



แนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ

Guidelines for Competency Development of the Royal Thai Air Force Cyber Workforce

นาวาอากาศเอก ณรงค์เวทย์ เรืองจวง

รองผู้อำนวยการสำนักนโยบายและแผน

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

Gp.Capt. Narongwate Ruangjuang

Deputy Director, Office of Policy and Plan, Directorate of Information and
Communication Technology, Royal Thai Air Force

E-mail: n_wej62@hotmail.com



บทคัดย่อ

ระบบเทคโนโลยีสารสนเทศมีความสำคัญต่อการปฏิบัติการทางทหารเป็นอย่างยิ่ง ถึงแม้จะมีการดำเนินการอย่างมีประสิทธิภาพ แต่ก็มีความเสี่ยงที่เกิดจากความผิดพลาดของระบบหรือถูกโจมตีทางไซเบอร์จากผู้ไม่หวังดี ซึ่งบุคลากรเป็นปัจจัยหนึ่งที่มีผลต่อการปฏิบัติการ จึงมีความจำเป็นต้องพัฒนาเพิ่มขีดความสามารถเพื่อรองรับเทคโนโลยีที่เปลี่ยนแปลงตลอดเวลา ในการวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ โดยวิธีการวิจัยเชิงคุณภาพ ด้วยการรวบรวมและวิเคราะห์ข้อมูลจากเอกสารที่เกี่ยวข้อง รวมถึงการสัมภาษณ์ผู้บังคับบัญชาและผู้ปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ และกำหนดขอบเขตการวิจัยเฉพาะในกองทัพอากาศ

ผลการวิจัยพบว่าขีดความสามารถการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติเชิงรับอยู่ในระดับดีและการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง มีนโยบาย กระบวนการ แผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติเกือบทุกด้าน แต่ยังขาดแนวความคิด การปฏิบัติการด้านไซเบอร์ รวมถึงมีระบบและอุปกรณ์ที่ทันสมัยมีประสิทธิภาพ ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านไซเบอร์คือ บุคลากร ซึ่งมีไม่เพียงพอ ขาดความรู้และทักษะในการปฏิบัติงานด้านไซเบอร์ ระบบการจัดการความรู้ข้อมูลไม่ครบถ้วน และโครงสร้างการจัดหน่วยสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น ดังนั้น เพื่อให้การปฏิบัติด้านไซเบอร์ของกองทัพอากาศมีขีดความสามารถเพิ่มขึ้นต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวนให้มีความรู้ความสามารถ มีทักษะ พร้อมทั้งจะปฏิบัติการด้านไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งบรรจุบุคลากรเพิ่มเติมให้เหมาะสมกับภารกิจที่ได้รับ รวมถึงเร่งดำเนินการจัดทำแนวความคิดการปฏิบัติการด้านไซเบอร์เพื่อให้บุคลากรนำไปเป็นแนวทางการปฏิบัติการ ทบทวนแผนงานให้ทันสมัยและครอบคลุมการปฏิบัติ และควรจัดทำระบบการจัดการความรู้ให้มีข้อมูลถูกต้อง ครบถ้วน หากมีภารกิจด้านไซเบอร์มากขึ้นจากปัจจุบันควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติการด้วย

คำสำคัญ: ไซเบอร์

ABSTRACT

Information technology system is significant for military missions. In spite of the efficient operations, the risks caused by system errors or from cyber attackers still occur. Personnel are one factor affecting the missions, it is therefore necessary to raise their level of competence to adapt to ever-changing technology. This research aimed to study the ways to develop the capabilities of cyber personnel of the Royal Thai Air Force by using qualitative research methodology to collect and analyse relevant documents including the Royal Thai Air Force commander and practitioner interviews. This research study focuses on the area of the Royal Thai Air Force.

The results of this research found that, defensive operations of the Royal Thai Air Force cyber competence are good, while proactive operations are moderate. The relevant policies, processes, master and action plans for supporting the implementation cover almost all aspects, however; lack of cyber concept of operations. There are also no modern and effective systems and devices. Factors affecting cyber competence include insufficient number of staff, lack of knowledgeable and skilled personnel in the field of cyber as well as incomplete information in the knowledge management system. Furthermore, the organisational structure can support only current staff. Accordingly, in order to enhance operational competencies in the field of cyber of the Royal Thai Air Force, practice and training practitioners must be provided for the purpose of readiness to perform their missions effectively. The number of personnel should be appropriate for the task. Moreover, implementing the cyber operational concept should be accelerated in order to be practice guidelines for staff. The action plans should be revised, updated and comprehended. The knowledge management system should contain completely accurate information. In case there are more cyber task, the organisational structure should be also reviewed whether or not the structure is still consistent with the missions.

Keywords: Cyber

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีความสำคัญต่อการปฏิบัติการทุกรูปแบบ ซึ่งกองทัพอากาศนำเทคโนโลยีสารสนเทศ และการสื่อสารมาประยุกต์ใช้ในการปฏิบัติการกิจเช่นกัน การดำเนินการในอดีตที่ผ่านมา การเก็บรวบรวมข้อมูลด้านต่าง ๆ ของกองทัพอากาศจะดำเนินการที่หน่วย ซึ่งกว่าจะส่งมาให้ผู้บังคับบัญชาทราบ และตัดสินใจต้องใช้เวลานาน เมื่อเทคโนโลยีมีการพัฒนาอย่างทันสมัยและมีความรวดเร็วยิ่งขึ้น กองทัพอากาศจึงนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติการกิจ การเตรียมกำลังกองทัพอากาศ การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพอากาศ โดยเฉพาะการป้องกันทางอากาศและด้านการสนับสนุนภายในกองทัพ รวมถึงสนับสนุนหน่วยงานความมั่นคงอื่นภายนอกกองทัพอีกด้วย การประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศทำให้ใช้เวลาในการดำเนินการสั้นลง รวมถึงสามารถจัดเก็บข้อมูลได้อย่างรวดเร็ว และสามารถจัดเก็บเป็นข้อมูลอิเล็กทรอนิกส์ในระบบสารสนเทศของกองทัพอากาศได้เป็นจำนวนมาก แต่ด้วยวิวัฒนาการทางเทคโนโลยีในรูปแบบดิจิทัลทั้งระบบอุปกรณ์ เครือข่ายทางสาย ไร้สาย และทางอินเทอร์เน็ต มีการใช้งานมากขึ้นและมีการพัฒนาอย่างรวดเร็ว จึงเป็นปัจจัยสำคัญที่ก่อให้เกิดจุดอ่อนในขณะปฏิบัติงานและถูกผู้ไม่หวังดีนำวิธีการทางไซเบอร์มาล้วงข้อมูลหรือโจมตีโครงสร้างระบบสารสนเทศและเครือข่ายเพื่อสร้างความได้เปรียบทางด้านข้อมูลของบุคคล หน่วยงาน หรือองค์กรต่าง ๆ ซึ่งกองทัพอากาศได้ถูกโจมตีทางไซเบอร์อยู่เนื่อง ๆ นับเป็นภัยอย่างยิ่งต่อความมั่นคงในการปฏิบัติการกิจของกองทัพอากาศ กระทรวงกลาโหมและความมั่นคงของชาติ โดยแนวโน้มจะมีความรุนแรงมากขึ้นตามลำดับ กองทัพอากาศจึงกำหนดให้มีการพัฒนาการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร กระบวนการทำงานบุคลากรและหน่วยงานของกองทัพอากาศให้สามารถปฏิบัติการกิจได้อย่างครบถ้วน ถูกต้อง ปลอดภัย ทันท่วง

สถานการณ์ และได้ขอปรับโครงสร้างกองทัพอากาศ โดยจัดตั้งกองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อรับผิดชอบงานด้านสงครามไซเบอร์โดยตรง

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและข้อจำกัด การปฏิบัติการกิจด้านไซเบอร์ของกองทัพอากาศ
2. เพื่อศึกษาปัจจัยที่มีผลกระทบต่อการปฏิบัติการกิจด้านไซเบอร์ของกองทัพอากาศ
3. เพื่อเสนอแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติการกิจด้านไซเบอร์ของกองทัพอากาศ

ขอบเขตของการวิจัย

การวิจัยครั้งนี้จะศึกษาและวิเคราะห์ถึงปัญหา ข้อจำกัด ปัจจัยที่เกี่ยวข้องในการปฏิบัติการกิจด้านไซเบอร์ของกองทัพอากาศ โดยเฉพาะอย่างยิ่งการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องกับการปฏิบัติการกิจด้านไซเบอร์ ซึ่งผู้วิจัยได้กำหนดขอบเขตของการวิจัยดังนี้

1. ขอบเขตประชากร

ประชากรที่ใช้ในการวิจัยครั้งนี้ประกอบด้วย ข้าราชการชั้นสัญญาบัตรของกองทัพอากาศที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยขึ้นตรงกองทัพอากาศที่ปฏิบัติงานในระหว่าง พ.ศ. 2559-2560 โดยมีผู้ให้ข้อมูลสำคัญประกอบด้วย ผู้บังคับบัญชาและ ผู้ปฏิบัติหน้าที่ของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ โดยเป็นการศึกษาในเรื่องการเตรียมบุคลากรในการปฏิบัติด้านไซเบอร์

2. ขอบเขตพื้นที่ กองทัพอากาศ

3. ขอบเขตระยะเวลาการวิจัย ตั้งแต่เดือนธันวาคม 2559-มิถุนายน 2560

ประโยชน์ที่ได้รับจากการวิจัย

1. ทราบถึงสภาพปัญหาและข้อจำกัดการปฏิบัติการกิจ
ด้านไซเบอร์ของกองทัพอากาศ
2. ทราบถึงปัจจัยที่มีผลกระทบต่อการปฏิบัติการกิจ
ด้านไซเบอร์ของกองทัพอากาศ
3. ข้อเสนอแนะแนวทางการพัฒนาบุคลากรและปัจจัย
ที่เกี่ยวข้องต่อการปฏิบัติการกิจด้านไซเบอร์กองทัพอากาศ
การทบทวนวรรณกรรม

การทำวิจัยเรื่องแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ ผู้วิจัยได้ศึกษาจากเอกสาร แนวความคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการปฏิบัติการด้านไซเบอร์ เพื่อเป็นกรอบแนวทางในการศึกษาค้นคว้า ได้แก่ แนวคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร ไซเบอร์กับการรักษาความปลอดภัย และการปฏิบัติการสงครามไซเบอร์ (Cyber Warfare) ยุทธศาสตร์กองทัพอากาศ และการพัฒนาบุคลากรของกองทัพอากาศ

ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร

1. สมรรถนะในองค์กร
- 1.1 สมรรถนะ หมายถึง ความรู้ ความสามารถ ทักษะที่ จะปฏิบัติหน้าที่ให้ประสบความสำเร็จและเกิด ประสิทธิภาพกับองค์กรอย่างสูงสุด ซึ่งสมรรถนะในองค์กร สามารถแบ่งออกเป็น 3 ประเภทหลัก ได้แก่ สมรรถนะหลัก (Core Competency) คือความสามารถหลักที่คาดหวังให้ พนักงานทุกคนทุกระดับขององค์กรจะต้องมีสมรรถนะ การบริหาร (Managerial Competency) คือความ สามารถในการบริหารจัดการงานที่คาดหวังกับกลุ่มพนักงาน แยกตามระดับตำแหน่งงาน และสมรรถนะตามหน้าที่ (Function Competency) คือความสามารถในงานเฉพาะ ด้านที่แตกต่างกันไปในแต่ละหน่วยงาน
- 1.2 องค์ประกอบที่สำคัญของสมรรถนะการเป็น ผู้นำของผู้บริหารองค์กร สมรรถนะทางการบริหาร (Managerial Competency: MC) หมายถึงสมรรถนะที่เป็น ความสามารถทางการจัดการซึ่งสะท้อนให้เห็นถึงทักษะใน การบริหารและจัดการงานต่าง ๆ กำหนดให้ต้องมีทั้งระดับ ผู้บริหารและระดับพนักงานปฏิบัติการ แต่จะแตกต่างกัน

ตามบทบาทหน้าที่และความรับผิดชอบ ได้แก่ วิสัยทัศน์
เชิงกลยุทธ์ การวางแผนงาน ภาวะผู้นำ การแก้ไขปัญหา
และตัดสินใจ และการบริหารการเปลี่ยนแปลง

2. บรรรยากาศขององค์กร หมายถึงสภาพแวดล้อมใน การทำงานที่เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกัน ระหว่างปัจจัยภายในและปัจจัยภายนอกตั้งแต่ละองค์กรจะ มีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความ รู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร ซึ่งแนวคิด เกี่ยวกับบรรยากาศองค์กรนั้น สเตียร์ส (Steers, 1977) ได้ แบ่งองค์ประกอบของบรรยากาศองค์กรไว้ 6 ด้าน ได้แก่ โครงสร้างการทำงาน ระบบรางวัลตอบแทน ความเป็นอิสระ ความอบอุ่นและการสนับสนุน การยอมรับความขัดแย้ง และความรักในหมู่คณะ

3. การพัฒนาบุคลากร หมายถึง กระบวนการที่จะเสริมสร้างและเปลี่ยนแปลง ผู้ปฏิบัติงานในด้านต่าง ๆ เพื่อเพิ่มประสิทธิภาพในการทำงาน เช่น ความรู้ความสามารถ ทักษะ ทัศนคติ วิธีการในการทำงาน เป็นต้น

4. การจัดการความรู้ (Knowledge Management) หมายถึงการรวบรวมองค์ความรู้ที่อยู่กระจัดกระจายทั้งใน ตัวบุคคลหรือเอกสารมาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนใน องค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้นำ ความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานให้เกิด ประสิทธิภาพอันจะส่งผลให้องค์กรมีความสามารถในการ แข่งขันสูงสุด ซึ่งชนิดของความรู้ (Types of Knowledge) ประกอบด้วย ความรู้ที่อยู่ในตัวคน ความรู้ที่ชัดเจน และ ความรู้ที่ชัดเจนแน่นอน ซึ่งประโยชน์ของการจัดการความรู้ นั้น จะช่วยประหยัดเวลาในการปฏิบัติงาน ช่วยการตัดสินใจ แก้ไขปัญหาได้ถูกต้อง พัฒนาทักษะของผู้ปฏิบัติงาน รวมถึงสร้างคู่มือ/แนวปฏิบัติในการทำงานและบันทึกความรู้ไว้ ให้กับองค์กร

ไซเบอร์กับการรักษาความปลอดภัยและการปฏิบัติ
การ (Cyber with Security and Operations) (ไซเบอร์
กับการรักษาความปลอดภัยและ การปฏิบัติการ, ออนไลน์,
2556)

1. ความหมายของ Cyber สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความสำคัญ

หมายของไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่า เกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) เป็นต้น และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริง ที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง”

2. การรักษาความปลอดภัยของไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้ห้องคอมพิวเตอร์ปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การโจรกรรมและความผิดพลาดต่าง ๆ ซึ่ง ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ การละเมิดการป้องกันข้อมูลส่วนตัว การรบกวนการทำงานหรือ การดำเนินธุรกรรม และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ มีมาตรการที่สำคัญ คือ มาตรการในการรักษาความปลอดภัยไซเบอร์ การปฏิบัติ การในห้วงไซเบอร์ การโจมตีทางไซเบอร์ และการป้องกันทางไซเบอร์

สงครามไซเบอร์ (Cyber Warfare)

1. ความหมายของสงครามไซเบอร์ หมายถึงการใช้ คอมพิวเตอร์และอินเทอร์เน็ตในการทำสงคราม เช่น การโจมตีเว็บไซต์ หรือบล็อกเว็บไซต์ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเทอร์เน็ต การเจาะข้อมูลลับโดยแฮกเกอร์ ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ ทำให้ ข้อมูลมีการเปลี่ยนแปลง การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐาน โดยการทำสงครามไซเบอร์มีแนวทางในการดำเนินการที่แตกต่างกันและหลากหลาย ได้แก่ การก่อการร้ายทางสารสนเทศ (Information Terrorism) เป็นลักษณะของการก่อความรุนแรง ความเสียหาย หรือก่อความไม่สงบบนระบบเครือข่ายที่เชื่อมต่อกัน การโจมตีทางความหมาย (Semantic Attack) เป็นการใช้เทคนิคและความสามารถ

ในการเป็นแฮกเกอร์แอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้าม เพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน

2. ภัยคุกคามทางไซเบอร์

2.1 ประเภทของภัยคุกคามทางไซเบอร์แบ่งออกเป็น 4 ประเภทดังนี้ ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (Application-based Threats) ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-based Threats) ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย และภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย ซึ่งผู้ก่อเหตุทางไซเบอร์อาจมีหลายส่วน ได้แก่ กลุ่มบุคคลและหรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์ เช่น ประเทศที่มีความประสงค์ร้าย ผู้ก่อการร้าย สายลับภาคเอกชน/องค์กรอาชญากรรม แฮกเกอร์ (Hackers) และแฮกทีวิส (Hacktivists) เป็นต้น

2.2 มาตรฐานการรักษาความปลอดภัยไซเบอร์ องค์กรที่เกี่ยวข้องได้กำหนดมาตรฐาน ISO/IEC 27001-2013 เพื่อใช้งานเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศขึ้น โดยมีวัตถุประสงค์เพื่อบริหารจัดการกับความปลอดภัยไซเบอร์ ซึ่งเป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่หลายองค์กรยึดถือร่วมกัน

ยุทธศาสตร์กองทัพอากาศ (ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2560)

1. ยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ. 2561-2580) (ฉบับเผยแพร่) ยุทธศาสตร์กองทัพอากาศ 20 ปี ให้ความสำคัญกับการพัฒนากองทัพอากาศในทุกด้านอย่างเป็นระบบ ทั้งนี้ เพื่อให้กองทัพอากาศมีขีดความสามารถที่เพียงพอและเหมาะสมในการปฏิบัติการกิจที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ โดยมีวัตถุประสงค์สำคัญเพื่อปรับปรุงขอบเขตการพัฒนากองทัพอากาศให้สอดคล้องกับสถานะแวดล้อม ด้านความมั่นคงที่เปลี่ยนแปลงไปในปัจจุบัน มีความสอดคล้องกับยุทธศาสตร์ชาติ ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม และยุทธศาสตร์ทหารกองทัพบก

2. ยุทธศาสตร์กองทัพอากาศได้กำหนดบทบาท หน้าที่ และภารกิจด้านไซเบอร์ โดยกำหนดให้เป็นมิติไซเบอร์ (Cyber Domain) ซึ่งเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเครือข่ายและอินเทอร์เน็ตได้รับการพัฒนาอย่างรวดเร็ว รวมทั้งการเกิดขึ้นของภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบ การโจรกรรมข้อมูล และการโจมตีเพื่อทำลายล้าง ล้วนก่อให้เกิดผลกระทบและความเสียหายในวงกว้าง กองทัพอากาศจึงกำหนดกลยุทธ์พัฒนาขีดความสามารถด้าน สงครามไซเบอร์ เพื่อพัฒนาหลักนิยมการปฏิบัติการในมิติ ไซเบอร์ทั้งเชิงรุกและเชิงรับ รวมทั้งพัฒนาระบบการฝึก ศึกษาสำหรับการปฏิบัติงานด้านไซเบอร์ และพัฒนาระบบ การจัดการความรู้ภายในกองทัพอากาศ

การพัฒนาบุคลากรของกองทัพอากาศ กองทัพอากาศได้จัดทำระเบียบกองทัพอากาศว่าด้วยการแยก ประเภทกำลังพลกองทัพอากาศ พ.ศ. 2552 (และที่แก้ไข เพิ่มเติม) เพื่อกำหนดเป็นแนวทางการบริหารกำลังพล ในด้านต่าง ๆ เช่น การบรรจุเข้าตำแหน่ง การให้ความรู้ด้าน การทหาร การให้ความรู้สายวิชาชีพ การฝึกงานในหน้าที่ เป็นต้น เพื่อพัฒนากำลังพลให้มีประสิทธิภาพ มีคุณสมบัติ ที่เหมาะสมกับตำแหน่งที่ตรงกับความรู้ความสามารถ ซึ่งการแยกประเภทกำลังพลกองทัพอากาศมีความสัมพันธ์ กับระบบงานอื่นคือ อัตรากองทัพอากาศ การบรรจุ การย้าย การศึกษา การฝึกงานในหน้าที่ และการทะเบียน ประวัติ

จากการรวบรวมข้อมูลเอกสาร แนวความคิด ทฤษฎี เกี่ยวกับสมรรถนะในองค์กรและองค์การสมัยใหม่ การปฏิบัติ การด้านสงครามไซเบอร์ การรักษาความปลอดภัยและการ ปฏิบัติการด้านไซเบอร์ ยุทธศาสตร์กองทัพอากาศ และ การพัฒนาบุคลากรตามระเบียบกองทัพอากาศ ว่าด้วยการ แยกประเภทกำลังพลกองทัพอากาศ ทำให้ทราบถึงแนวทาง การรวบรวมข้อมูลที่เกี่ยวข้องกับงานด้านไซเบอร์ รวมถึง แนวทางการดำเนินการของกองทัพอากาศในส่วนที่ เกี่ยวข้องกับการปฏิบัติงานด้านไซเบอร์ในปัจจุบัน

ระเบียบวิธีวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาและ วิเคราะห์จากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือ เอกสารที่เผยแพร่โดยทั่วไปด้านสงครามไซเบอร์ นโยบาย ระดับชาติ นโยบายระดับกองทัพ นโยบายและแนวปฏิบัติ ในการรักษาความปลอดภัยด้านสารสนเทศของกองทัพอากาศ และการปฏิบัติงานด้านสงครามไซเบอร์ดังนี้

1. รวบรวมเอกสารที่เกี่ยวข้อง เช่น ตำรา วารสาร บทความ เอกสารทางวิชาการ นโยบายที่เกี่ยวข้อง ตลอดจน ค้นคว้าทางอินเทอร์เน็ต เป็นต้น
2. สัมภาษณ์ผู้บังคับบัญชา ผู้เชี่ยวชาญ และผู้ปฏิบัติงานด้านสงครามไซเบอร์ โดยคำถามที่ใช้ในการสัมภาษณ์ ดังนี้

- 2.1 การดำเนินการด้านไซเบอร์ตามวงรอบการ ป้องกันทางไซเบอร์ (Cyber Defense) ดำเนินการอย่างไร
- 2.2 การดำเนินการด้านไซเบอร์ตามวงรอบการ โจมตีทางไซเบอร์ (Cyber Attack) ของกองทัพอากาศ ดำเนินการอย่างไร
- 2.3 โครงสร้างหน่วยงานด้านไซเบอร์ที่เกี่ยวข้อง
- 2.4 บุคลากรทุกระดับ (ประสิทธิภาพ จำนวน และ ความรู้ความสามารถ)
- 2.5 สถานที่ทำงานมีความเหมาะสมและเพียงพอ ต่อการปฏิบัติหรือไม่ อย่างไร
- 2.6 อื่น ๆ

ผลการวิจัย

จากผลการศึกษาวิจัยพบว่ากองทัพอากาศได้ให้ความสำคัญ การปฏิบัติงานด้านไซเบอร์เพื่อเตรียมรับมือกับภัย คุกคามที่อาจจะเกิดขึ้น ด้วยการจัดหาเทคโนโลยีพร้อม อุปกรณ์และระบบป้องกันมาใช้ในการปฏิบัติงาน มีการ จัดทำแผนงานที่เกี่ยวข้อง รวมถึงพัฒนาบุคลากรด้านไซเบอร์ และจัดให้มีการตรวจสอบระบบอย่างต่อเนื่องดังนี้

1. สรุปผลจากการสัมภาษณ์ผู้บังคับบัญชาและผู้ปฏิบัติ หน้าที่ด้านไซเบอร์ของกองทัพอากาศสามารถสรุปผลดังนี้
 - 1.1 การดำเนินการด้านไซเบอร์ตามวงรอบการ ป้องกันทางไซเบอร์ ประกอบด้วย การป้องกัน การตรวจจับ

การตอบสนองและการฟื้นฟูนั้น กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศดำเนินการตามขั้นตอนแล้ว โดยการจัดหา ระบบ อุปกรณ์ และมีการควบคุมระบบที่เหมาะสม รวมถึง จัดทำแผนงานรองรับและแผนการบริหารความเสี่ยงใน ภาพรวมทั้งหมดจนได้รับมาตรฐาน ISO 27001(2013) และ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศจัด ทำแผนงานและระเบียบการปฏิบัติให้ผู้เกี่ยวข้องดำเนินการ

1.2 การดำเนินการด้านไซเบอร์ตามวงรอบการ โจมตีทางไซเบอร์ ประกอบด้วย การรวบรวมข้อมูลเป้าหมาย การตรวจสอบหาช่องโหว่ของระบบ การปฏิบัติการโจมตี การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป และการลบ ร่องรอยการโจมตีนั้น กรมเทคโนโลยีสารสนเทศและการ สื่อสารทหารอากาศรับผิดชอบในการปฏิบัติ มีข้อจำกัดใน การดำเนินการหลายด้าน เนื่องจากไม่มีเป้าหมายที่เป็นภัย อย่างชัดเจน แต่มีการจัดหาระบบอุปกรณ์ที่เกี่ยวข้องมาฝึก ปฏิบัติการ

1.3 โครงสร้างหน่วยงานด้านไซเบอร์

1.3.1 หน่วยงานด้านสารสนเทศขึ้นตรง กองทัพอากาศ ส่วนมากเป็นระดับฝ่าย ซึ่งจะปฏิบัติการกิจ ที่ได้รับตามความรับผิดชอบภายในหน่วย และประสานการ ปฏิบัติงานร่วมกับกรมเทคโนโลยีสารสนเทศและการสื่อสาร ทหารอากาศและหน่วยงานอื่นที่เกี่ยวข้อง โครงสร้างอัตรา ที่ได้รับจึงเพียงพอสำหรับภารกิจเริ่มต้นใหม่ หากมีการกิจ เพิ่มเติมควรปรับโครงสร้างให้สอดคล้องด้วย

1.3.2 กองส่งครามไซเบอร์ กรมเทคโนโลยี สารสนเทศและการสื่อสารทหารอากาศ เป็นโครงสร้างที่ ยกระดับความสำคัญขึ้นมาจากเดิม งานที่ดำเนินการเป็น งานฝ่ายเสนาธิการและผู้ปฏิบัติงานด้านไซเบอร์โดยตรง การ ดำเนินการและกำกับดูแลการฝึกด้านไซเบอร์ รวมถึงต้อง ไปบรรยายให้สถานศึกษาและหน่วยเกี่ยวข้อง พร้อมกับ ปฏิบัติงานร่วมกับหน่วยอื่น ๆ ซึ่งโครงสร้างยังสามารถ รองรับภารกิจได้ระดับหนึ่ง หากมีการกิจเพิ่มเติมควรปรับ โครงสร้างและอัตราให้เหมาะสม

1.3.3 ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นหน่วยที่จะต้องปรนนิบัติดูแล ระบบเทคโนโลยีสารสนเทศของกองทัพอากาศ บุคลากรมี

คุณภาพและปฏิบัติงานได้อย่างมีประสิทธิภาพ มีโครงสร้าง ที่เหมาะสมกับภารกิจ แต่บุคลากรมีไม่เพียงพอต่อการ ปฏิบัติงาน

1.4 บุคลากร บุคลากรมีประสิทธิภาพในระดับปาน กลาง เนื่องจากเทคโนโลยีสารสนเทศมีการพัฒนาตลอด เวลา การได้รับระบบสารสนเทศเพิ่มเติมนั้นบุคลากรจะต้อง เรียนรู้ในการใช้งานและแก้ไขข้อบกพร่องที่อาจจะเกิดขึ้น ซึ่งระบบเดิมคงใช้งานอยู่ทำให้มีการกระหม่อมที่เพิ่มขึ้น ทำให้ มีความต้องการบุคลากรที่มีทักษะมาปฏิบัติงาน และมีปัจจัย หลายอย่างที่ทำให้บุคลากรไม่อยู่ในระบบ เช่น ย้ายไปดำรง ตำแหน่งที่สูงขึ้น เกษียณอายุราชการ ลาออก เป็นต้น จึงมี ความจำเป็นต้องจัดหาบุคลากรมาทดแทน การพัฒนา บุคลากรจึงต้องดำเนินการอย่างต่อเนื่องเพื่อให้ทันต่อการ ปฏิบัติ

1.5 สถานที่ทำงาน หน่วยสารสนเทศขึ้นตรงกับ กองทัพอากาศ ถึงแม้จะเป็นหน่วยที่จัดตั้งขึ้นใหม่แต่มี ความพร้อมในการปฏิบัติหน้าที่ บุคลากรสามารถใช้งานได้ อย่างเหมาะสม ส่วนสถานที่ทำงานของกรมเทคโนโลยี สารสนเทศและการสื่อสารทหารอากาศยังไม่เพียงพอที่จะ รองรับการปฏิบัติงานด้านไซเบอร์ ซึ่งผู้บังคับบัญชา ระดับสูงได้กำหนดพื้นที่เพิ่มเติมให้แล้ว อยู่ระหว่างการ ปรับปรุง และสถานที่ทำงานศูนย์คอมพิวเตอร์ กรมสื่อสาร อิเล็กทรอนิกส์ทหารอากาศ มีพื้นที่คับแคบไม่เพียงพอต่อ การติดตั้งระบบเทคโนโลยีสารสนเทศเนื่องจากมีการจัดหา ระบบเทคโนโลยีสารสนเทศเพิ่มเติมตลอดเวลา การติดตั้ง ระบบภายในอาคารไม่เพียงพอ ซึ่งได้ขอรับการสนับสนุน การสร้างอาคารใหม่โดยอยู่ในระหว่างการดำเนินการของ หน่วยเกี่ยวข้อง

2. สภาพปัญหาและข้อจำกัด การปฏิบัติการกิจด้าน ไซเบอร์ของกองทัพอากาศ

2.1 ปัญหา

2.1.1 บุคลากรบางส่วนละเลยไม่ปฏิบัติตาม นโยบายที่เกี่ยวข้อง รวมถึงบุคลากรด้านไซเบอร์มีจำนวน ไม่เพียงพอและขาดทักษะในการปฏิบัติงาน

2.1.2 การศึกษาเฉพาะด้านยังไม่ครอบคลุม ไม่มีนักพัฒนาโปรแกรมประสมค์ร้าย รวมถึงระบบการ

จัดการความรู้ยังไม่ครอบคลุมเทคโนโลยีและคู่มือการใช้งานอุปกรณ์

2.1.3 ระเบียบกองทัพอากาศที่เกี่ยวข้องด้านสารสนเทศและไซเบอร์ไม่ครอบคลุมการปฏิบัติงาน

จากสภาพปัญหาดังกล่าว กองทัพอากาศควรฝึกอบรมทบทวนบุคลากรให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ รวมถึงควรสนับสนุนงบประมาณและจัดบุคลากรเข้ารับการศึกษาดูงานหลักสูตร และเร่งผลิตบุคลากรให้พร้อมปฏิบัติงาน อีกทั้งให้ผู้เกี่ยวข้องรวบรวมองค์ความรู้เพื่อให้สามารถสืบค้นและเป็นแนวทางในการปฏิบัติงาน รวมถึงดำเนินการจัดคู่มือการใช้งานอุปกรณ์และโปรแกรมให้ครอบคลุมการใช้งานอย่างเร่งด่วน และควรมีการลงโทษบุคลากรที่ไม่ได้ปฏิบัติตาม กฎ ระเบียบและข้อบังคับ

2.2 ข้อจำกัด

2.2.1 ด้านสถานที่ระบบเทคโนโลยีเชิงป้องกันที่จัดทำมาใช้งานทั้งเชิงป้องกันและเชิงป้องกันปรามติดตั้งใช้งาน 2 สถานที่ ทำให้ไม่สะดวกต่อการปฏิบัติงานของบุคลากร

2.2.2 ด้านลิขสิทธิ์ ระบบเทคโนโลยีที่จัดทำมาใช้งานต้องมีลิขสิทธิ์จากบริษัทผู้ผลิต ทำให้ต้องใช้งบประมาณมากขึ้น

2.2.3 ด้านเทคโนโลยี เทคโนโลยีมีการพัฒนาจึงต้องมีการติดตามและจัดทำใช้งานเพื่อป้องกันช่องโหว่ที่อาจจะเกิดขึ้น ทำให้ต้องใช้งบประมาณในการจัดหาตลอดเวลา

จากข้อจำกัดดังกล่าว เห็นควรให้ติดตั้งเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องกันปรามในอาคารเดียวกัน รวมถึงต้องเพิ่มงบประมาณอย่างเหมาะสมในการจัดหาเทคโนโลยีและเป็นค่าลิขสิทธิ์มาใช้งาน

3. ปัจจัยที่มีผลกระทบต่อการปฏิบัติการกิจด้านไซเบอร์ของกองทัพอากาศ

ปัจจัยการปฏิบัติการไซเบอร์ กองทัพอากาศมีการปฏิบัติตามองค์ประกอบ 3 องค์ประกอบดังนี้

3.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง กองทัพอากาศมีการดำเนินการในหลายด้าน เช่น จัดทำระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ การ

จัดการแข่งขัน Cyber Operations Contest การจัดการองค์ความรู้ เป็นต้น ซึ่งการดำเนินการตามแผนและขั้นตอนดังกล่าวยังไม่ครอบคลุมการปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ

การดำเนินการตามแผนงานและขั้นตอนที่กำหนดไว้ หากสามารถดำเนินการได้จะทำให้การปฏิบัติการกิจด้านไซเบอร์เป็นไปอย่างมีประสิทธิภาพ รวมถึงเร่งการจัดทำเอกสารคู่มือการปฏิบัติงานและการจัดองค์ความรู้ให้ครอบคลุมการปฏิบัติงาน

3.2 ปัจจัยด้านเทคโนโลยี กองทัพอากาศได้ดำเนินการจัดหาระบบเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องกันปรามมาใช้งาน เช่น ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรอง และระบบจำลองยุทธทางไซเบอร์ เป็นต้น ซึ่งการจัดหาเทคโนโลยีมาใช้งานในกองทัพนั้น มีการจัดหาตามแผนงานที่กำหนดไว้ แต่จากการที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็วจึงต้องมีการจัดหาเทคโนโลยีใหม่มาใช้งาน

การจัดหาเทคโนโลยีมาใช้งานนั้นเห็นควรให้จัดสรรงบประมาณสนับสนุนและเร่งสร้างบุคลากรรองรับการปฏิบัติการกิจอย่างเหมาะสม

3.3 ปัจจัยด้านบุคลากร กองทัพอากาศมีการดำเนินการด้านความรู้เพื่อรองรับบุคลากร โดยจัดทำหลักสูตรเพื่อพัฒนาบุคลากร เช่น หลักสูตรพื้นฐานรองรับผู้ปฏิบัติงาน หลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศ หลักสูตรอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งส่งบุคลากรเข้ารับการฝึกอบรมนอกกองทัพ เป็นต้น อีกทั้งมีการสร้างจิตสำนึกและการแจ้งเตือนให้มีการเสริมสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ ตามที่กองทัพอากาศได้ดำเนินการมาแล้วนั้น สามารถให้ความรู้และความสามารถบุคลากรได้ในระดับหนึ่ง แต่บุคลากรยังขาดทักษะและความชำนาญ รวมถึงมีจำนวนไม่เพียงพอต่อการปฏิบัติงาน

ตามที่กองทัพอากาศได้ดำเนินการมานั้น สามารถให้ความรู้และความสามารถบุคลากรได้ในระดับหนึ่ง แต่ยังขาดทักษะและความชำนาญในการปฏิบัติงาน จึงเห็นควรต้องมีการฝึกอบรมและทบทวนอย่างต่อเนื่อง รวมถึงต้อง

มีเอกสารคู่มือการปฏิบัติงานและการจัดองค์ความรู้ด้วย พร้อมทั้งควรส่งบุคลากรไปฝึกศึกษาอบรมจากหน่วยงานภายนอกตามความเหมาะสมและบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติงาน

4. แนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ

4.1 การพัฒนาบุคลากรในการปฏิบัติการด้านไซเบอร์

4.1.1 บุคลากร

4.1.1.1 ผู้บังคับบัญชาระดับหัวหน้าหน่วยขึ้นตรงกองทัพอากาศมีความเข้าใจในการดำเนินการด้านไซเบอร์เป็นอย่างดี แต่ควรมีการควบคุมและกำกับดูแลการดำเนินงานด้านไซเบอร์ภายในหน่วยให้ปฏิบัติตามแผนงานให้เกิดประสิทธิภาพสูงสุด

4.1.1.2 ผู้ตรวจสอบ ผู้ที่เป็นวิทยากรให้การอบรม ผู้รับผิดชอบดูแลระบบ และผู้ปฏิบัติงาน เห็นควรให้มีการควบคุมและกำกับดูแล ในการทบทวนขั้นตอนการปฏิบัติหน้าที่อย่างต่อเนื่อง พร้อมให้จัดทำคู่มือการปฏิบัติงานและการใช้งานเทคโนโลยีเป็นเอกสารเพื่อถ่ายทอดให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง จัดอบรมบุคลากรภายในหน่วยให้ทราบถึงเทคโนโลยีใหม่และควรส่งบุคลากรไปศึกษาอบรมกับหน่วยงานภายนอก มหาวิทยาลัย หรือบริษัทที่เกี่ยวข้อง

4.1.1.3 กำลังพลไม่เพียงพอต่อการปฏิบัติงาน ควรบรรจุกำลังพลให้หน่วยทุกระดับให้เพียงพอต่อการปฏิบัติงานโดยไม่น้อยกว่าร้อยละ 60 ของอัตราอนุมัติกำลังพล และที่สำคัญต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจนว่าต้องการบุคลากรที่มีคุณวุฒิและความรู้ความสามารถที่ตรงกับการปฏิบัติงาน

4.1.2 การดำเนินการด้านหลักสูตรที่เกี่ยวข้อง

4.1.2.1 จัดเตรียมหลักสูตรและทบทวนหลักสูตรที่ใช้ในการฝึกศึกษาและอบรมด้านไซเบอร์อย่างต่อเนื่อง รวมถึงพิจารณาสถานศึกษาภายนอกเพื่อส่งบุคลากรไปฝึกศึกษาและอบรมให้เหมาะสม

4.1.2.2 จัดทำและปรับปรุงการตรวจ

สอบระบบให้ทันสมัย และให้มีการสุ่มตรวจสอบระบบในภาพรวม หากพบข้อบกพร่องให้แจ้งหน่วยเกี่ยวข้องทราบเพื่อแก้ไข และเมื่อพบบุคลากรกระทำผิดให้พิจารณาลงโทษตามแนวทางที่กองทัพอากาศกำหนด

4.1.2.3 พิจารณาจัดส่งบุคลากรไปอบรมภายนอกหน่วย จนกระทั่งได้ใบรับรองความสามารถ (Cyber Certification) และให้นำความรู้ความสามารถกลับมาถ่ายทอดให้กับบุคลากรภายในกองทัพอากาศ อีกทั้งส่งเสริมบุคลากรเข้าร่วมการฝึก การฝึกพร้อม/ผสม และเข้าศึกษาอบรมดูงานในประเทศและต่างประเทศในทุกระดับ

4.2 ปัจจัยที่เกี่ยวข้อง

4.2.1 การจัดทำแผนและแนวทางการปฏิบัติงานยังไม่ครอบคลุมการปฏิบัติงาน รวมถึงแนวทางการตรวจสอบระบบที่กำหนดไว้ในแผนยังไม่ทันสมัยนั้น ควรจัดทำแผนและคู่มือการปฏิบัติเมื่อมีเหตุการณ์ อีกทั้งต้องจัดทำคู่มือการใช้งานระบบอุปกรณ์และโปรแกรมที่มีใช้งานอยู่ และที่จะจัดหาใหม่เพิ่มเติมเมื่อได้รับระบบ เพื่อใช้ในการปฏิบัติการของหน่วย รวมถึงควรมีการสร้างแรงจูงใจให้กับผู้ปฏิบัติงานเห็นควรให้ผู้บังคับบัญชาลำดับต้นในการดำเนินการขอเงินเพิ่มพิเศษเป็นค่าตอบแทนให้กับผู้ปฏิบัติงานด้านไซเบอร์

4.2.2 ระบบอุปกรณ์และโปรแกรมที่มีใช้งานต้องมีลิขสิทธิ์จากบริษัทผู้ผลิตและจำเป็นต้องจัดหาต่อเนื่องทุกปี ควรสนับสนุนงบประมาณค่าลิขสิทธิ์และการจัดหาเทคโนโลยีที่ทันสมัยตามความจำเป็นใช้งาน โดยเฉพาะเทคโนโลยีเชิงป้องกัน รวมถึงต้องพัฒนายุทธวิธีทางไซเบอร์โดยเน้นที่การพัฒนา การแลกเปลี่ยน หรือใช้งานทรัพยากรทางไซเบอร์ร่วมกับหน่วยงานอื่น ๆ

4.2.3 ปัจจัยสถานที่ เนื่องจากมีการติดตั้งอุปกรณ์ไซเบอร์ไว้ 2 แห่ง หากมีการสร้างอาคารใหม่รองรับงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เห็นควรให้ติดตั้งระบบด้านไซเบอร์เชิงป้องกันไว้ภายในอาคารเดียวกันเพื่อสะดวกต่อการปฏิบัติงาน

4.2.4 จัดทำระบบการจัดการความรู้ (Knowledge Management System) ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพอากาศ และกำหนดให้ใช้งานได้ตามสิทธิ์ที่ได้รับ

บทสรุป

กองทัพอากาศได้ตระหนักถึงความสำคัญการปฏิบัติงานด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามที่อาจเกิดขึ้น โดยการจัดตั้งหน่วยงานรับผิดชอบโดยตรง จัดหาเทคโนโลยี อุปกรณ์ และระบบมาใช้ในการปฏิบัติการกิจกรรมถึงจัดทำแผนงาน กฎระเบียบในส่วนที่เกี่ยวข้อง พัฒนาบุคลากรให้มีความรู้ความสามารถอย่างต่อเนื่อง พร้อมทั้งจัดให้มีการตรวจสอบระบบและบุคลากรอย่างต่อเนื่อง ซึ่งในบางส่วนยังมีข้อขัดข้องและดำเนินการได้ไม่เต็มประสิทธิภาพ จึงมีข้อเสนอแนะดังนี้

1. ปัจจุบันโครงสร้างหน่วยงานและอัตราที่ได้รับการอนุมัติไว้ อาจจะไม่สามารถรองรับการปฏิบัติงานด้านไซเบอร์ในอนาคตได้ เห็นสมควรให้มีการศึกษาวิจัยเพิ่มเติมในส่วนโครงสร้างและอัตราของหน่วยงานด้านไซเบอร์ให้สอดคล้องกับงานเชิงป้องกันและป้องกันปราม

2. การพัฒนาบุคลากร ควรมีการจัดการฝึกศึกษา การอบรม การทบทวน และส่งไปศึกษานอกหน่วยให้กับบุคลากรทุกระดับ รวมถึงให้มีการจัดทำคู่มือในการปฏิบัติงาน อีกทั้งควรบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติการกิจโดยต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน พร้อมกับให้ผู้รับผิดชอบผลักดันการดำเนินการขอเงินเพิ่มพิเศษให้กับผู้ปฏิบัติงานด้านไซเบอร์

3. ควรมีการทบทวน ปรับปรุง การจัดทำแผนแม่บท แผนงาน แนวทางการปฏิบัติที่เกี่ยวข้องด้านไซเบอร์ให้ครอบคลุมการปฏิบัติ พร้อมทั้งจัดทำแผนและคู่มือการปฏิบัติเมื่อมีเหตุการณ์แจกจ่ายให้หน่วยเกี่ยวข้อง และควรจัดให้มีการซักซ้อมการดำเนินการตามแผนงานอย่างต่อเนื่อง รวมถึงควรจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพ

4. สนับสนุนงบประมาณให้เพียงพอต่อการปฏิบัติการกิจด้านไซเบอร์และค่าลิขสิทธิ์ของระบบเทคโนโลยีตามแผนงานที่กำหนดไว้ และหากมีการสร้างอาคารใหม่รองรับระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม เห็นควรให้ติดตั้งระบบงานด้านไซเบอร์ไว้ภายในอาคารเดียวกัน

บรรณานุกรม

หนังสือ

- กรมกำลังพลทหารอากาศ. **ระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ**. กรุงเทพฯ: กองทัพอากาศ, 2552.
- กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. **นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอากาศ**. กรุงเทพฯ: กองทัพอากาศ, 2558.
- ประยูร ธรรมาธิวัฒน์, นาวาอากาศเอก. **“แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ”**. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557
- สุชาติ ผ่องพุฒิ, พลตรี. **“แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย”**. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2556
- สุทธิศักดิ์ สลักคำ, พลตรี. **“ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม”**. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557

ฐานข้อมูลอิเล็กทรอนิกส์

- “คู่มือ Cyber Security สำหรับประชาชน”**. (ออนไลน์). เข้าถึงได้จาก [http://www.nbtc.go.th/News/รวมบทความ-\(1\)/คู่มือ-Cyber-Security-สำหรับประชาชน.aspx](http://www.nbtc.go.th/News/รวมบทความ-(1)/คู่มือ-Cyber-Security-สำหรับประชาชน.aspx).
- “แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ”**. (ออนไลน์). เข้าถึงได้จาก <https://www.acisonline.net/?p=5040&lang=th>, 2559.
- “ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security”**. (ออนไลน์). เข้าถึงได้จาก <https://www.techtalkthai.com/cdic-2016-cyber-security-threats-and-trends/>, 2559
- “มาตรฐาน ISO/IEC 27001 : 2013”**. (ออนไลน์). เข้าถึงได้จาก <http://www.rtna.ac.th/download/27001-2013.pdf>, 2556.

- “ยุทธศาสตร์กองทัพอากาศ 20 ปี”**. (ออนไลน์). เข้าถึงได้จาก http://www.rtaf.mi.th/Th/Documents/Publication/RTAF_Strategy_20y_2560-2579.pdf, 2560.
- “ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. 2552”**. (ออนไลน์). เข้าถึงได้จาก http://www.rtaf.mi.th/Th/Documents/Publication/RTAF_ICT_E_book_v4.0_E.pdf.
- “ศัพท์น่ารู้ในโลกไซเบอร์”**. (ออนไลน์). เข้าถึงได้จาก <https://krujayja.wordpress.com/blog-d-d/classroom/คำศัพท์น่ารู้ในโลกไซเบอร์>.
- “หลักการและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์”**. (ออนไลน์). เข้าถึงได้จาก [http://www.dmsc.moph.go.th/itc/userfiles/files/law_lecture%20\(2\).pdf](http://www.dmsc.moph.go.th/itc/userfiles/files/law_lecture%20(2).pdf).