธ รวมทั้งสอนวิธีการทำ การหาสมาชิกมาร่วมอุดมการณ์และก่อการร้ายเป็นภัยต่อความมั่นคงของชาติ ด้านการโจมตีไซเบอร์ก่อให้เกิดความเสียหายต่อพื้นที่ไซเบอร์ที่ถูกใช้เป็นส่วนหนึ่งในการทำงานของกองทัพบก ทั้งในการเก็บข้อมูลที่สำคัญต่อความมั่นคงของประเทศ การสั่งการบัญชาการ การควบคุมระบบอาวุธยุทโธปกรณ์ และโครงสร้างพื้นฐานที่สำคัญ รวมไปถึงวิธีปฏิบัติการไซเบอร์ในระดับยุทธการและยุทธวิธี ด้วยเหตุนี้ การต่อต้านการก่อการร้ายทางไซเบอร์ ด้วยการเฝ้าระวัง การติดตาม การตรวจสอบวิเคราะห์ไซเบอร์และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง ช่วยสนับสนุนการปฏิบัติการข่าวของกองทัพบก

ด้านเศรษฐกิจ (Economic) ในช่วงการระบาดของโควิด–19 มีการปรับเปลี่ยนรูปแบบการทำงาน โดยการนำระบบสารสนเทศ มาใช้ในการทำงาน อาทิเช่น การประชุมผ่านโปรแกรม Zoom การทำธุรกรรมออนไลน์ต่างๆ ทำให้เกิดช่องโหว่ เกิดการโจมตีทางไซเบอร์ในรูปแบบใหม่ๆ จึงต้องรักษาความปลอดภัยของข้อมูลส่วนตัว ผ่านระบบเทคโนโลยีสารสนเทศ ป้องกันความเสี่ยงจากความเชื่อมโยงทางการเงินการเคลื่อนย้ายเงินทุน และปริมาณธุรกรรมที่เพิ่มขึ้น นอกจากนั้น การเปลี่ยนแปลงหลังยุคโควิด – 19 โลกได้ก้าวจาก VUCA World ไปสู่ BANI World ส่งผลต่อภาคธุรกิจ อุตสาหกรรม เกิดการเปลี่ยนแปลงอย่างรวดเร็ว หรือถูกทำลายได้ตลอดเวลา เกิดความกังวล อยู่กับสภาวะที่คาดเดาได้ยาก และอาจกระทบต่อการวางแผนที่จะควบคุมสถานการณ์ต่างๆ

ด้านสังคม (Social) การใช้สื่อออนไลน์ในการปล่อยข่าวลวง ทำให้เกิดผลกระทบต่อความมั่นคงแห่งชาติ เกิดความแตกแยกของผู้คน ทั้งทางด้านเชื้อชาติ และศาสนา โดยเป็นการทำลายสังคมพหุวัฒนธรรม ในโลกไซเบอร์ และเครือข่ายสังคมออนไลน์ มีการนำประเด็นในอดีตทั้งประวัติศาสตร์ที่จริง และข้อมูลที่บิดเบือน การเชื่อมโยงข้อมูลจากข้อเท็จจริงที่แฝงด้วยเจตนาร้าย เป็นทั้งข้อมูลที่ผิดในแง่การตีความ และบิดเบือนเพราะจงใจเล่าด้วยเจตนาให้ร้าย มาใช้เป็นเงื่อนไขสร้างสถานการณ์รุนแรงก่อความไม่สงบเป็นภัยต่อความมั่นคงของชาติ

ด้านข้อมูลข่าวสาร (Information) ภัยคุกคามที่เกิดจากการใช้ หรือเผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม ทำลายความน่าเชื่อถือของบุคคล หรือสถาบัน เพื่อ

ก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าตามแฟลตฟอร์มต่างๆ (SPAM) รวมไปถึง การใช้สื่อสังคมออนไลน์ในการบิดเบือนข่าวสาร โดยมีทั้งข่าวที่เป็นความจริงและความจริงที่บิดเบือนเพื่อประโยชน์บางอย่าง เนื่องจากสื่อสังคมออนไลน์ไม่มีการควบคุมหรือควบคุมยาก จากเดิมสื่อถูกควบคุมโดยภาครัฐ แต่ปัจจุบันการเผยแพร่ข้อมูลเปลี่ยนไปโดยเทคโนโลยีและไม่มีการควบคุมกลั่นกรอง ทำให้การบิดเบือนและการกระจายข้อมูลข่าวสารไปในวงกว้างและง่ายขึ้นรวมถึงการควบคุมทำได้ยากอีกด้วย

ด้านโครงสร้างพื้นฐาน (Infrastructure) กองทัพบกมียุทธศาสตร์ชาติด้านไซเบอร์อย่างเป็นรูปธรรม มีการเตรียมความพร้อมในการต่อต้านการก่อการร้ายทางไซเบอร์ โดยอาศัยกรอบการดำเนินการ 5 ขั้นตอน ดังเช่น เดียวกับประเทศสหรัฐอเมริกา ประกอบด้วย ทราบภัยคุกคาม (Identify) ป้องกันภัยคุกคาม (Protect) ตรวจจับภัยคุกคาม (Detect) ตอบสนอง (Response) และคืนสภาพระบบ (Recovery) ซึ่งขั้นตอนเหล่านี้เป็นพื้นฐานของการรับมือกับการโจมตีด้านไซเบอร์ที่ทั่วโลกยอมรับ ป้องกันความเสี่ยงการโจมตีโดยการใช้มัลแวร์โจมตีระบบตรวจสอบและควบคุมการทำงานของระบบสาธารณูปโภคหรือต่อบริการสาธารณะ

ปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายนอกตามหลัก PEST Analysis สามารถสรุปแยกเป็นโอกาส และอุปสรรค ได้ดังนี้

นโยบาย กฎระเบียบ (Policy)

โอกาส กองทัพบกจัดมีแผนปฏิบัติราชการของกองทัพบก ซึ่งได้มีการเชื่อมโยงความสอดคล้องกับแผนระดับต่าง ๆ ของยุทธศาสตร์ชาติ

อุปสรรค ระเบียบราชการไม่เอื้ออำนวยในการปฏิบัติงานในการจัดอุปกรณ์ระบบสารสนเทศ ที่ทันสมัยเข้ามาใช้งาน ปัญหาการตั้งงบประมาณ จัดซื้อจัดจ้างที่ล่าช้า รวมไปถึงการเปลี่ยนแปลงระดับนโยบาย อีกทั้งการปรับปรุงโครงการบ่อยทำให้ขาดความต่อเนื่อง

เศรษฐกิจ (Economic)

โอกาส การเติบโตของเศรษฐกิจไทยรองรับการเติบโต และพัฒนาทางด้านเทคโนโลยีดิจิทัลมากขึ้น

อุปสรรค เนื่องจากตั้งแต่ปี 2019 ที่ผ่านมา เกิดการระเบิดของโควิด - 19 ส่งผลกระทบกับการเติบโตทางด้านเศรษฐกิจ จึงมีการปรับเปลี่ยนรูปแบบการทำงานที่ใช้ระบบสารสนเทศเข้ามามากขึ้น จึงเป็นโอกาสเกิดการโจมตีทางไซเบอร์ในรูปแบบใหม่ๆ

สังคม วัฒนธรรม (Social)

โอกาส การใช้สื่อ ดิจิทัล ที่เพิ่มมากขึ้นในยุคปัจจุบัน

อุปสรรค ความไม่เข้าใจในการใช้งานเทคโนโลยีที่มีความซับซ้อน รวมถึงภัยคุกคามที่คาดไม่ถึง

เทคโนโลยีสารสนเทศ (Technology)

โอกาส มีความก้าวหน้าและแนวโน้มของเทคโนโลยีที่เอื้อต่อการนำมาใช้ในหน่วยงาน มีการนำเทคโนโลยี มาประยุกต์กับงานของหน่วยงานอื่นๆ ได้หลากหลายมากขึ้น และ ทำให้มีนวัตกรรมและช่องทางการใช้งานเพิ่มขึ้น

อุปสรรค มีการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็วทำให้ปรับตัวไม่ทัน ข้อมูลถูกบิดเบือนในเครือข่ายสังคมออนไลน์ ที่สร้างความสับสน ขัดแย้งและเข้าใจผิด อีกทั้งภัยคุกคามทางไซเบอร์ในภาพรวมระดับนานาชาติทวีความรุนแรงมากขึ้น

การวิเคราะห์ขีดความสามารถของกำลังพลหน่วยไซเบอร์ทางทหาร

ปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในตามหลัก 4 M สามารถสรุปแยกเป็นจุดแข็ง และจุดอ่อนได้ดังนี้

กำลังพล (Man)

จุดแข็ง มีกำลังพลปฏิบัติงานด้านไซเบอร์ มีการวางแผนและจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานตามยุทธศาสตร์ มีการเสริมสร้างทักษะความรู้ให้กำลังพล ด้วยการจัดอบรม อาทิ หลักสูตรการพัฒนาขีดความสามารถศักยภาพ ด้านงานข่าวกรองทางไซเบอร์ มีการสร้างแรงจูงใจให้กำลังพลเพื่อเสริมสร้างศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากล

จุดอ่อน กำลังพลของกองทัพบกยังขาดการบูรณาการและการพัฒนาขีดความสามารถศักยภาพ ด้านงานต่อต้านการก่อการร้ายทางไซเบอร์ ซึ่งนับเป็นส่วนสำคัญในการทำความเข้าใจกับภัยคุกคามรูปแบบต่างๆ ส่วนใหญ่ยังขาดความรู้ ขาดกำลังพลที่เชี่ยวชาญ ขาดจิตสำนึกด้านการรักษาความปลอดภัยทางไซเบอร์

งบประมาณ (Money)

จุดแข็ง กองทัพบกมีการจัดสรรงบประมาณประจำปีให้กับศูนย์ไซเบอร์กองทัพบกและสนับสนุนงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์เป็นประจำทุกปี

จุดอ่อน งบประมาณที่ได้รับในแต่ละปี ไม่เพียงพอต่อการพัฒนางานด้านไซเบอร์ บุคลากรในการทำงาน ขาดการวางแผนการนำเสนอโครงการ เพื่อขอรับการสนับสนุนงบประมาณ ทำให้การพัฒนางานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ไม่มีความต่อเนื่อง

วัสดุอุปกรณ์ (Material)

จุดแข็ง ศูนย์ไซเบอร์ของกองทัพบก มีเครื่องมือระบบตรวจจับ โปรแกรมป้องกันความเสี่ยงระบบสารสนเทศ และป้องกันการโจมตีทางไซเบอร์ ที่ครอบคลุมเครือข่ายข้อมูลทั้งหมดภายในของแต่ละหน่วย และมีอุปกรณ์สื่อสารที่สามารถเข้าถึงอินเทอร์เน็ต

จุดอ่อน อุปกรณ์ที่ใช้ในชีวิตประจำวันอาศัยการใช้งานจากอินเทอร์เน็ตมากขึ้น ทำให้เสี่ยงต่อการเกิดภัยทางไซเบอร์ได้ง่ายขึ้น หน่วยงานมีอุปกรณ์ไม่เพียงพอและทันสมัย ขาดการบำรุงรักษาอุปกรณ์ทำให้บางชนิดไม่สามารถใช้งานได้ และระบบงานที่พัฒนาขึ้นเองบางโปรแกรม ไม่ได้สอดคล้องตามมาตรฐานการรักษาความปลอดภัยสารสนเทศสากล

การจัดการ (Management)

จุดแข็ง กองทัพบกมีนโยบาย และยุทธศาสตร์ที่ชัดเจน เกี่ยวกับการพัฒนางานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ มีโครงสร้างการจัดหน่วยงานที่รับผิดชอบงานไซเบอร์ขึ้นตรงกับกองทัพบก

จุดอ่อน โครงสร้างการทำงานมีสายการบังคับบัญชาที่ยาว บุคลากรผู้ใช้งานระบบคอมพิวเตอร์ยังขาดจิตสำนึกด้านความรักษาความปลอดภัย ขาดการบูรณาการเกี่ยวกับระบบการบริหารจัดการเครือข่ายเพื่อเสริมความมั่นคงของประเทศ ขาดการประสานงานระหว่างหน่วยงานภายในและภายนอกกองทัพบก ขาดการพัฒนาระบบและเทคโนโลยีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

จากการวิเคราะห์ด้วย SWOT จุดแข็ง จุดอ่อน โอกาส และอุปสรรคซึ่งประกอบด้วยปัจจัยภายในและปัจจัยภายนอกในภาพรวม มีรายละเอียดดังนี้ได้ดังนี้

จุดแข็ง (Strength) กองทัพบกมีหน่วยงานป้องกันภัยคุกคามทางไซเบอร์ระดับชาติ หน่วยงานป้องกันการครอบงำทางไซเบอร์ หน่วยงานไซเบอร์ทางการทหาร กฎหมายไซเบอร์ และเทคโนโลยีสมัยใหม่ มีโครงสร้างของหน่วยงานของรัฐบาลที่รับผิดชอบด้านความมั่นคงไซเบอร์ เป็นศูนย์ต่อต้านข่าวปลอม

จุดอ่อน (Weakness) กองทัพบกมีความเชื่อมโยงยุทธศาสตร์ และยุทธวิธีทางไซเบอร์ของหน่วยงานต่างๆ ยังไม่ชัดเจน กำลังพลที่ปฏิบัติงานด้านไซเบอร์ไม่เพียงพอ ขาดทักษะ ความเชี่ยวชาญด้านไซเบอร์ และขาดความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์

โอกาส (Opportunity) กองทัพบกมีหน่วยงาน ที่ปฏิบัติงานด้านสารสนเทศและเฝ้าระวังการครอบงำทางไซเบอร์บนสื่อสังคมออนไลน์ มีต้นแบบที่ดีของการจัดตั้งหน่วยงานป้องกันการครอบงำทางไซเบอร์ของต่างประเทศ อีกทั้งประเทศไทยมี พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ที่กำหนดให้มีการจัดทำกระบวนการ และมาตรการด้านไซเบอร์ มีความต่อเนื่องในการกำกับดูแลด้านไซเบอร์อย่างต่อเนื่อง โดยกำหนดและปรับปรุงกฎหมายที่เกี่ยวข้องต่างๆอย่างต่อเนื่อง

อุปสรรค (Threat) ปัจจุบันสังคมไทยบางส่วน มีทัศนคติเกี่ยวกับไซเบอร์ในเชิงลบ ทำให้การปฏิบัติด้านไซเบอร์ของกองทัพบกถูกมองในแง่ร้าย และไม่ได้รับการสนับสนุนเต็มที่ อีกทั้งหน่วยงานภายในประเทศไทยยังไม่เข้าใจเกี่ยวกับแนวทางปฏิบัติ บทลงโทษหรือข้อยกเว้นต่างๆ ตาม พ.ร.บ.

จากการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค SWOT ซึ่งประกอบด้วยปัจจัยภายใน และปัจจัยภายนอกที่ได้รับ นำเข้าสู่การวิเคราะห์ด้วยเครื่องมือ TOWS Matrix ตามขั้นตอนเพื่อกำหนดกลยุทธ์ จำนวน 4 ด้าน ประกอบด้วย กลยุทธ์เชิงรุก กลยุทธ์เชิงแก้ไข กลยุทธ์เชิงรับ กลยุทธ์เชิงป้องกัน มีรายละเอียดดังนี้

กลยุทธ์เชิงรุก (S,O) กองทัพบกมีหน่วยงานป้องกันภัยคุกคามทางไซเบอร์ทางการทหาร และเทคโนโลยีสมัยใหม่ ที่รับผิดชอบด้านความมั่นคงไซเบอร์ เป็นศูนย์ต่อต้านข่าวปลอมมี ปฏิบัติงานด้านสารสนเทศ และเฝ้าระวังการครอบงำทางไซเบอร์บนสื่อสังคมออนไลน์ มีการพัฒนาโครงสร้างพื้นฐาน และเทคโนโลยีด้านไซเบอร์อย่างเป็นระบบ ให้สนับสนุนภารกิจอย่างมีประสิทธิภาพ พร้อมทั้งส่งเสริมหน่วยงานในสังกัดใช้งานระบบสารสวนเทศอย่างปลอดภัยเพื่อป้องกันการถูกโจมตีทางไซเบอร์

กลยุทธ์เชิงแก้ไข/กำจัดจุดอ่อน (W,O) กองทัพบกมีความเชื่อมโยงยุทธศาสตร์และยุทธวิธีทางไซเบอร์ของหน่วยงานต่างๆ ยังไม่ชัดเจน จึงมีการบูรณาการถ่ายทอดองค์ความรู้อย่างเป็นระบบ ฝึกทักษะ อบรมให้กับกำลังพลที่ปฏิบัติงานด้านการต่อต้านการร้ายทางไซเบอร์ เพื่อให้เกิดความเชี่ยวชาญด้านไซเบอร์ ตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ พัฒนาขีดความสามารถของกำลังพลร่วมกับหน่วยงานภายนอกที่มีความรู้

กลยุทธ์เชิงตั้งรับ/เปลี่ยนวิกฤติเป็นโอกาส (S,T) กองทัพบกได้มีการบูรณาการการพัฒนาขีดความสามารถการต่อต้านการก่อการร้ายทางไซเบอร์ให้กับกำลังพล ฝึกอบรม

ทักษะ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ การบูรณาร่วมกันระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการทำงาน มีการบริหารจัดการงานด้านไซเบอร์ในภาพรวม มีเป้าหมายและแผนระยะยาวที่ชัดเจน ให้เป็นในทิศทางเดียวกัน

กลยุทธ์เชิงป้องกัน/สร้างภูมิคุ้มกัน (W,T) มีระบบป้องกันการโจมตีทางไซเบอร์สามารถป้องกันข้อมูลจากการโจมตีทางไซเบอร์ที่สอดคล้องกับหลักสากล ตลอดจนโครงสร้างพื้นฐานสำคัญทางไซเบอร์ และมีส่วนร่วมในฐานะหน่วยงานด้านความมั่นคง เพื่อสร้างความตระหนักถึงภัยคุกคามสมัยใหม่ เสริมสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการพัฒนาขีดความสามารถในการเฝ้าตรวจ ระวังป้องกัน และแก้ไขปัญหาภัยคุกคามตลอดจนเสริมสร้างขีดความสามารถให้มีความพร้อมใช้งานสนับสนุนภารกิจได้อย่างมีประสิทธิภาพ

วิเคราะห์แนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

ประเทศไทยได้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ มี พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ บังคับใช้ตั้งแต่วันที่ 27 พฤษภาคม 2562[20] เพื่อเป็นแนวทางในการจัดการ ป้องกัน รับมือ และการลดความเสี่ยงทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ ความสามารถของกำลังพล และผู้เชี่ยวชาญ รวมถึงการให้ความรู้ และความตระหนักถึงภัยไซเบอร์ กองทัพบกได้รับมอบหมายให้ดำเนินการแผนการพัฒนาทางไซเบอร์ ได้แก่ การเสริมสร้างบุคลากรด้านเทคโนโลยีดิจิทัลและไซเบอร์ การดำรงขีดความสามารถการปฏิบัติการทางไซเบอร์ การเสริมสร้างขีดความสามารถ การปฏิบัติการทางไซเบอร์สำหรับกำลังพลกองทัพบก ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSOC) กองทัพบกระยะที่ 3 การจัดตั้งชุดรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ระดับกองทัพบกและระดับกองทัพภาค อีกทั้งได้มีการเตรียมความพร้อม และพัฒนากำลังพลด้านความมั่นคงปลอดภัยไซเบอร์ โดยให้ศูนย์ไซเบอร์กองทัพบก จัดหลักสูตรพัฒนาการฝึกอบรมกำลังพลของกองทัพบก เพื่อรับมือต่อสถานการณ์การก่อการร้ายทางไซเบอร์ต่างๆ มีความมั่นคง ปลอดภัยมากยิ่งขึ้น

จากยุทธศาสตร์ชาติ การพัฒนากำลังพลของกองทัพบกให้มีความรู้ ความเข้าใจ ทักษะ และความเชี่ยวชาญ ตามแผนพัฒนา ดังนี้ การพัฒนาระบบการเรียนรู้ให้กับกำลังพล การกำหนดบทบาท หน้าที่ ความรับผิดชอบระหว่างหน่วยงานด้านไซเบอร์ การพัฒนาระบบการรับรองความสามารถทางไซเบอร์ เพื่อให้สามารถจำแนกระดับความชำนาญของกำลังพลสร้างมาตรฐานของผู้ปฏิบัติงานให้อยู่ในระดับสากล และสนับสนุนด้านความ

มั่นคงปลอดภัยเชิงรุก ทั้งภายในและภายนอกประเทศ การปฏิบัติการเชิงรุก สามารถใช้เป็นกำลังอำนาจในการปฏิบัติการบนโลกไซเบอร์ เป็นที่ทราบกันดีว่า ภัยคุกคามไซเบอร์ (Cyber Threats) ถูกนำมาใช้เป็นเครื่องมือทางการทหาร ไม่ว่าจะเป็นการเจาะระบบ (Hack /Crack) การฝังโปรแกรมลักลอบโจรกรรมข้อมูล เช่น สปายแวร์ (Spyware) หรือประตูหลัง (Back Door) โจมตีด้วยโปรแกรมมัลแวร์ (Malware) เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Computer Worm) หรือ ม้าโทรจัน (Trojan Horse) การใช้โปรแกรมตั้งเวลาทำงานเพื่อการทำลาย (Logic Bomb) การโจมตีแบบ DoS/DDos การใช้โปรแกรมหุ่นยนต์โจมตีเพื่อเป็นฐานโจมตีอุปกรณ์คอมพิวเตอร์บนเครือข่ายสารสนเทศ (BOTNET/Robot Network) การสร้างข้อมูลขยะ (Spam) เป็นต้น[21]

แนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายของกรมข่าวทหารบก มีแนวทางดังต่อนี้

1. การปรับโครงสร้างหน่วยและอัตรากำลังพลให้เหมาะสมกับปริมาณงานที่ดำเนินการทั้งในปัจจุบันและอนาคต

2. สนับสนุนการฝึกอบรม เกี่ยวกับไซเบอร์ในระดับมาตรฐานสากลให้กับกำลังพลได้เรียนรู้ เพื่อทันต่อการพัฒนาเทคโนโลยีสมัยใหม่อยู่เสมอ

3. ให้การสนับสนุนงบประมาณต่างๆ เช่น งบประมาณการพัฒนากำลังพล งบประมาณวัสดุ อุปกรณ์ งบประมาณในการพัฒนาและวิจัยในหน่วยงาน

4. ให้การพิจารณาเพิ่มค่าตอบแทนพิเศษของผู้ปฏิบัติงานไซเบอร์และผู้ที่ผ่านการอบรมวิชาชีพด้านไซเบอร์ตามที่หน่วยกำหนด

5. การบริหารจัดการสภาพแวดล้อมที่ดีในหน่วยงาน เน้นการทำงานเป็นทีมแบบมีส่วนร่วม สร้างความสัมพันธ์ที่ดีงามในหน่วยงานให้กับกำลังพลทุกระดับ

6. การออกแบบระบบเตือนภัยและเตรียมพร้อมรับมือกับความเสี่ยงไซเบอร์ซึ่งต้องเป็นกระบวนการที่ปฏิบัติซ้ำได้ (Repeatable processes) และการทดสอบระบบผ่านการซ้อมปฏิบัติการทางไซเบอร์

7. มีการบูรณาการความร่วมมือระหว่างหน่วยงานของกองทัพบก กองทัพบก กองทัพเรือ กองทัพไทย หน่วยงานความมั่นคงของภาครัฐ และเอกชน โดยเฉพาะอย่างยิ่งการออกแบบระบบเตือนภัย และเตรียมพร้อมรับมือกับความเสี่ยงไซเบอร์

8. การรู้เท่าทันสื่อดิจิทัล (Digital literacy) จึงเป็นสิ่งจำเป็นในการรับมือกับข้อมูลที่บิดเบือนที่สำเร็จ

ปัจจุบันกองทัพบกเพื่อพัฒนาศักยภาพกำลังพล ได้มีการจัดทำหลักสูตรเพิ่มศักยภาพด้านไซเบอร์ ประจำปีงบประมาณ 2566[22] ดังนี้

1. หลักสูตรการปฏิบัติการไซเบอร์ขั้นต้น
2. หลักสูตรการปฏิบัติการไซเบอร์ขั้นสูง
3. หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ขั้นต้น
4. หลักสูตรเจ้าหน้าที่รักษาความปลอดภัยไซเบอร์ขั้นสูง
5. หลักสูตรพิเศษเฉพาะทางด้านการรักษาความปลอดภัยไซเบอร์
6. หลักสูตรหลักการใช้งานเครือข่ายสังคมออนไลน์
7. หลักสูตรการผลิตสื่อด้านไซเบอร์

การจัดทำแผนการฝึกอบรมหลักสูตรเพิ่มศักยภาพด้านไซเบอร์สำหรับกำลังพลนี้ เพื่อเป็นการเตรียมการจัดการฝึกอบรม และพิจารณากำลังพลเข้ารับการฝึกอบรมในหลักสูตร เป็นการเพิ่มศักยภาพให้กับกำลังพล ทำหน้าที่ เสริมสร้างความรู้ ความเข้าใจ สร้างความตระหนัก ติดตาม กำกับดูแลการปฏิบัติของหน่วย ตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิทัล ได้อย่างมีประสิทธิภาพ ในการพัฒนาศักยภาพของกองทัพบกภายใต้ยุทธศาสตร์ชาติ ได้แก่ การเสริมสร้างบุคลากรด้านเทคโนโลยีดิจิทัล และไซเบอร์ของกองทัพบก การดำรงขีดความสามารถการปฏิบัติด้านไซเบอร์ การเสริมสร้างขีดความสามารถการปฏิบัติด้านไซเบอร์สำหรับกำลังพลกองทัพบก ศูนย์ปฏิบัติการรักษาความปลอดภัยไซเบอร์ (CSOC) กองทัพบก จัดตั้งชุดรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (CSIRT) ระดับกองทัพบก และระดับกองทัพภาค

บทที่ 3

การก่อการร้ายทางไซเบอร์ เป็นการทำสงครามบนโลกดิจิทัล ในยุคที่มิได้มุ่งเน้นในการทำลายเพื่อให้เกิดการสูญเสียชีวิต แต่เป็นการใช้กลยุทธ์ในการรบเพื่อขัดขวางระบบและเครือข่าย ทำให้ระบบเครือข่ายไม่สามารถดำเนินการได้ตามปกติ เกิดปัญหากับระบบโครงสร้างสาธารณูปโภคขั้นพื้นฐานที่สำคัญ ได้แก่ ระบบไฟฟ้า ระบบน้ำประปา ระบบธนาคาร การขนส่งพลังงาน การสื่อสารโทรคมนาคม และเครือข่ายคอมพิวเตอร์ การโจมตีทางไซเบอร์ยังคงมีแนวโน้มที่สร้างความรุนแรง และความซับซ้อนมากขึ้นในรูปแบบที่ไม่สามารถคาดเดาได้ ดังนั้นเพื่อให้เป็นแนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

การปฏิบัติงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

ศูนย์ไซเบอร์ของกองทัพบก จัดตั้งขึ้นเพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบก รับผิดชอบในการอำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการไซเบอร์ และพัฒนาศักยภาพด้านไซเบอร์ ในการต่อต้านภัยคุกคามทางด้านไซเบอร์ทางการทหาร จากการสอดแนมข้อมูลผ่านอุปกรณ์ การแพร่ระบาดของไวรัสค่าไถ่ การโจมตีระบบแม่ข่ายคอมพิวเตอร์ และยุทธการทางข้อมูลข่าวสาร จากการแพร่เนื้อหาที่เป็นภัย และกำหนดระดับภัยคุกคามส่งผลกระทบต่อความมั่นคงของประเทศ ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) ส่งผลกระทบต่อสถาบันฯ และส่งผลกระทบต่อภาพลักษณ์ของกองทัพบก จากปัญหาภัยการครอบงำทางไซเบอร์ หรือครอบงำทางความคิดโดยไม่รู้ตัว จากกระแสสื่อออนไลน์ ในการสร้างข้อมูลข่าวสารอันเป็นเท็จ เพื่อโจมตี ยั่วยุ โฆษณาชวนเชื่อ สร้างกระแสความเกลียดชัง เกิดความแตกในสังคม จนเกิดเป็นภัยความมั่นคงของชาติ ดังนั้น การปฏิบัติงานของกำลังพลในหน่วยข่าว จำเป็นต้องเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างรวดเร็ว ไม่ว่าจะเป็นการเมือง เศรษฐกิจ สังคมจิตวิทยา การทหาร วิทยาศาสตร์ เทคโนโลยี พลังงาน ทรัพยากรธรรมชาติและสิ่งแวดล้อม ดังนั้นการต่อต้านการก่อการร้ายทางไซเบอร์ จึงมีบทบาทสำคัญต่อชาติเป็นอย่างมาก สอดคล้องกับงานวิจัยของ พงษ์ศักดิ์ ผกามาศ และคณะ[25] เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย พบว่า การใช้เครือข่ายสังคมออนไลน์เพื่อการบ่อนทำลายความน่าเชื่อถือของเจ้าหน้าที่รัฐ ใช้หลักจิตวิทยา และการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี สร้างกระแสข่าวเชิงลบ และการสร้างความขัดแย้ง การก่อวินาศกรรมโดยใช้เครือข่ายอินเตอร์เน็ต ดังนั้นแนวทางดำเนินการ ได้แก่ 1) การจัดโครงสร้างพื้นฐานของประเทศไทย

สำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ 2) การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน 3) การพัฒนาความก้าวหน้าด้านไซเบอร์ 4) การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 5) การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน 6) การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร และ 7) การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตีเพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ให้กับประเทศชาติต่อไป

ขีดความสามารถในการต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

การต่อต้านการก่อการร้ายทางไซเบอร์ของกองทัพบก มีนโยบายและยุทธศาสตร์ที่ชัดเจน มีศูนย์ไซเบอร์เป็นศูนย์กลางในการปฏิบัติและพัฒนากำลังพล เสริมสร้างกระบวนการ ทักษะ ความรู้ในการใช้สื่อดิจิทัลให้กำลังพล วางแผนการจัดสรรงบประมาณประจำปี ในการจัดซื้อ จัดจ้าง อุปกรณ์ เครื่องมือเทคโนโลยี ระบบตรวจจับ โปรแกรมป้องกันความเสี่ยงของระบบสารสนเทศ และสนับสนุนงานด้านการต่อต้านการก่อการร้ายทางไซเบอร์ ป้องกันการโจมตีทางไซเบอร์ และเป็นศูนย์ต่อต้านข่าวปลอม กำหนดกลยุทธ์เชิงรุก กลยุทธ์เชิงแก้ไข กลยุทธ์เชิงรับ กลยุทธ์เชิงป้องกัน เพื่อเสริมสร้างขีดความสามารถให้มีความพร้อมใช้งาน สนับสนุนภารกิจ ได้อย่างมีประสิทธิภาพ สอดคล้องกับงานวิจัยของ ศึกษา พันเอกหญิง นริศรา พลอยประไพ[26] ศึกษา แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง พบว่า บุคลากรของหน่วยไซเบอร์ยังขาดทักษะ และความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การปรับโครงสร้างหน่วยไซเบอร์ทางทหาร โดยจัดตั้งโรงเรียนไซเบอร์ทางทหารขึ้นเพื่อเป็นศูนย์กลางในการถ่ายทอดความรู้ ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นรูปธรรม ซึ่งจะทำให้บุคลากรของหน่วยไซเบอร์ทางทหารมีขีดความสามารถเพิ่มขึ้น สามารถปฏิบัติภารกิจรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างมีประสิทธิภาพต่อไป สอดคล้องกับงานวิจัยของ นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง[27] ศึกษาเรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ ระบบเทคโนโลยีสารสนเทศมีความสำคัญต่อการปฏิบัติภารกิจทางทหารเป็นอย่างยิ่ง พบว่าการพัฒนาเพิ่มขีดความสามารถการปฏิบัติด้านไซเบอร์ พัฒนาเชิงรับและเชิงรุก มีนโยบายกระบวนการแผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติ มีการพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวนให้มีความรู้ความสามารถมีทักษะพร้อมที่จะปฏิบัติภารกิจด้านไซเบอร์ได้อย่างมีประสิทธิภาพ

แนวทางการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ของกรมข่าวทหารบก

การพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ โดยดำเนินการแผนการพัฒนาทางไซเบอร์ โดยให้ศูนย์ไซเบอร์กองทัพบก จัดหลักสูตรพัฒนาการฝึกอบรมให้กำลังพลของกรมข่าวทหารบก หรือหน่วยงานที่สนใจและเกี่ยวข้อง เข้าพัฒนา ฝึกการอบรม เพื่อรับมือต่อสถานการณ์การก่อการร้ายทางไซเบอร์ต่างๆ ให้กำลังพลมีความรู้ทักษะ และความเชี่ยวชาญ รู้เท่าทันภัยที่เกิดจากการคุกคามทางไซเบอร์ วางแผนการทำงาน กำหนดบทบาท หน้าที่ ความรับผิดชอบระหว่างหน่วยงานด้านไซเบอร์ พัฒนาระบบการรับรองความสามารถทางไซเบอร์ สร้างมาตรฐานของผู้ปฏิบัติงานให้อยู่ในระดับสากล และสนับสนุนด้านความมั่นคงปลอดภัยเชิงรุก และเชิงรับ ทั้งภายในและภายนอกประเทศ สอดคล้องกับงานวิจัยของ อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร[28] ศึกษาเรื่อง แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พบว่า การกำหนดนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สร้างเครือข่ายไซเบอร์เชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวม ได้รับการสนับสนุนจากหน่วยงานที่เกี่ยวข้องควรผลิตซอฟต์แวร์/ฮาร์ดแวร์ทางไซเบอร์ขึ้นใช้เอง ควรมีการฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ เตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด ผลิตและพัฒนาบุคลากรด้านไซเบอร์หน่วยงานทางด้านไซเบอร์สามารถรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ และควรสร้างความตระหนักรู้ให้แก่กำลังพล และประชาชนทั่วไป

บทที่ 4
บทสรุป

แนวทางในการพัฒนาประสิทธิภาพงานต่อต้านการก่อการร้ายทางไซเบอร์ สำหรับการต่อต้านภัยคุกคามทางด้านไซเบอร์ทางการทหาร จำเป็นต้องเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างรวดเร็ว ป้องกันการโจมตีและต่อต้านการก่อการร้ายทางไซเบอร์ เพื่อเสริมสร้างการปฏิบัติภารกิจต่อต้านการก่อการร้ายทางไซเบอร์ ป้องกันการโจมตีทางไซเบอร์ และเป็นศูนย์ต่อต้านข่าวปลอม กำหนดกลยุทธ์เชิงรุก และเชิงรับ เพื่อเสริมสร้างขีดความสามารถให้กับกำลังพลให้มีความพร้อมใช้งาน สนับสนุนภารกิจ โดยดำเนินการแผนการพัฒนาทางไซเบอร์ จัดหลักสูตรพัฒนาการฝึกอบรมให้กำลังพล พัฒนาระบบเทคโนโลยีของกองทัพบก เพื่อรองรับภัยคุกคามทางไซเบอร์ สร้างมาตรฐานของผู้ปฏิบัติงาน และหน่วยงานให้อยู่ในระดับสากล

ข้อเสนอแนะจากงานวิจัย

1. ควรเสริมสร้างความรู้ความเข้าใจถึงบริบท และความรุนแรงของภัยคุกคามด้านไซเบอร์แก่กำลังพลกองทัพบก ด้านนโยบายรักษาความมั่นคงปลอดภัยมุ่งเน้นมาตรการป้องกัน มีการบูรณาการความร่วมมือระหว่างภาครัฐ เอกชนและกองทัพและหน่วยงานอื่นๆ

2. สนับสนุนหน่วยงานวิจัยของกองทัพบกบูรณาร่วมกับกรมวิทยาศาสตร์และเทคโนโลยีกลาโหม สถาบันเทคโนโลยีป้องกันประเทศ เพื่อวิจัยและสร้างเครื่องมือ ขึ้นมาใช้เองภายในประเทศ เพื่อรักษาความปลอดภัย ออกแบบระบบเตือนภัยเตรียมพร้อมรับมือกับความเสี่ยง และความมั่นคงของประเทศ

3. ควรมีการวิเคราะห์สภาพการณ์ความเสี่ยง โอกาสและความท้าทายทางไซเบอร์ของประเทศภาพรวม ในปัจจุบันโดยวิเคราะห์ความพร้อม และจุดอ่อนของระบบและโครงสร้างพื้นฐานไซเบอร์ และความเสี่ยงไซเบอร์อันเกิดจากความก้าวหน้าของการพัฒนาเทคโนโลยี

ข้อเสนอแนะการวิจัยครั้งต่อไป

1. กองทัพบกควรเพิ่มค่าตอบแทนให้กับกำลังพลที่ผ่านการฝึกอบรม หรือมีความรู้ ความสามารถทางด้านเทคนิคเพิ่มเติม เพื่อสร้างแรงจูงใจ ในการปฏิบัติภารกิจด้านไซเบอร์ เพื่อป้องกันไม่ให้บุคคลที่มีความเสี่ยงต่อการก่อภัยไซเบอร์เข้ามาอยู่ในกองทัพ

2. ควรมีการศึกษาการจัดทำแผนการบริหารจัดการกับภัยคุกคามจากภายในและภายนอก ที่อาจจะเกิดขึ้นกระทบต่อความมั่นคงของประเทศได้ รวมถึงการแบ่งปันข้อมูลจากหน่วยงานอื่น เพื่อให้ทัดเทียมกับมาตรฐานการรักษาความปลอดภัยด้านไซเบอร์สากลและเกิดประโยชน์ในการนำไปใช้แก้ปัญหาด้านความมั่นคงของชาติต่อไป

3. ควรมีการศึกษาวิจัยการสร้างเครื่องมือ ระบบรักษาความปลอดภัยด้านไซเบอร์ เน้นการผลิตในประเทศลดการนำเข้าระบบจากจากภายนอก เพื่อป้องกันความปลอดภัยข้อมูลความมั่นคง และสามารถทราบช่องโหว่ในการถูกโจมตีจากภายนอก โดยสามารถเชื่อมโยงกับมาตรฐานสากล

เอกสารอ้างอิง

1. กองทัพบก, สรุปผลการศึกษาภัยคุกคามทางไซเบอร์และหน่วยงานรักษาความมั่นคงปลอดภัยไซเบอร์, ศูนย์ประสานงานสารนิเทศ ศูนย์ปฏิบัติการกองทัพบก, 2564.

2. คณะกรรมการยุทธศาสตร์ชาติ, ยุทธศาสตร์ชาติ (พ.ศ.2561 - 2580), กรุงเทพฯ : สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2562.

3. กองทัพบก, ร่างแผนปฏิบัติราชการประจำปีงบประมาณ 2566 ของ กองทัพบก, กรุงเทพฯ : สำนักงานปลัดบัญชีกองทัพบก, 2564.

4. อริย์ธัช แก้วเกาะสะบ้า, ศูนย์ไซเบอร์กองทัพบก, สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2560.

1. เรื่องเดียวกัน 1

6. สุเมธ ตั้งประเสริฐ, แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก, วิทยาลัยการทัพบก, 2564.

7. ศูนย์ไซเบอร์กองทัพบก, ประวัติศูนย์ไซเบอร์กองทัพบก ไซเบอร์มั่นคงปลอดภัย เฝ้าระวังภัยในโลกไซเบอร์, [อินเทอร์เน็ต]; 2565. [เข้าถึงเมื่อ 20 กุมภาพันธ์ 2566]. เข้าถึงได้จาก https://cyber.rta.mi.th/about/

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

9. In Focus: Cyber Attack คลื่นใต้น้ำแห่งยุคดิจิทัลที่ต้องจับตามอง. สำนักข่าวอินโฟเควสท์, 2564.

10. สถาบันเทคโนโลยีป้องกันประเทศ, ภัยคุกคามทางไซเบอร์ (Cyber Security), ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ, 2559.

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

12. Ronald J. Deibert and Rafal Rohozinski, “Risking Security: Policies and Paradoxes of Cyberspace Security,”International Political Sociology 4, no. 1 (2010): 16, 2010

13. Osonde A. Osoba and William Welser IV, The Risks of Artificial Intelligence to Security and the Future of Work (Santa Monica, California: RAND corporation, 2017), 5. 2017.

14. Willie D. Jones, “Declarations of Cyberwar,” IEEE Spectrum, July 24, 2012, https://spectrum.ieee.org/computing/ networks/declarations-of-cyberwar (accessed March 12, 2019). 2019

15. Thomas Rid, “Cyber War Will Not Take Place,” Journal of Strategic Studies 35, no. 1 (2012): 6. 2012.

16. ศูนย์การประสานงานสารนิเทศ, สรุปผลการศึกษาภัยคุกคามทางไซเบอร์และหน่วยงานรักษาความมั่นคงทางไซเบอร์, ศูนย์การประสานงานสารนิเทศ กองทัพบก, 2564

17. เตชิต ทิวาเรืองรอง, การออกแบบระบบความปลอดภัยทางกายภาพ (Physical Security Design), คณะกรรมการร่างมาตรฐาน ซีซีทีวี ไอโอที เอไอ และการแลกเปลี่ยนเชื่อมโยงข้อมูลร่วมกันวิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์, 2564.

18. เศรษฐพงค์ มะลิสุวรรณ, เปิดแนวคิด “เศรษฐพงค์” ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์, 2559

19. The Crowdstrike global Threat Repoet, Crowdstrike, 2021

17. Joseph Aghatise. Cybercrime definition. 2006.

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

21. The Global Cybersecurity Capacity Centre แห่ง University of Oxford, National Cybersecurity Capacity Maturity Model (CMM), [อินเทอร์เน็ต]; [เข้าถึงเมื่อ 20 กุมภาพันธ์ 2566]. เข้าถึงได้จาก https://gcscc.ox.ac.uk/the-cmm

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

23. ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์.... [อินเทอร์เน็ต]; [เข้าถึงเมื่อ 20 กุมภาพันธ์ 2566]. เข้าถึงได้จาก https://ictlawcenter.etda.or.th.

24. ศูนย์ไซเบอร์ทหารบก, หนังสือเชิญกำลังพลสมัครหลักสูตรอบรมด้านไซเบอร์ของกองทัพบก, 2565.

25. พงษ์ศักดิ์ ผกามาศ, ชัยวัฒน์ ประสงค์สร้าง, เศรษฐชัย ชัยสนิท, ชูเกียรติ ช่วยเพชร, และราชิต อรุณรังษี, ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย, The Liberal Arts Journal Faculty of Liberal Arts, Mahidol University 2562.

26. นริศรา พลอยประไพ, แนวทางการพัฒนาขีดความสามารถของบุคลากรหน่วยไซเบอร์ทางทหารรองรับยุทธศาสตร์ชาติด้านความมั่นคง, วิทยาลัยการทัพบก, 2564.

27. ณรงค์เวตย์ เรืองจวง, แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ, วารสารรัฏฐาภิรักษ์, 60(3), 2561.

28. อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร, แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์, วารสารสถาบันวิชาการป้องกันประเทศ, 2560.

ประวัติย่อผู้วิจัย

ยศ ชื่อ พันเอกหญิง สุชาดา บุญวัฒนะ

วัน เดือน ปีเกิด 10 ตุลาคม พ.ศ. 2522

ประวัติสำเร็จการศึกษา

พ.ศ. 2540 – 2544	ปริญญาตรี ศิลปศาสตรบัญฑิต (สาขาวิชาภาษาไทย) มหาวิทยาลัยเชียงใหม่
พ.ศ. 2546 – 2548	ปริญญาโท ศิลปศาสตรมหาบัณฑิต (กฎหมายปกครองและการบริหารงานภาครัฐ) มหาวิทยาลัยราชภัฏสวนดุสิต

ประวัติการทำงาน

พ.ศ. 2545 – 2547	ประจำสำนักงานสรรพาวุธทหารบก
พ.ศ. 2548 – 2550	ประจำสำนักงานสรรพาวุธทหารบก
พ.ศ. 2551 – 2556	ประจำสำนักงานเลขานุการกองทัพบก
พ.ศ. 2556 – 2562	ประจำสำนักงานเลขานุการกองทัพบก
พ.ศ. 2562 – 2564	ประจำสำนักงานตรวจสอบภายในทหารบก

ตำแหน่งปัจจุบัน

พ.ศ. 2564 – ปัจจุบัน	ประจำสำนักงานตรวจสอบภายในทหารบก