แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก

เอกสารวิจัยส่วนบุคคล

โดย

นาย สุเมธ ตั้งประเสริฐ

กรรมการผู้จัดการบริษัทเด็พธเฟิร์สทจำกัด

วิทยาลัยการทัพบก

กันยายน 2564

เอกสารวิจัยเรื่อง แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก

โดย นาย สุเมธ ตั้งประเสริฐ

อาจารย์ที่ปรึกษา พันเอกหญิง ปัทมา สมสนั่น

วิทยาลัยการทัพบก อนุมัติให้เอกสารวิจัยส่วนบุคคลฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรหลักประจำ วิทยาลัยการทัพบก ปีการศึกษา 2564 และเห็นชอบให้เป็นเอกสารวิจัยส่วนบุคคลที่อยู่ในเกณฑ์ระดับ

พลตรี ..... **ผู้บัญชาการวิทยาลัยการทัพบก**

(มหศักดิ์ เทพหัสดิน ณ อยุธยา)

คณะกรรมการควบคุมเอกสารวิจัยส่วนบุคคล

พันเอก ..... **ประธานกรรมการ**

(ประภาส แก้วศรีงาม)

..... **ผู้ทรงคุณวุฒิที่ปรึกษา**

(ดร. เมธวิน กิติคุณ)

พันเอกหญิง ..... **กรรมการ**

(ศศพินธุ์ วัชรธรรม)

พันเอกหญิง ..... **กรรมการ**

(ฐิติญา จันทวุฒิ)

พันเอกหญิง ..... **กรรมการ**

(ปัทมา สมสนั่น)

บทคัดย่อ

ผู้วิจัย นาย สุเมธ ตั้งประเสริฐ

เรื่อง แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก

วันที่ กันยายน 2564 **จำนวนคำ :** 7,593 **จำนวนหน้า :** 21

คำสำคัญ การปฏิบัติงานด้านไซเบอร์, พัฒนาบุคลากร, กองทัพบก

ชั้นความลับ ไม่มีชั้นความลับ

เอกสารวิจัยฉบับนี้ มีวัตถุประสงค์เพื่อศึกษาสถานการณ์กำลังพลในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก เพื่อศึกษาทฤษฎีที่เกี่ยวข้องกับการพัฒนากำลังพลด้านไซเบอร์ และเปรียบเทียบแนวทางการพัฒนากำลังพลในการปฏิบัติงานด้านไซเบอร์ของของหน่วยงานอื่น ๆ และเพื่อหาแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก ผลการวิจัยสรุปว่า แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ โดยการสร้างขีดความสามารถ การพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ เพื่อนำมาเป็นแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก เนื่องจากการพัฒนาศักยภาพบุคลากร และเทคโนโลยี แนวทางการดำเนินงานการพัฒนาศักยภาพขององค์กรและบุคลากรให้มีทักษะความรู้ เพื่อเพิ่มขีดความสามารถในการป้องกันตนเอง และหน่วยงานลดความเสี่ยง ลดความเสียหายจากการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้น พัฒนากำลังคนในทุกระดับตั้งแต่การส่งเสริมระดับสถานศึกษาเพื่อการสร้างบุคลากรรองรับความต้องการในอนาคต เพื่อยกระดับความพร้อมของประเทศในการรับมือ และจัดการกับภาวะความเสี่ยงภัยคุกคามทางไซเบอร์ ในปัจจุบัน และอนาคต โดยต้องเพิ่มจำนวน และคุณภาพของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความรู้ และทักษะเทียบเท่ากับสากล เช่น มีเอกสารรับรองคุณวุฒิ หรือการอบรม ที่เป็นที่ยอมรับของสากลกำหนดมาตรฐานวิชาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากลสร้างแรงจูงใจ และให้การสนับสนุนในการสร้างความเติบโตในสายอาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ยั่งยืน

ABSTRACT

AUTHOR : Mr. Sumet Tangprasert

TITLE : Guidelines for human resource development in the Army's cyber practice.

DATE: September, 2021 **WORD COUNT :** 7,593 **PAGES :** 21

KEY TERMS : Cyber operations, Personnel Development, Army

CLASSIFICATION : Unclassified

This research paper The objective is to study the personnel situation in Army cyber operations. To study theories which related to the development of cyber manpower. And compare guidelines for developing personnel in the cyber operations of other agencies and to find ways to develop personnel in Army cyber operations.

The results of the research concluded that Human Resource Development guidelines for cyber operations by building capacity development and raising awareness to be used as a guideline for personnel development in the Army's cyber operations. Accounting to the development of human potential and technology, operational guidelines, development of organizational potential and personnel to have the skills and knowledge to increase the capacity of self-defenses and risk mitigation agencies reduce the damage from potential cyber-attacks. Developing manpower at all levels, from the promotion of the school level to the creation of personnel to support future needs. To raise the level of the country's readiness to cope and address the current and future risks of cyber threats. By increasing the number of and the quality of personnel in the field of cybersecurity. To improve skills equivalent to international standards such as having documents certifying international

qualifications or training that are recognized internationally, setting professional standards in cybersecurity that are in line with international standards; And to provide support to grow in a sustainable cybersecurity career.

กิตติกรรมประกาศ

เอกสารวิจัยส่วนบุคคลฉบับนี้สำเร็จลงได้ด้วยความกรุณาจากประธานกรรมการที่ปรึกษาคอยให้คำแนะนำ คำปรึกษา ให้กำลังใจ ตรวจสอบแก้ไขให้งานวิจัยครั้งนี้สำเร็จลงได้ด้วยดี ขอกราบขอบพระคุณสำหรับความกรุณาของอาจารย์ที่สละเวลาอันมีค่า จนงานวิจัยเสร็จสมบูรณ์

นอกจากนี้ขอขอบคุณผู้ให้ข้อมูลสำคัญ ตลอดจนความคิดเห็น ซึ่งเป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับงานวิจัยครั้งนี้ ขอขอบคุณผู้ทรงคุณวุฒิทุกท่านที่เสียสละ และทุ่มเทเวลาในการนัดหมายให้การสัมภาษณ์บรรลุผลได้ด้วยดี

ประโยชน์อันเกิดจากงานวิจัยเล่มนี้ ขอมอบแด่อาจารย์ที่ปรึกษา ครอบครัว และเพื่อน ๆ ผู้ที่ให้การสนับสนุนทุกท่าน ทั้งด้านการทำงาน และกำลังใจจนสามารถสำเร็จการศึกษา

สารบัญ

หน้า

บทที่ 1 บทนำ 1

ที่มา และความสำคัญของปัญหา 1

วัตถุประสงค์ของการวิจัย 2

กรอบแนวคิดในการวิจัย 3

วิธีการวิจัย 3

ประโยชน์ที่ได้รับ 4

บทที่ 2 บทวิเคราะห์ 5

วิเคราะห์สาเหตุของปัญหา 6

การวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์ 6

วิเคราะห์แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก 15

บทที่ 3 บทอภิปรายผล 17

บทที่ 4 บทสรุป 21

ข้อเสนอแนะ 22

เอกสารอ้างอิง 24

ประวัติย่อผู้วิจัย 26

บทที่ 1
บทนำ

ที่มา และความสำคัญของปัญหา

จากการใช้อินเทอร์เน็ตที่เพิ่มมากขึ้นประกอบกับการที่รัฐบาลไทยมีนโยบายการพัฒนาบรอดแบรนด์อินเทอร์เน็ตให้ครอบคลุมทั้งประเทศ และการแข่งขันในตลาดโทรคมนาคมจึงทำให้ประชากรไทยสามารถเข้าถึงระบบอินเทอร์เน็ตได้ง่าย และสะดวกรวดเร็ว เกิดความสะดวกสบายในการใช้ชีวิตประจำวันมากขึ้น การใช้งานอินเทอร์เน็ตมีความจำเป็นและกลายเป็นส่วนหนึ่งของชีวิตประจำวัน ในการดำเนินกิจกรรมต่าง ๆ (สำนักงาน กสทช., 2561) ทั้งในด้านการใช้งานส่วนบุคคล ตลอดจนระดับชาติ ทั้งด้านเศรษฐกิจ สังคม ความมั่นคง-การป้องกันประเทศ การสื่อสารโทรคมนาคม และการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานสำคัญ ด้วยเหตุนี้ประชาชน รวมถึงองค์กรต่าง ๆ และกองทัพบก แทบจะมีส่วนหนึ่งของเวลาในชีวิตเข้าไปเกี่ยวข้องกับไซเบอร์สเปซอย่างหลีกเลี่ยงไม่ได้

อย่างไรก็ตาม ปริมาณที่เพิ่มขึ้นของผู้ใช้งาน และขนาดของเครือข่ายที่ขยายมากขึ้นเรื่อย ๆ ก็สามารถทำให้เกิดความเสี่ยงต่อการนำไปใช้งานในทางที่ผิด หรือตกเป็นเหยื่อของกลุ่มมิจฉาชีพ หรืออาชญากรรมข้ามชาติในรูปแบบต่าง ๆ ได้เช่นกัน ดังนั้น การเตรียมการรับภัยคุกคามด้านไซเบอร์ องค์การต้องการบุคลากรที่มีคุณภาพสูง สามารถปฏิบัติงานด้านไซเบอร์ได้อย่างมีประสิทธิภาพ และมีความประสานสอดคล้องกับการรักษาความมั่นคงของชาติในภาพรวม ทั้งนี้ ในแผนปฏิบัติการเพื่อรองรับยุทธศาสตร์ชาติ 20 ปี (2561 – 2580) ด้านการบริหาร และพัฒนาบุคลากร (ราชกิจจานุเบกษา, ยุทธศาสตร์ชาติ 20 ปี พุทธศักราช 2561 - 2580) โดยเฉพาะอย่างยิ่งบุคลากรด้านไซเบอร์ เป็นกลุ่มบุคคลที่มีความสำคัญต่อการดำรงสภาพของระบบเทคโนโลยีสารสนเทศ

โดยเฉพาะปฏิบัติการทางทหารมีการใช้เทคโนโลยีในด้านการข่าว ที่อาศัยไซเบอร์สเปซ (ณรงค์เวตย์ เรืองจวง, 2561) เป็นสื่อกลางในการค้นหารวบรวม ดักฟัง ขโมยข้อมูลของฝ่ายตรงข้าม เพื่อช่วงชิงความได้เปรียบในเรื่องข้อมูลข่าวสารประกอบการตัดสินใจของผู้นำระดับสูง การใช้ความก้าวหน้าทางเทคโนโลยีด้านไซเบอร์ล้วนเป็นเครื่องมือที่สำคัญสนับสนุนการทำสงครามในรูปแบบเดิม ๆ หรือแม้แต่ใช้ความได้เปรียบทางพลังอำนาจทางไซเบอร์มา

เป็นเครื่องมือในประกอบการเจรจาทางการทูตเพื่อลดความขัดแย้งในเรื่องผลประโยชน์ของชาติ ดังนั้น การพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ จึงมีความสำคัญมากต่อกองทัพบก

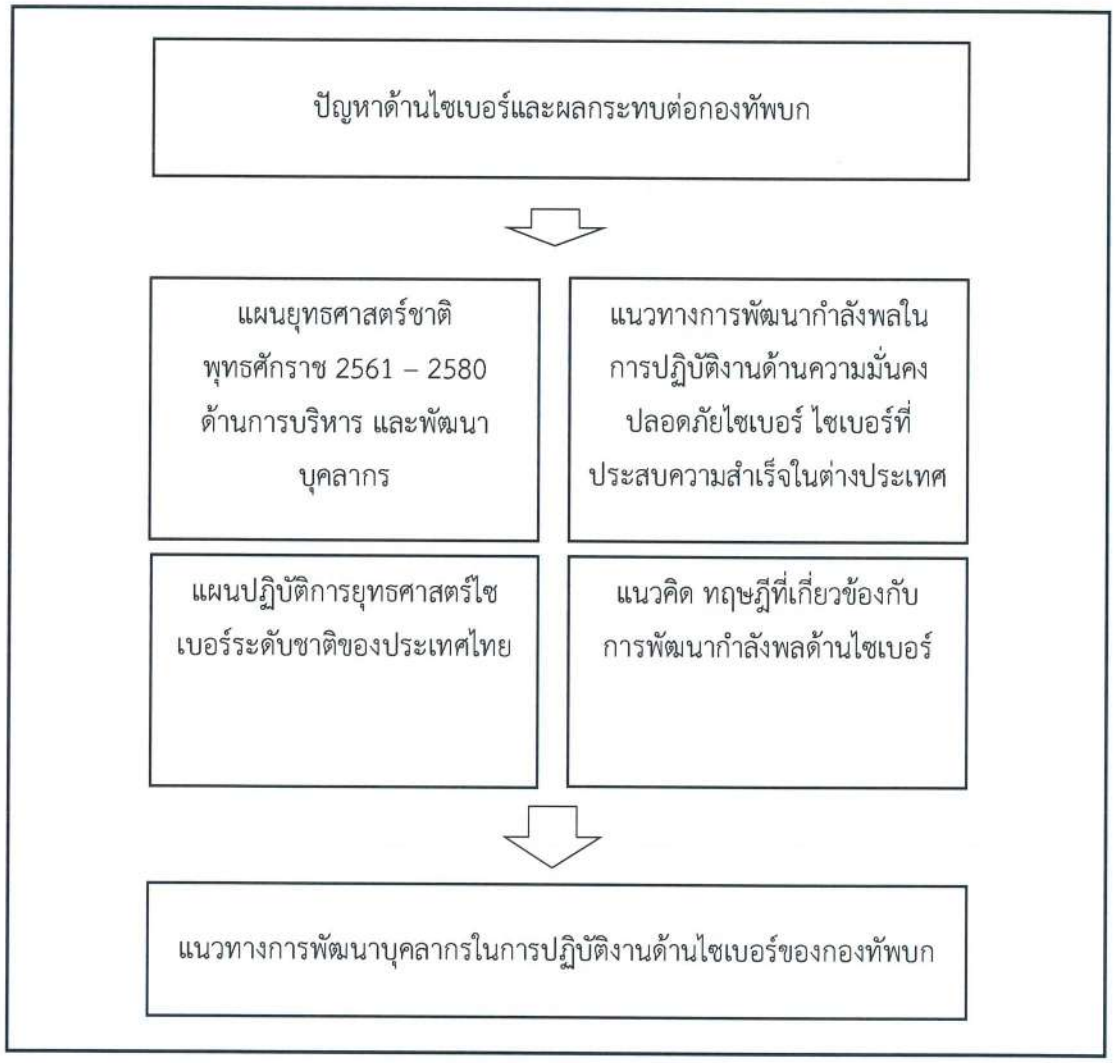
ปัจจุบันกองทัพบกยังประสบปัญหาการขาดแคลนบุคลากรอีกเป็นจำนวนมาก ซึ่งอาจเกิดจากปัญหาด้านแรงจูงใจในค่าตอบแทน หรือขาดแคลนเจ้าหน้าที่ที่เข้าใจปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง และเกิดจากความยากของเนื้อหา และความสลับซับซ้อนของปัญหาที่ทำให้เป็นอุปสรรคต่อบุคคลทั่วไปที่มีความรู้พื้นฐานเพียงแค่ทำงานในระบบสารสนเทศให้เข้าใจ และสามารถปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

ดังนั้น งานวิจัยนี้จะมุ่งศึกษาใน 3 ประเด็น ประการแรกต้องการศึกษาเพื่อศึกษายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี และผมกระทบต่อกองทัพบก ประการที่สอง แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก ปัจจุบัน เป็นอย่างไร และประการสุดท้าย แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก ควรเป็นอย่างไร เพื่อนำเสนอแนวทางการพัฒนาบุคลากรในการปฏิบัติ ศึกษาวิเคราะห์สถานการณ์ โดยคำนึงถึงการบูรณาการแนวความคิดจากประเด็นปัญหาในด้านต่าง ๆ ทั้งปัจจัยด้านเวลา การพัฒนา และด้านการเสริมสร้างกำลังพลไซเบอร์

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี และผลกระทบ ต่อกองทัพบก
2. เพื่อศึกษาทฤษฎีที่เกี่ยวข้องกับการพัฒนากำลังพลด้านไซเบอร์ ต่อกองทัพบก
3. เสนอแนะแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ให้ให้สอดคล้องกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและ ยุทธศาสตร์ชาติ 20 ปี เพื่อให้สามารถนำมาปฏิบัติจริงได้อย่างมีประสิทธิผลและประสิทธิภาพของกองทัพบก

กรอบแนวคิดในการวิจัย



ภาพที่ 1.1 กรอบแนวคิดการวิจัย

วิธีการวิจัย

1. **รูปแบบการวิจัย** ใช้แบบการวิจัยเชิงยุทธศาสตร์ตามที่ วิทยาลัยการทัพบก กำหนดเป็นแนวทางในการศึกษา

2. **ขอบเขตการวิจัย** ขอบเขตด้านเนื้อหา มุ่งศึกษาจากแนวคิด ทฤษฎีที่เกี่ยวข้องกับการพัฒนากำลังพลด้านไซเบอร์ ในมุมมองที่สอดคล้องกับยุทธศาสตร์ชาติ ขอบเขตด้านพื้นที่ และ

ประชากร ดำเนินการศึกษาจากกำลังพลที่ปฏิบัติงานด้านไซเบอร์ของกองทัพบก ขอบเขตด้านระยะเวลา ดำเนินการเก็บรวบรวมข้อมูลในห้วง พฤศจิกายน 63 - พฤษภาคม 64

3. การเก็บรวบรวมข้อมูล สืบค้นข้อมูลจากเอกสาร รายงาน กฎ ระเบียบ คำสั่ง ของทางราชการจากหน่วยงานราชการ และแหล่งความรู้จากตำราทั้งของไทย และต่างประเทศ รวมทั้งแหล่งข้อมูลเสริมจากอินเตอร์เน็ตโดยพิจารณาเลือกใช้ข้อมูลจากเว็บไซต์ที่เชื่อถือได้

4. การวิเคราะห์ข้อมูล ใช้กรอบการคิดเชิงยุทธศาสตร์เป็นแนวทางในการวิเคราะห์ข้อมูลแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก เพื่อนำข้อเสนอแนะและนำแนวทางดังกล่าวไปใช้ประโยชน์ได้ต่อไป

5. ขั้นตอนการดำเนินงาน

ตารางที่ 1.1 ขั้นตอนการดำเนินงาน

เวลา / กิจกรรม	พ.ย. 63	ธ.ค. 63	ม.ค. 64	ก.พ. 64	มี.ค. 64	เม.ย. 64	พ.ค. 64
1. การเสนอโครงร่างการวิจัย	←	→					
2. การเก็บรวบรวมข้อมูล		←	—	→			
3. การวิเคราะห์สังเคราะห์ข้อมูล			←	—	→		
4. การสรุปผลการวิจัย					←	→	
5. การเขียนรายงานการวิจัย						←	→
6. การนำเสนอผลการวิจัย							*

ประโยชน์ที่ได้รับ

1. ให้กองทัพบกทราบถึงสถานการณ์ปัญหาด้านไซเบอร์ ที่มีผลกระทบความมั่นคงของชาติ

2. ทราบถึงปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพบก

3. ข้อเสนอแนะแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์กองทัพบก ที่เหมาะสม และสอดคล้องกับแผนยุทธศาสตร์ชาติ 20 ปี

บทที่ 2
บทวิเคราะห์

กองทัพบกมีหน้าที่ ปกป้องอธิปไตย และความมั่งคงของประเทศ เป็นหนึ่งในองค์กรที่ต้องเตรียมการรับมือปัญหาภัยคุกคามไซเบอร์ ปัจจุบันกองทัพบกยังประสบปัญหาการขาดแคลนเจ้าหน้าที่ที่เข้าใจปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง และเกิดจากความยากของเนื้อหา และความสลับซับซ้อนของปัญหาที่ทำให้เป็นอุปสรรคต่อบุคคลทั่วไปที่มีความรู้พื้นฐานเพียงแค่ทำงานในระบบสารสนเทศ

จากกระแสการเปลี่ยนแปลงที่เกิดจากเทคโนโลยีดิจิทัล (Digital disruption) และกระบวนการในการนำเทคโนโลยีมาสร้างสิ่งใหม่ (Digital transformation) ทั่วโลก ทำให้เราคงปฏิเสธไม่ได้ว่า การเปลี่ยนแปลงทางดิจิทัลของโลกมีผลต่อการดำเนินชีวิตประจำวันของมนุษย์ ทุกคนบนโลกใบนี้อย่างหลีกเลี่ยง ปัจจัยทั้ง 4 อย่างที่มีผลต่อการเปลี่ยนแปลงทางดิจิทัลดังกล่าว (The four IT mega trends in S-M-C-I Era) ได้แก่ S หมายถึง สังคมออนไลน์ (Social media) M หมายถึง เครือข่ายไร้สาย (Mobile computing) C หมายถึง การประมวลผลแบบคลาวด์ (Cloud computing) และ I หมายถึง ข้อมูล (Information) หรือ เทคโนโลยีการวิเคราะห์ข้อมูลขนาดใหญ่ (Big data) ตลอดจนการเปลี่ยนแปลงของโลกจากเทคโนโลยี ปัญญาประดิษฐ์ (Artificial intelligence) และ อินเทอร์เน็ตในทุกสิ่ง (Internet of things) กำลังมีการพัฒนาและประยุกต์ใช้อย่างแพร่หลายทั่วโลก ทำให้ประเทศไทยต้องมีการปรับตัวเพื่อรองรับ Digital transformation แต่ปัญหาใหญ่ที่ตามมาภัยคุกคามไซเบอร์ และเปลี่ยนมาเป็นสงครามไซเบอร์ มีการต่อสู้ แบบ การปฏิบัติการข่าวสาร (Information Operations : IO) กล่าวคือ เป็นการเปลี่ยนแปลงข่าวสารการรับรู้ต่าง ๆ ของประชาชน เพื่อต้องการดึงประชาชนรวมถึงสื่อต่างๆ และ การโจมตีเทคโนโลยีปฏิบัติการ (Operational Technology) อันครอบคลุมถึงเทคโนโลยีที่ดูแลระบบไฟฟ้าเขื่อน ตลอดจนพลังงานนิวเคลียร์ ซึ่งหากกระทำได้สำเร็จก็จะสร้างความเสียหายที่ร้ายแรงกว่าในอดีต รัฐบาล ได้เห็นความสำคัญของภัยคุกคามไซเบอร์จึงมีการระบุประเด็นนี้ ไว้ในยุทธศาสตร์ชาติด้านความมั่นคงและประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขันในเอกสารยุทธศาสตร์ชาติ ระยะ 20 ปี (พุทธศักราช 2561 - 2580) ในด้านของความมั่นคงมีการกล่าวถึงเรื่อง ปัญหาภัยคุกคามไซเบอร์ อาชญากรรมไซเบอร์ที่ซับซ้อนขึ้น รูปแบบการ

ก่อสงครามที่ใช้เทคโนโลยีเป็นเครื่องมือ ซึ่งครอบคลุมความมั่นคงปลอดภัยไซเบอร์ ความมีจริยธรรม และการไม่ละเมิดสิทธิส่วนบุคคล และ การปกป้องอธิปไตยไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติ

วิเคราะห์สาเหตุของปัญหา

สาเหตุกองทัพบกยังประสบปัญหาการขาดแคลนเจ้าหน้าที่ที่เข้าใจปัญหาการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังนี้

1. องค์กร (Organization) ภารกิจหน้าที่ของกองทัพบก ยังไม่ใช่ การรับมือปัญหาภัยคุกคามไซเบอร์ทำให้องค์กรไม้ได้กำหนดทิศทาง การจัดการในทุกระดับ

2. บุคลากร (People) จำนวนคนในกองทัพบก มีบุคลากรที่เกี่ยวข้องกับภัยคุกคามไซเบอร์อยู่จำนวนน้อยมากเมื่อเทียบกับจำนวนบุคลากรในกองทัพบก บุคลากรส่วนมากยังไม่มีความรู้ทักษะ ความชำนาญในการจัดการ ด้านภัยคุกคามไซเบอร์

3. ขั้นตอนการปฏิบัติงาน (Process) กำหนดกลไก การขับเคลื่อนยุทธศาสตร์ โครงการ แผนปฏิบัติงาน และขั้นตอนการปฏิบัติงานด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ไม่ชัดเจน ในระดับผู้ใช้งานทั่วไป

4. เทคโนโลยี (Technology) เทคโนโลยีดิจิทัลที่ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์มีความซับซ้อนสูง และมีสิ่งใหม่เกิดขึ้นตลอดเวลา

5. งบประมาณ (Budget) ไม่ได้มีการกำหนดงบประมาณด้านการจัดการ การความมั่นคงปลอดภัยไซเบอร์ อยากชัดเจน

การวิเคราะห์สภาพแวดล้อมทางยุทธศาสตร์

วิเคราะห์ยุทธศาสตร์ด้านไซเบอร์ในต่างประเทศ

ประเทศสหรัฐอเมริกา สำนักงานความมั่นคงปลอดภัยและโครงสร้างพื้นฐานทางไซเบอร์ (Cybersecurity and infrastructure security agency : CISA) กระทรวงความมั่นคงแห่งมาตุภูมิได้มีการจัดทำยุทธศาสตร์ชาติด้านการรักษาความมั่นคงปลอดภัยของโลกไซเบอร์สเปซ (National strategy to secure cyberspace) ล่าสุด ปี2561 ได้กำหนด ยุทธศาสตร์ไซเบอร์ของประเทศ (National cyber strategy) มีหัวข้อหลัก 4 ด้าน ดังนี้

1. การปกป้องผืนแผ่นดินและวิถีชีวิตของอเมริกันชน (Protect the American people, the homeland, and the American way of life) ประกอบด้วย การรักษาความมั่นคงปลอดภัยให้กับเครือข่ายกิจการโทรทัศน์ และกิจการโทรคมนาคมของสหพันธรัฐ และข้อมูลของสหพันธรัฐ (Secure federal networks and information) โดยการกำหนดมาตรฐานในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ที่มีประสิทธิภาพ และการรวมศูนย์การสั่งการและมอบหมายหน้าที่ความรับผิดชอบ รวมถึงกำกับดูแลภาพรวมการทำงานของหน่วยงานที่เกี่ยวข้อง, การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Secure critical infrastructure) โดยการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ที่เกี่ยวข้องกับโครงสร้างพื้นฐาน การกระจายและจัดสรรความเสี่ยงระหว่างภาครัฐและภาคเอกชน ในลักษณะของการร่วมลงทุนระหว่างภาครัฐและเอกชน (PPPs) การจัดลำดับความสำคัญของปฏิบัติการ (Consequence-driven) ที่ลดความรุนแรงและความยาวนานของการหยุดชะงักของโครงสร้างพื้นฐาน ,การรับมืออาชญากรรมทางไซเบอร์และการพัฒนาการรายงานอุบัติการณ์ (Combat cybercrime and improve incident reporting) โดยอาศัยความร่วมมือระหว่างมลรัฐ ท้องถิ่น ชนเผ่า และเขตแดน ในการตรวจตรา ป้องกัน ต่อต้าน และสืบสวนสอบสวนเกี่ยวกับภัยคุกคามทางไซเบอร์ต่อประเทศสหรัฐ

2. การเสริมสร้าง ความมั่งคั่งของอเมริกา (Promote American prosperity) ประกอบด้วย การพัฒนาเศรษฐกิจดิจิทัลให้มีความมั่นคั่งและมีความทนทานต่อภัยคุกคามทางไซเบอร์ (Foster a vibrant and resilient digital economy) โดยการสนับสนุนการกำหนดมาตรฐานของการรักษาความมั่นคงปลอดภัยทางเศรษฐกิจ ตลาดกลางการพาณิชย์ (Marketplace) และนวัตกรรม ,การพัฒนาและคุ้มครองทรัพย์สินทางปัญญาของประเทศสหรัฐอเมริกา (Foster and protect United States ingenuity) โดยการคุ้มครองสิ่งประดิษฐ์ เทคโนโลยี และนวัตกรรมของประเทศสหรัฐอเมริกาจากการจารกรรมทรัพย์สินทางปัญญา รวมถึงการผลักดันบทบาทผู้นำด้านเทคโนโลยี เช่น ปัญญาประดิษฐ์ (Artificial intelligence: AI) และโครงสร้างพื้นฐานโทรคมนาคมสำหรับอนาคต (Next generation telecommunication infrastructure) การพัฒนากำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เหนือกว่า (Develop a superior cybersecurity workforce) โดยพัฒนาศูนย์รวมบุคลากรมากความสามารถ (Talent pool) และดึงดูดผู้เชี่ยวชาญจากต่างประเทศ

3. การรักษาสันติภาพ ด้วยพลัง (Preserve peace through strength) ประกอบด้วย การสร้างเสถียรภาพทางไซเบอร์ผ่านพฤติกรรมความรับผิดชอบของรัฐที่เป็นบรรทัดฐานทางสังคม (Enhance cyber stability through norms of responsible state Behavior) ผ่านกรอบความรับผิดชอบของรัฐภายใต้กฎหมายระหว่างประเทศ ,การหยุดยั้งพฤติกรรมที่ไม่เหมาะสมในโลกไซเบอร์สเปซ (Attribute and deter unacceptable behavior in cyberspace) กิจกรรมไซเบอร์ที่เป็นภัยต่อประเทศสหรัฐอเมริกา ด้วยวิธีการทางการทูต การข่าวสาร การทหาร การเงิน การข่าวกรอง และการบังคับใช้กฎหมาย

4. การขยายอิทธิพลของสหรัฐอเมริกา (Advance American influence) ประกอบด้วย การสนับสนุนเสรีภาพบนระบบอินเทอร์เน็ต เชื่อมโยงกันได้ เชื่อถือได้ และมั่นคงปลอดภัย (Promote an open, interoperable, reliable, and secure internet) การสร้างขีดความสามารถไซเบอร์ระหว่างประเทศ (Build international cyber capacity) โดยส่งเสริมการพัฒนาขีดความสามารถไซเบอร์ให้ประเทศพันธมิตร เพื่อให้ประเทศพันธมิตรสามารถปกป้องตนเองได้ และสามารถสนับสนุนประเทศสหรัฐอเมริกาในการรับมือกับปัญหาภัยคุกคามไซเบอร์อย่างมีประสิทธิภาพ แลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์กับประเทศพันธมิตร เพื่อป้องกันโครงสร้างพื้นฐานที่สำคัญยิ่งยวดและห่วงโซ่อุปทานของโลก รวมถึงขยายความร่วมมือทางด้านการทูต การเศรษฐกิจ และความมั่นคงปลอดภัย

ประเทศสิงคโปร์ มีหน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติแห่งสิงคโปร์ (Cybersecurity agency of Singapore: CSA) เป็นผู้รับผิดชอบได้เผยแพร่ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ในปี 2559 โดยกำหนดให้ยุทธศาสตร์ประกอบด้วย 4 ด้าน ดังนี้

1. การสร้างโครงสร้างพื้นฐานที่มีความทนทานต่อภัยคุกคามทางไซเบอร์ (Building resilient infrastructure) ประกอบด้วย การปกป้องบริการที่สำคัญยิ่งยวด (Protect our essential services) โดยการจัดทำกระบวนการบริหารจัดการความเสี่ยง การสร้างวัฒนธรรมความตระหนักรู้ถึงความเสี่ยง การเพิ่มแนวปฏิบัติความมั่นคงด้วยการออกแบบ (Secure by design) การเพิ่มขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์อย่างเด็ดขาด (Respond decisively to cyber threats) โดยการสร้างความตระหนักรู้ต่อเหตุการณ์ การฝึกซ้อมแผนรับมือด้วยการจำลองสถานการณ์ที่ซับซ้อน และเกี่ยวโยงหลายภาคส่วน การสร้างความเข้มแข็งของโครงสร้างทางกฎหมายและการกำกับดูแลของภาครัฐ

(Strengthen governance and legislative framework) การรักษาความปลอดภัยให้กับเครือข่ายของรัฐบาล (Secure government networks) โดยการกำหนดสัดส่วนงบประมาณด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ที่ร้อยละ 8 ของวงเงินงบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสาร การลด การโจมตีเครือข่ายของรัฐบาล การสร้างความตระหนักรู้ต่อเหตุการณ์ในหน่วยงานภาครัฐ

2. การสร้างโลกไซเบอร์สเปซที่ปลอดภัยยิ่งขึ้น (Creating a safer cyberspace) ประกอบด้วย การต่อสู้กับอาชญากรรมทางไซเบอร์ (Combat cybercrime) โดยแผนปฏิบัติการระดับชาติ ที่เพิ่มองค์ความรู้ เพิ่มขีดความสามารถรับมือให้กับหน่วยงานภาครัฐ พัฒนากรอบกฎหมายในการตัดสินคดีอาชญากรรมทางไซเบอร์ และสร้างความร่วมมือระหว่างประเทศ การพัฒนาสู่การเป็นศูนย์กลางแห่งความเชื่อมั่น (Enhance Singapore's standing as a trusted hub) โดยการสร้างระบบนิเวศของข้อมูลที่เชื่อถือได้ ทั้งต่อผู้ใช้งานข้อมูล และหน่วยงานที่ให้บริการข้อมูล การพัฒนาเจ้าหน้าที่คุ้มครองข้อมูลที่มีความ เชี่ยวชาญ การสนับสนุนความรับผิดชอบต่อส่วนรวม (Promote collective responsibility) โดยภาคธุรกิจและประชาชนต้องมีความพร้อมรับข่าวสารเพื่อป้องกันระบบคอมพิวเตอร์ และอุปกรณ์ดิจิทัลของตนเองจากผู้ประสงค์ร้ายที่อาจจารกรรมระบบหรืออุปกรณ์

3. การพัฒนาระบบนิเวศของความมั่นคงปลอดภัยไซเบอร์ (Developing a vibrant cybersecurity ecosystem) ประกอบด้วย การสร้างกำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่มีความเชี่ยวชาญ (Establish a professional cybersecurity workforce) โดยสร้างเส้นทางการเจริญก้าวหน้าในสายอาชีพที่ชัดเจน สนับสนุนการให้ใบรับรองที่เป็นที่ยอมรับในระดับสากล การให้ทุนการศึกษา หลักสูตรการศึกษาเฉพาะอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ การพัฒนาทักษะที่มีอยู่เดิม (Up-skilling) และการเรียนรู้ทักษะใหม่ (Re-skilling) การสร้างนวัตกรรมเพื่อเร่งการพัฒนา (Innovate to accelerate) โดยอาศัยความพร้อมด้านสิ่งอำนวยความสะดวกด้านการวิจัยและพัฒนาที่ได้มาตรฐานระดับโลก การพัฒนาบุคลากรผู้มีความสามารถโดดเด่น การสร้างความร่วมมือในการวิจัยและพัฒนาระหว่างภาครัฐ ภาคเอกชน ภาควิชาการ และภาคอุตสาหกรรม

4. การสร้างความร่วมมือระหว่างประเทศ (Strengthening international partnership) ประกอบด้วย การสร้างความร่วมมือระดับภูมิภาคอาเซียนและความร่วมมือระหว่างประเทศ

เพื่อรับมือกับภัยคุกคามไซเบอร์และอาชญากรรมทางไซเบอร์ (Forge international and ASEAN cooperation to counter cyber threats and cybercrime) โดยเพิ่มประสิทธิภาพให้กับกระบวนการรายงานและการรับมือ การอาศัยความร่วมมือกับเครือข่ายการทำงานขององค์การตำรวจอาชญากรรมระหว่างประเทศ (Interpol) และการพัฒนาขีดความสามารถในการรับมือกับอาชญากรรมทางไซเบอร์ การริเริ่มสร้างขีดความสามารถด้านไซเบอร์ระดับยอดเยี่ยมของภูมิภาคอาเซียนและระดับสากล (Champion international and ASEAN cyber capacity building initiatives) ในด้านปฏิบัติการ เทคนิค กฎหมาย นโยบาย และการทูต การแลกเปลี่ยนเรียนรู้ประสบการณ์ในด้านการบังคับใช้กฎหมายและบรรทัดฐานไซเบอร์ของภูมิภาคและระดับสากล (Facilitate international and regional exchanges on cyber norms and legislation)

วิเคราะห์ยุทธศาสตร์ด้านไซเบอร์ในประเทศไทย

สถานการณ์ไซเบอร์ภายในประเทศไทยนับว่ายังไม่มีความรุนแรงมากนัก การโจมตีในลักษณะที่เป็นการทำสงครามไซเบอร์ระดับประเทศนั้นยังไม่ปรากฏเหตุการณ์ชัดเจน มีเพียงแต่เหตุการณ์ที่เว็บไซต์ของหน่วยงานต่าง ๆ ถูกโจมตีด้วยการเปลี่ยนหน้าเว็บไซต์จากบุคคลเฉพาะกลุ่ม เช่น กลุ่มพลเมืองต่อต้านการเชื่อมต่ออินเทอร์เน็ต (Single Gateway) กลุ่มพลเมืองต่อต้าน พระราชบัญญัติ คอมพิวเตอร์ โดยผู้กระทำผิด หรือแฮกเกอร์กลุ่มดังกล่าวต้องการต่อต้านอำนาจของรัฐ หรือทำให้รัฐเกิดความวุ่นวาย และเสียหาย นอกจากนี้ ยังมีการโจมตีอีกรูปแบบหนึ่งที่เกิดขึ้น คือ การปฏิบัติการข่าวสาร (Information Operations : IO) กล่าวคือ เป็นการเปลี่ยนแปลงข่าวสารการรับรู้ต่าง ๆ ของประชาชน เช่น การแฮกเข้าไปบนเว็บไซต์เพื่อทิ้งข้อความบางอย่างไว้ การที่หน่วยงานภาครัฐทำ IO ผลงานนายกรัฐมนตรีเป็นอินโฟกราฟิกเผยแพร่ออกไป แต่กลุ่มดังกล่าวก็ทำการเปลี่ยนแปลงด้วยการตัดต่อเป็นรูปตลกขบขัน ซึ่งถือเป็นสงคราม IO ที่เกิดขึ้น เพื่อต้องการดึงประชาชนรวมถึงสื่อต่างประเทศที่เลือกฝั่งชัดเจนและไม่เลือกฝั่งชัดเจนเข้ามาในสนามนี้ด้วย

จะเห็นได้ว่า ความรุนแรงของสงครามไซเบอร์ในปัจจุบันมีความเปลี่ยนแปลงไปจากเดิม ที่เน้นโจมตีเทคโนโลยีสารสนเทศเป็นหลัก เช่น โทรศัพท์มือถือเครื่องคอมพิวเตอร์ เป็นการเข้าถึงโดยไม่ได้รับอนุญาต การรบกวนการทำงานของคอมพิวเตอร์ การใช้คอมพิวเตอร์เพื่อการหลอกลวง และทำลายข้อมูลรวมถึงการสอดแนมข้อมูลทางการเมือง และการทหาร และ

การโจมตีที่ส่งผลกระทบร้ายแรงต่อนานับประเทศคงหนีไม่พ้นการโจมตีเทคโนโลยีปฏิบัติการ (Operational Technology) อันครอบคลุมถึงเทคโนโลยีที่ดูแลระบบไฟฟ้าเขื่อน ตลอดจนพลังงานนิวเคลียร์ ซึ่งหากกระทำได้สำเร็จก็จะสร้างความเสียหายที่ร้ายแรงกว่าในอดีต ซึ่งกลุ่มแฮกเกอร์ที่มีประสิทธิภาพจะกระทำการในลักษณะนี้ได้ มักเป็นกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากประเทศมหาอำนาจหรือจากประเทศใดประเทศหนึ่ง

จากความมั่นคงรูปแบบใหม่ โดยเฉพาะอาชญากรรมไซเบอร์ ในระดับประเทศขณะนี้ สำนักงานสภาความมั่นคงแห่งชาติกำลังดำเนินการจัดทำนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อใช้เป็นกรอบกำหนดทิศทางการรักษาความปลอดภัยของประเทศ อันจะนำไปสู่การออก พระราชบัญญัติ และกฎหมายอื่น ๆ ที่เกี่ยวข้องตามมา นอกจากนี้ รองนายกรัฐมนตรีฝ่ายความมั่นคง และรัฐมนตรีว่าการกระทรวงกลาโหมได้มีนโยบายต่อภัยคุกคามด้านไซเบอร์ โดยให้เสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์กระทรวงกลาโหมทั้งในด้านโครงสร้าง การจัดหน่วยระดับนโยบาย และระดับปฏิบัติ การสรรหาและการพัฒนาความรู้ให้กับบุคลากรที่จะบรรจุในอัตราของหน่วยที่เกี่ยวข้องกับการปฏิบัติงานไซเบอร์ การพัฒนาหลักนิยม และหลักการสำหรับการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับ รวมทั้งการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ให้กับกำลังพลโดยทั่วไป เพื่อให้เห็นถึงความสำคัญและมีความตื่นตัวในการปฏิบัติตามมาตรการรักษาความปลอดภัยด้านไซเบอร์ (กระทรวงกลาโหม, 2560) เช่นเดียวกับกองบัญชาการกองทัพไทยโดยผู้บัญชาการทหารสูงสุดก็ได้มีนโยบายให้จัดตั้งและบูรณาการหน่วยงานรับผิดชอบงานด้านไซเบอร์ให้มีขีดความสามารถทั้งเชิงรุกและเชิงรับ และพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยจะเชื่อมโยงกับการตั้งศูนย์ไซเบอร์ (Cyber Center) ของ กองบัญชาการกองทัพไทย และ 3 เหล่าทัพ มี ขอบเขตอำนาจหน้าที่ ในการประสานนโยบายไซเบอร์กับระดับชาติ รวมทั้งรับผิดชอบด้านนโยบาย ยุทธศาสตร์ และปฏิบัติงานด้านไซเบอร์ในระดับยุทธศาสตร์ของกระทรวงกลาโหมใน และเพื่อรองรับยุทธศาสตร์ชาติ 20 ปี (2561 - 2580) ของหน่วยเหนือ โดยกำหนดแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พุทธศักราช2560 - 2564 แบ่งเป็น 6 แผนงาน ดังนี้ 1. แผนการจัดองค์กรด้านไซเบอร์ โดย กห. บก.ทท. และเหล่าทัพ ดำเนินการจัดตั้ง หน่วยงานไซเบอร์/ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง 2. แผนการป้องกันระบบโครงสร้างพื้นฐาน โดย กระทรวงกลาโหม และกองบัญชาการกองทัพไทย และเหล่าทัพเตรียม จัดตั้ง

ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Operation Center ; CSOC) เพื่อรองรับภัยคุกคามด้านไซเบอร์ที่จะมาโจมตีระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูลรวมทั้งการจัดตั้งทีมจัดการปัญหาฉุกเฉิน ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response Team/ Computer Security Incident Response Team ; CSIRT) 3. แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการ สงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ ทั้งเชิงรุกและเชิงรับเพื่อการป้องกัน สะกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มี ผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่าง ๆ รวมถึงการจัดให้มีการแข่งขันทักษะการ ปฏิบัติการไซเบอร์ (Cyber Contest) ทั้งนี้ มิได้มุ่งหมายเพื่อสร้างนักรบไซเบอร์ (Cyber Warrior) 4. แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโนโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตาม ความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว 5. แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ กองทัพเป็น หน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับ รัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain) 6. แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือ ทุกภาคส่วน ทั้งภาครัฐ ธุรกิจเอกชน และประชาชน

สถานการณ์ด้านไซเบอร์ของกองทัพบก

ศูนย์ไซเบอร์กองทัพบก เป็นผู้รับผิดชอบภารกิจด้านไซเบอร์ของกองทัพบก โดยได้มีการทำหน้าที่ เฝ้าระวัง ตรวจสอบ พร้อมทั้งการฝึกกำลังพลให้สามารถแก้ไขหรือตอบโต้ได้ในกรณีที่ถูกโจมตี ทางไซเบอร์ และกำหนดให้การรักษาความมั่นคงทางด้านไซเบอร์เป็นภารกิจที่สำคัญในด้านความมั่นคงของชาติ โดยศูนย์ไซเบอร์กองทัพบก ได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์เป็น 4 ด้าน ดังนี้

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศหรือ ระดับชาติผู้ที่ก่อภัยคุกคามอาจใช้วิธีนำข่าวสารเหล่านั้นลงเผยแพร่ในเว็บไซต์ของ

ประเทศตนเองเพื่อให้ ข่าวสารเหล่านั้นเผยแพร่เข้ามาสู่ประเทศไทยจนสงผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิด ความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศไทย และ การแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ที่เป็นภัยคุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่ เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าว ไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัว จนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็น การปฏิบัติการข่าวสาร (Information Operation) ที่เป็นการปฏิบัติการจิตวิทยา

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติ เป็นสิ่งที่กระทำได้ง่ายและยากต่อการดำเนินคดี ต่อผู้กระทำผิดคือการเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์การวิจารณ์สถาบันในทางเสื่อมเสีย ซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิด ไม่ได้อยู่ในประเทศไทยแต่ได้ใช้เว็บไซต์หรือสื่อโซเชียลในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย 4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพไทย ทำให้ภาพลักษณ์ของผู้นำกองทัพ ไทยเสียหายหรือลดความน่าเชื่อถือในสังคมไทย รวมทั้งลดความเชื่อมั่นของประชาชนต่อการปกป้องประเทศไทย และการบังคับบัญชาของเหล่าทัพ

การรักษาความปลอดภัยทางไซเบอร์ของกองทัพบก จะเน้นความร่วมมือ กับหน่วยงานภาครัฐและองค์กรภาคเอกชนโดยร่วมมือทั้งเรื่ององค์ความรู้และการเฝ้าระวังภัยคุกคามทางด้าน ไซเบอร์ การฝึกผู้เชี่ยวชาญด้านไซเบอร์โดยเน้นการรักษาความปลอดภัยทางไซเบอร์ 3 ประการดังนี้ 1. การป้องกัน (Identify & Protect) โดยการตรวจสอบช่องโหว่ที่มีในระบบ การทดสอบ การเจาะการเข้าสู่ระบบ หากตรวจพบช่องโหว่ในระบบจะได้ดำเนินการแก้ไขให้มีความปลอดภัยเพิ่มขึ้น 2. การเฝ้าระวังแบบเรียลไทม์ (Detect) ต้องทำการตรวจสอบวิเคราะห์ภัยคุกคามทางด้าน ไซเบอร์ขั้นสูง การรวบรวมและศึกษาข่าวกรอง และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่จะเกิดขึ้น 3. การสนองตอบภัยคุกคามแบบเรียลไทม์ (Respond) โดยจัดทำแผนตอบสนองต่อภัยคุกคาม ตามขั้นตอนที่ได้กำหนดไว้คือการสืบสวน

สอบสวนทางดิจิทัลและนิติวิทยาศาสตร์การวิเคราะห์หาสาเหตุ ของภัยคุกคามที่เกิดขึ้น รวมถึงการประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อดำเนินงานตามขั้นตอนของกฎหมาย ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) ในฐานะที่เป็นหน่วยรับผิดชอบงานด้านไซเบอร์ยังได้เพิ่มการพัฒนา โดยการฝึกอบรมกำลังพลของกองทัพบกซึ่งเป็นนายทหารสัญญาบัตรและชั้นประทวนประจำปี 2560 ขึ้นอีก 7 หลักสูตร ดังนี้ หลักสูตรที่ 1 คือ การปฏิบัติการด้านไซเบอร์เบื้องต้น ประกอบไปด้วยการปฏิบัติการไซเบอร์ (Kali Linux) การเจาะระบบเบื้องต้น องค์ประกอบพื้นฐานของ Information Security ประเภทภัยคุกคาม (Threat) ขั้นตอนการโจมตี Ethical Hacker 9 ขั้นตอน Network Mapping และการทำ Scanning เบื้องต้น หลักสูตรที่ 2 การปฏิบัติการไซเบอร์ขั้นสูง ศึกษาช่องโหว่ระบบปฏิบัติการต่าง ๆ ขั้นตอนการทดสอบการเจาะระบบข้อมูลของผู้ทดสอบเจาะระบบ โปรมแกรมทดสอบการเจาะระบบ (Metasploit Framework) การโจมตี Web Application หลักสูตรที่ 3 - 4 การรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity) สำหรับนายทหาร สัญญาบัตรและนายทหารชั้นประทวน การติดตั้งระบบปฏิบัติการเครื่องแม่ข่ายให้ปลอดภัย การรักษาความ ปลอดภัย Intrusion Detection System (IDS) ระบบตรวจจับการบุกรุกเป็นระบบที่ใช้สำหรับการเฝ้าระวัง และแจ้งเตือนภัยถ้ามีการบุกรุก Internet Service Provider (ISP) ระบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต วิเคราะห์ ภัยคุกคามและเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัย เช่น ไฟร์วอล เป็นต้น Firewall, Virus, Malware, Ransomware และการป้องกันการโจมตี Web Application กฎหมายอาชญากรรมทางไซเบอร์ หลักสูตรที่ 5 - 6 นายทหารรักษาความปลอดภัยไซเบอร์และเจ้าหน้าที่รักษาความปลอดภัย ของนายทหารชั้นประทวน ฝึกอบรมความตะหนักและการรักษาความปลอดภัยทางด้านไซเบอร์คอมพิวเตอร์ และระบบปฏิบัติการ ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) VA and Penetration Tesing, Vulnerability Scaning, Penetration Testing, Log Analysis หลักสูตรที่ 7 การบริหารจัดการข่าวสารทางไซเบอร์ของนายทหารระดับชั้นสัญญาบัตร และ นายทหารชั้นประทวน โดยฝึกอบรมพื้นฐานด้านการข่าวและวงรอบข่าวกรอง หลักการประชาสัมพันธ์และ การสื่อสารมวลชน กฎหมายที่เกี่ยวข้องกับพระราชบัญญัติคอมพิวเตอร์และพระราชบัญญัติลิขสิทธิ์เทคนิคการโฆษณาประชาสัมพันธ์ทางอินเทอร์เน็ตรูปแบบต่าง ๆ

วิเคราะห์แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก

จากการศึกษาสภาวะแวดล้อมทางยุทธศาสตร์ และสาเหตุ พบว่า เพื่อให้ได้แนวทางการแก้ไขปัญหาและอุปสรรคแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก จึงมีข้อเสนอแนวทางใหม่ ดังนี้

ทางเลือกที่ 1 สร้างขีดความสามารถ การพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้

1. ส่งเสริมความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Implement a coordinated cybersecurity awareness-raising programme) โดยมอบหมายหน่วยงานรับผิดชอบที่มีความเหมาะสม ผ่านโครงการรณรงค์ และกิจกรรม เพื่อเพิ่มความตระหนักรู้ในระดับกองทัพบก โดยเจาะจงกลุ่มเป้าหมาย ทุกระดับ เป็นต้น

2. พัฒนาหลักสูตรการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Develop cybersecurity curricula) เพื่อเร่งการพัฒนาทักษะและความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบการศึกษา ตั้งแต่เข้ารับราชการทหาร ไปจนถึงระดับ ผู้บริหารโดยบูรณาการหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์เข้ากับหลักสูตรที่เกี่ยวข้องกับวิทยาศาสตร์คอมพิวเตอร์ และเทคโนโลยีสารสนเทศ การสร้างคุณวุฒิบัตรด้านความมั่นคงปลอดภัยไซเบอร์ และการฝึกงานภาคปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

3. ส่งเสริมการพัฒนาทักษะและฝึกอบรมการทำงานด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ (Stimulate skills development and workforce training) สำหรับตำแหน่งผู้บริหาร ผู้เชี่ยวชาญ การฝึกอบรมเพื่อการปฏิบัติงาน ให้สอดคล้องตำแหน่งงาน ยุทธศาสตร์นี้ควรเร่งริเริ่มเพื่อพัฒนาเส้นทางความก้าวหน้าในสายอาชีพ และเพิ่มอุปทานด้านผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยควรสร้างความร่วมมือกับสถาบันการศึกษาภาคเอกชน และภาคประชาสังคม

ดังนั้น การพัฒนาบุคลากรกองทัพบก ต้องมีการดำเนินการภายในกองทัพบก โดยเมื่อบรรจุกำลังพลเข้าดำรงตำแหน่งจะจัดให้มีการเข้ารับการศึกษาในหลักสูตรที่เกี่ยวข้องกับการปฏิบัติหน้าที่ รวมถึงมีการจัดอบรมระยะสั้นเพื่อให้ทราบถึงการเปลี่ยนแปลงเทคโนโลยี และวิธีการ

ปฏิบัติ และมีการจัดส่งไปฝึกศึกษา อบรมจากหน่วยงานภายนอก บริษัทเอกชน และมหาวิทยาลัย เพื่อเพิ่มประสิทธิภาพ รวมถึงมีพิจารณาเข้าดำรงตำแหน่งที่สูงขึ้น

ทางเลือกที่ 2 นำผู้มีความรู้จากเอกชน สร้างความร่วมมือระหว่างหน่วยงานภายในประเทศหรือต่างประเทศ เข้ามาช่วยทำงานในกองทัพ

1. การพัฒนา บุคลากรด้านไซเบอร์ ซึ่งเป็นเรื่องยากต่อการผลิตบุคลากร ทำให้มีแนวคิดที่จะให้มีการ เชิญผู้เชี่ยวชาญมาช่วยกำกับดู และพยายามลดช่องว่างของไซเบอร์ให้มากที่สุด และใช้กระบวนการจัดการ สู่การปฏิบัติ

2. สร้างกระบวนการความร่วมมือระหว่างหน่วยงานภายในประเทศ (Establish inter organisational processes) โดยมีหน่วยงานหลักที่บูรณาการอำนาจหน้าที่ความรับผิดชอบของแต่ละหน่วยงานให้ปฏิบัติตามกฎหมายว่าด้วยการป้องกันอาชญากรรมทางไซเบอร์ และปกป้องโครงสร้างพื้นฐานที่สำคัญยิ่งยวด และอาจตั้งหน่วยงานที่เกี่ยวข้องโดยตรง เช่น ทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response teams: CERTs) เป็นต้น

โดยสนับสนุนการเข้าร่วมความตกลง และร่วมมือระหว่างประเทศในการต่อต้านอาชญากรรมทางไซเบอร์ (Support international cooperation to combat cybercrime) โดยกฎหมายในประเทศควรเปิดโอกาสในการจัดทำความตกลงและความร่วมมือระหว่างประเทศ

บทที่ 3
บทอภิปรายผล

การวิจัยเรื่อง แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก จะมีการศึกษายุทธศาสตร์ด้านความมั่งคงไซเบอร์ ของต่างประเทศ หน่วยงานในประเทศ และหน่วยงานของกองทัพ ผู้วิจัยพบว่าปัจจัยหลักในการที่จะทำให้สำเร็จสูงสุด คือ ปัจจัยด้านบุคลากร (People) ซึ่งมีประเด็นที่น่าสนใจ ดังนี้

จากการวิเคราะห์สภาวะแวดล้อมทางยุทธศาสตร์ สาเหตุของปัญหา ผู้วิจัยขอเสนอทางเลือกที่ 1 ในการสร้างขีดความสามารถ การพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ นำมาเป็นแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก เนื่องจากการพัฒนาศักยภาพบุคลากร และเทคโนโลยี แนวทางการดำเนินงานการพัฒนาศักยภาพขององค์กร และบุคลากรให้มีทักษะความรู้ เพื่อเพิ่มขีดความสามารถในการป้องกันตนเอง และหน่วยงานลดความเสี่ยง ลดความเสียหายจากการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้น พัฒนากำลังคนในทุกระดับตั้งแต่การส่งเสริมระดับสถานศึกษาเพื่อการสร้างบุคลากรรองรับความต้องการในอนาคต เพื่อยกระดับความพร้อมของประเทศในการรับมือ และจัดการกับภาวะความเสี่ยงภัยคุกคามทางไซเบอร์ ในปัจจุบัน และอนาคตโดยต้องเพิ่มจำนวน และคุณภาพของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความรู้ และทักษะเทียบเท่ากับสากล เช่น มีเอกสารรับรองคุณวุฒิ หรือการอบรม ที่เป็นที่ยอมรับของสากลกำหนดมาตรฐานวิชาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากลสร้างแรงจูงใจ และให้การสนับสนุนในการสร้างความเติบโตในสายอาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ยั่งยืน

โดยระยะต่อไปควรนำแนวทางเลือกที่ 2 นำผู้มีความรู้จากเอกชน สร้างความร่วมมือระหว่างหน่วยงานภายในประเทศ หรือต่างประเทศ เข้ามาช่วยทำงานในกองทัพมาปฏิบัติจะได้เป็นการยกระดับ และส่งเสริมความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Implement a coordinated cybersecurity awareness-raising programme) โดยมอบหมายหน่วยงานรับผิดชอบที่มีความเหมาะสม ผ่านโครงการรณรงค์ และกิจกรรมเพื่อเพิ่มความตระหนักรู้ในระดับกองทัพบก โดยเจาะจงกลุ่มเป้าหมาย ทุกระดับ ดำเนินการ

พัฒนาหลักสูตรการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Develop cybersecurity curricula) เพื่อเร่งการพัฒนาทักษะและความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบการศึกษา ตั้งแต่เข้ารับราชการทหาร ไปจนถึงระดับ ผู้บริหารโดยบูรณาการหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์เข้ากับหลักสูตรที่เกี่ยวข้องกับวิทยาศาสตร์คอมพิวเตอร์ และเทคโนโลยีสารสนเทศ การสร้างคุณวุฒิบัตรด้านความมั่นคงปลอดภัยไซเบอร์ และการฝึกงานภาคปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมการพัฒนาทักษะและฝึกอบรมการทำงานด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ (Stimulate skills development and workforce training) สำหรับตำแหน่งผู้บริหาร ผู้เชี่ยวชาญ การฝึกอบรมเพื่อการปฏิบัติงาน ให้สอดคล้องตำแหน่งงาน ยุทธศาสตร์นี้ควรเร่งริเริ่มเพื่อพัฒนาเส้นทางความก้าวหน้าในสายอาชีพ และเพิ่มอุปทานด้านผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยควรสร้างความร่วมมือกับสถาบันการศึกษา ภาคเอกชน และภาคประชาสังคม

การเปรียบเทียบกับวิธีการปฏิบัติที่ดี (Good practice)

การสร้างโครงสร้างพื้นฐานที่มีความทนทานต่อภัยคุกคามทางไซเบอร์ (Building resilient infrastructure) ประกอบด้วย การปกป้องบริการที่สำคัญยิ่งยวด (Protect our essential services) โดยการจัดทำกระบวนการบริหารจัดการความเสี่ยง การสร้างวัฒนธรรมความตระหนักรู้ถึงความเสี่ยง การเพิ่มแนวปฏิบัติความมั่นคงด้วยการออกแบบ (Secure by design) การเพิ่มขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์อย่างเด็ดขาด (Respond decisively to cyber threats) โดยการสร้างความตระหนักรู้ต่อเหตุการณ์ การฝึกซ้อมแผนรับมือด้วยการจำลองสถานการณ์ที่ซับซ้อน และเกี่ยวโยงหลายภาคส่วน การสร้างความเข้มแข็งของโครงสร้างทางกฎหมายและการกำกับดูแลของภาครัฐ (Strengthen governance and legislative framework) การรักษาความปลอดภัยให้กับเครือข่ายของรัฐบาล (Secure government networks) โดยการกำหนดสัดส่วนงบประมาณด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ที่ร้อยละ 8 ของวงเงินงบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสาร การลด การโจมตีเครือข่ายของรัฐบาล การสร้างความตระหนักรู้ต่อเหตุการณ์ในหน่วยงานภาครัฐ เช่นเดียวกันกับประเทศสหรัฐอเมริกา สำนักงานความมั่นคงปลอดภัยและโครงสร้างพื้นฐานทางไซเบอร์ (Cybersecurity and

infrastructure security agency : CISA) กระทรวงความมั่นคงแห่งมาตุภูมิได้มีการจัดทำยุทธศาสตร์ชาติด้านการรักษาความมั่นคงปลอดภัยของโลกไซเบอร์สเปซ (National strategy to secure cyberspace) ล่าสุด ปี2561 ได้กำหนด ยุทธศาสตร์ไซเบอร์ของประเทศ (National cyber strategy) มีหัวข้อหลัก 4 ด้าน คือ การปกป้องผืนแผ่นดินและวิถีชีวิตของอเมริกันชน การเสริมสร้างความมั่งคั่งของอเมริกา การรักษาสันติภาพด้วยพลัง และการขยายอิทธิพลของสหรัฐอเมริกา

การเปรียบเทียบกับผลงานวิจัยที่เกี่ยวข้อง

แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก ที่ผู้วิจัยได้ทำการศึกษา สอดคล้องกับ นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง (2560) เรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ พบว่า ขีดความสามารถการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติเชิงรับอยู่ในระดับดีและการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง มีนโยบาย กระบวนการแผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติเกือบทุกด้าน แต่ยังขาดแนวความคิดการปฏิบัติการด้านไซเบอร์ รวมถึงมีระบบและอุปกรณ์ที่ทันสมัยมีประสิทธิภาพ ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านไซเบอร์ คือ บุคลากร ซึ่งมีไม่เพียงพอ ขาดความรู้ และทักษะในการปฏิบัติงานด้านไซเบอร์ ระบบการจัดการความรู้มีข้อมูลไม่ครบถ้วน และโครงสร้างการจัดหน่วยสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น ดังนั้น เพื่อให้การปฏิบัติด้านไซเบอร์ของกองทัพอากาศมีขีดความสามารถเพิ่มขึ้น ต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวน ให้มีความรู้ ความสามารถ มีทักษะ พร้อมที่จะปฏิบัติภารกิจด้านไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งบรรจุบุคลากรเพิ่มเติมให้เหมาะสมกับภารกิจที่ได้รับ รวมถึงเร่งดำเนินการจัดทำแนวความคิดการปฏิบัติการด้านไซเบอร์เพื่อให้บุคลากรนำไปเป็นแนวทางการปฏิบัติภารกิจทบทวนแผนงานให้ทันสมัยและครอบคลุมการปฏิบัติ และควรจัดทำระบบการจัดการความรู้ให้มีข้อมูลถูกต้องครบถ้วน หากมีภารกิจด้านไซเบอร์มากขึ้นจากปัจจุบันควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติภารกิจด้วย และยังสอดคล้องกับ กัลยา ชินาธิวร (2562) พบว่า จากการศึกษาปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ พบว่าสอดคล้องกับประเด็นยุทธศาสตร์ชาติด้านความมั่นคงและด้านการสร้างความสามารถในการ

แข่งขัน จึงเห็นว่าสามารถนำปัจจัยความสำเร็จและวิธีดำเนินนโยบายของสิงคโปร์ โดยเฉพาะประเด็น 5 ด้านหลัก ได้แก่ ด้านกฎหมาย ด้านเทคนิค ด้านองค์กรด้านการเสริมสร้างศักยภาพ และด้านความร่วมมือ มาปรับใช้เพื่อการพัฒนาแนวทางการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยได้ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสามารถนำผลการศึกษานี้ใช้ประกอบการพิจารณาดำเนินการเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562 และเพื่อให้เกิดความร่วมมือในมิติด้านการต่างประเทศอย่างเป็นรูปธรรม เห็นควรเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมขยายความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับกระทรวงสื่อสารและสารสนเทศของสิงคโปร์ ภายใต้บันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนทศและการสื่อสารแห่งราชอาณาจักรไทยและกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับลงนามเมื่อวันที่ 31 พฤษภาคม 2559 อย่างไรก็ดี โดยที่บันทึกความเข้าใจฉบับดังกล่าวมีผลใช้บังคับในวันที่ลงนามโดยคู่ภาคี และมีผลใช้บังคับเป็นระยะเวลา 36 เดือน หลังจากนั้น ประกอบกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เปลี่ยนเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงเห็นควรเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการเจรจากับกระทรวงการสื่อสารและสารสนเทศของสิงคโปร์เพื่อขอขยายระยะเวลาของบันทึกความเข้าใจดังกล่าว และจัดทำรายละเอียดความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์แนบท้ายบันทึกความเข้าใจ

บทที่ 4
บทสรุป

การศึกษาเรื่องแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก สามารถสรุปผลการวิจัยได้ ดังนี้

แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก

แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก ผู้วิจัยใช้ทางเลือกที่ 1 แนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ โดยการสร้างขีดความสามารถการพัฒนาขีดความสามารถ และการสร้างความตระหนักรู้ เพื่อนำมาเป็นแนวทางการพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบก เนื่องจากการพัฒนาศักยภาพบุคลากรและเทคโนโลยี แนวทางการดำเนินงานการพัฒนาศักยภาพขององค์กร และบุคลากรให้มีทักษะความรู้ เพื่อเพิ่มขีดความสามารถในการป้องกันตนเอง และหน่วยงานลดความเสี่ยง ลดความเสียหายจากการถูกโจมตีทางไซเบอร์ที่อาจเกิดขึ้น พัฒนากำลังคนในทุกระดับตั้งแต่การส่งเสริมระดับสถานศึกษาเพื่อการสร้างบุคลากรรองรับความต้องการในอนาคต เพื่อยกระดับความพร้อมของประเทศในการรับมือ และจัดการกับภาวะความเสี่ยงภัยคุกคามทางไซเบอร์ ในปัจจุบัน และอนาคตโดยต้องเพิ่มจำนวน และคุณภาพของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความรู้ และทักษะเทียบเท่ากับสากล เช่น มีเอกสารรับรองคุณวุฒิ หรือการอบรม ที่เป็นที่ยอมรับของสากลกำหนดมาตรฐานวิชาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากลสร้างแรงจูงใจ และให้การสนับสนุนในการสร้างความเติบโตในสายอาชีพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ยั่งยืน

โดยระยะต่อไปควรนำแนวทางเลือกที่ 2 นำผู้มีความรู้จากเอกชน สร้างความร่วมมือระหว่างหน่วยงานภายในประเทศ หรือต่างประเทศ เข้ามาช่วยทำงานในกองทัพมาปฏิบัติจะได้เป็นการยกระดับ และส่งเสริมความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Implement a coordinated cybersecurity awareness-raising programme) โดยมอบหมายหน่วยงานรับผิดชอบที่มีความเหมาะสม ผ่านโครงการรณรงค์ และกิจกรรมเพื่อเพิ่มความตระหนักรู้ในระดับกองทัพบก โดยเจาะจงกลุ่มเป้าหมาย ทุกระดับ ดำเนินการ

พัฒนาหลักสูตรการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Develop cybersecurity curricula) เพื่อเร่งการพัฒนาทักษะและความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านระบบการศึกษา ตั้งแต่เข้ารับราชการทหาร ไปจนถึงระดับ ผู้บริหารโดยบูรณาการหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์เข้ากับหลักสูตรที่เกี่ยวข้องกับวิทยาศาสตร์คอมพิวเตอร์ และเทคโนโลยีสารสนเทศ การสร้างคุณวุฒิบัตรด้านความมั่นคงปลอดภัยไซเบอร์ และการฝึกงานภาคปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และส่งเสริมการพัฒนาทักษะและฝึกอบรมการทำงานด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ (Stimulate skills development and workforce training) สำหรับตำแหน่งผู้บริหาร ผู้เชี่ยวชาญ การฝึกอบรมเพื่อการปฏิบัติงาน ให้สอดคล้องตำแหน่งงาน ยุทธศาสตร์นี้ควรเร่งริเริ่มเพื่อพัฒนาเส้นทางความก้าวหน้าในสายอาชีพ และเพิ่มอุปทานด้านผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยควรสร้างความร่วมมือกับสถาบันการศึกษา ภาคเอกชน และภาคประชาสังคม

ข้อเสนอแนะ

1. การพัฒนากำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เหนือกว่า (Develop a superior cybersecurity workforce) โดยพัฒนาศูนย์รวมบุคลากรมากความสามารถ (Talent pool) และดึงดูดผู้เชี่ยวชาญจากต่างประเทศ

2. การพัฒนาระบบนิเวศของความมั่นคงปลอดภัยไซเบอร์ (Developing a vibrant cybersecurity ecosystem) ประกอบด้วย การสร้างกำลังแรงงานด้านความมั่นคงปลอดภัยไซเบอร์ที่มีความเชี่ยวชาญ (Establish a professional cybersecurity workforce) โดยสร้างเส้นทางการเจริญก้าวหน้าในสายอาชีพที่ชัดเจน สนับสนุนการให้ใบรับรองที่เป็นที่ยอมรับในระดับสากล การให้ทุนการศึกษา หลักสูตรการศึกษาเฉพาะอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ การพัฒนาทักษะที่มีอยู่เดิม (Up-skilling) และการเรียนรู้ทักษะใหม่ (Re-skilling)

3. การหยุดยั้งพฤติกรรมที่ไม่เหมาะสมในโลกไซเบอร์สเปซ (Attribute and deter unacceptable behavior in cyberspace) กิจกรรมไซเบอร์ที่เป็นภัยต่อประเทศด้วยวิธีการทางการทูต การข่าวสาร การทหาร การเงิน การข่าวกรอง และการบังคับใช้กฎหมาย

4. แนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์

4.1 ด้านองค์กร (Organization) ต้องระบุความสำเร็จของการจัดการคุกคามไซเบอร์เป็นกิจกรรมหลักของหน่วยงาน ระบุภัยคุกคามไซเบอร์ในแต่ละหน่วยงานภายในองค์กรให้ชัดเจน

4.2 บุคลากร (People) ควรมีการทำข้อสอบพื้นฐานในเรื่อง คุกคามไซเบอร์ ก่อนเข้ารับราชการ หรือมีหลักฐานรับรองคุณวุฒิ ผ่านเกณฑ์ หรือการอบรมทางไซเบอร์

4.3 ขั้นตอนการปฏิบัติงาน (Process) กำหนดกลไก การขับเคลื่อนยุทธศาสตร์ โครงการ แผนปฏิบัติงาน และขั้นตอนการปฏิบัติงานด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจนในทุกระดับงาน

4.4 เทคโนโลยี (Technology) เทคโนโลยีดิจิทัลที่ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์มีความซับซ้อนสูง และมีสิ่งใหม่เกิดขึ้นตลอดเวลา ต้องตามให้ทัน

4.5 งบประมาณ (Budget) ต้องมีการกำหนดงบประมาณด้านการจัดการ 4. การกำหนดสัดส่วนงบประมาณด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจนเพื่อนำไปพัฒนาบุคลากรอย่างชัดเจน

ข้อเสนอแนะในการวิจัยครั้งต่อไป

ข้อเสนอแนะในการวิจัยครั้งต่อไป ควรศึกษาเกี่ยวกับการสร้างเครือข่ายความร่วมมือในการแลกเปลี่ยนเรียนรู้ และพึ่งพาทั้งจากภายในประเทศและต่างประเทศเกี่ยวกับเทคโนโลยีใหม่ ๆ ประกอบด้วย ด้านวิชาการ ทักษะการปฏิบัติงาน การวิจัยและพัฒนานวัตกรรม การศึกษาจากกฎหมาย ระเบียบ คำสั่ง และพระราชบัญญัติ รวมทั้งการถ่ายทอดองค์ความรู้ต่าง ๆ เพื่อพัฒนาบุคลากรในการปฏิบัติงานด้านไซเบอร์ของกองทัพบกที่เหมาะสมและสอดคล้องกับแผนยุทธศาสตร์ชาติ 20 ปี

เอกสารอ้างอิง

กัลยา ชินาธิวร (2562). *ปัจจัยความสำเร็จของสิงคโปร์ : กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย*. รายงานการฝึกอบรมหลักสูตรนักบริหารการทูต รุ่นที่ 11 ปี 2562. สถาบันการต่างประเทศ กระทรวงการต่างประเทศ.

กองทัพไทย. (2560). *นโยบายผบ.ทสส./ผบ.ศบท.ประจำปีงบประมาณ2560*. เอกสารอัดสำเนา.

สำนักงาน กสทช.. *คู่มือ Cybersecurity สำหรับประชาชน*. 18 ธันวาคม 2563. จาก http://www.nbtc.go.th/News/รวมบทความ-(1)/คู่มือ-Cyber-Security-สำหรับประชาชน.aspx.

ณรงค์เวตย์ เรืองจวง. นอ.. (2560). *แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ*. เอกสารวิจัยส่วนบุคคล. หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 59. วิทยาลัยป้องกันราชอาณาจักร.

ณรงค์เวตย์ เรืองจวง. นอ.. (2561). *แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ*. วารสารราย 4 เดือน ปีที่ 60 ฉบับที่ 3 กันยายน – ธันวาคม 2561.

ปกรณ์ ปรียากร. (2538). *ทฤษฎีและแนวคิดเกี่ยวกับการพัฒนาในการบริหารการพัฒนา*. กรุงเทพมหานคร : สามเจริญพานิช.

พิไลวรรณ อินทรักษา. (2550). *การดำเนินงานในส่วนงานการฝึกอบรม*. วิทยานิพนธ์. บริหารธุรกิจ มหาวิทยาลัยบูรพา. ชลบุรี.

เมธา สุวรรณสาร. (2564). *ผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของชาติ : ปัญหาอธิปไตยไซเบอร์ และแนวทางการกำหนดยุทธศาสตร์ชาติ*. จาก http://www.itgthailand.com/ผลกระทบต่อความมั่นคงปล-2/

ยุทธศาสตร์ชาติ 20 ปี (พุทธศักราช 2561 - 2580). ราชกิจจานุเบกษา. เล่ม 135 ตอนที่ 82 ก. 13 ตุลาคม 2561.

ยุวัฒน์ วุฒิเมธี. (2526). *หลักการพัฒนาชุมชนและการพัฒนาชนบท*. กรุงเทพมหานคร : ไทยอนุเคราะห์ไทย.

ราชบัณฑิตสถาน. (2538). *พจนานุกรมฉบับราชบัณฑิตยสถาน พุทธศักราช 2538*. กรุงเทพมหานคร : อักษรเจริญทัศน.

สนธยา พลศรี. (2547). *ทฤษฎีและหลักการพัฒนาชุมชน*. พิมพ์ครั้งที่ 5. กรุงเทพมหานคร : โอเดียนสโตร.

อริย์ธัช แก้วเกาะสะบ้า. (2560). *ศูนย์ไซเบอร์กองทัพบก*. วิทยากรชำนาญการพิเศษ. กลุ่มงานบริการวิชาการ 1 สำนักวิชาการ.

AMColarikandLJanczewski. (2001). *Establishing Cyber Warfare Doctrine*. Journal of Strategic Security, VolWarfare : ANewDoctrineandTaxonomy. USAirForce, April 2001.

DavidJSmith. (2012). *Russia Cyber Operations*. July 2012.

Seiler,J.P. (1975). *The molecular mechanism of benzimidazole mutagenicity: in vitro studies on transcription and translation 13 : 635* - 641.

Szilagyi, Andrew D. (1984). *Management and Performance*. 3rd ed. Glenview : Scot, Foresman.

Steers, R.M. (1977). *Organization Effectiveness*. California : Good year PublishersInc.

ประวัติย่อผู้วิจัย

ยศชื่อ นาย สุเมธ ตั้งประเสริฐ

วันเดือนปีเกิด 25 พฤษภาคม 2520

ประวัติสำเร็จการศึกษา

พ.ศ. 2542	วิทยาศาสตร์บัณฑิตสาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ มหาวิทยาลัยธรรมศาสตร์
พ.ศ. 2547	บริหารธุรกิจมหาบัณฑิตวิทยาลัยการจัดการ มหาวิทยาลัยมหิดล

ประวัติการทำงาน

พ.ศ. 2558	เลขานุการนายกองค์การบริหารส่วนจังหวัดตาก
พ.ศ. 2562	คณะทำงานกลุ่มย่อย (Intersect) เพื่อพัฒนาระบบบัญชีชุดเดียว
พ.ศ. 2562	กรรมการบริหารสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
พ.ศ. 2563	คณะกรรมการเทคโนโลยีสารสนเทศสถาบันพระปกเกล้า
พ.ศ. 2563	กรรมการบริหารสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์
พ.ศ. 2563	ที่ปรึกษาประจำคณะกรรมาธิการป้องกันและบรรเทาผลกระทบจากภัยธรรมชาติและสาธารณภัย
พ.ศ. 2563	ที่ปรึกษาประจำคณะกรรมาธิการสามัญประจำผู้แทนราษฎร

ตำแหน่งปัจจุบัน

พ.ศ. 2563 - ปัจจุบัน	กรรมการผู้จัดการบริษัทเด็พธเฟิร์สทจำกัด