แนวทางการพัฒนาขีดความสามารถการปฏิบัติ
ด้านสงครามไซเบอร์ของกองทัพอากาศ

โดย

นาวาอากาศเอก ประยูร ธรรมาธิวัฒน์
รองผู้อำนวยการสำนักระบบบัญชาการและควบคุม
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
กองทัพอากาศ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 57
ประจำปีการศึกษา พุทธศักราช 2557 - 2558

บทคัดย่อ

เรื่อง แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย นาวาอากาศเอกประยูร ธรรมาธิวัฒน์ **หลักสูตร** วปอ. **รุ่นที่** 57

การวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ขอบเขตการวิจัยเฉพาะในกองทัพอากาศ เป็นการวิจัยเป็นการวิจัยแบบผสมผสาน ประชากร คือ ข้าราชการกองทัพอากาศที่เกี่ยวข้องกับการปฏิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในการวิจัยใช้กลุ่มตัวอย่างด้วยวิธีการสุ่ม เครื่องมือที่ใช้ในการศึกษาเป็นแบบสอบถาม และการสัมภาษณ์

ผลการวิจัยพบว่า ขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศเชิงรุกอยู่ในระดับต่ำ แต่การปฏิบัติเชิงรับอยู่ในระดับปานกลาง สำหรับปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านสงครามไซเบอร์คือ กำลังพล พบว่ายังขาดความรู้และทักษะในด้านสงครามไซเบอร์ รองลงมาคือโครงสร้างการจัดหน่วยที่ไม่เอื้ออำนวยต่อการปฏิบัติภารกิจ ไม่มีแผนแม่บทด้านสงครามไซเบอร์ จึงไม่มีแนวทางการปฏิบัติที่ชัดเจนให้กับหน่วยเกี่ยวข้อง ท้ายสุดคือ เครื่องมือที่ใช้ในการปฏิบัติภารกิจมีอายุการใช้งานมานาน ไม่ทันสมัย ไม่ทันเทคโนโลยี สาเหตุมาจากขาดการสนับสนุนงบประมาณที่พอเพียง ดังนั้น เพื่อให้การปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศมีขีดความสามารถเพิ่มขึ้น ประการแรก ต้องลงทุนด้านงบประมาณเพื่อเตรียมกำลังพล และฝึกอบรมให้มีความรู้ความสามารถ มีทักษะ พร้อมที่จะปฏิบัติภารกิจด้านสงครามไซเบอร์ได้อย่างมีประสิทธิภาพ ประการที่สอง ต้องปรับปรุงยุทธศาสตร์กองทัพอากาศกำหนดเป้าหมายการทำสงครามไซเบอร์ให้ชัดเจน จัดทำแผนแม่บทด้านสงครามไซเบอร์เพื่อให้หน่วยเกี่ยวข้องนำไปปฏิบัติ จัดทำระบบแจ้งเตือนภัยเมื่อถูกกระทำทางไซเบอร์ สนับสนุนงบประมาณให้เพียงพอ และสรรหานักรบไซเบอร์พร้อมอาวุธไซเบอร์ที่ทันสมัย เพื่อเตรียมการรับมือกับภัยคุกคามรูปแบบใหม่ที่มากับไซเบอร์ และพิจารณารักษากำลังพลที่มีความรู้ความสามารถเหล่านี้ให้ปฏิบัติงานกับกองทัพอากาศให้ได้นานที่สุด โดยดูแลสวัสดิการและพิจารณาค่าตอบแทนพิเศษให้กับผู้ที่บรรจุเป็นนักรบไซเบอร์ของกองทัพอากาศ

คำนำ

การศึกษาวิจัยเรื่องการพัฒนารูปแบบเทคโนโลยีสารสนเทศเพื่อการพัฒนาการเรียนการสอนมีวัตถุประสงค์เพื่อ ๑) ศึกษาสภาพและปัญหาการใช้เทคโนโลยีสารเทศเพื่อการพัฒนาการเรียนและการสอน ๒) เพื่อพัฒนารูปแบบการใช้เทคโนโลยีสารสนเทศเพื่อการพัฒนาการเรียนและการสอน ๓) เพื่อเสนอแนวทางที่เหมาะสมในการใช้รูปแบบเทคโนโลยีสารสนเทศเพื่อการพัฒนาการเรียนและการสอน และ ๔) เพื่อนำเสนอรูปแบบการใช้เทคโนโลยีสารสนเทศในการพัฒนาการเรียนและการสอนไปปรับใช้ระดับประเทศ ซึ่งหากดำเนินการได้ตามวัตถุประสงค์จะก่อให้เกิดประโยชน์ต่อกองบัญชาการกองทัพไทย โดยทำให้ทราบข้อมูลสภาพปัญหาในการใช้เทคโนโลยี และสามารถนำมาสร้างรูปแบบเพื่อใช้ในการพัฒนาการเยนการสอนในกองบัญชาการกองทัพไทยได้

หากเอกสารนี้มีข้อผิดพลาดประการใด ทางผู้วิจัยขอน้อมรับคำแนะนำในการแก้ไขและปรับปรุงให้ดียิ่งขึ้นต่อไป เพื่อให้การศึกษาวิจัยในครั้งนี้สามารถช่วยแก้ปัญหาการเรียนการสอน และสามารถขยายผลไปสู่การพัฒนาการเรียนการสอนในหน่วยอื่นต่อไปได้

พ.อ.

(กฤติกร รัสมิภูตานนท์)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร รุ่นที่ ๕๗

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในอดีตที่ผ่านมา เมื่อมีปัญหาที่เกิดขึ้นระหว่างประเทศไม่ว่าเรื่องใดก็ตาม เมื่อใช้การเจรจาด้านการทูตไม่ประสบผลสำเร็จ สุดท้ายต้องจบด้วยการใช้กำลังทางทหารเข้าทำการต่อสู้กัน ฝ่ายใดมีศักยภาพและขีดความสามารถหรือมีสมรรถนะดีกว่าจะเป็นฝ่ายได้ชัยชนะและทำให้ได้มาซึ่งผลประโยชน์แห่งชาติของประเทศนั้นๆ ขีดความสามารถดังกล่าวประกอบด้วยจำนวนกำลังพล จำนวนอาวุธยุทโธปกรณ์ที่ใช้เทคโนโลยีขั้นสูง ยุทธศาสตร์และยุทธวิธีการรบที่ใช้เทคโนโลยีขั้นสูงเข้าช่วยอำนวยความสะดวกในการบัญชาการและควบคุมการรบ ทุกวันนี้ทุกประเทศต่างมีกำลังพล อาวุธและการส่งกำลังบำรุงที่ไม่แตกต่างกันมากนัก แต่สิ่งที่แตกต่างกันคือเทคโนโลยีที่นำมาช่วยอำนวยความสะดวกในการรบ

ปัจจุบันกิจการวิทยาศาสตร์และเทคโนโลยีได้มีการพัฒนาในทุกๆ ด้านอย่างรวดเร็ว แต่ละประเทศจึงลงทุนพัฒนาและนำเทคโนโลยีเข้ามาใช้งานทั้งภาคเอกชนและภาคราชการ โดยนำมาใช้ในกิจการด้านความมั่นคง กิจการทางทหาร กิจการสื่อสาร กิจการขนส่งทางอากาศและพื้นดิน กิจการเพาะปลูก กิจการผลิตอาหารของคนและสัตว์ กิจการทางการแพทย์ กิจการด้านการเงินการธนาคาร กิจการด้านรักษาสิ่งแวดล้อม เป็นต้น ซึ่งจะเห็นได้ว่า เทคโนโลยีสารสนเทศสมัยใหม่ได้เข้ามามีบทบาทในทุกกิจการซึ่งจะเชื่อมโยงเป็นโครงข่ายที่เกื้อหนุนซึ่งกันและกัน หากกิจการใดมีเหตุทำให้ต้องหยุดชงักหรือบกพร่องในการปฏิบัติ จะส่งผลให้กิจการอื่นๆ เกิดขัดข้องและหยุกชงักตามไปด้วย จากเหตุดังกล่าวจึงนำมาสู่แนวคิดการทำสงครามสมัยใหม่ที่ทำการรบโดยไม่ต้องใช้กำลังทางทหาร แต่ทำการรบโดยใช้การกระทำให้ระบบสารสนเทศและระบบเครือข่ายที่เกี่ยวข้องเกิดข้อขัดข้องไม่สามารถให้บริการได้ทำให้กิจการต่างๆ หยุดชงักหรือชำรุดเสียหาย ต้องใช้เวลานานในการซ่อมบำรุงเพื่อให้สามารถนำกลับมาใช้งานได้ตามปกติส่งผลเสียหายต่อเศรษฐกิจของประเทศ เสียหายต่อบุคคลและองค์กร ซึ่งการกระทำดังกล่าวเป็นส่วนหนึ่งของการทำสงครามไซเบอร์ (Cyber Warfare)

กองทัพอากาศเป็นกองทัพที่ต้องใช้เทคโนโลยีขั้นสูงในการปฏิบัติภารกิจให้บรรลุวัตถุประสงค์โดยใช้กำลังพลน้อยแต่ได้ประสิทธิภาพมาก จึงได้ศึกษาและนำระบบเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเป็นส่วนหนึ่งในการปฏิบัติงาน เรียกว่า “การปฏิบัติที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations)” ซึ่งในระบบดังกล่าวจะประกอบด้วยเครือข่ายสารสนเทศเครือข่ายการสื่อสารโทรคมนาคม ที่จะต้องเชื่อมโยงระบบเข้าด้วยกันเพื่อให้สามารถติดต่อรับส่งข้อมูลทุกประเภทได้อย่างรวดเร็ว ถูกต้องและเชื่อถือได้ พร้อมที่จะให้ผู้บังคับบัญชาสั่งใช้กำลังทางอากาศได้ตลอดเวลาหากมีการกระทำที่ทำให้เครือข่ายดังกล่าวขัดข้องไม่สามารถรับส่งข้อมูลได้จะทำให้การสั่งใช้กำลังทางอากาศมีข้อขัดข้องทันที การกระทำที่มีผลให้ระบบเครือข่ายดังกล่าวขัดข้องหรือชำรุดเสียหายไม่สามารถใช้การได้ ถือได้ว่าเป็นส่วนหนึ่งของการทำสงครามไซเบอร์ (Cyber Warfare) ใน

ปัจจุบันทุกหน่วยงานทั่วโลกได้ให้ความสำคัญในเรื่องนี้เป็นอย่างยิ่ง โดยจัดตั้งหน่วยงานขึ้นมากำกับดูแลโดยเฉพาะ

กระทรวงกลาโหมได้อนุมัติเมื่อเดือนสิงหาคม 2557 ให้กองทัพไทยปรับปรุงโครงสร้างหน่วยงานของแต่ละเหล่าทัพให้มีประสิทธิภาพ เพื่อรองรับการปฏิบัติภารกิจที่เพิ่มมากขึ้นนอกเหนือจากการป้องกันประเทศและให้มีขีดความสามารถรับมือกับภัยคุกคามรูปแบบใหม่ๆ ได้อย่างมีประสิทธิภาพรวมทั้งการช่วยเหลือประชาชนชาวไทย ทั้งในประเทศและต่างประเทศเมื่อได้รับความเดือดร้อนหรือเสียหายจาก ภัยธรรมชาติประเภทต่างๆ เช่น อุทกภัย วาตภัย อัคคีภัย แผ่นดินไหว ภูเขาไฟระเบิด สึนามิและภัยอันเกิดจากไวรัสคอมพิวเตอร์ทุกชนิด รวมทั้งการกระทำของบุคคลที่ไม่หวังดีหรือด้วยความคึกคะนองและรู้เท่าไม่ถึงการณ์ ในการทำให้ระบบเครือข่าย ระบบสารสนเทศขัดข้องไม่สามารถใช้งานได้

กองทัพอากาศจึงได้ปรับโครงสร้างหน่วยงานใหม่ เพื่อให้รองรับภัยคุกคามที่เกิดจากการกระทำของบุคคลที่เรียกว่า “แฮ็กเกอร์” และภัยคุกคามที่เกี่ยวข้องกับไวรัสคอมพิวเตอร์และอื่นๆ ที่จะทำให้ระบบเครือข่ายและระบบสารสนเทศ รวมทั้งระบบการสื่อสารขัดข้อง โดยกำหนดให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศมีหน้าที่รับผิดชอบงานด้านนโยบาย ควบคุม กำกับดูแลการปฏิบัติด้านสงครามไซเบอร์ (Cyber warfare) การปฏิบัติด้านสงครามอิเล็กทรอนิกส์ (Electronic warfare) การปฏิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสาร การปฏิบัติด้านการสื่อสารอิเล็กทรอนิกส์ และการปฏิบัติด้านระบบบัญชาการและควบคุมของกองทัพอากาศ

การปฏิบัติงานด้านอื่นๆ ของกองทัพอากาศในปัจจุบันมีขีดความสามารถอยู่ในระดับหนึ่ง มีอุปกรณ์และบุคลากรพร้อมปฏิบัติภารกิจเมื่อได้รับคำสั่ง แต่การปฏิบัติงานด้านสงครามไซเบอร์นั้นยังมีขีดความสามารถและศักยภาพไม่มากนัก เนื่องจากเป็นหน่วยงานที่ตั้งขึ้นมาใหม่ อุปกรณ์และบุคลากร มีจำกัดไม่เพียงพอต่อการปฏิบัติงาน อีกทั้งแนวทางการปฏิบัติยังไม่มีแผนแม่บทและแนวทางปฏิบัติที่ชัดเจน จากหลายเหตุการณ์ที่ผ่านมาพบว่าถูกภัยคุกคามจากไซเบอร์ทำให้ระบบเครือข่ายและระบบสารสนเทศของกองทัพอากาศมีข้อขัดข้องในการรับส่งข้อมูลอยู่เสมอ ทั้งในที่ตั้งดอนเมืองและต่างจังหวัด การทำสงครามไซเบอร์จะไม่มีการแจ้งเตือนล่วงหน้าแต่จะแอบกระทำอย่างเงียบๆ ค่อยเป็นค่อยไป กองทัพอากาศก็เป็นเป้าหมายหนึ่งที่ถูกกระทำอยู่เรื่อยมาและเจ้าหน้าที่ได้ทำการแก้ไขให้ระบบสามารถกลับมาทำงานได้ตามปกติ ซึ่งต้องใช้เวลาพอสมควร การทำสงครามไซเบอร์ดังกล่าวที่ตรวจพบประกอบด้วยการแอบเจาะระบบเครือข่ายการปล่อยไวรัสเข้าระบบเครือข่ายการเปลี่ยนแปลงระบบเครือข่ายให้ทำงานผิดพลาดในการรับส่งข้อมูล เป็นต้น การกระทำดังกล่าวสร้างความเสียหายต่อการปฏิบัติภารกิจในภาพรวมของกองทัพเป็นอย่างมาก ทำให้ทราบว่าระบบการป้องกันและการปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ ยังมีศักยภาพและประสิทธิภาพไม่ดีเท่าที่ควร จึงเห็นสมควรที่ต้องปรับปรุง แก้ไขและพัฒนาเพื่อให้การปฏิบัติงานด้านสงครามไซเบอร์มีขีดความสามารถหรือมีศักยภาพเพิ่มขึ้น

ผู้วิจัยมีหน้าที่รับผิดชอบการปฏิบัติด้านระบบบัญชาการและควบคุมและการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ทั้งสองด้านมีความสำคัญเท่าเทียมกันในการใช้กำลังทางอากาศเพื่อป้องกันประเทศและช่วยเหลือประชาชน แต่ปัจจุบันผู้วิจัยมีความสนใจเกี่ยวกับการปฏิบัติด้านสงครามไซเบอร์เป็นอันดับต้น จึงมีความตั้งใจทำการวิจัยในเรื่องนี้ซึ่งจะทำให้กองทัพอากาศได้ทราบ

แนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ให้มีศักยภาพและมีประสิทธิภาพดียิ่งขึ้น

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
2. เพื่อศึกษาปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
3. เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ

ขอบเขตของการวิจัย

การศึกษาเรื่องแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ผู้วิจัยได้กำหนดขอบเขตของการวิจัยดังต่อไปนี้

1. ขอบเขตประชากร

ประชากรที่ใช้ในการวิจัยครั้งนี้ประกอบด้วยข้าราชการของกองทัพอากาศและหน่วยขึ้นตรงของกองทัพอากาศที่ปฏิบัติงานด้านเครือข่ายสารสนเทศ ด้านสงครามไซเบอร์ ด้านระบบสื่อสาร ที่ปฏิบัติงานในปี 2557 ถึง 2558 โดยการสุ่มตัวอย่าง

2. ขอบเขตตัวแปร

การวิจัยครั้งนี้ เป็นการศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยมีตัวแปรที่ใช้ในการวิจัยดังนี้

2.1 ปัจจัยด้านบุคคล

2.1.1 เพศ แบ่งออกเป็นเพศชาย และเพศหญิง

2.1.2 ช่วงอายุ แบ่งออกเป็น 25-35 ปี, 36–46 ปี และสูงกว่า 46 ปีขึ้นไป

2.1.3 ระดับการศึกษา แบ่งออกเป็น ต่ำกว่าปริญญาตรี,ปริญญาตรี และสูงกว่าปริญญาตรี

2.1.4 ระดับชั้นยศ แบ่งเป็น ระดับชั้นต่ำกว่าสัญญาบัตร และชั้นสัญญาบัตร

2.1.5 ตำแหน่งปัจจุบัน และ อายุการทำงานในตำแหน่งปัจจุบัน

2.2 ตัวแปรอิสระ ได้แก่ ปัจจัยที่ส่งผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

2.2.1 ด้านความรู้ ความเข้าใจ การปฏิบัติงานด้านสงครามไซเบอร์

2.2.2 ด้านทักษะและความสามารถในการปฏิบัติงานด้านสงครามไซเบอร์

2.2.3 ด้านพฤติกรรมการปฏิบัติงานของกำลังพลด้านสงครามไซเบอร์

2.2.4 ด้านกำลังพล การบริหาร/การจัดการและเทคโนโลยี

2.2.5 ด้านงบประมาณ

2.3 ตัวแปรตาม ได้แก่ ระดับขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

2.3.1 ขีดความสามารถเชิงรุก (คน/กระบวนการ/เทคโนโลยี)

2.3.2 ขีดความสามารถเชิงรับ (คน/กระบวนการ/เทคโนโลยี)

3. ขอบเขตพื้นที่ กองทัพอากาศ

4. ผู้ให้ข้อมูลสำคัญ ประกอบด้วยผู้บังคับบัญชาชั้นสูงของกองทัพอากาศ ผู้บริหารระดับสูงที่ควบคุมกำกับดูแลการปฏิบัติด้านสงครามไซเบอร์ ด้านระบบสื่อสารและด้านระบบเครือข่ายสารสนเทศ

5. ขอบเขตระยะเวลาการวิจัย ตั้งแต่เดือน พ.ย.57 ถึงเดือน ส.ค.58

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

2. ทำให้ทราบปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

3. ได้ทราบแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

คำจำกัดความ

สงครามข่าวสาร (Information Warfare)	หมายถึง	การดำเนินการเพื่อให้เป็นฝ่ายได้เปรียบด้านข่าวสาร โดยการบ่อนทำลาย ข่าวสาร การดำเนินกรรมวิธีต่อข่าวสาร ระบบข่าวสาร และเครือข่ายคอมพิวเตอร์ของข้าศึก ในขณะเดียวกันก็ทำการป้องกันข่าวสาร การดำเนินกรรมวิธีต่อข่าวสารระบบข่าวสารและเครือข่ายคอมพิวเตอร์ของตนจากการบ่อนทำลายของข้าศึก
สงครามไซเบอร์ (Cyber Warfare)	หมายถึง	การใช้คอมพิวเตอร์และอินเทอร์เน็ตในการทำสงครามเช่น การโจมตีเว็บหรือบล็อคเว็บ โฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต การเจาะข้อมูลลับ โดยแฮ็กเกอร์ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ การทำลายอุปกรณ์การทหารที่ใช้คอมพิวเตอร์ควบคุม เป็นต้น
ระบบบัญชาการและควบคุม (Command and Control System)	หมายถึง	ระบบที่ใช้ในการวางแผนบริหารจัดการทรัพยากรที่มีอยู่ขององค์กรในการสั่งการและควบคุมสำหรับปฏิบัติการต่างๆ เพื่อให้เกิดความได้เปรียบ และประสบความสำเร็จตามวัตถุประสงค์ขององค์กร

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	หมายถึง	ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่าย ระบบคอมพิวเตอร์โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วนและความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม
แฮ็กเกอร์ (Hacker)	หมายถึง	ผู้ที่มีความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างสูงมากไม่ว่าจะเป็นเรื่องเครือข่าย ระบบปฏิบัติการ จนสามารถเข้าใจว่าระบบมีช่องโหว่ตรงไหน หรือสามารถไปค้นหา ช่องโหว่ได้จากตรงไหนบ้าง เมื่อก่อนภาพลักษณ์ของ Hacker จะเป็นพวกชั่วร้าย ชอบขโมยข้อมูล หรือ ทำลายให้เสียหาย แต่เดี๋ยวนี้คำว่า Hacker หมายถึง Security Professional ที่คอยใช้ความสามารถช่วยตรวจตราระบบและแจ้งเจ้าของระบบว่ามีช่องโหว่ตรงไหนบ้าง อาจพูดง่ายๆ ว่าเป็น Hacker ที่มีจริยธรรมนั่นเอง
สนิฟเฟอร์ (Sniffer)	หมายถึง	โปรแกรมที่เอาไว้ดักจับข้อมูล บนระบบ Network เนื่องจากคอมพิวเตอร์เน็ตเวิร์คเป็นระบบการสื่อสารที่ใช้ร่วมกัน เพื่อประหยัดค่าใช้จ่าย การแบ่งกันใช้หมายถึง คอมพิวเตอร์สามารถรับข้อมูลที่คอมพิวเตอร์เครื่องอื่น (sharing) ตั้งใจจะส่งไป ให้อีกเครื่องหนึ่ง
นักรบไซเบอร์ (Cyber warrior)	หมายถึง	บุคคลที่ใช้อาวุธไซเบอร์ในการป้องกันระบบของฝ่ายตนหรือใช้อาวุธในการโจมตีระบบของฝ่ายตรงกันข้าม
อาวุธไซเบอร์ (Cyber weapon)	หมายถึง	ซอฟต์แวร์หรือฮาร์ดแวร์ที่นักรบไซเบอร์ใช้ในการปฏิบัติในสงครามไซเบอร์
การปฏิบัติการโดยใช้เครือข่ายเป็นศูนย์กลาง (Network centric operation)	หมายถึง	การปฏิบัติการทางทหารที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ ใช้กับระบบควบคุมและสั่งการ ระบบตรวจจับ และระบบอาวุธยุทโธปกรณ์

บทที่ 2
แนวคิด ทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

การทำวิจัย เรื่อง แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ผู้ศึกษาได้ศึกษาจากเอกสาร แนวคิด ทฤษฎีและงานวิจัยต่างๆ ที่เกี่ยวข้อง เพื่อนำมาเป็นกรอบแนวทางในการศึกษาค้นคว้า โดยใช้แนวคิด ทฤษฎีและงานวิจัยต่างๆ ที่เกี่ยวข้อง ดังกล่าวนำมาเป็นกรอบแนวทางในการศึกษาค้นคว้า ดังนี้

1. แนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศองค์กรและองค์กรสมัยใหม่
2. การจัดการความรู้และการบริหารความเสี่ยง
3. ภัยคุกคามรูปแบบใหม่
4. สงครามสารสนเทศและสงครามไซเบอร์
5. ยุทธศาสตร์การพัฒนาของกองทัพอากาศ
6. หน่วยงานรับผิดชอบการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
7. การเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
8. งานวิจัยที่เกี่ยวข้อง

แนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศองค์กรและองค์กรสมัยใหม่

1. สมรรถนะในองค์การ

1.1 ความหมายสมรรถนะ ผู้วิจัยได้ศึกษาการนิยามความหมายของสมรรถนะของนักวิชาการและผู้เชี่ยวชาญหลายท่านซึ่งสามารถสรุปได้ว่า สมรรถนะ หมายถึง ความรู้ ความสามารถ ทัศนคติ ที่จะปฏิบัติหน้าที่ให้ประสบความสำเร็จและเกิดประสิทธิภาพกับองค์กรอย่างสูงสุด

1.2 ประเภทของสมรรถนะ อาภรณ์ ภู่วิทยพันธุ์ (2552:17-18) กล่าวว่า สมรรถนะในองค์กรสามารถแบ่งออกเป็น 3 ประเภทหลัก ได้แก่

1.2.1 สมรรถนะหลัก (Core Competency) หมายถึง ความสามารถหลักที่คาดหวังให้พนักงานทุกคนทุกระดับองค์กรจะต้องมีองค์การบางแห่งเรียกสมรรถนะหลัก ซึ่งเป็นสิ่งที่ทำให้เป้าหมาย วิสัยทัศน์และภารกิจขององค์การประสบความสำเร็จ ทั้งนี้สมรรถนะหลักที่ถูกปฏิบัติเหมือนๆ กัน ในองค์กรจะนำไปสู่การสร้างนวัตกรรมองค์กร (Corporate Culture) ที่หลักปฏิบัติที่สืบทอดต่อไปยังพนักงานคนอื่นๆ ต่อไปได้ พบว่าสมรรถนะหลักที่กำหนดขึ้นในองค์กรนั้นไม่ควรมีจำนวนมากนักประมาณ 3-5 ข้อ

1.2.2 สมรรถนะทางการบริหาร (Managerial Competency) หมายถึง ความสามารถในการบริหารจัดการงานที่คาดหวังกับกลุ่มพนักงานแยกตามระดับตำแหน่งงาน ถ้าตำแหน่งงานเหมือนกันคาดหวังว่าจะมี สมรรถนะประเภทนี้เหมือนกัน เช่น ผู้จัดการฝ่าย ไม่ว่าจะเป็นฝ่ายใดๆ ก็ตามจะต้องมีสมรรถนะในเรื่อง วิสัยทัศน์เชิงกลยุทธ์ การวางแผนงาน การบริหารการเปลี่ยนแปลง การสร้างเครือข่ายที่เหมือนกัน พบว่าการกำหนดสมรรถนะทางการบริหารนั้น จะกำหนดขึ้นจากบทบาทหน้าที่และความรับผิดชอบหลักที่เหมือนกันตามระดับตำแหน่งงาน และจำนวนข้อของสมรรถนะทางการบริหารจะต้องมีจำนวนไม่มาก อยู่ระหว่าง 3-5 ข้อต่อระดับตำแหน่งงาน

1.2.3 สมรรถนะตามหน้าที่ (Function Competency) หมายถึง ความสามารถในงานเฉพาะด้านที่แตกต่างกันไปในแต่ละหน่วยงาน พบว่าการกำหนดสมรรถนะตามหน้าที่ขึ้นอยู่กับลักษณะงานที่รับผิดชอบ (Job Description) โดยพิจารณาว่าในแต่ละตำแหน่งงานคาดหวังความรู้ ทักษะ และคุณลักษณะส่วนบุคคลในเรื่องใดบ้าง ซึ่งความสามารถเหล่านี้จะส่งผลการทำงานที่ผู้บังคับบัญชามอบหมายให้ประสบความสำเร็จ โดยสามารถวัดความสำเร็จของงานได้จากตัวชี้วัดผลงานหลัก (Key Performance Indicators) ดังนั้นจำนวนสมรรถนะตามหน้าที่จึงมีความแตกต่างกันไปแต่ละหน่วยงาน โดยปกติแล้วจะมีไม่มากเช่นเดียวกันอยู่ระหว่าง 5-7 ข้อ นอกจากนี้ยังพบว่าการจัดแบ่งสมรรถนะตามหน้าที่นั้นสามารถแบ่งได้อีก 2 ประเภทย่อยได้แก่ 1. Common Function Competency เป็นความสามารถในงานที่เป็นเรื่องทั่วๆ ไป ตำแหน่งงานอื่นในฝ่ายอื่นๆ และ 2. Specific Function Competency เป็นความสามารถในงานทางเทคนิคเฉพาะด้านที่ต้องอาศัยความชำนาญและระยะเวลาในการเรียนรู้และฝึกฝน

1.3 องค์ประกอบที่สำคัญของสมรรถนะการเป็นผู้นำของผู้บริหารองค์กร

สมรรถนะทางการบริหาร (Managerial Competency : mc) หมายถึง สมรรถนะที่เป็นความสามารถทางการจัดการซึ่งสะท้อนให้เห็นถึงทักษะในการบริหารและจัดการงานต่างๆ กำหนดให้ต้องมีทั้งระดับผู้บริหารและระดับพนักงานปฏิบัติการ แต่จะแตกต่างกันตามบทบาทหน้าที่และความรับผิดชอบโดยแบ่งเป็นข้อย่อย ดังนี้

1.3.1 วิสัยทัศน์เชิงกลยุทธ์ (Strategic Visioning) ความเข้าใจถึงวิสัยทัศน์ พันธกิจของธนาคาร เพื่อกำหนดกลยุทธ์และยุทธศาสตร์การดำเนินงานของธนาคาร ตลอดจนการรวบรวมติดตามและวิเคราะห์กลยุทธ์การดำเนินงานต่างๆ

1.3.2 การวางแผนงาน (Planning) ความรู้ความเข้าใจแนวคิดหลักการ กระบวนการ วิธีการวางแผนและติดตามงานรวมทั้งการประมวลผลเพื่อประยุกต์ใช้ในการวางแผนและติดตามงานให้มีประสิทธิภาพและประเมินผลการปฏิบัติงานตามแผนที่กำหนดขึ้น

1.3.3 ภาวะผู้นำ (Leadership) ความเหมาะสมของการวางตน แสดงออกถึงความเป็นผู้นำ มีความน่าเชื่อถือศรัทธา รับผิดชอบต่อผลงานที่เกิดขึ้นของตนเอง ทีมงาน หน่วยงาน รวมทั้งกระตุ้นจูงใจให้ผู้อื่นปฏิบัติตามโดยอยู่บนพื้นฐานของความถูกต้องตรวจสอบได้

1.3.4 การแก้ไขปัญหาและตัดสินใจ (Problem Solving and Decision Making) ความสามารถในการวิเคราะห์สาเหตุ และผลกระทบของปัญหาพร้อมทั้งสามารถวิเคราะห์และค้นหา การแก้ไขปัญหาได้หลากหลายวิธี สามารถตัดสินใจแก้ไขปัญหาได้อย่างเหมาะสมกับสถานการณ์และเกิดประโยชน์สูงสุดแก่ธนาคาร

1.3.5 บริหารการเปลี่ยนแปลง (Change Management) การวิเคราะห์และการคาดการณ์การเปลี่ยนแปลงที่เกิดภายองค์กรและหน่วยงานรวมทั้งการคิดหาเครื่องมือ และวิธีการใหม่ๆ มาใช้ในองค์กร

2. แนวความคิดและทฤษฎีเกี่ยวกับบรรยากาศขององค์กร

2.1 ความหมายของบรรยากาศขององค์กร

ผู้วิจัยได้ศึกษาและสรุปความหมายของบรรยากาศองค์กรจากนักวิชาการด้านทรัพยากรมนุษย์หลายท่าน เพื่อนำมาใช้ประโยชน์ในการปรับปรุงและพัฒนาองค์กรให้เหมาะสมกับลักษณะการทำงานที่เป็นมาตรฐานซึ่งสรุปได้ว่า บรรยากาศองค์กร หมายถึง สภาพแวดล้อมในการทำงานที่เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอก ซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร

2.2 แนวคิดเกี่ยวกับบรรยากาศองค์กร

สเตียร์ส (Steers, 1977) ได้แบ่งองค์ประกอบของบรรยากาศองค์การไว้ 6 ด้านดังนี้

2.2.1 โครงสร้างการทำงาน (Task Structure) จากการสำรวจความรู้สึกนึกคิดของพนักงานในองค์กรเห็นว่าโครงสร้างในการทำงานเป็นอุปสรรคหรือบั่นทอนต่อจิตใจในการทำงานหรือไม่ตัวอย่างโครงสร้างในการทำงานที่เป็นอุปสรรค เช่น การรวบอำนาจในการบังคับบัญชา ระบบงบประมาณที่ค่อนข้างเข้มงวด กฎระเบียบที่ไม่ยืดหยุ่นและกรรมวิธีในการทำงานมีขั้นตอนที่ยุ่งยากซับซ้อน เป็นต้น

2.2.2 ระบบรางวัลตอบแทน (Reward Systems) ต้องวิเคราะห์ว่าเป็นระบบที่มีความยุติธรรมและเพียงพอต่อมาตรฐานการครองชีพหรือไม่

2.2.3 ความเป็นอิสระ (Autonomy) หมายถึง ความรู้สึกของพนักงานที่เห็นว่าเขามีอิสระและได้รับอนุญาตจากองค์กรให้สามารถแสดงออกซึ่งความคิดสร้างสรรค์งานใหม่ๆ ขึ้นมา

2.2.4 ความอบอุ่นและการสนับสนุน (Warmth and Support) หมายถึง ภาวะการเป็นผู้นำของหัวหน้าที่ให้ความอบอุ่นหรือการสนับสนุนต่อสมาชิกภายในองค์กรในการทำงานและความก้าวหน้ามากน้อยเพียงใด

2.2.5 การยอมรับความขัดแย้ง (Tolerance of Conflict) หมายถึง การวิเคราะห์ดูว่าองค์การทำให้สมาชิกเกิดความรู้สึกว่าความคิดเห็นที่แตกต่างกันสามารถได้รับการยอมรับให้เกิดขึ้นได้หรือไม่

2.2.6 ความรักในหมู่คณะ (Esprit) หมายถึง ความรู้สึกนึกคิดของพนักงานที่เห็นว่าสมาชิกภายในองค์กรมีความรักกันฉันเพื่อนในการทำงานร่วมกันหรือไม่

3. องค์กรสมัยใหม่ (Modern Organization)

ในปัจจุบันการพัฒนาองค์กรของไทยได้รับเอาแนวคิดการบริหารจากต่างประเทศมาใช้อย่างกว้างขวาง ทั้งนี้ก็เพื่อความอยู่รอดในกระแสการแข่งขันอันเชี่ยวกรากในระบบทุนนิยม (Capitalist) ดังนั้นสถานภาพที่องค์กรต้องการ คือ การสร้างความยั่งยืนให้กับองค์กร เครื่องมือทางด้านการบริหารที่จะมีส่วนช่วยให้องค์กรได้รับความสำเร็จอันยั่งยืนคือ องค์กรแห่งการเรียนรู้ (Learning Organization) ซึ่งได้รับการกล่าวถึงกันอย่างกว้างขวางทั้งในภาครัฐและเอกชน โดยภาครัฐได้กำหนดให้มีการตราไว้ในกฎหมายคือพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546 หมวด 3 มาตรา 11 “ส่วนราชการมีหน้าที่พัฒนาความรู้ในส่วนราชการเพื่อให้มีลักษณะเป็นองค์กรแห่งการเรียนรู้อย่างสม่ำเสมอ โดยต้องรับรู้ข้อมูลข่าวสารและสามารถประมวลผลความรู้ในด้านต่างๆ เพื่อนำมาประยุกต์ใช้ในการปฏิบัติราชการได้อย่างถูกต้องรวดเร็วและเหมาะสมกับสถานการณ์ รวมทั้งต้องส่งเสริมและพัฒนาความรู้ความสามารถสร้างวิสัยทัศน์ และปรับเปลี่ยนทัศนคติของข้าราชการในสังกัดให้เป็นบุคลากรที่มีประสิทธิภาพและมีการเรียนรู้ร่วมกัน” จากภาวะปัจจัยต่างๆ จึงทำให้เกิดความปรารถนาที่จะสร้างและพัฒนาองค์กรให้เป็นองค์การสมัยใหม่ บุคลากรสามารถเพิ่มพูนความรู้ความสามารถได้อย่างต่อเนื่องและสามารถสร้างผลงานได้ตามความปรารถนา อีกทั้งเป็นแหล่งสร้างความคิดทางปัญญา โดยการเรียนรู้ที่จะเรียนรู้ร่วมกัน ดังนั้นองค์กรสมัยใหม่ควรจะมีลักษณะสำคัญคือ ต้องเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง 5 ระบบขององค์กรแห่งการเรียนรู้ ได้แก่ การเรียนรู้ (Learning) องค์กร (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology) ให้เป็นตัวขับเคลื่อนและพัฒนาองค์การ เพราะการเรียนรู้ประเภทนี้ไม่สามารถจะเกิดขึ้นและไม่สามารถคงอยู่ได้หากปราศจากความเข้าใจและการพัฒนาระบบย่อยที่สัมพันธ์กัน

การจัดการความรู้และการบริหารความเสี่ยง(Knowledge and Risk Management)

1. การจัดการความรู้ (Knowledge Management)

1.1 Dave Snowden (2002) ได้กล่าวว่า การจัดการความรู้ หมายถึง การรวบรวมองค์ความรู้ที่อยู่กระจัดกระจายทั้งในตัวบุคคลหรือเอกสารมาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนใน

องค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ นำความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานให้เกิดประสิทธิภาพอันจะส่งผลให้องค์กรมีความสามารถในเชิงแข่งขันสูงสุด (อ้างอิงจาก http://thaiocaladmin.go.th/work/km)

1.2 ชนิดของความรู้ (Types of knowledge) แบ่งเป็น 3 ประเภท ประกอบด้วย 1. ความรู้ที่อยู่ในตัวคน (tacit knowledge) หมายถึง ความรู้ ประสบการณ์ พรสวรรค์ต่างๆ ที่ผู้นั้นมีอย่างเชี่ยวชาญ 2. ความรู้ที่ชัดแจ้ง (explicit knowledge) ได้แก่ ความรู้ที่ถ่ายทอดออกมาอยู่ในรูปของหนังสือ วารสาร สื่อโสตทัศนวัสดุ 3. ความรู้ที่ชัดเจนแน่นอน (Implicit) เป็นความรู้ที่ชัดแจ้งและผ่านการถกเถียงและสรุปผลว่าเป็นความรู้ที่เหมาะสมกับวัตถุประสงค์ที่ต้องการมากที่สุด

1.3 กระบวนการจัดการความรู้ Demarest (1997) ได้อธิบายถึง กระบวนการในการจัดการความรู้ไว้ 5 ขั้นตอนได้แก่ กระบวนการสร้างความรู้ (construction) กระบวนการรวบรวมความรู้ (embodiment) กระบวนการเผยแพร่ความรู้ (dissemination) กระบวนการใช้ความรู้หรือนำความรู้ไปใช้ (use) และกระบวนการจัดการองค์ความรู้ (management)

1.4 การจัดการความรู้มีประโยชน์ คือ ช่วยประหยัดเวลาในการปฏิบัติงานและช่วยในการตัดสินใจเพื่อแก้ไขปัญหาได้ถูกต้องช่วยในการคิดผลิตสิ่งใหม่ๆ ช่วยพัฒนาทักษะของผู้ปฏิบัติงาน ส่งเสริมให้เกิดเครือข่ายและการปฏิบัติการณ์ของกลุ่มเพราะมีชุมชนนักปฏิบัติ ช่วยขับเคลื่อนกลยุทธ์ขององค์กร รับรู้ปัญหาขององค์กรได้อย่างรวดเร็ว ช่วยแพร่กระจายแนวปฏิบัติที่ดีระหว่างหน่วยงานในองค์กรช่วยสร้างคู่มือ/แนวปฏิบัติในการทำงานสำหรับหน่วยงานที่มีสาขามากจะช่วยให้สามารถปฏิบัติงานเหมือนกันหรืองานในหน้าที่เดี่ยวกันได้ไม่แตกต่างกัน ช่วยทำให้ผลผลิตและการบริการดีขึ้น ช่วยให้เกิดการแลกเปลี่ยนความคิดข้ามสายงานทำให้เกิดการพัฒนาและสร้างนวัตกรรมใหม่ๆ ช่วยเพิ่มความสามารถในการแข่งขันให้กับองค์กร ช่วยบันทึกความรู้ไว้ให้ให้กับองค์กร (กรณีคนลาออกเกษียณ) ช่วยลดช่องว่างทางความคิดระหว่างพนักงานเก่ากับพนักงานใหม่ ช่วยถ่ายโอนความรู้จากรุ่นไปสู่รุ่น และช่วยตอบสนองความต้องการของลูกค้าได้ตรงจุด

2. การบริหารความเสี่ยง (Risk Management)

ความเสี่ยงมีความหมายในหลากหลายแง่มุม เช่น ความเสี่ยงคือโอกาสที่เกิดขึ้นแล้วธุรกิจจะเกิดความเสียหาย (Chance of Loss) ความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ (Possibility of Loss) ความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event) และ การคลาดเคลื่อนของการคาดการณ์ (Dispersion of Actual Result)

2.1 องค์ประกอบการบริหารความเสี่ยง

2.1.1 การระบุชี้ว่าองค์กรกำลังมีภัย เป็นการระบุชี้ว่าองค์กรมีภัยอะไรบ้างที่มาเผชิญอยู่และอยู่ในลักษณะใดหรือขอบเขตเป็นอย่างไร นับเป็นขั้นตอนแรกของการบริหารความเสี่ยง

2.1.2 การประเมินผลกระทบของภัย เป็นการประเมินผลกระทบของภัยที่จะมีต่อองค์กรซึ่งอาจเรียกอีกอย่างหนึ่งว่า การประเมินความเสี่ยงที่องค์กรต้องเตรียมตัวเพื่อรับมือกับภัยแต่ละชนิดได้อย่างเหมาะสมมากที่สุด

2.1.3 การจัดทำมาตรการตอบโต้ตอบความเสี่ยงจากภัย การจัดทำมาตรการตอบโต้ตอบความเสี่ยงเป็นมาตรการที่จัดเรียงลำดับความสำคัญแล้ว ในการประเมินผลกระทบของภัย มาตรการตอบโต้ที่นิยมใช้เพื่อการรับมือกับภัยแต่ละชนิด อาจจำแนกดังนี้

2.1.3.1 มาตรการขจัดหรือลดความรุนแรงของความอันตรายของภัยที่ต้องประสบ

2.1.3.2 มาตรการที่ป้องกันผู้รับภัยมิให้ต้องประสบภัยโดยตรง เช่น ภัยจากการที่ต้องปีนไปในที่สูงก็มีมาตรการป้องกันโดยต้องติดเข็มขัดนิรภัย กันการพลาดพลั้งตกลงมา ภัยจากไอระเหยหรือสารพิษก็ป้องกันโดยออกมาตรการให้สวมหน้ากากป้องกันไอพิษ เป็นต้น

2.1.3.3 มาตรการลดความรุนแรงของสถานการณ์ฉุกเฉินเช่น กรณีเกิดเพลิงไหม้ในอาคารได้มีการขจัดและลดความรุนแรง โดยออกแบบตัวอาคารให้มีผนังกันไฟกันเพลิงไหม้รุกลามไปยังบริเวณใกล้เคียงและมีการติดตั้งระบบสปริงเกอร์ ก็จะช่วยลดหรือหยุดความรุนแรงของอุบัติภัยลงได้

2.1.3.4 มาตรการกู้ภัยก็เป็นการลดความสูญเสียโดยตรง ลงได้มาก

2.1.3.5 มาตรการกลับคืนสภาพ เป็นการลดความเสียหายต่อเนื่องจากภัยและอุบัติภัยแต่ละครั้งลงได้

2.2 ขั้นตอนการบริหารความเสี่ยง ประกอบด้วย

2.2.1 การกำหนดวัตถุประสงค์ (Objective Establishment)

2.2.2 การระบุความเสี่ยง (Risk Identification)

2.2.3 การประเมินความเสี่ยง (Risk Assessment)

2.2.4 การสร้างแผนจัดการ(Risk Management Planning)

2.2.5 การติดตามสอบทาน (Monitoring & Review)

2.3 การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)

The Committee of Sponsoring Organization (COSO) เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กร (Internal Control Framework) อย่างเป็นระบบเมื่อช่วงต้นทศวรรษของ ปี ค.ศ.1990 จนกระทั่งเป็นที่รู้จักและมีความนิยมอย่างแพร่หลาย การบริหารความเสี่ยงตามมาตรฐาน COSO ประกอบด้วยองค์ประกอบ 8 ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน การบริหารความเสี่ยง ดังนี้

2.3.1 สภาพแวดล้อมภายในองค์กร (Internal Environment) เป็นองค์ประกอบที่สำคัญในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการเช่น

วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศระเบียบเป็นต้น

2.3.2 การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

2.3.3 การบ่งชี้เหตุการณ์ (Event Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กรเช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชีภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี

2.3.4 การประเมินความเสี่ยง (Risk Assessment) เป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กร

2.3.5 การตอบสนองความเสี่ยง (Risk Response) เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้ อยู่ในระดับที่องค์กรยอมรับได้

2.3.6 กิจกรรมการควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กรเพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

2.3.7 สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพเพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาจัดทำการบริหารความเสี่ยงให้เป็นไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

2.3.8 การติดตามประเมินผล (Monitoring) องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

2.4 การประเมินความเสี่ยงขององค์กร (Risk Assessment) การรักษาความปลอดภัยของระบบต่างๆ ในองค์กรจะเกี่ยวข้องกับการบริหารความเสี่ยง ถ้าไม่เข้าใจความเสี่ยงขององค์กรแล้วการใช้ทรัพยากรขององค์กรเพื่อการรักษาความปลอดภัยนั้นอาจมากเกินความจำเป็นหรือ

น้อยเกินไปก็ได้ กระบวนการบริหารความเสี่ยงตามมาตรฐาน ISO/IEC27001 ประกอบด้วย 2 ส่วนหลักๆ คือ

2.4.1 การประเมินความเสี่ยง (Risk Assessment) ขั้นตอนนี้จะเป็นขั้นการประเมินระดับของความเสี่ยงที่มีทั้งหมดต่อข้อมูลทรัพย์สินต่างๆ ขององค์กร โดยปกติระดับความเสี่ยงจะพิจารณาจาก 2 ปัจจัยคือ

2.4.1.1 ความน่าจะเป็น โดยปกติคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคามและช่องโหว่ที่มีต่อข้อมูล ร่วมกับวิธีการควบคุมและแก้ไขความเสี่ยงที่มีในปัจจุบัน

2.4.1.2 ความรุนแรง โดยปกติจะคำนวณค่าโดยการพิจารณาจากระดับความสำคัญของข้อมูลหรือทรัพย์สินนั้นๆที่มีต่อองค์กร

2.4.2 การรักษาความเสี่ยง (Risk Treatment) แนวทางการควบคุมและแก้ไขความเสี่ยงมีอยู่ 4 ทางคือ 1. การลดความเสี่ยง คือ การพิจารณาหาวิธีในการควบคุมแก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับที่สามารถยอมรับได้ 2. การยอมรับความเสี่ยง คือ การที่องค์กรพิจารณาแล้วว่าการดำเนินการแก้ไขและควบคุมความเสี่ยงนั้นไม่เหมาะสมไม่สามารถกระทำได้ในทางปฏิบัติหรือไม่คุ้มค่า 3. การหลีกเลี่ยงความเสี่ยง คือ การหลีกเลี่ยงความเสี่ยงโดยการยกเลิกกระบวนการทำงาน มักกระทำเมือการแก้ไขด้วยวิธีอื่นนั้นไม่คุ้มกับผลที่จะได้รับ 4. การย้ายโอนความเสี่ยง คือ การถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย

สรุปการบริหารความเสี่ยงจะมีประโยชน์อย่างยิ่งต่อองค์กร สามารถลดความสูญเสียที่จะเกิดขึ้นได้ไม่มากก็น้อย ดังนั้นกระบวนการบริหารความเสี่ยงบุคลากรทั่วทั้งองค์กรต้องมีส่วนร่วมในการคิดวิเคราะห์และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการตามกรอบวิสัยทัศน์และพันธกิจขององค์กร

ภัยคุกคามรูปแบบใหม่ (Non-Traditional Threat)

การสิ้นสุดของยุคสงครามเย็นเป็นการเปลี่ยนแปลงสภาพแวดล้อมทางยุทธศาสตร์ความมั่นคงโลกภายใต้กระแสโลกาภิวัฒน์ ส่งผลให้ภัยคุกคามรูปแบบเดิม (Yraditional threats) หรือภัยคุกคามตามแบบ (Conventional threats) ที่กระทำโดยรัฐต่อรัฐ ต่ออำนาจอธิปไตยและบูรณภาพเหนือดินแดนของรัฐ ซึ่งเป็นภัยคุกคามทางทหาร (Military threats) นั้นได้ลดน้อยลงอย่างเห็นได้ชัด ในขณะที่ภัยคุกคามรูปแบบอื่นที่มิใช่คุกคามทางทหาร (Non-Traditional threats) กลับมาสร้างปรากฏขึ้นให้เห็นโดยทั่วไปและมีแนวโน้มที่จะทวีความรุนแรงขยายวงกว้างไปทั่วโลก

ความหมายของภัยคุกคามรูปแบบใหม่(Non-Traditional threats) มีการอธิบายกันอย่างกว้างขวางในกลุ่มนักวิชาการ แต่ที่โดดเด่นที่สุด คือ กลุ่มของ คริสต์ แอบบอต, พอล โรเจอร์ส และจอห์น สโลโบดา(Christ Abbott,paul rogers and John Sloboda)พวกเขาได้เขียนหนังสือ “Global Response to Global Threats” ซึ่งได้แบ่งประเภทของภัยคุกคามรูปแบบใหม่ออกได้เป็น

4 ประเภท คือ 1. ภัยจากการเปลี่ยนแปลงภูมิอากาศ (Climate Change) 2. ภัยจากการแข่งขันแย่งชิงทรัพยาการ (Competition over Resources) 3. ภัยจากการเกิดขึ้นใหม่ของชนกลุ่มน้อยในสังคมใหญ่ (Marginalization of the Majority World) และ 4. ภัยจากการแพร่ขยายอิทธิพลทางทหาร (Global MilitariZation) นอกจากนี้ยังมีการให้คำนิยามและแบ่งประเภทของภัยคุกคามรูปแบบใหม่ในลักษณะแยกย่อยลงไป เช่น ภัยคุกคามจากโรคระบาด (Epidemiology) ภัยคุกคามทางสารสนเทศ (Information) ภัยจากอาชญากรรมข้ามชาติ (Transnational crime) ภัยคุกคามต่อความมั่นคงของมนุษย์ (Human Security) และภัยคุกคามทางด้านภูมิรัฐศาสตร์ (Geopolitics)

สำหรับประเทศไทยต้องเผชิญกับภัยคุกคามรูปแบบใหม่ที่ส่งผลกระทบต่อความมั่นคงของประเทศโดยตรง ทั้งทางด้านเศรษฐกิจ สังคมจิตวิทยาและการทหาร ในลักษณะที่ภัยคุกคามได้ทวีความรุนแรงเพิ่มขึ้นตามลำดับจากปัจจัยบวกของกระแสโลกาภิวัตน์ ที่มีการเปิดเสรีการค้า การเงิน การลงทุน ความก้าวหน้าทางการสื่อสารและเทคโนโลยีสารสนเทศ ตลอดจนผู้คนมีการย้ายถิ่นฐานระหว่างประเทศมากยิ่งขึ้น ทั้งนี้ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรใดๆ ที่ได้ให้คำนิยามและแบ่งประเภทของภัยคุกคามรูปแบบใหม่ที่ชัดเจน จนกระทั่งประมาณต้นปี พ.ศ.2550 สภาความมั่นคงแห่งชาติ หรือ สมช.จึงได้อาศัยอำนาจตามความในมาตรา 8 ฉ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ.2535 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ 4) พ.ศ.2543 นายกรัฐมนตรีได้ออกกฎกระทรวง ตามข้อ 1 ให้ สมช. มีอำนาจในการกำหนดประเภทของภัยคุกคามรูปแบบใหม่ที่ส่งผลกระทบต่อความมั่นคงของไทย 9 ประการ คือ 1. ความแตกแยกทางความคิดของคนในสังคม 2. ความไม่เชื่อมั่นต่อระบบและสถาบันการเมือง 3. การขาดการสมดุลของการจัดการทรัพยากรธรรมชาติและสิ่งแวดล้อม 4. ภัยพิบัติจากการเปลี่ยนแปลงของสภาพแวดล้อมทางธรรมชาติและโรคระบาด 5. ความมั่นคงในพื้นที่ 3 จังหวัดชายแดนภาคใต้ 6. การก่อการร้ายและอาชญากรรมข้ามชาติ 7. แรงงานต่างด้าว และผู้หลบหนีเข้าเมือง 8. ยาเสพติด และ 9. ความยากจน ซึ่งภัยคุกคามรูปแบบใหม่นี้ กองทัพบกได้นำไปเป็นบทนำของคู่มือการปฏิบัติงานตามกลยุทธ์ของการรักษาความมั่นคง ในขณะที่กองอำนวยการรักษาความมั่งคงภายใน หรือ กอ.รมน. ก็ได้นำไปกำหนดเป็นกรอบภัยคุกคามเพื่อกำหนดแผนงานรักษาความมั่นคงภายในประจำปี 2550

ในระดับรัฐบาล การจัดการกับปัญหาภัยคุกคามรูปแบบใหม่ยังมีปัญหาและอุปสรรคอาทิ ข้อจำกัดทางด้านกฎหมายในประเทศ ความร่วมมือระหว่างประเทศ ทรัพยากรของประเทศ และเจ้าหน้าที่ทุกภาคส่วนที่เกี่ยวข้องกับภัยคุกคามรูปแบบใหม่ยังมีการตื่นตัวน้อย ในขณะที่การแสดงบทบาทของกองทัพไทยที่ผ่านมา กองทัพก็ประสบปัญหาและข้อจำกัดเช่นกัน กล่าวคือ ประการแรก กองทัพมีโครงสร้างการจัดองค์กรเพื่อจัดการด้านภัยคุกคามรูปแบบใหม่ที่ไม่เด่นชัด เพราะโครงสร้างการจัดของกองทัพปัจจุบันเป็นการจัดเพื่อรองรับภัยคุกคามรูปแบบเดิมที่มองภัยคุกคามทางทหารเป็นหลัก โครงสร้างการจัดจึงได้อิงอยู่กับภารกิจป้องกันประเทศเสียเป็นส่วนใหญ่ ประการที่สองสืบเนื่องมาจากเหตุผลการจัดโครงสร้างกองทัพบกเพื่อป้องกันประเทศ กองทัพจึงมิได้กำหนดภารกิจโดยตรงเป็นการเฉพาะที่จะดำเนินการต่อเป้าหมายภัยคุกคามรูปแบบใหม่ได้ ประการที่สามไม่มีกฎหมายรองรับให้อำนาจของกองทัพในการบริหารจัดการกับภัยคุกคามรูปแบบใหม่ ประการที่สี่กำลังพลส่วนใหญ่ขาดความรู้ปละประสบการณ์ ประการที่ห้าการขาดแคลนงบประมาณและเครื่องมือสิ่งอุปกรณ์ที่จำเป็น และประการสุดท้ายกองทัพยังไม่มีหลักนิยมที่ชัดเจน ในเรื่องการปฏิบัติการทาง

ทหารที่มิใช่สงคราม (Military Operations Other Than War : MOOTW) เพื่อเป็นกรอบรองรับการจัดโครงสร้าง ภารกิจ บุคลากร การบริการจัดการเฉพาะที่จะเผชิญกับภัยคุกคามรูปแบบใหม่

แนวโน้มภัยคุกคามรูปแบบใหม่จะเป็นภัยที่มีความซับซ้อน หลากหลายมิติร่วมกันและจะทวีความรุนแรงขึ้นเรื่อยๆ ภัยคุกคามนี้จะส่งผลกระทบต่อโครงสร้างของสังคมไทยโดยตรง เฉพาะอย่างยิ่งปัญหาความมั่นคงของ 3 จังหวัดชายแดนภาคให้ซึ่งเป็นการผสมผสานระหว่างปัญหารากเหง้าของประวัติศาสตร์และปัญหาการ่อการร้าย ซึ่งมีความเชื่อมโยงของผู้ก่อการร้าย อาชญากรรมและขบวนการค้ายาเสพติดทั้งในประเทศและนอกประเทศ ทั้งนี้การป้องกันและแก้ไขภัยคุกคามรูปแบบใหม่ของรัฐบาลปัจจุบันมีลักษณะต่างคนต่างทำ ไม่มีองค์กรที่ชัดเจนรับผิดชอบบูรณาการ นโยบาย ยุทธศาสตร์ และการแปลงนโยบายไปสู่การปฏิบัติที่ชัดเจน ทำให้ไม่สามารถป้องกัน ยับยั้ง และแจ้งเตือนภัยล่วงหน้าได้อย่างมีระบบตั้งแต่ก่อนเกิดเหตุการณ์ และเมื่อเกิดเหตุการณ์ภัยที่ร้ายแรงสังคมไทยอาจจะต้องตกอยู่ในสภาวะระส่ำระสาย เสียขวัญ จนขยายวงกว้างไปสู่ความมั่นคงด้านอื่นๆ ในสถานการณ์วิกฤตร้ายแรงเช่นนี้ จึงมีความจำเป็นอย่างยิ่งที่กองทัพไทย ซึ่งเป็นกลไกทางด้านความมั่นคงของรัฐบาล ที่มีขีดความสามารถและศักยภาพสูงในการจัดการกับปัญหาความมั่นคงในลักษณะภัยคุกคามรูปแบบใหม่ที่เป็นองค์รวม(Holistic) จะได้เตรียมปรับบทบาทและโครงสร้างการจัดของกองทัพให้เหมาะสม เพื่อเผชิญกับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างเร่งด่วน เฉียบพลันในอนาคต อันจะทำให้กองทัพได้เป็นที่พึ่งและมีคุณค่ามากยิ่งขึ้นต่อสังคมไทย (ศูนย์ข้อมูล&ข่าวสืบสวนฯ(TCIJ) สถาบันอิศรา มูลนิธิพัฒนาสื่อมวลชนแห่งประเทศไทย, “ภัยคุกคามรูปแบบใหม่”, 2557)

สงครามสารสนเทศ และ สงครามไซเบอร์

1. สงครามสารสนเทศ (Information Warfare)

เทคโนโลยีสารสนเทศมีบทบาทเป็นอย่างมากในปัจจุบัน หน่วยงานต่างๆ เช่น รัฐบาล ภาครัฐ ภาคเอกชน หรือแม้กระทั้ง ประชาชนทั่วไป ต่างมีแนวความคิดที่จะนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานในกิจกรรมต่างๆ เพื่อให้กิจกรรมนั้นๆ เกิดประสิทธิภาพสูงสุด จนมีคำกล่าวว่า ปัจจุบันเป็นยุคของ “สังคมสารสนเทศ” เมื่อสารสนเทศได้ถูกนำมาใช้กับกิจกรรมต่างๆ อย่างแพร่หลาย ย่อมเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่กิจกรรมทางทหารจะนำสารสนเทศมาใช้งาน ทั้งทางด้านการบริหารจัดการและในสนามรบ ทำให้สารสนเทศเปรียบเสมือนทรัพยากรที่มีความสำคัญยิ่ง ที่แต่ละฝ่ายของคู่สงครามต่างที่จะครองความเหนือกว่าทางด้านสารสนเทศ หรือที่เรียกว่า “Information Superiority” ดังนั้นกิจกรรมใด ๆ ทั้งมวล ที่นำมาซึ่งความได้เปรียบทางด้านสารสนเทศของฝ่ายเราที่มีเหนือฝ่ายตรงข้าม และการป้องกันสารสนเทศของฝ่ายเราจากฝ่ายตรงข้าม เราจะเรียกว่า “สงครามสารสนเทศ” หรือ “Information Warfare” เรียกย่อ ๆ ว่า “IW” โดยสารสนเทศในที่นี้จะรวมถึงข้อมูล สารสนเทศ องค์ความรู้ เทคโนโลยีสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

2. สงครามไซเบอร์ (Cyber Warfare)

2.1 ความหมายของสงครามไซเบอร์ สงครามไซเบอร์ (อังกฤษ: Cyber warfare) เป็นคำที่นิยามขึ้นมาโดยผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลที่ชื่อ ริชาร์ด เอ.คลาร์ก ในหนังสือที่ชื่อ Cyber War (พฤษภาคม 2010) โดยนิยามว่า “เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก" และวิลเลียม

เจ.ลิน รองรัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐอเมริกา กล่าวว่า "โดยหลักการแล้ว เพนตากอนได้ยอมรับอย่างเป็นทางการแล้วว่า เป็นเหตุให้เกิดสงครามที่กลายเป็นเรื่องอันตรายต่อการปฏิบัติการทหาร ทั้งภาคพื้นดิน อากาศ ทะเล และทางอากาศ” อีกนัยหนึ่งสงครามไซเบอร์ (Cyber Warfare) หมายถึง การใช้คอมพิวเตอร์และอินเตอร์เน็ต ในการทำสงคราม เช่น การโจมตีเว็บ หรือบล็อคเว็บ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ตการเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ ทำให้ข้อมูลมีการเปลี่ยนแปลง การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก เป็นต้น

2.2 แนวคิดเกี่ยวกับการทำสงครามไซเบอร์ จุดกำเนิดแนวคิดของสงครามนี้ก่อตัวเป็นรูปร่างขึ้นจากนวนิยายชื่อนิวโรแมนเซอร์ (Neuromancer) ที่ชนะการประกวดจนถูกยกย่องเป็นวรรณกรรมประวัติศาสตร์ของแนวคิดใหม่จากผลงานเขียนของวิลเลียม กิ๊บสัน เป็นเรื่องราวของการนำเสนอ “ปัญญาประดิษฐ์”(Artificial Intelligence-AI) ในปี พ.ศ.2527 จนก่อให้เกิดแนวคิดต่อมาในการผลิตคอมพิวเตอร์โครงการที่ 3 ของโลกเพื่อให้ทำหน้าที่ทางด้านนี้และนำไปสู่คำนิยามของคำว่า “ไซเบอร์” ที่ชัดเจนเป็นรูปธรรมว่าไม่ใช่เพียงแต่ในความหมายของทางคอมพิวเตอร์ที่มักตีความคำว่า “ไซเบอร์” โดยนำไปรวมกับคำว่า ไซเบอร์สเปซ (Cyberspace) มีความหมายว่าทุกแห่งทุกหนที่ไปได้ทั่ว ปัจจุบันไซเบอร์สเปซ จะหมายถึง การอยู่ในเครือข่ายอินเทอร์เน็ตที่อยู่ทุกแห่งทุกหนที่ระบบอินเทอร์เน็ตเชื่อมต่อไปถึง เมื่อได้นำคำว่าไซเบอร์เนติกส์ (Cybernetics) ที่บัญญัติขึ้นโดย นอร์เบิร์ต วีเนอร์ นักคณิตศาสตร์ที่มีชื่อเมื่อ 48 ปีก่อนให้ความหมายว่า หมายถึง ระบบควบคุมการทำงานของเครื่องจักร หรือร่างกายที่สมบูรณ์ในตัวเอง และสามารถเรียนรู้ได้ภายในตัวของร่างกายด้วยระบบสื่อสารภายในหรือเชิงโทรจิตที่ติดกับตัวตน (mindset) จึงมีการพิจารณาลักษณะสงครามไซเบอร์นี้ลึกซึ่งเป็นสงครามความคิดที่ประยุกต์ใช้ระหว่างความคิดของความเป็นมนุษย์ที่มีตัวตนกับความเป็นเชิงมนุษย์หรือเลียนแบบมนุษย์ที่เรียกว่า “ไซเบอร์ก” (Cyborg) การดำเนินการสงครามไซเบอร์มีแนวทางในการดำเนินที่แตกต่างและหลากหลาย ซึ่งได้แก่

2.2.1 การก่อการร้ายทางสารสนเทศ (Information Terrorism) : เป็นลักษณะของการก่อความรุนแรง ความเสียหาย หรือก่อความไม่สงบบนระบบเครือข่ายที่เชื่อมต่อกัน

2.2.2 การโจมตีทางความหมาย (Semantic Attack) : เป็นการใช้เทคนิคและความสามารถในการเป็นแฮกเกอร์แอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้าม เพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน เช่น การใช้แฮกเกอร์เจาะระบบตรวจจับของฝ่ายตรงข้ามแล้วทำการแก้ไขโปรแกรมให้ทำงานผิดผลาด โดยตรวจจับเครื่องบินฝ่ายเราได้แล้วแสดงเป็นเครื่องบินฝ่ายเดียวกันกับเครื่องบินฝ่ายตรงข้าม ทำให้ฝ่ายตรงข้ามไม่สามารถตรวจจับเครื่องบินของฝ่ายเราได้

2.3 ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 4 ประเภท ดังนี้

2.3.1 ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (application-based threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่า มัลแวร์ (malware) นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่ง

ข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

2.3.2 ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (web-based threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งานซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี

2.3.3 ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่างๆ อาจได้รับผลกระทบโดยตรง

2.3.4 ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย (targeted attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ (hackers) ในประเทศต่างๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤติ สถาบันการเงิน และองค์กรอื่นๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.4 ผู้ก่อเหตุทางไซเบอร์ คือ กลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม (นงรัตน์ สายเพชร, 2556) คือ 1. ประเทศที่มีความประสงค์ร้าย 2. ผู้ก่อการร้าย 3. สายลับภาคเอกชน/องค์กรอาชญากรรม 4. แฮกเกอร์ (hackers) และ 5. แฮกทิวิส (hacktivists)

2.5 ชนิดของภัยคุกคามจากไซเบอร์ ภัยคุกคามไซเบอร์สามารถจำแนกออกเป็น 2 กลุ่ม ได้แก่ การจำแนกตามประเภทของภัยคุกคาม และการจำแนกตามลักษณะ/ผลของภัยคุกคาม แต่ละกลุ่มมีรายละเอียดดังนี้

2.5.1 การจำแนกภัยคุกคามตามประเภท หน่วยงาน The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามออกเป็น 9 ประเภท (ไทยเซิร์ต, “การตรวจจับภัยคุกคามและอาชญากรรมไซเบอร์ในประเทศไทย”, 2556) ประกอบด้วย บอตเน็ต (Botnet) สแปม (Spam) โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) บรูตฟอร์ซ (Brute Force) มัลแวร์ยูอาร์แอล (Malware URL) สแกนนิ่ง (Scanning) โอเพ่นพร๊อกซี่เซิร์ฟเวอร์ (Open Proxy Server) ฟิชชิ่ง (Phishing) สตอร์มเวิร์ม (Storm Worm) และดีดอส (DDoS)

2.5.2 การจำแนกภัยคุกคามตามลักษณะ/ผลของภัยคุกคาม (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์ ผู้เขียนบทความเรื่องความเป็นมาของไทยเซิร์ตจากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที ในเอกสาร Cyber Security Articles 2012 ของไทยเซิร์ต ได้แสดงรายละเอียดของภัยคุกคามจำแนกตามลักษณะ/ผลของภัยคุกคามจำนวน 8 ด้าน ประกอบด้วย เนื้อหาที่เป็นภัยคุกคาม (abusive content) การโจมตีสภาพความพร้อมใช้งานของระบบ (availability) การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (fraud) ความพยายามรวบรวมข้อมูลของระบบ (information gathering) ความ

พยายามจะบุกรุกเข้าระบบ (intrusion attempts) การเจาะระบบได้สำเร็จ (intrusions) โค๊ดมุ่งร้าย (malicious code or malware) การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต (information security) และภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (others)

2.6 การรักษาความปลอดภัยไซเบอร์ (ปริญญา หอมเอนก."Cyber security". แผ่นภาพ,2557) ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนา และมีประยุกต์ใช้งานกันอย่างแพร่หลาย ข้อมูลสารสนเทศ การติดต่อสื่อสาร และการใช้งานคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ต่างๆ เป็นสิ่งที่มีความสำคัญ จำเป็นที่จะต้องได้รับการป้องกันจากภัยไซเบอร์เพื่อให้ข้อมูลสารสนเทศและเครือข่ายต่างๆ มีความปลอดภัย สามารถทำงานได้อย่างมีเสถียรภาพ ปราศจากภัยคุกคาม และลดระดับความรุนแรงที่อาจเกิดขึ้น ในการที่จะทำให้องค์กรสร้างความมั่นใจว่าการป้องกันและรักษาเป็นไปอย่างถูกต้องครบถ้วน ย่อมต้องมีมาตรฐานหรือแนวทางปฏิบัติที่มีประสิทธิภาพ ล่าสุดได้มีการกำหนดมาตรฐาน ISO/IEC 27001-2013 ซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศขึ้น โดยมีวัตถุประสงค์เพื่อบริหารจัดการกับความปลอดภัยไซเบอร์ ISO/IEC 27001-2013 เป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่หลายองค์กรยึดถือร่วมกัน มีการนำไปใช้อย่างแพร่หลายทั่วโลก และได้มีการปรับปรุงอย่างต่อเนื่อง มาตรฐานนี้มีความเกี่ยวข้องกับข้อมูลโดยตรงเนื่องจากการรักษาความปลอดภัยของข้อมูลซึ่งถือเป็นส่วนสำคัญส่วนหนึ่งขององค์กร มาตรฐานนี้เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 โดยองค์กรมาตรฐาน International Organization for Standardization (ISO) เป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ระบบคุณภาพนี้กำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ ซึ่งเป็นมาตรฐานที่ยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก

หน่วยงานในประเทศไทยมีการนำมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ (รุ่น 2.5) มาเป็นแม่แบบของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เช่นการจัดทำแผนแม่บท ICT Security แห่งชาติของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร การจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศโดย NECTEC รวมถึงหน่วยงานเอกชนอื่นๆ มีการนำมาตรฐานนี้มาใช้ในการจัดการระบบความปลอดภัยกันอย่างแพร่หลาย อย่างไรก็ตาม การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐานสากล ISO/IEC 27001-2013 ให้มีประสิทธิภาพนั้นควรอยู่บนพื้นฐานของการประเมินความเสี่ยง และจัดการความเสี่ยงในด้านต่างๆ ควบคู่กันไป ได้แก่ 1. การรักษาความลับของข้อมูลต่างๆ ภายในหน่วยงาน (confidentiality) ซึ่งอาจกระทำได้หลากหลายวิธีด้วยกัน เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลตามระดับความสำคัญของข้อมูล 2. ความถูกต้องครบถ้วนของข้อมูล (integrity) เป็นการกำหนดมาตรการ หรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันความผิดพลาดหรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต และ

3. ความพร้อมใช้ (availability) ผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงานต้องสามารถเข้าใช้ข้อมูลได้ในกรอบเวลาที่ต้องการ

2.7 ตัวอย่างของภัยที่เกิดจากการทำสงครามไซเบอร์

2.7.1 เมื่อวันที่ 7-9 กรกฎาคม ค.ศ.2010 สำนักข่าวรอยเตอร์รายงานว่าเครือข่ายคอมพิวเตอร์และเว็บไซต์หน่วยงานรัฐบาลเกาหลีใต้ถูกแฮ็กเกอร์ไม่ทราบสัญชาติ ส่งข้อมูลเข้าไปทำลายระบบเน็ตเวิร์ก จนเว็บไซต์ใช้งานไม่ได้นานกว่า 4 ชั่วโมง เว็บไซต์เกาหลีใต้ที่ถูกโจมตีไม่ใช่เว็บไซต์ทั่วไป แต่เป็นเว็บไซต์ของกระทรวงกลาโหมเว็บไซต์ทำเนียบประธานาธิบดี รวมถึงบริษัทที่ให้บริการอินเทอร์เน็ตที่เรียกว่า “ไอเอสพี”ด้วย ศูนย์ต่อต้านการก่อการร้ายไซเบอร์ของเกาหลีใต้ หรือ “ซีทีอาร์ซี” (The Cyber Terror Response Centre) ซึ่งตั้งอยู่ในสำนักงานตำรวจแห่งชาติเกาหลีใต้เปิดเผยว่า สงครามไซเบอร์ครั้งนี้ไม่ได้เกิดขึ้นเฉพาะในเกาหลีใต้เท่านั้น แต่เครือข่ายเว็บไซต์ของรัฐบาลสหรัฐก็โดนด้วยเช่นกัน เบื้องต้นได้รับรายงานว่าเว็บไซต์สำคัญของสหรัฐกับเกาหลีใต้ไม่ต่ำกว่า 25 แห่งโดนโจมตีเรียบร้อยแล้ว โดยเจ้าหน้าที่รายหนึ่งเปิดเผยว่า เป็นการโจมตีโดยใช้วิธี “ดีดีโอเอส๐” (DDoS : Distributed Denial-of-Service) คือการใช้วิธีส่งข้อมูลจำนวนมหาศาลให้ไหลเข้าไปในเว็บไซต์ หรือเครือข่ายเน็ตเวิร์กของเป้าหมายที่ต้องการโจมตี เพื่อให้ระบบทำงานหนักขึ้นและช้าลงเรื่อยๆ จนในที่สุดต้องหยุดการทำงานลง และไม่สามารถใช้งานได้

2.7.2 เมื่อวันที่ 9 ธันวาคม ค.ศ.2010 สำนักข่าวต่างประเทศรายงานว่าเว็บไซต์ของบริษัทวีซ่าและมาสเตอร์การ์ดผู้ให้บริการบัตรเครดิตรายใหญ่ได้ถูกกลุ่มแฮ็กเกอร์เข้าโจมตีโดยทางกลุ่มแฮ็กเกอร์ที่เรียกตัวเองว่ากลุ่มผู้ไม่เปิดเผยนาม (Anonymous group) ได้ประกาศว่าจะไล่ล่าบริษัทที่หยุดการให้บริการกับวิกิลีกส์ ไม่ว่าจะเป็น amazon.com และ paypal.com ซึ่งหยุดให้การเชื่อมต่อกับวิกิลีกส์ ส่งผลให้ไม่สามารถรับเงินบริจาคได้ บุคคลกลุ่มนี้เป็นกลุ่มที่สนับสนุน นายจูเลียน อัสซานจ์ ผู้ก่อตั้งเว็บวิกิลีกส์ เกิดความไม่พอใจในกรณีนายจูเลียน ชาวออสเตรเลียวัย 39 ปี ถูกจับกุมตัวที่กรุงลอนดอน ประเทศอังกฤษ สำนักข่าวบีบีซีรายงานว่าพวกเขาได้รับการติดต่อจากบริษัทบริการชำระเงินแห่งหนึ่งซึ่งเชื่อมโยงกับมาสเตอร์การ์ด โดยกล่าวว่าลูกค้าของพวกเขามีปัญหาไม่สามารถใช้บริการได้อย่างสิ้นเชิง โดยเฉพาะในส่วนบริการพิสูจน์ยืนยันก่อนการชำระเงินออนไลน์ที่เรียกว่า Master card's Secure Code ก็มีปัญหาถูกรบกวน ด้านมาสเตอร์การ์ดกล่าวยอมรับว่ามีปัญหาด้านการให้บริการเกิดขึ้นจริงในระบบ Secure Code แต่ก็กล่าวเสริมด้วยว่า “ระบบปฏิบัติการหลักของเราไม่มีปัญหาและไม่มีความเสี่ยงใดกับข้อมูลบัญชีของผู้ถือบัตร” (www.thanonline.com) และข่าวล่าสุดเมื่อวันที่ 10 ธันวาคม ค.ศ.2010 วิกิลีกส์ยังคงเดินหน้าทำสงครามในโลกไซเบอร์ต่อไปอีก โดยเปิดโปงข้อมูลทางการทูตสหรัฐว่า เกาหลีเหนือได้ส่งคนงาน 300 คน เข้าไปช่วยพม่าสร้างโรงงานอาวุธนิวเคลียร์ มีคนเห็นรถบรรทุกขนเหล็กเป็นจำนวนมากเพื่อนำไปสร้างโรงงานนิวเคลียร์ดังกล่าว ดังนั้น จะเห็นว่าการทำสงครามไซเบอร์ในศตวรรษที่ 21 เริ่มมีอุณหภูมิร้อนแรงขึ้นทุกขณะ อย่าพึงคิดว่ามันจบสิ้นลงแล้วแต่ทว่ามันกำลังเริ่มต้นขึ้น

2.7.3 เมื่อวันพุธที่ 20 มีนาคม 2013 พนักงานของบริษัททั่วไปๆ ในกรุงโซลได้เปิดเครื่องคอมพิวเตอร์ที่ทำงานเพื่อเช็คอีเมล์ (e-mail) แต่อีเมล์นั้นกลายเป็น“Malicious Software” ซึ่งก็คือ โปรแกรมคอมพิวเตอร์ (software) ที่ถูกสร้างขึ้นมาโดยมีจุดมุ่งหมายเพื่อที่จะทำลายหรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์....ไม่นานหลังจากนั้น คอมพิวเตอร์กว่า

48,000 เครื่องในสถาบันการเงินสามแห่งและสถานีโทรทัศน์สามสถานีต่างก็เกิดอาการทำงานผิดปกติไปตามๆ กันบนจอภาพของเครื่องคอมพิวเตอร์เหล่านี้มีข้อความแสดงที่หน้าจอเหมือนกันทุกเครื่องว่า “กรุณาติดตั้งระบบปฏิบัติการในฮาร์ดดิสก์ของท่าน” (Please install an operating system on your hard disk) และในเวลาเดียวกันเครื่อง ATM ของธนาคารสามแห่งที่ถูกโจมตีก็ไม่สามารถทำงานได้เพราะ malware (ภายหลังถูกตั้งชื่อว่า “DarkSeoul” หรือ“กรุงโซลที่มืดมิด”) ได้ลบข้อมูลในฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่มีปัญหาเหล่านั้นหายไปหมด

2.7.4 วันที่ 17 พฤษภาคม ปี 2007 ประเทศเอสโทเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่างๆ จนข้อมูลเสียหายพังยับเยิน

2.7.5 เมื่อต้นเดือนกันยายน ปี 2007 ตึกเพนทากอน กระทรวงกลาโหมสหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา

2.7.6 วันที่ 14 ธันวาคม ปี 2007 เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

2.8 การสัมมนาเกี่ยวกับสงครามไซเบอร์

ในงาน Defence & Security 2013 ซึ่งจัดขึ้นที่อิมแพคเมืองทองธานี กระทรวงกลาโหมเป็นเจ้าภาพ ได้มีการถกกันในหัวข้อ “สงครามไซเบอร์ สิ่งที่ท้าทายความร่วมมือในอนาคตของชาติอาเซียน” Dr.Marwan Jamal หัวหน้าฝ่ายเทคโนโลยีของมหาวิทยาลัยแห่งชาติกลาโหม ไอคอลเลจ ประเทศสหรัฐอเมริกา ได้รับเชิญมาบรรยายในหัวข้อ “สงครามไซเบอร์ เป็นอย่างไร?”

ดร.มาร์วัน เปิดประเด็นว่า การทำสงครามไซเบอร์นั้นสามารถเอาชนะฝ่ายตรงข้ามได้โดยที่ไม่ต้องสู้รบกันแบบเผชิญหน้าเหมือนในอดีต จึงทำให้เวลานี้เกิดความวิตกกังวลและปั่นป่วนไปทั่วโลก ตัวอย่างเช่น การทำสงครามสมัยก่อน ถ้าข้าศึกต้องการจะโจมตีระบบสื่อสารของฝ่ายเราก็อาจใช้วิธีทำลายระบบสื่อสาร ด้วยการลักลอบเข้ามาตัดสายเคเบิลหรือนำระเบิดมาทิ้ง จนระบบสื่อสารของเราใช้การไม่ได้ แต่ทุกวันนี้ข้าศึกในยุคสงครามไซเบอร์ อาจไม่จำเป็นต้องทำเช่นนั้น แค่เพียงหาทางโจมตีระบบคอมพิวเตอร์ของศูนย์บัญชาการของฝ่ายเรา เพื่อให้เกิดความสูญเสียหรือใช้การไม่ได้ เท่านี้ระบบการติดต่อสื่อสารก็พังยับไม่เป็นท่าแล้ว...นี่คือตัวอย่างรูปแบบการรบสมัยใหม่ที่เรียกว่า “สงครามไซเบอร์” ในสงครามไซเบอร์ อาจมีชาติหนึ่งชาติใดแฝงตัวอยู่เบื้องหลัง การโจมตีกันด้วยช่องทางนี้เกิดขึ้นทั่วโลกนับล้านครั้งต่อเดือน ฝ่ายที่โจมตีไม่จำเป็นต้องใช้ต้นทุนสูง แค่เชี่ยวชาญในระบบคอมพิวเตอร์และอินเตอร์เน็ต สามารถเจาะผ่านระบบรักษาความปลอดภัย จนสามารถเข้าถึงข้อมูลในคอมพิวเตอร์ของอีกฝ่ายได้ เขายกตัวอย่าง ผู้โจมตีบางรายอาจเลือกใช้วิธีรบกวนเรดาร์หรือระบบเตือนภัยของอีกฝ่าย ขโมย ทำลาย หรือ ดัดแปลงแก้ไขข้อมูลเพื่อให้เกิดความสับสน เข้าใจผิด ทั้งนี้ขึ้นอยู่กับสถานการณ์ หนึ่งในวิธีที่นิยมใช้กันมาก คือ โจมตีไปที่เซิร์ฟเวอร์ (server) หรือระบบ ปฏิบัติการซึ่งทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งแก่เครื่องคอมพิวเตอร์ จนเซิร์ฟเวอร์ทำงานหนักมากจนเครื่องร้อนจัด ไหม้หรือต้องปิดตัวเอง ใครก็ตามที่เคยคิดว่า เรื่องทำนองนี้คงมีแต่ให้อ่านเล่นเอาสนุก

ในนิยายเหนือจริงทางวิทยาศาสตร์ หรือหนังแนวโลกเหนือจินตนาการของฮอลลีวูด นาทีนี้ต้องรีบคิดใหม่ เดี๋ยวนี้ข้าศึกในโลกแห่งสงครามไซเบอร์ยังสามารถพัฒนาวิธีการโจมตีแบบแปลกๆ เช่น สามารถส่งผ่านคำสั่งระยะไกล เข้าไปเปิดสวิตช์ หรือทำให้การแก้ไขตัวเซ็นเซอร์ต่างๆ ภายในเครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรือแม้แต่เซ็นเซอร์ภายในรถยนต์ ถูกขัดขวางจนก่อปัญหา เช่น สั่งเปิดตัวเซ็นเซอร์ เพื่อให้ไปทำลายแบตเตอรี่ของอุปกรณ์เหล่านั้น เป็นต้น “บางทีเขาอาจใช้วิธีโจมตีดาวเทียมของฝ่ายตรงข้าม โดยผู้โจมตีจะส่งสัญญาณเข้าไปปิดสวิตช์การทำงานของดาวเทียม หรือไม่ก็อาจใช้วิธีแฮกฯ เข้าไป ทำให้ภาพการติดตามเครื่องบินต่างๆ ทางเรดาร์ซึ่งเป็นระบบการป้องกันภัยทางอากาศถูกคุกคามโดยทำให้ภาพเครื่องบินลำจริงหายไปจากจอเรดาร์แล้วใส่ภาพลำปลอมที่ถูกสร้างภาพขึ้นมาไปปรากฏบนจอเรดาร์แทน” ปัญหาก็คือ ถ้าเป็นเครื่องบินรบของฝ่ายตรงข้ามที่ลักลอบเข้ามาโจมตีแต่เรดาร์จับภาพไว้ไม่ได้ เพราะภาพจริงถูกทำให้หายไปจากจอกลายเป็นภาพปลอมขึ้นมาแทนที่ กรณีเช่นนี้ย่อมทำให้เกิดการตัดสินใจผิดพลาดอย่างมหันต์ ทั้งนี้ เพราะหากต้องไปเจอกับ “มัลแวร์” (Malware) หรือโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อระบบคอมพิวเตอร์และเครือข่าย บุกรุกเข้าไปในอุปกรณ์คอมพิวเตอร์เหล่านั้น โดยที่ผู้ใช้ไม่รู้ตัวย่อมสร้างความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่ายนั้นๆ ยกตัวอย่าง สมมติว่า ฝ่ายจู่โจมส่งผ่านมัลแวร์เข้าไป แล้วระบบของคอมพิวเตอร์ หรือโทรศัพท์มือถือสามารถทำการอัพเดทตัวเองได้ หากเกิดขึ้นกับในทางการทหาร จะมีความเสี่ยงสูงมากเพราะรูปแบบการจู่โจมในสงครามไซเบอร์ ตามตัวอย่างข้างต้นล้วนก่อให้เกิดผลกระทบต่อศักยภาพในการสู้รบ ระบบควบคุม หรือการออกคำสั่ง หรือไม่ก็ทำให้ข้อมูลที่ส่งกลับเกิดความผิดพลาดอย่างมหันต์

ดร.มาร์วัน สรุปว่า ทางแก้หนึ่งที่ได้ผล ก็คือ นอกจากต้องมีการอัพเดทข้อมูลต่างๆ ของฝ่ายเราเป็นประจำ นานาชาติต้องมีมาตรการเตรียมความพร้อม เพื่อรับมือกับการโจมตีทางไซเบอร์ มียุทธศาสตร์ที่ครอบคลุมสงครามไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม ถ้ามีโอกาส สงครามไซเบอร์ จะลงเอยอย่างไร ณ วันนี้คงไม่มีใครตอบได้ ที่ทำได้อย่างเดียวก็คือ อยู่กับมันอย่างทันเกม หรือรู้เท่าทัน (ข่าว นสพ.ไทยรัฐ : วันที่ 2 ม.ค.58. (ออนไลน์). เข้าถึงได้จาก: http://www.thairath.co.th/content/382273, 2558)

ยุทธศาสตร์การพัฒนาของกองทัพอากาศ

1. ยุทธศาสตร์การพัฒนากองทัพอากาศ

(อ้างถึงในจตุชัย แพงจันทร์, 2555,4) กองทัพอากาศได้กำหนดยุทธศาสตร์ในการพัฒนากองทัพด้วยการเป็น “กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ภายในปี 2562 โดยจะทำให้กองทัพอากาศมีข้อมูลข่าวสารในลักษณะดิจิตอล และมีระบบสารสนเทศที่สามารถตอบสนองต่อการปฏิบัติภารกิจของกองทัพอากาศได้อย่างมีประสิทธิภาพ โดยกำหนดยุทธศาสตร์การพัฒนาเพื่อให้บรรลุวัตถุประสงค์ของวิสัยทัศน์ดังกล่าวไว้ 3 ประการ ได้แก่

1.1 เพื่อพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นส่วนหนึ่งในการเตรียมกำลังและการใช้กำลังทางอากาศโดยสนับสนุนแต่ละสายงานให้บรรลุเป้าหมายตามยุทธศาสตร์แต่ละสายงาน

1.2 นำเทคโนโลยีสารสนเทศและการสื่อสารมาพัฒนาให้กองทัพอากาศเป็นองค์กรแห่งการเรียนรู้อย่างต่อเนื่องและยั่งยืน มุ่งสู่สังคมฐานความรู้ (Knowledge-based society)

1.3 พัฒนาการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารด้วยการบูรณาการระบบสารสนเทศของกองทัพอากาศให้มีความเชื่อมโยงทั้งระบบ (Total integration) เพื่อให้สามารถใช้ประโยชน์ได้ในทุกมิติคือ มิติการบัญชาการและควบคุม มิติการสนับสนุนการรบและมิติการบริหารจัดการ เพื่อเชื่อมโยงข้อมูลผลการปฏิบัติภารกิจของทุกส่วนราชการภายในกองทัพอากาศ

2. แผนพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ พ.ศ. 2557-2562

2.1 วัตถุประสงค์ด้าน ICT กองทัพอากาศ

เพื่อให้กองทัพอากาศมีความพร้อมรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ด้วยการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร กระบวนการทำงาน บุคลากร และหน่วยงานของกองทัพอากาศ ให้สามารถปฏิบัติภารกิจโดยใช้เครือข่ายที่เป็นศูนย์กลางได้อย่างครบถ้วน ถูกต้อง ปลอดภัยและทันต่อสถานการณ์

2.2 ยุทธศาสตร์ด้าน ICT กองทัพอากาศ พ.ศ.2557 – 2562

2.2.1 ยุทธศาสตร์ที่ 1 การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารให้คุ้มค่าและพอเพียง (Optimal Technology) เป็นการพัฒนาและใช้ทรัพยากรด้าน ICT ที่ประกอบด้วย Network, Hardware, Software, Sensor และ Security ให้เกิดประโยชน์สูงสุดและคุ้มค่ากับงบประมาณ ที่ลงทุนโดยต้องให้ครอบคลุม ทั่วถึง ปลอดภัย และพอเพียง

2.2.2 ยุทธศาสตร์ที่ 2 การพัฒนากระบวนการทำงานให้ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Process) เป็นการพัฒนาและปรับปรุงกระบวนการทำงานของแต่ละหน่วยงานให้มีการบูรณาการข้อมูลข่าวสาร (Information Integration) ของแต่ละระบบงานที่มีความเกี่ยวข้องกันเข้ามาเชื่อมโยงแลกเปลี่ยนข้อมูลข่าวสาร (Information Sharing) กันได้อย่างสมบูรณ์แบบ

2.2.3 ยุทธศาสตร์ที่ 3 การพัฒนากำลังพลให้สามารถปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพ (Smart People) เป็นการพัฒนาบุคลากรในแต่ละหน่วยงานให้มีความรู้ความเข้าใจและสามารถปฏิบัติงานโดยใช้เครือข่ายที่เป็นศูนย์กลางได้จริง อย่างครบถ้วน ถูกต้อง ปลอดภัยและทันต่อสถานการณ์ เพื่อให้เกิดการทำงานร่วมกัน (Collaboration) และแลกเปลี่ยนข้อมูลข่าวสารกัน (Information Sharing) ระหว่างหน่วยงานที่เกี่ยวข้องกันได้อย่างแท้จริง

2.2.4 ยุทธศาสตร์ที่ 4 การพัฒนากองทัพอากาศให้เป็นองค์กรที่ชาญฉลาด (Smart Organization) เป็นการพัฒนาหน่วยงานของกองทัพอากาศให้มีการทำงานร่วมกัน (Collaboration) และมีการแลกเปลี่ยนข้อมูลข่าวสารกัน (Information Sharing) ระหว่างหน่วยงาน และสามารถนำข้อมูลข่าวสารไปใช้สนับสนุนการปฏิบัติงานที่ใช้เครือข่ายเป็นศูนย์กลาง โดยเฉพาะหน่วยในระบบบัญชาการและควบคุมที่ต้องทำให้สามารถรับรู้เท่าทันสถานการณ์ (Shared Situation Awareness) มีความเร็วในการสั่งการ (Speed of Command) มีจังหวะของการปฏิบัติการที่ถูกต้อง (Tempo of Operation) และมีการปฏิบัติที่สอดประสานกัน (Self Synchronization) ได้อย่างสมบูรณ์

2.3 การพัฒนาด้าน Cyber Warfare

Cyber Warfare คือ การใช้กำลังที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ เพื่อครองความได้เปรียบในห้วงไซเบอร์ (Cyberspace Superiority) สามารถบังคับหรืออนุญาตให้การปฏิบัติการดำเนินการไปอย่างเชื่อมั่นและปลอดภัย โดยหน่วยกำลังที่ปฏิบัติบนพื้นที่ปฏิบัติการที่เกี่ยวข้อง ทั้งภาคพื้นดิน, ภาคทะเล, ภาคอากาศและภาคอวกาศ ปราศจากการขัดขวางของฝ่ายศัตรู และการปฏิบัติการทางทหารที่ดำเนินการเพื่อขัดขวางการปฏิบัติงานระบบสารสนเทศและอาวุธของศัตรู รวมทั้งเพื่อดำรงการปฏิบัติงานระบบสารสนเทศและอาวุธของตนให้มีประสิทธิภาพ การปฏิบัติการดังกล่าวรวมถึงการโจมตีทางไซเบอร์ (Cyber Attack), การป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions) ในการพัฒนาด้าน Cyber Warfare นั้น ต้องมีการพัฒนาทั้งด้าน Cyber Defense และ Cyber Attack เพื่อป้องกันระบบของ ทอ. และนำศักยภาพด้าน Cyber Attack มาสร้างความได้เปรียบในการปฏิบัติภารกิจต่างๆ ของ ทอ.

3. นโยบายผู้บัญชาการทหารอากาศด้านเทคโนโลยีสารสนเทศและการสื่อสาร

การพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญที่ขับเคลื่อนกองทัพอากาศไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางได้อย่างสมบูรณ์ จึงกำหนดนโยบายเฉพาะด้านเทคโนโลยีสารสนเทศและการสื่อสาร ไว้ดังนี้

3.1 พัฒนาการบูรณาการข้อมูลฝ่ายเสนาธิการ เพื่อการบัญชาการและควบคุมอาคารศูนย์ปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCOC Portal)

3.2 พัฒนาให้มีศูนย์โทรคมนาคมสำรองและระบบสำรองฐานข้อมูลที่เพียงพอให้กับคอมพิวเตอร์แม่ข่ายที่ศูนย์ข้อมูลกองทัพอากาศและที่อาคารศูนย์ปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง เพื่อให้รองรับกรณีระบบงานใดขัดข้องให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง ตลอดจนสามารถกู้ข้อมูลเดิมได้ทันสถานการณ์

3.3 พัฒนาระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศภูมิศาสตร์ โดยจัดลำดับความสำคัญพื้นที่ดำเนินการให้สอดคล้องตามแผนแม่บท ทอ. ด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้สามารถบูรณาการข้อมูลข่าวสารของแต่ละระบบงานภายในกองทัพอากาศที่มีความเกี่ยวข้องกันเพื่อแลกเปลี่ยนข้อมูลข่าวสารกันได้อย่างสมบูรณ์และปลอดภัย

3.4 กำหนดแนวความคิดในการปฏิบัติภารกิจสงครามอิเล็กทรอนิกส์ และปรับปรุงกระบวนการทำงานด้านการสงครามอิเล็กทรอนิกส์ เพื่อสนับสนุนการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ตลอดจนกำหนดแนวทางในการพัฒนาระบบปฏิบัติการจำลองทางยุทธวิธีสงครามอิเล็กทรอนิกส์

3.5 พัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ โดยเฉพาะการกระตุ้นและพัฒนากำลังพลด้านไซเบอร์ให้มีความพร้อมในการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับตามมาตรฐานสากล

3.6 ตรวจสอบระบบรักษาความปลอดภัยเครือข่ายสารสนเทศ และกำหนดแนวทางการพัฒนาระบบรักษาความปลอดภัยเครือข่ายสารสนเทศให้สามารถตรวจจับ ป้องกันการบุกรุก

รวบรวม วิเคราะห์เหตุการณ์ละเมิดการรักษาความปลอดภัย และรายงานผลที่เกิดขึ้นได้ทันต่อสถานการณ์

3.7 ตรวจสอบขีดความสามารถเครือข่ายของกองทัพอากาศ และกำหนดแนวทางการพัฒนาเครือข่ายของกองทัพอากาศให้มีความแข็งแกร่ง สามารถติดต่อสื่อสารข้อมูลได้อย่างรวดเร็ว ปลอดภัย รองรับปริมาณความต้องการใช้งาน

4. นโยบายผู้บัญชาการทหารอากาศด้านการพัฒนาประสิทธิภาพกำลังพลของกองทัพอากาศ

นโยบายเฉพาะของ ผบ.ทอ. ด้านการพัฒนากำลังพล เป็นปัจจัยสำคัญยิ่งต่อการขับเคลื่อนกองทัพอากาศเพื่อให้บรรลุวิสัยทัศน์กองทัพอากาศในปี พ.ศ.2562 และเพื่อเตรียมความพร้อมกองทัพอากาศในการเข้าสู่ประชาคมอาเซียน ในปี พ.ศ.2558 จึงกำหนดแนวทางการดำเนินงานดังนี้

4.1 นำสมรรถนะกองทัพอากาศมาเป็นเครื่องมือในการบริหารกำลังพลเพื่อเสริมสร้างศักยภาพกำลังพลในทุกสายวิทยาการให้มีขีดสมรรถนะสูงขึ้น สามารถคิด วิเคราะห์ ตัดสินใจและปฏิบัติงานได้อย่างเหมาะสมกับสถานการณ์ โดยให้ความ สำคัญกับการพัฒนากำลังพลในสายวิทยาการที่เกี่ยวข้องกับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง รวมทั้งพัฒนาระบบการประเมินผลการปฏิบัติงานของกำลังพลให้สอดคล้องตามแนวคิดสมรรถนะกองทัพอากาศเพื่อเป็นแนวทางในการวางแผนบริหารและพัฒนากำลังพล

4.2 ทบทวนและกำหนดความต้องการกำลังพลทั้งเชิงปริมาณและเชิงคุณภาพให้สอดรับกับกรอบงบประมาณประจำปีที่กองทัพอากาศได้รับ ตลอดจนจัดทำแผนการสรรหาและเลือกสรรกำลังพลให้มีความเหมาะสมในทุกสายวิทยาการที่มีการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางเพื่อให้บรรลุวิสัยทัศน์กองทัพอากาศ โดยมุ่งพัฒนากำลังพลที่ปฏิบัติงานด้านสงครามอิเล็กทรอนิกส์และสงครามไซเบอร์

4.3 พัฒนาระบบบริหารกำลังพลให้สอดคล้องกับการปฏิบัติภารกิจและยุทธศาสตร์กองทัพอากาศ โดยมุ่งเน้นการบริหารจัดการกำลังพลที่มีส่วนร่วมในการปฏิบัติภารกิจและยุทธศาสตร์กองทัพอากาศ เช่น กำลังพลที่ปฏิบัติงานกับระบบ อากาศยานไร้คนขับให้มีความเหมาะสม รวมทั้งให้ความสำคัญกับการพัฒนาระบบข้าราชการพลเรือนกลาโหมให้เป็นไปตาม กรอบที่ทางกระทรวงกลาโหมกำหนด

4.4 เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียนในปี พ.ศ.2558 โดยให้ความสำคัญกับการพัฒนาความรู้ และทักษะการใช้ภาษาอังกฤษของกำลังพลในทุกระดับ เพื่อให้สามารถนำ ไปประยุกต์ใช้ในการ ปฏิบัติงานและการติดต่อสื่อสารได้อย่างเหมาะสม

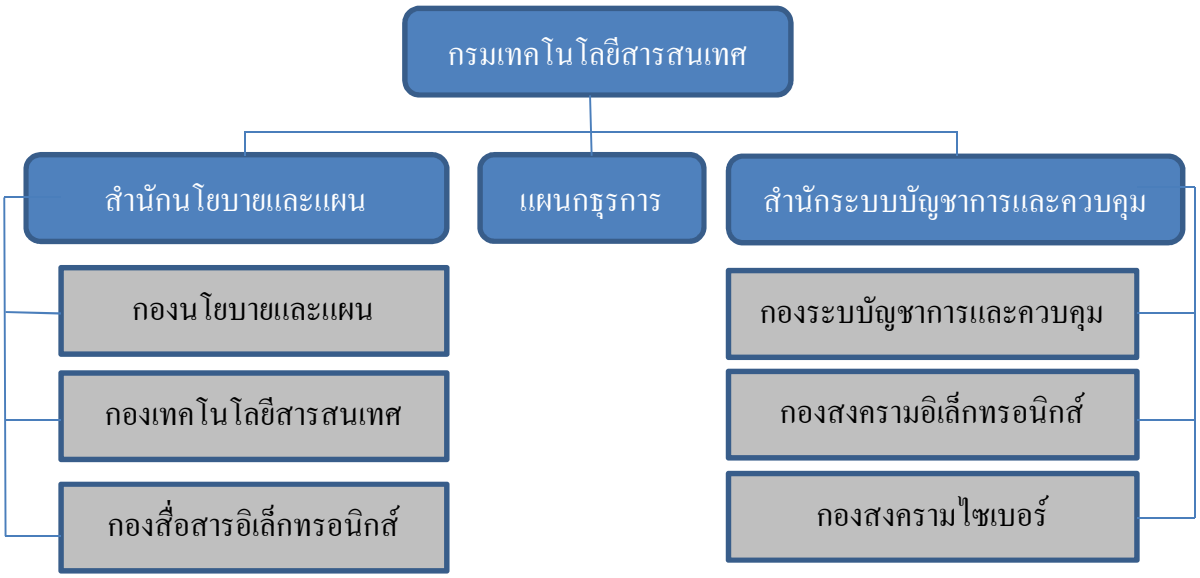
4.5 ส่งเสริมและสนับสนุนการดูแลสวัสดิการเพื่อพัฒนาคุณภาพชีวิตของกำลังพลอย่างทั่วถึง เป็นธรรมและเหมาะสมในทุกๆ ด้าน โดยเฉพาะด้านสวัสดิการบ้านพักอาศัยจะต้องมีความพร้อมและพอเพียงทั้งในเชิงปริมาณและเชิงคุณภาพ

หน่วยงานรับผิดชอบการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

1. โครงสร้างการจัดหน่วย

หน่วยงานที่รับผิดชอบการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ได้แก่ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนาและดำเนินการด้านระบบบัญชาการและควบคุม ข่าย เครือข่าย เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ และการสงครามอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุมประเมินผล และตรวจตรากิจการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเป็นผู้บังคับบัญชารับผิดชอบ

แผนภาพที่ 2-1 โครงสร้างการจัดหน่วยกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ



2. ภารกิจและหน้าที่ของหน่วยเกี่ยวข้อง

2.1 สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการประสานงาน ควบคุม กำกับการพัฒนา ระบบบัญชาการและควบคุม สงครามอิเล็กทรอนิกส์สงครามสารสนเทศ และสงครามไซเบอร์ มีผู้อำนวยการสำนักระบบบัญชาการควบคุมเป็นผู้บังคับบัญชารับผิดชอบ แบ่งส่วนราชการออกเป็น

2.1.1 กองระบบบัญชาการและควบคุม มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านระบบการเฝ้าตรวจระบบการลาดตระเวนและภูมิสารสนเทศ ระบบบัญชาการและควบคุม ระบบบัญชาการและควบคุมร่วม/ผสมการ บูรณาการข่ายควบคุมสั่งการในการใช้กำลังทางอากาศและภาคพื้น การบูรณาการเครือข่ายเชื่อมโยงทั้งภายในและภายนอกประเทศ และการใช้ประโยชน์ข้อมูลการยุทธ์ใน

ห้องปฏิบัติการรบหรือศูนย์สั่งการของหน่วยในระบบการใช้กำลัง มีผู้อำนวยการกอง กองระบบบัญชาการและควบคุม เป็นผู้บังคับบัญชารับผิดชอบ

2.1.2 กองสงครามอิเล็กทรอนิกส์ มีหน้าที่ พิจารณา วางแผน อำนวยการประสานงาน ควบคุมกำกับการ พัฒนาและดำเนินการด้านการสงครามอิเล็กทรอนิกส์ รวบรวมข้อมูล วิเคราะห์กำหนดแนวทาง มาตรการ การรหัสข้อมูล ในการปฏิบัติสงครามอิเล็กทรอนิกส์ มีผู้อำนวยการกองกองสงครามอิเล็กทรอนิกส์ เป็นผู้บังคับบัญชารับผิดชอบ

2.1.3 กองสงครามไซเบอร์ มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงานควบคุม กำกับการ พัฒนาและดำเนินการด้านสงครามสารสนเทศและสงครามไซเบอร์ กำหนดแนวทางและมาตรการในการป้องกันและการรักษาความปลอดภัยระบบสารสนเทศ มีผู้อำนวยการกองกองสงครามไซเบอร์ เป็นผู้บังคับบัญชารับผิดชอบ

2.2 สำนักนโยบายและแผน มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการประสานงาน ควบคุมกำกับการ พัฒนา แผนงานและโครงการ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ข่าย เครือข่ายการสื่อสารอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศกับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผลและตรวจตราภิจการในสายวิทยาการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีผู้อำนวยการสำนักสำนักนโยบายและแผน เป็นผู้บังคับบัญชารับผิดชอบ แบ่งส่วนราชการออกเป็น

2.2.1 กองนโยบายและแผน มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการประสานงานควบคุม กำกับการ พัฒนา และดำเนินการด้านการกำหนดความต้องการ การควบคุมขีดความสามารถและระดับความพร้อมด้านเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ให้ครอบคลุมการปฏิบัติภารกิจของกองทัพอากาศ การจัดทำแผนแม่บท แผนงาน โครงการ และงบประมาณ และการบูรณาการแผนงานรองรับแผนการเตรียมกำลังและใช้กำลัง การจัดทำสัญญาข้อตกลง ความร่วมมือ บันทึกเจรจาด้านเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ร่วมกับภาครัฐและเอกชน การกำหนดมาตรฐานยุทโธปกรณ์ อัตราจ่ายพัสดุสายเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่ จัดการความรู้ บริหารการฝึกและศึกษาบริหารกำลังพลและการตรวจตราภิจการในสายวิทยาการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีผู้อำนวยการกอง กองนโยบายและแผน เป็นผู้บังคับบัญชารับผิดชอบ

2.2.2 กองสื่อสารอิเล็กทรอนิกส์ มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงานควบคุม กำกับการ พัฒนา และดำเนินการด้านระบบสื่อสารอิเล็กทรอนิกส์ ระบบเครื่องช่วยเดินอากาศการบริหารคลื่นความถี่ ระบบสื่อสารโทรคมนาคมทั้งภายในและภายนอกประเทศ มาตรวิทยากิจการกระจายเสียงและกิจการโทรทัศน์ และการใช้ประโยชน์อุปกรณ์สื่อสารอิเล็กทรอนิกส์มีผู้อำนวยการกอง กองสื่อสารอิเล็กทรอนิกส์ เป็นผู้บังคับบัญชารับผิดชอบ

2.2.3 กองเทคโนโลยีสารสนเทศ มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงานควบคุม กำกับการ พัฒนา และดำเนินการด้านเทคโนโลยีสารสนเทศ ให้

ครอบคลุมการปฏิบัติภารกิจของกองทัพอากาศ ตามแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ รองรับแผนการเตรียมกำลังและใช้กำลัง การวิเคราะห์ กำหนดความต้องการ บูรณาการ รวมทั้งติดตามสถานภาพการใช้ประโยชน์ระบบเทคโนโลยีสารสนเทศ และแลกเปลี่ยนวิชาการด้านเทคโนโลยีสารสนเทศ มีผู้อำนวยการกอง กองเทคโนโลยีสารสนเทศ เป็นผู้บังคับบัญชารับผิดชอบ

2.3 แผนกธุรการ มีหน้าที่ ดำเนินการเกี่ยวกับการธุรการ การสารบรรณ การพัสดุ ตลอดจนดูแลสถานที่และเครื่องมือเครื่องใช้ของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหัวหน้าแผนกธุรการเป็นผู้บังคับบัญชารับผิดชอบ

การเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

1. การเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์

(อ้างถึงใน จตุชัย แพงจันทร์, 2555, 35) ผลวิจัยพบว่า กองทัพอากาศมีความจำเป็นอย่างยิ่งที่ต้องเตรียมการในการป้องกันภัยคุกคามจากโลกโซเบอร์ และในขณะเดียวกันจำเป็นที่ต้องพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ซึ่งจะเป็นการทวีกำลังทางทหารในการต่อสู้ในสงครามที่อาจจะเกิดขึ้นในอนาคต จึงต้องเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์ไว้ตั้งแต่ยามปกติ ประกอบด้วย 3 ส่วน คือ คน (People), กระบวนการ (Process) และเทคโนโลยี (Technology) ในส่วนของเทคโนโลยี หมายถึง เครื่องมือหรืออาวุธไซเบอร์ ส่วนกระบวนการหมายถึง รูปแบบหรือขั้นตอนในการทำสงคราม ส่วนคน หมายถึง นักรบไซเบอร์ที่จะต้องมีการฝึกให้พร้อมที่จะปฏิบัติงานจริงๆ ได้ ในหัวข้อนี้จะกล่าวถึงคุณสมบัติที่สำคัญของนักรบไซเบอร์ รวมถึงการฝึกอบรมที่จำเป็นสำหรับการที่จะเป็นนักรบไซเบอร์จริงๆ มีรายละเอียดดังนี้

1.1 นักรบไซเบอร์ (Cyber warrior) หมายถึง คนที่จะทำหน้าที่ปฏิบัติการเครือข่ายคอมพิวเตอร์ตามภารกิจที่ได้รับมอบหมายเพื่อให้บรรลุเป้าหมายทางทหาร ในอนาคตความขัดแย้งในโลกไซเบอร์อาจมีความรุนแรงและซับซ้อนมากขึ้น ดังนั้นจึงจำเป็นที่ต้องมีนักรับไซเบอร์ที่มีทักษะและความชำนาญเฉพาะทางมากขึ้น ซึ่งความรู้ความชำนาญที่ว่านี้นักรบต้องมีการฝึกและผ่านการทดสอบ ก่อนที่จะได้รับภารกิจที่เหมาะสมเหล่านั้น คุณสมบัติที่สำคัญของนักรบคือความรู้ความชำนาญเฉพาะด้าน เนื่องจากในสายวิทยาการด้านการรักษาความปลอดภัยข้อมูลนั้นเป็นวิทยาการที่ค่อนข้างใหม่เมื่อเทียบกับสายวิทยาการด้านอื่นๆ ดังนั้นจึงอาจไม่มีรูปแบบการฝึกอบรมที่เป็นมาตรฐานมากนัก อย่างไรก็ตามเนื่องจากผู้ที่มีความรู้ความชำนาญด้านการรักษาความปลอดภัยข้อมูลนั้นจำเป็นต้องมีความรู้พื้นฐานด้านอื่นๆ มาก่อน

1.1.1 ความรู้ เกิดจากการศึกษาซึ่ง หมายถึง การศึกษาตั้งแต่ในระดับปริญญาตรีหรือก่อนที่จะเข้ามารับตำแหน่งหน้าที่ในสายวิทยาการการรักษาความปลอดภัย หรือโดยเฉพาะการปฏิบัติหน้าที่ในฐานะนักรบไซเบอร์นั้นจำเป็นที่ต้องมีความรู้พื้นฐานที่สำคัญและจำเป็นสำหรับการทำหน้าที่ด้านนี้ โดยส่วนใหญ่แล้วนักรบไซเบอร์นั้นจะจบการศึกษาระดับปริญญาตรีและมี

จำนวนมากเช่นกันที่จบปริญญาโทด้วย สำหรับคนที่จบในสาขาเทคนิคไม่ว่าจะเป็น วิทยาการคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์ เทคโนโลยีสารสนเทศ การรักษาความปลอดภัยข้อมูล และสาขาอื่นที่ใกล้เคียงกัน เป็นสาขาที่เมื่อจบแล้วสามารถเข้ามาทำงานได้ทันที

1.1.2 ทักษะ คุณสมบัติที่สำคัญของนักรบไซเบอร์ที่ต้องมีคือการผ่านการฝึกอบรมที่ได้มาตรฐานและได้รับใบรับรอง (Certificate) สำหรับในสายการรักษาความปลอดภัยข้อมูลทั่วไป ใบเซอร์ติฟิเกตที่ได้รับการยอมรับมากที่สุดคือ CISSP (Certified Information Systems Security Professional) ซึ่งออกให้โดยสถาบันนานาชาติ (ISC)2 (International Information Systems Security Certification Consortium) นอกจากนี้ยังมีใบรับรองที่ออกให้บริษัทเอกชนสำหรับผู้ที่มีความรู้ความชำนาญเกี่ยวกับผลิตภัณฑ์ของตน ไม่ว่าจะเป็นบริษัท Guidance Software ที่ออกใบ ENCE (EnCase Certified Examiner) เป็นต้น

สำหรับกระทรวงกลาโหมของสหรัฐฯ ได้มีคำสั่งเฉพาะที่ 8570 (DoD Directive 8570) ซึ่งเป็นคำสั่งที่บังคับให้กำลังพลที่ทำงานด้านการรักษาความปลอดภัยข้อมูล หรือ IA (Information Assurance) จะต้องผ่านการฝึกอบรมและมีใบรับรองหรือเซอร์ติฟิเกต (Certificate) ที่ออกให้โดยสถาบันเอกชน เพื่อเพิ่มความมั่นใจว่ากำลังพลที่ทำงานด้านนี้มีความรู้ ความชำนาญ และประสบการณ์ที่เพียงพอ ต่อการปฏิบัติงานในตำแหน่งต่างๆที่ตัวเองได้รับการบรรจุลง โดยคำสั่งดังกล่าวนี้ได้แบ่งสายอาชีพออกเป็น 2 สายและแต่ละสายแบ่งความชำนาญออกเป็น 3 ระดับ คนที่จะถูกบรรจุในตำแหน่งที่จัดอยู่ในสายใดและระดับอะไรจะต้องได้รับใบรับรองความชำนาญหรือเซอร์ติฟิเกตอย่างต่ำตามที่กำหนด

กำลังพลที่ต้องมีใบรับรองความชำนาญการนั้นจะถูกระบุโดยตำแหน่ง และในตำแหน่งงานนั้นก็จะระบุถึงระดับความชำนาญการหรือหน้าที่ที่รับผิดชอบว่ามีสิทธิ์ในการเข้าถึงข้อมูลได้ในระดับไหน ตำแหน่งงานที่เกี่ยวข้องกับระบบสารสนเทศนั้น จะแบ่งสายงานของกำลังพลออกเป็น 2 ประเภทคือ สายเทคนิค หรือ IAT (Information Assurance Technical) และสายบริหาร หรือ IAM (Information Assurance Management) และแต่ละสายงานก็มีการแบ่งระดับ (Level) ความชำนาญการออกเป็น 3 ระดับเหมือนกันคือ ระดับ 1 (Level I) เป็นระดับที่มีความชำานาญและประสบการณ์ต่ำสุด มีความรู้เบื้องต้นเกี่ยวกับการไอทีหรือคอมพิวเตอร์ทั่วไป ระดับ 2 (Level II) เป็นระดับที่มีความชำนาญและประสบการณ์ในระดับกลาง มีความรู้ด้านเครือข่ายคอมพิวเตอร์เป็นสำคัญ และระดับ 3 (Level III) เป็นระดับที่มีความชำนาญและประสบการณ์สูงสุด ซึ่งจะรับผิดชอบเกี่ยวกับระบบที่มีความลับมากๆ หรือระบบที่ปกปิด (Enclave)

1.1.3 ความเป็นมืออาชีพ (Proficiency) นักรบไซเบอร์จำเป็นอย่างยิ่งที่ต้องมีประสบการณ์ในการทำงาน ซึ่งประสบการณ์นี้สามารถพัฒนาได้ด้วยการฝึกรบ โดยหน่วยงานนั้นควรจัดให้มีการฝึกรบเป็นประจำทุกปี เหมือนอย่างกระทรวงกลาโหมสหรัฐฯ จะจัดให้มีการฝึกรบบนโลกโซเบอร์ ซึ่งมีชื่อเรียกว่า “พายุไซเบอร์ (Cyber Storm)” ซึ่งเป็นการฝึกนักรบไซเบอร์ประจำปี โดยมีการกำหนดสถานการณ์ที่เหมาะสมกับสถานการณ์ ณ ขณะนั้น และมีการเตรียมเครื่องมือหรือฝึกใช้อาวุธไซเบอร์ที่ทันสมัยและมีการพัฒนายุทธวิธีใหม่ โดยทั้งมวลก็เพื่อพัฒนาศักยภาพของนักรบไซเบอร์ให้พร้อมปฏิบัติการอยู่ตลอดเวลา

1.2 อาวุธไซเบอร์ (Cyber weapon) เป็นซอฟต์แวร์ที่นักรบไซเบอร์ใช้ในการโจมตีระบบของฝ่ายตรงกันข้าม ซึ่งเครื่องมือหรือซอฟต์แวร์ที่เหล่าแฮ็กเกอร์ทั่วไปใช้ในการแฮ็กค์ระบบต่างๆ แต่การใช้เครื่องมือเดียวกันนี้เพื่อใช้สำหรับการปฏิบัติการทางทหาร โดยใช้กับเป้าหมายทางทหารเช่น ระบบบัญชาการและควบคุม (Command and control) ระบบเรดาร์ (Radar system) หรือระบบที่ใช้ในการควบคุมการส่งกำลังบำรุง (Logistic system) ซึ่งระบบเหล่านี้ล้วนแล้วแต่มีผลต่อประสิทธิภาพในการรบแทบทั้งสิ้น ถึงแม้จะเป็นเครื่องมือเดียวกันแต่เมื่อใช้กับการต่อสู้ในสงครามเราอาจเรียกได้ว่าเป็นอาวุธสงครามหรืออาวุธไซเบอร์ก็ได้

2. สถานภาพด้าน Cyber Security ของหน่วยงานในกองทัพอากาศ

(อ้างถึงใน น.อ.รศ.ดร.ประสงค์ ปราณีตพลกรัง, 2557, 11) ผลวิจัยพบว่า

2.1 ภัยคุกคามทางไซเบอร์ที่ร้ายแรงและน่าเป็นห่วงของ ทอ. 3 อันดับแรก ได้แก่

2.1.1 การโจมตีหรือเข้าควบคุมระบบของโครงสร้างพื้นฐานสำคัญยิ่งยวด (Critical Infrastructure) เพื่อให้ใช้งานไม่ได้ตามปกติ

2.1.2 การเข้าถึงข้อมูลส่วนบุคคลเพื่อนำไปใช้ทำลายชื่อเสียง สร้างความแตกแยก

2.1.3 การเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลของหน่วยงานเพื่อนำไปใช้ฉ้อโกงหรือหลอกลวงหาผลประโยชน์ทางการเงิน และ การเข้าถึงหรือเปลี่ยนแปลงข้อมูลเพื่อทำลายภาพลักษณ์หรือความน่าเชื่อถือของหน่วยงาน ทอ.

2.2 จุดอ่อนในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของ ทอ. ได้แก่

2.2.1 ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยทางไซเบอร์

2.2.2 บุคลากรขาดการตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์

2.2.3 ผู้ใช้เทคโนโลยีขาดความรู้ความเข้าใจในการใช้เทคโนโลยีอย่างมั่นคงปลอดภัย

2.3 สาเหตุหลักของการเกิดภัยคุกคามทางไซเบอร์ ของ ทอ. ได้แก่

2.3.1 บุคลากรในหน่วยงาน ทอ.

2.3.2 เกิดจากไวรัสหรือเวิร์ม

2.3.3 ช่องโหว่ในโปรแกรมประยุกต์ที่ติดมากับระบบ

2.4 ช่องทาง (Channel) ที่มีความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ ของ ทอ. ได้แก่

2.4.1 ทางเครือข่าย (Network) เช่น การลักลอบใช้เครือข่ายไร้สายของหน่วยงาน

2.4.2 ทางแอปพลิเคชัน เช่น การปลอมแปลงเว็บไซต์ที่ไม่ได้ใช้เทคโนโลยี SSL

2.4.3 ทางกายภาพ (Physical) เช่น การทำการโจมตีแบบวิศวกรรมสังคม (Social Engineering) กับพนักงานที่เคาน์เตอร์ของหน่วยงาน เป็นต้น

2.5 ปัญหาหลักในการป้องกันภัยคุกคามทางไซเบอร์ คือ

2.5.1 ผู้ใช้งานไอทีในหน่วยงาน ทอ. ยังขาดความตระหนักในด้านมั่นคงปลอดภัย

2.5.2 ทอ. ขาดแคลนบุคลากรผู้เชี่ยวชาญด้าน ความมั่นคงปลอดภัยไซเบอร์

2.5.3 ทอ. ขาดระบบการเฝ้าระวังและเตือนภัยด้านไซเบอร์ที่มีประสิทธิภาพ

2.6 การดำเนินการกรณีที่เกิดเหตุการณ์ (Incident) ทางไซเบอร์ สิ่งที่หน่วยงานในกองทัพอากาศดำเนินการ หรือจัดการปัญหาโดยส่วนใหญ่คือ วิเคราะห์หาสาเหตุของปัญหาและเก็บข้อมูลเป็นพยานหลักฐานเพื่อใช้ในการดำเนินคดี รองลงมาคือไม่ได้ดำเนินการใดๆ ได้ทันท่วงที เพราะขาดแนวทางในการแก้ไขปัญหาเบื้องต้น และดำเนินการร้องเรียนผ่านหน่วยงานที่เกี่ยวข้องต่อไป ผลการวิจัยพบอีกว่า สถานภาพโดยรวมด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศในประเด็นบุคลากร กระบวนการและเทคโนโลยี นั้นพบว่า ทอ. ยังขาดแคลนทรัพยากรด้านนี้อยู่ในระดับมาก ปัญหาภัยคุกคามหลักคือการเข้าควบคุมระบบของโครงสร้างพื้นฐานสำคัญยิ่งยวดเพื่อให้ใช้งานไม่ได้ตามปกติ สาเหตุหลักของการเกิดภัยคุกคามทางไซเบอร์มาจากกำลังพลในหน่วยงานขาดความรู้ความเข้าใจ รองลงมาเกิดจากไวรัสหรือเวิร์ม

3. แนวโน้มภัยคุกคามด้านสงครามไซเบอร์

ISF : The Information Security Forum เป็นองค์กรที่ไม่แสวงหากำไร มีสมาชิกประกอบด้วยองค์กรชั้นนำต่างๆ ทั่วโลก ได้จัดทำผลสำรวจ วิเคราะห์ และรายงาน “Threat Horizon Report” เพื่อพยากรณ์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ล่วงหน้าทุกๆ 2 ปี โดยระบุประเด็นที่ส่งผลกระทบอย่างมีนัยสำคัญต่อองค์กร พร้อมทั้งแนวทางดำเนินการเพื่อป้องกันหรือช่วยลดผลกระทบที่อาจเกิดขึ้น

จากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 “Threat Horizon 2016” รายงานสรุปทิศทางในเชิงลบเป็นภัยความเสี่ยง 3 ประเด็นหลัก คือ 1. ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (No-one left to trust in cyberspace) 2. ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ (Confidence in accepted solutions crumbles) และ 3. ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Failure to deliver the cyber resilience promise) ภัยความเสี่ยงทั้ง 3 ประเด็นหลัก ประกอบด้วยเรื่องที่องค์กรต้องให้ความสำคัญ ดังนี้

3.1 ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (No-one left to trust in cyberspace)

3.1.1 การจารกรรมไซเบอร์ที่สนับสนุนโดยหน่วยงานภาครัฐ จะกลายเป็นกระแสหลัก

3.1.2 การควบคุมอินเทอร์เน็ตภายในประเทศหรือภูมิภาค จะสร้างความยุ่งยากต่อธุรกิจ

3.1.3 ผลสืบเนื่องที่ไม่พึงประสงค์ จากการแทรกแซงของภาครัฐ

3.2 ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ (Confidence in accepted solutions crumbles)

3.2.1 ผู้ให้บริการ จะกลายเป็นช่องโหว่สำคัญ

3.2.2 Big Data จะกลายเป็นปัญหาใหญ่

3.2.3 แอพพลิเคชั่นมือถือ จะกลายเป็นช่องทางหลักที่ถูกเจาะข้อมูล

3.2.4 การเข้ารหัสข้อมูล ไม่เกิดผล

3.3 ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Failure to deliver the cyber resilience promise)

3.3.1 CEO รับรู้ ถึงเวลาที่ต้องป้อนข้อมูลวางแนวทาง

3.3.2 ความแตกต่างด้านทักษะ จะมีช่องห่างกว้างมากขึ้น

3.3.3 ความมั่นคงปลอดภัยสารสนเทศ จะไม่สามารถใช้ได้กับคนรุ่นใหม่

ISF ได้ระบุเพิ่มเติมว่า นอกจากประเด็นและหัวข้อที่ระบุใน “Threat Horizon 2016” แล้ว องค์กรจะต้องพิจารณาต่อเนื่องจากประเด็นหัวข้อภัยคุกคามที่ได้นำเสนอมาตั้งแต่ “Threat Horizon 2014” ที่ส่งผลถึงภัยคุกคาม 2016 โดยเน้นย้ำว่า “การเตรียมรับมือภัยไซเบอร์ตอนนี้ไม่ใช่เป็นแค่ทางเลือก แต่เป็นสิ่งจำเป็นที่สุดที่ต้องทำเลยทันที”

จากรายงาน Threat Horizon สำหรับปี 2014 และ 2015 มาถึงปี 2016 ความรุนแรงของภัยคุกคามไซเบอร์ยังคงมีต่อเนื่อง องค์กรไม่มีความสามารถในการปรับตัวและรับมือ CEO เริ่มเข้าใจ แต่ผู้บริหารที่รับผิดชอบ ไม่สามารถจะให้ข้อมูลแผนงานและแนวทางดำเนินการได้ และมาตรการความมั่นคงปลอดภัยที่มีก็ไม่เหมาะกับคนรุ่นใหม่ ขณะที่โซลูชั่นที่ใช้งานกันโดยทั่วไปจะกลายเป็นภัยคุกคามสำคัญเสียเอง ทั้งจากการใช้งานผู้ให้บริการภายนอก แอพพลิเคชั่นมือถือ การเข้ารหัสข้อมูล และการจัดการข้อมูลขนาดใหญ่ขององค์กร ตลอดจนบทบาทภาครัฐที่เข้ามาแทรกแซงหรือควบคุมอินเทอร์เน็ต รวมทั้งการสนับสนุนเต็มที่ของภาครัฐในการจารกรรมทางไซเบอร์ ภายในอีก 2 ปีข้างหน้า“จะไม่มีใครที่จะน่าเชื่อถือและไว้ใจในโลกไซเบอร์อีกต่อไป” (No-one left to trust in cyberspace) เพราะทุกสิ่งทุกอย่างในโลกไซเบอร์ดูจะเชื่อถือไม่ได้อีกแล้ว การหลอกลวงเอาข้อมูลผ่านรูปแบบและช่องทางต่างๆ ทางอินเทอร์เน็ต การดาวน์โหลดข้อมูลจากอินเทอร์เน็ต การปลอมข้อมูลในเว็บโซเชี่ยล ฯลฯ ล้วนทำให้เชื่อถือไม่ได้และยิ่งไปกว่านั้นเป็นการจารกรรมไซเบอร์ด้วยโปรแกรมและซอฟต์แวร์ที่สนับสนุนพัฒนาขึ้นโดยภาครัฐ เพื่อติดตามพฤติกรรมกลุ่มเป้าหมายที่ต้องการที่จะมีวงกว้างมากขึ้น การกล่าวหาไปมาระหว่างกันของประเทศมหาอำนาจที่ อ้างว่ารัฐบาลหรือหน่วยงานรัฐของฝ่ายตรงข้าม เป็นผู้แฮกระบบหรือล้วงข้อมูลความลับของประเทศตน ดังนั้นแนวโน้มการควบคุมหรือแทรกแซงระบบอินเทอร์เน็ต หรือ อาจเรียกได้ว่าปิดประเทศด้านไซเบอร์เฉพาะบางช่องทางที่ต้องการควบคุมจะมีให้เห็นมากขึ้น (“Threat Horizon Report”.(ออนไลน์). เข้าถึงได้จาก : https://www.acisonline.net/?p=5040)

งานวิจัยที่เกี่ยวข้อง

บุญมี บุญเอี่ยม ได้วิจัยเรื่องการนำอิทธิบาท 4 ไปใช้ในการทำงานของพนักงานศูนย์ควบคุมการบินภูเก็ต บริษัท วิทยุการบินแห่งประเทศไทย จำกัด เพื่อเปรียบเทียบการนำอิทธิบาท 4 ไปใช้ในการทำงาน จากตัวแปรประวัติการฝึกอบรม ผลการวิจัยพบว่าพนักงานศูนย์ควบคุมการบินภูเก็ต มีการนำอิทธิบาท 4 ไปใช้ในการทำงานโดยภาพรวม อยู่ในระดับมาก และมีการนำอิทธิบาท 4 ไปใช้ในการทำงานให้ประสบความสำเร็จโดยอาศัยแรงจูงใจภายนอกและใช้อิทธิบาท 4 มากน้อยขึ้นอยู่กับลักษณะของงาน วิธีการนำอิทธิบาท 4 ไปใช้ คือ ต้องสร้างฉันทะให้เกิดขึ้นในใจของตนเป็นเบื้องแรกก่อนเพื่อให้เกิดความชอบหรืออยากที่จะทำงานนั้นๆ จากนั้นต้องใช้วิริยะ คือความเพียรพยายามความอดทนในการต่อสู้กับอุปสรรคต่างๆ เพื่อที่จะทำงานนั้นให้สำเร็จตามเป้าหมาย ในขณะที่ทำงานต้องมีจิตตะคือ ความตั้งใจหรือเอาใจใส่ ความรับผิดชอบต่องานที่ทำ เพื่อให้ได้ผลงานที่ดีมี

คุณภาพ และสุดท้ายต้องใช้วิมังสา คือ พิจารณาไตร่ตรองงานที่ทำอย่างรอบคอบ มีการตรวจสอบข้อบกพร่องจากการทำงานแล้วหาทางแก้ไขปรับปรุงให้ดีขึ้นในครั้งต่อๆ ไป เพื่อให้การทำงานมีประสิทธิภาพสูงสุด

อำพน ธรรมโชติ ได้วิจัยเรื่อง การพัฒนาประสิทธิภาพการทำงานของพนักงาน การไฟฟ้าส่วนภูมิภาค จังหวัดเพชรบุรี ผลการวิจัยพบว่า การพัฒนาประสิทธิภาพการทำงานของพนักงานการไฟฟ้าส่วนภูมิภาคจังหวัดเพชรบุรี ด้านความรู้ความสามารถในงานภาพรวมอยู่ในระดับมาก โดยระดับความเป็นจริงมากเกี่ยวกับการแสวงหาความรู้เพิ่มเติมอยู่ตลอดเวลา เพื่อก้าวให้ทันกับการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นอย่างรวดเร็วเป็นอันดับหนึ่ง รองลงมาคือความสนใจศึกษานวัตกรรมต่างๆ เพื่อนำมาปรับปรุงระบบงานให้ดียิ่งขึ้น และการเข้ารับการอบรมตรงตามสายงานที่ปฏิบัติและสามารถนำมาประยุกต์ใช้ได้อย่างสัมฤทธิ์ผลตามลำดับ

พลตรี สุชาติ ผ่องพุฒิ ได้วิจัยเรื่อง แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย ผลการวิจัยพบว่า ภัยคุกคามที่กองทัพไทยให้ความสำคัญมี 4 รูปแบบ ขอบเขตการรองรับสงครามไซเบอร์ในมุมมองของกองทัพตามระดับภัยคุกคามแบ่งเป็น 3 ระดับ กำหนดกรอบในการดำเนินการรองรับสงครามไซเบอร์ในอนาคตไว้ 4 ด้าน แบ่งกรอบระยะเวลาออกเป็น 3 ระยะ เสนอแนะให้ปรับภารกิจในภาพรวมของหน่วยในกองทัพเพื่อการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกเป็น 2 รูปแบบคือ งานสนับสนุนการรบหลัก และงานในสายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ นำเสนอโครงสร้างหน่วยงานของกองทัพที่จะรองรับสงครามไซเบอร์อย่างเป็นรูปธรรมต่อไป

พลเรือตรี วิโรจน์ ธันวรักษ์กิจ ได้วิจัยเรื่อง แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย ผลการวิจัยพบว่า การดำเนินการในภาพรวมยังขาดการบูรณาการงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ บุคลากรมีจำนวนจำกัด เสนอแนะให้ สมช. เป็นหน่วยหลักรับผิดชอบการดำเนินการในภาพรวม เสนอแนะให้ตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ รวมทั้งการดำเนินการด้านอื่นๆ ควบคู่กันไป ผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต ผลักดันหน่วยงาน National CERT ให้เป็น ศูนย์ปฏิบัติการระดับประเทศ ผลักดันให้เป็นวาระแห่งชาติเร่งด่วน จะเป็นประโยชน์โดยตรงกับประเทศทำให้มีศักยภาพและขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

นาวาอากาศเอก รศ.ดร.ประสงค์ ปราณีตพลกรัง ได้วิจัยเรื่อง แผนยุทธศาสตร์การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ ผลการวิจัยพบว่า สาเหตุหลักของการเกิดภัยคุกคามด้านไซเบอร์ของกองทัพอากาศเกิดจากปัจจัยภายใน อาทิ กำลังพลที่รู้เท่าไม่ถึงการณ์และขาดความตระหนักรู้ และสาเหตุรองคือระบบหรือเทคโนโลยีที่ใช้งานเช่น ช่องโหว่

ในซอฟต์แวร์ ไวรัสหรือเวิร์ม ต่อมาเป็นสาเหตุจากปัจจัยภายนอกเช่นเกิดจากแฮกเกอร์ เกิดจากการก่ออาชญากรรมและเกิดจากการก่อการร้าย นอกจากนั้น ในงานวิจัยนี้ ยังได้ค้นพบ 4 ยุทธศาสตร์ และ 15 แผนงานวิจัยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดี งานวิจัยนี้ ยังได้ค้นพบดัชนีสภาพความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ สำหรับกองทัพอากาศ โดยอิง ITU & ABI Research และ ISO-27032 ประกอบกับการทำการสนทนากลุ่มกับผู้เชี่ยวชาญ ได้ดัชนี จำนวน 7 ด้าน ผลของการวิจัย สามารถนำไปใช้เป็นแนวทางกำหนดยุทธศาสตร์ และนโยบายเชิงรุกของกองทัพอากาศด้านความมั่นคงปลอดภัยทางไซเบอร์ได้

นาวาอากาศโท จตุชัย แพงจันทร์ ได้วิจัยเรื่อง รูปแบบการปฏิบัติการสงครามไซเบอร์และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ผลการวิจัยพบว่า แนวทางมีความเหมาะสมที่จะนำไปใช้เพื่อพัฒนาบุคลากร การจัดองค์กร และการพัฒนาขีดความสามารถของระบบอาวุธยุทโธปกรณ์ ให้มีความพร้อมที่จะปฏิบัติการสงครามไซเบอร์ได้ทุกรูปแบบและสามารถรองรับเทคโนโลยีที่ใช้ระบบเครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพ โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนวทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือ มีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ และมีความยั่งยืน บนพื้นฐานการพึ่งพาตนเอง

นาวาอากาศโท วัชรพงศ์ ธรรมรักษ์ ได้วิจัยเรื่อง ตัวแบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) สำหรับกองทัพอากาศ มีเนื้อหาโดยสรุปคือ จากการวิจัยพบว่า ระดับความพร้อมด้านบุคลากรของการรักษาความมั่นคงปลอดภัย เครือข่ายข้อมูลสารสนเทศต่างๆ มีค่าน้อยที่สุด และระดับความเสี่ยงด้านบุคลากรก็มีค่าสูงที่สุด ประกอบกับข้อมูลที่ได้รับพบว่าบุคลากรของกองทัพอากาศส่วนใหญ่ร้อยละ 96 ไม่เคยเข้ารับการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายข้อมูลสารสนเทศเลย ดังนั้น การที่กองทัพอากาศจะพัฒนาไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) ได้อย่างมีประสิทธิภาพและสมบูรณ์แบบนั้น กองทัพอากาศควรให้ความสนใจในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยระดับสากล ISO 27001 ผู้บังคับบัญชาทุกระดับต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และที่สำคัญต้องสร้างความตระหนักให้บุคลากรในทุกหน่วยงาน ได้รับรู้ถึงกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ถูกต้องควรจัดให้มีการฝึกอบรมบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศ เพื่อให้มีความรู้ มีทักษะ มีความชำนาญและมีความสามารถในการรับมือกับเหตุการณ์ ความเสี่ยง และภัยคุกคามด้านสารสนเทศต่างๆ ที่อาจจะเกิดขึ้นในอนาคตได้

สรุปแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้อง

1. สรุปแนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศขององค์กรและองค์กรสมัยใหม่

องค์กรเป็นกระบวนการ เมื่อมีการจัดองค์กรก็ต้องนำเทคนิคการบริหารจัดการมาใช้การบริหารเป็นส่วนหนึ่งของการจัดการองค์กรที่เหมาะสมที่สุดคือ องค์กรที่มีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้นๆ ซึ่งรวมถึงสภาพภูมิศาสตร์ วัฒนธรรม ค่านิยม ความเชื่อ การสนับสนุน และความต้องการของสมาชิกในองค์กรนั้นด้วย องค์กรสมัยใหม่ต้องเป็นองค์การแห่งการเรียนรู้ (Learning Organization) ซึ่งจะต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง 5 ระบบขององค์การแห่งการเรียนรู้อันได้แก่ การเรียนรู้ (Learning) องค์การ (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology) เนื่องจากการบริหารเป็นกระบวนการทำงานให้สำเร็จโดยใช้บุคคลอื่น พฤติกรรมของบุคคลในองค์การจึงมีความสำคัญต่อการเพิ่มผลผลิต และประสิทธิผลขององค์การ หากเข้าใจพฤติกรรมของมนุษย์ในองค์การอย่างถ่องแท้จะสามารถนำไปใช้ในการเพิ่มผลผลิตและความพึงพอใจของบุคลากร อันนำไปสู่การเพิ่มประสิทธิผลขององค์การในภาพรวม การบริหารจัดการเป็นสิ่งที่สำคัญต่อการปฏิบัติงาน ถ้าต้องการให้การบริหารจัดการและการปฏิบัติงานเกิดประสิทธิภาพสูงสุด สิ่งที่ทุกองค์การควรนำมาปรับใช้ในการบริหาร คือ การวางแผน (Planning) การจัดองค์การ (Organizing) การบังคับบัญชาสั่งการ (Commanding) การประสานงาน (Coordinating) และการควบคุม (Controlling)

ทฤษฎีการบริหารของ Henri Fayol การบริหารของ Dr.William Edwards Deming และกระบวนการบริหารของ Gulick L. and Urwick J. ต่างได้กล่าวถึง อำนาจหน้าที่และความรับผิดชอบของทุกส่วนที่เกี่ยวข้อง ให้ความสำคัญต่อเป้าหมายที่สำคัญขององค์การ คือ ความเป็นระเบียบ ความมั่นคง ความคิดริเริ่ม และความสามัคคี ผู้บริหารจะต้องมีคุณลักษณะพร้อมความสามารถทางร่างกาย จิตใจ ไหวพริบ การศึกษาหาความรู้ เทคนิคในการทำงานและประสบการณ์ต่างๆ ทฎษฎีที่เหมาะสมที่ควรนำมาใช้ในหน่วยงานของทหารคือ ทฤษฎีการบริหารของ Dr.William Edwards Deming คือ Plan-Do-Check-Action เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการวางแผนและตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้น และแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม การตรวจสอบที่นำไปสู่การแก้ไขปรับปรุง ทำให้ปัญหาที่เกิดขึ้นแล้วไม่เกิดซ้ำ หรือลดความรุนแรงของปัญหา ถือเป็นการนำความผิดพลาดมาใช้ให้เกิดประโยชน์

การนำระบบสมรรถนะมาใช้ในการบริหารองค์กรนับว่ามีประโยชน์อย่างยิ่งในยุคปัจจุบัน เพราะเป็นการสร้างบุคลากรให้มีความรู้ ความสามารถ ทัศนคติ ที่จะปฏิบัติหน้าที่ให้ประสบความ

สำเร็จและเกิดประสิทธิภาพกับองค์กรอย่างสูงสุด และผู้บริหารองค์กรจำเป็นต้องมีสมรรถนะด้านการบริหารอันประกอบด้วย การมีวิสัยทัศน์ การวางแผน ภาวะผู้นำ การแก้ปัญหาและการตัดสินใจ สุดท้ายต้องมีความสามารถในการบริหารความเปลี่ยนแปลงที่อาจเกิดขึ้นได้ทุกเวลาอีกด้วย

สภาพแวดล้อมในการทำงานเป็นสิ่งสำคัญที่จะทำให้บรรยากาศการทำงานภายในองค์มีประสิทธิภาพ เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอก ซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร ประกอบด้วย โครงสร้างการทำงานที่ดี มีระบบรางวัลตอบแทนที่เหมาะสม มีความเป็นอิสระในการทำงาน มีความอบอุ่นมีการสนับสนุนช่วยเหลือกันและกัน มีการยอมรับความขัดแย้ง ยอมรับฟังความคิดเห็นผู้อื่น และสุดท้ายต้องมีความรักในหมู่คณะด้วย

2. สรุปการจัดการความรู้และการบริหารความเสี่ยง

เพื่อให้การพัฒนาคน พัฒนางาน พัฒนาองค์กรให้มีประสิทธิภาพ องค์กรจะต้องมีการจัดการความรู้ (Knowledge Management) เพื่อรวบรวมความรู้ที่เป็นประโยชน์กับองค์กรหรือบุคคลและนำความรู้นั้นมาจัดการความรู้อย่างเป็นระบบอาจใช้เทคโนโลยีสารสนเทศมาช่วยในการจัดการความรู้หรือไม่ก็ได้ สำหรับในภาครัฐ (public Sector) มีความต้องการองค์ความรู้ ทั้งองค์ความรู้ภายใน (Internal) และองค์ความรู้ภายนอกองค์กร (External) มาใช้เพื่อประกอบการตัดสินใจและเพื่อการปรับปรุงการให้บริการของหน่วยงานภาครัฐ กรอบการบริหารความเสี่ยงองค์กรนั้นสามารถสะท้อนให้เห็นถึงนโยบายการบริหารจัดการและการกำกับดูแลกิจการของแต่ละองค์กร โดยหากมีการบริหารความเสี่ยงอย่างมีประสิทธิภาพ จะส่งผลให้สามารถบรรลุวัตถุประสงค์องค์กรทั้งในเชิงประสิทธิภาพและประสิทธิผลของงาน ผลที่ได้จากการประเมินความเสี่ยง คือ ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ดังนั้นทุกองค์กรควรจะจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารองค์กรให้มีประสิทธิภาพอีกทางหนึ่งด้วย

3. สรุปแนวคิดเกี่ยวกับภัยคุกคามรูปแบบใหม่

หลักการพื้นฐานในทำสงครามที่กองทัพของแต่ละประเทศ กำหนดให้หน่วยทหารของตนยึดถือเป็นแนวทางในการวางแผนและอำนวยการปฏิบัติการรบ เพื่อให้บรรลุความสำเร็จของการดำเนินสงครามเป็นส่วนรวม หลักการต่อสู้เบ็ดเสร็จ เป็นหลักการสงครามที่กองทัพไทยได้นำมาใช้ โดยนำมาจากบทเรียนจากการรบที่ผ่านมาของกองทัพไทยคือการผนึกกำลัง และกิจกรรมในการป้องกันประเทศทั้งมวลเข้าด้วยกันโดยใช้กองทัพเป็นแกนกลาง หลักการในข้อนี้คือ การจัดให้มีกำลังประจำถิ่น กำลังประชาชนเข้ามามีส่วนร่วมในการป้องกันประเทศ วัตถุประสงค์ของการใช้หลักการในข้อนี้ คือ การสร้างความเตรียมพร้อมในการที่จะเผชิญ ต่อภัยคุกคาม โดยเพิ่มสภาพความพร้อมรบและขยายกำลังเต็มขนาดได้อย่างรวดเร็ว

การปฏิบัติการทางทหารนอกเหนือการสงคราม (Military Operations Other Than War : MOOTW) ได้ถูกนำมาพัฒนามาเป็นหลักนิยม (Doctrine) ที่ใช้เป็นกรอบของแนวความคิดในการปฏิบัติการทางทหารที่ไม่ใช่เพื่อการรบ รูปแบบของการปฏิบัติการทางทหารได้มีการพัฒนาการเปลี่ยนไป จากเดิมที่กิจการทางทหารจะมุ่งเน้นแต่การปฏิบัติการในสงคราม เปลี่ยนมาเป็นการปฏิบัติการทางทหาร ในสงครามร่วมกับการปฏิบัติการทางทหารนอกเหนือการสงคราม ซึ่งเป็นการเปลี่ยนแปลงไปตามสภาวะแวดล้อมที่เปลี่ยนแปลง

ในสภาวะการณ์ปัจจุบัน โลกกำลังเผชิญอยู่กับภัยคุกคามทั้งสองด้านคือ ภัยคุกคามแบบดั้งเดิมที่ก่อให้เกิดการสะสมกำลังทหารกันต่อไปอย่างขมักเขม่นในหลายประเทศ กับภัยคุกคามรูปแบบใหม่ที่ต้องอาศัยแนวทางที่มีความสมดุลอันนำไปสู่ความมั่นคงที่ยั่งยืน ทำให้ผู้ที่เกี่ยวข้องกับการกิจการด้านความมั่นคงจะต้องทำงานที่หนักขึ้นเป็นสองเท่าหรือมากกว่า จะต้องมีมุมมองที่กว้างขวาง รอบรู้ มองปัญหาอย่างองค์รวม (Holistic) และรวมไปถึงการตอบสนองต่อสิ่งต่างๆ ได้อย่างรวดเร็ว เพราะความเกี่ยวเนื่องและความเกี่ยวพันของปัญหาต่างๆ ที่ถูกนำมาร้อยเข้าด้วยกันก่อให้เกิดภัยคุกคามใหม่ๆ ที่มีความสลับซับซ้อนมากยิ่งขึ้น แนวโน้มภัยคุกคามรูปแบบใหม่จะเป็นภัยที่มีความซับซ้อนหลากหลายมิติร่วมกัน และจะทวีความรุนแรงขึ้นเรื่อยๆ ภัยคุกคามนี้จะส่งผลกระทบต่อโครงสร้างของสังคมไทยโดยตรง ทั้งนี้การป้องกันและแก้ไขภัยคุกคามรูปแบบใหม่ปัจจุบันมีลักษณะต่างคนต่างทำ ไม่มีองค์กรที่ชัดเจนรับผิดชอบบูรณาการ นโยบาย ยุทธศาสตร์ และการแปลงนโยบายไปสู่การปฏิบัติที่ชัดเจน ทำให้ไม่สามารถป้องกัน ยับยั้ง และแจ้งเตือนภัยล่วงหน้าได้อย่างมีระบบตั้งแต่ก่อนเกิดเหตุการณ์ และเมื่อเกิดเหตุการณ์ภัยที่ร้ายแรง สังคมไทยอาจจะต้องตกอยู่ในสภาวะระส่ำระสาย เสียขวัญจนขยายวงกว้างไปสู่ความมั่นคงด้านอื่นๆ จึงมีความจำเป็นอย่างยิ่งที่กองทัพไทย ซึ่งเป็นกลไกทางด้านความมั่นคงของรัฐบาล ที่มีขีดความสามารถและศักยภาพสูงในการจัดการกับปัญหาความมั่นคงในลักษณะภัยคุกคามรูปแบบใหม่ที่เป็นองค์รวม (Holistic) จะได้เตรียมปรับบทบาทและโครงสร้างการจัดของกองทัพให้เหมาะสม เพื่อเผชิญกับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างเร่งด่วน เฉียบพลันในอนาคตอันจะทำให้กองทัพได้เป็นที่พึ่งและมีคุณค่ามากยิ่งขึ้นต่อสังคมไทย

4. สรุปแนวคิดเกี่ยวกับสงครามสารสนเทศ และ สงครามไซเบอร์

แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 โดย ISF ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ข้อสรุปหลักๆ ทั้งหมด 3 ประเด็น ได้แก่ 1. ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป 2. ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ 3. ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น องค์กรทั่วโลกต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลง และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่

ภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามมีการเปลี่ยนแปลงไปจากเดิมอย่างมาก ตลอดจนมีรูปแบบในการโจมตีเป้าหมายที่หลากหลาย มีรูปแบบมากมายในการปฏิบัติโดยไม่ต้องใช้กำลังพลมากมาย จนทำให้ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามแทบไม่ทัน ดังนั้นแนวความคิดและแนวทางในการป้องกันระบบและทรัพย์สินขององค์กรให้ได้ประสิทธิผล (effectiveness) จำเป็นอย่างยิ่งที่จะต้องปรับความคิดและปรับกลยุทธ์ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป องค์กรต้องเตรียมตัวรับมือกับภัยคุกคามใหม่ๆ ที่มาทางไซเบอร์ โดยผ่านช่องทาง Social Network, Mobile Devices หรือ Cloud Services ต่างๆ ต้องมีการวางแผนป้องกันจากภัยจากสงครามไซเบอร์ ควรนำระบบมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก นอกจากนั้นถ้าเราต้องการให้ระบบขององค์กรมั่นคงปลอดภัย เราควร “ลดเวลาในการตรวจจับลง” (decrease Detect time) และ “ลดเวลาในการตอบสนองลง” (decrease React time) ด้วยเช่นกัน ดังนั้นปัจจัยที่เราต้องนำมาพิจารณาไตร่ตรองอย่างรอบคอบในการวางแผนกลยุทธด้านความมั่นคงปลอดภัย (Security Strategy) ได้แก่ Protection (การป้องกัน) Detection (การตรวจจับ) Reaction (การตอบสนอง) และTime (เวลา) สำหรับการป้องกันอีกทางหนึ่งคือ ต้องมีการอัพเดทข้อมูลต่างๆ ของฝ่ายเราเป็นประจำ นานาชาติต้องมีมาตรการเตรียมความพร้อม เพื่อรับมือกับการโจมตีทางไซเบอร์ มียุทธศาสตร์ที่ครอบคลุมสงครามไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม

การแก้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศนั้น ควรมีมุมมอง 3 ด้าน (PPT Concept) ได้แก่ People, Process and Technology การปรับกระบวนการโดยการปฏิบัติตามมาตรฐาน ISO/IEC 27001:2013 เป็นการแก้ปัญหาที่ Process และ Technology แต่ปัจจัยสำคัญอยู่ที่ “มนุษย์” หรือ “People” ดังนั้นการเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศทั่วไป และการให้ความรู้ด้านภัยสารสนเทศ จึงเป็นเรื่องจำเป็นที่องค์กรต้องทำเป็นประจำทุกปี เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูงได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติ มีความพร้อมต่อการรับมือ “Incident” ต่างๆ ที่จะเกิดขึ้น นอกจากนี้กลไกกระบวนการและเทคนิคในการตรวจจับความผิดปกติในระบบแบบ Real-Time ก็มีความจำเป็นเช่นกัน เพราะฉะนั้นเราจึงต้องเตรียมพร้อมกับเหตุการณ์ที่ไม่พึงประสงค์อยู่ตลอดเวลา ก็จะช่วยให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของเรามีประสิทธิผลมากขึ้นโดยลำดับ สามารถทำให้องค์กรมี “Cyber Resilience” และ “Business Resilience” ในที่สุด

แนวโน้มในอนาคต ภัยคุกคามด้านไซเบอร์ (cyber threat) นับวันจะทวีความเข้มข้นและความรุนแรงมากยิ่งขึ้น ดังจะเห็นได้ว่า ที่ผ่านมามีเหตุการณ์การโจรกรรมทางไซเบอร์เกิดขึ้นบ่อยครั้งและต่อเนื่อง และมีแนวโน้มที่จะรุนแรงขึ้นเรื่อยๆ องค์กรสำคัญในหลายประเทศได้ถูกผู้ก่อเหตุทางไซเบอร์เจาะระบบและโจรกรรมข้อมูล เพื่อนำไปใช้หาประโยชน์ในทางมิชอบ การโจมตีทางไซเบอร์มีการยกระดับถึงขั้นการทำสงครามทางไซเบอร์ ด้วยเหตุนี้หลายประเทศเริ่มให้ความสำคัญกับการรักษาความปลอดภัยไซเบอร์ มีการกำหนดมาตรฐานระบบบริหารความมั่งคนปลอดภัยทางสารสนเทศ รวมถึง มีการรวมกลุ่มความร่วมมือเพื่อจัดการกับภัยไซเบอร์อย่างจริงจัง

5. สรุปยุทธศาสตร์การพัฒนาของกองทัพอากาศ

กองทัพอากาศได้กำหนดยุทธศาสตร์ในการพัฒนากองทัพด้วยการเป็น “กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ภายในปี 2562 ซึ่งถ้าดำเนินการตามยุทธศาสตร์จะทำให้กองทัพอากาศมีข้อมูลข่าวสารในลักษณะดิจิตอลและมีระบบสารสนเทศให้มีความเชื่อมโยงทั้งระบบ (Total integration) ที่สามารถตอบสนองต่อการปฏิบัติภารกิจเพื่อให้สามารถใช้ประโยชน์ได้ในทุกมิติ เชื่อมโยงข้อมูลผลการปฏิบัติภารกิจของทุกส่วนราชการภายในกองทัพอากาศได้อย่างมีประสิทธิภาพ การปฏิบัติที่กองทัพอากาศให้ความสำคัญอย่างยิ่งทางด้านสารสนเทศ คือ การปฏิบัติการโจมตีทางไซเบอร์ (Cyber Attack), การป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions) สำหรับการพัฒนาด้าน Cyber Warfare นั้น ต้องมีการพัฒนาทั้งด้าน Cyber Defense และ Cyber Attack เพื่อป้องกันระบบของ ทอ. และนำศักยภาพด้าน Cyber Attack มาสร้างความได้เปรียบในการปฏิบัติภารกิจต่างๆ ของ ทอ. นอกจากนั้นการพัฒนาด้านกำลังพล ได้นำระบบสมรรถนะ (Competency Model) มาเป็นเครื่องมือในการบริหารกำลังพลเพื่อเสริมสร้างศักยภาพของกำลังพลในทุกสายวิทยาการให้มีขีดสมรรถนะสูงขึ้น โดยมุ่งพัฒนากำลังพลที่ปฏิบัติงานด้านสงครามอิเล็กทรอนิกส์และสงครามไซเบอร์ ให้ความสำคัญกับการพัฒนาความรู้และทักษะการใช้ภาษาอังกฤษของกำลังพลในทุกระดับ

6. สรุปการปฏิบัติของหน่วยรับผิดชอบด้านสงครามไซเบอร์ของกองทัพอากาศ

กองทัพอากาศได้ให้ความสำคัญกับการปฏิบัติด้านสงครามไซเบอร์เป็นอันดับต้น จะเห็นได้จากนโยบายของผู้บัญชาการทหารอากาศที่ให้จัดทำยุทธศาสตร์และแผนปฏิบัติการเพื่อให้กองทัพอากาศมีความพร้อมรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ด้วยการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร กระบวนการทำงาน บุคลากร และหน่วยงานของ ทอ. กำหนดให้มีการพัฒนาด้านกำลังพล กระบวนการทำงาน และความรู้ให้กับกำลังพลด้านนี้โดยเฉพาะ เพื่อเพิ่มขีดความสามารถในการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ปรับปรุงโครงสร้างการจัดหน่วยใหม่ กำหนดให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เป็นกรมฝ่าย

อำนวยการและขึ้นการบังคับบัญชาโดยตรงกับผู้บัญชาการทหารอากาศ และกำหนดให้มีกองสงครามไซเบอร์ อยู่ภายใต้สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหน้าที่ดูและรับผิดชอบการปฏิบัติเกี่ยวกับสงครามไซเบอร์ของกองทัพอากาศ เนื่องจากเป็นหน่วยที่ตั้งขึ้นใหม่เมื่อเดือน ส.ค.57 จึงยังไม่มีแนวทางที่ชัดเจนในการปฏิบัติ ระบบงานต่างๆ ต้องใช้เวลาอีกระยะหนึ่งเพื่อให้การปฏิบัติมีความพร้อมมากยิ่งขึ้นและสามารถพึ่งพาตนเองได้

7. สรุปการเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

ขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ ณ เวลานี้ยังไม่สามารถกำหนดได้ แต่สามารถวิเคราะห์ภัยคุกคามและจุดอ่อนในด้านสงครามไซเบอร์ ของ ทอ. จากผลการวิจัยของ น.อ.รศ.ดร.ประสงค์ ปราณีตพลกรัง พบว่า สถานภาพโดยรวม ด้านความมั่นคงปลอดภัยทางไซเบอร์ของ ทอ. ในประเด็น บุคลากร กระบวนการและ เทคโนโลยี นั้น ทอ. ยังขาดแคลนทรัพยากรด้านนี้อยู่ในระดับมาก ปัญหาภัยคุกคามหลักคือการเข้าควบคุมระบบของโครงสร้างพื้นฐานสำคัญยิ่งยวด เพื่อให้ใช้งานไม่ได้ตามปกติ สาเหตุหลักของการเกิดภัยคุกคามทางไซเบอร์มาจากกำลังพลในหน่วยงานขาดความรู้ความเข้าใจ รองลงมาเกิดจากไวรัสหรือเวิร์ม อย่างไรก็ตามเพื่อให้กองทัพอากาศมีความพร้อมในการปฏิบัติด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ อันดับแรกได้กำหนดยุทธศาสตร์พร้อมทั้งมาตรการ แผนงานและโครงการต่างๆ เพื่อผลักดันให้ทุกหน่วยงานมีความพร้อมในการปฏิบัติด้านสงครามไซเบอร์ และพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ซึ่งจะเป็นการทวีกำลังทางทหารในการต่อสู้ในสงครามที่อาจจะเกิดขึ้นในอนาคต จึงต้องเตรียมความพร้อมการปฏิบัติด้านสงครามไซเบอร์ไว้ตั้งแต่ยามปกติ ประกอบด้วย 3 ส่วน คือ คน (People), กระบวนการ (Process) และเทคโนโลยี (Technology) ซึ่งองค์ประกอบดังกล่าวสามารถนำมากำหนดหลักการในการเตรียมกำลังให้พร้อมประกอบด้วย นักรบไซเบอร์ และ อาวุธไซเบอร์ ทั้งสองส่วนจะต้องมีการสรรหา ทำการฝึกและทดสอบให้มีความพร้อมอยู่เสมอ อีกทั้งนำเทคโนโลยีใหม่มาปรับปรุงการปฏิบัติให้สามารถรับมือกับสงครามไซเบอร์ในปัจจุบันและในอนาคตให้ได้ โดยสรุปแล้วการเตรียมรับมือกับภัยจากไซเบอร์ตอนนี้ไม่ใช่เป็นแค่ทางเลือก แต่เป็นสิ่งจำเป็นที่สุดที่ต้องทำเลยทันที

8. สรุปงานวิจัยที่เกี่ยวข้อง

ในเรื่องการปฏิบัติงานให้มีประสิทธิภาพ สามารถนำอิทธิบาท 4 ไปใช้ คือ ฉันทะ วิริยะ จิตตะและวิมังสาโดยจะต้องเข้าใจในงานที่ทำมีความเพียรพยายามทำให้สำเร็จมีความตั้งใจรับผิดชอบต่อหน้าที่ พิจารณาไตร่ตรองงานที่ทำอย่างรอบคอบ มีการตรวจสอบข้อบกพร่องจากการทำงานแล้วหาทางแก้ไขปรับปรุงให้ดีขึ้นในครั้งต่อๆ ไป และต้องมีการทำงานเป็นทีม มีการปรึกษาหารือกัน มีการจัดเก็บความรู้ มีการถ่ายทอดความรู้ให้กับผู้ที่เข้ามาทำหน้าที่ใหม่

ภัยคุกคามด้านไซเบอร์ที่กองทัพไทยให้ความสำคัญมี 4 รูปแบบ ขอบเขตการรองรับสงครามไซเบอร์ในมุมมองของกองทัพตามระดับภัยคุกคามแบ่งเป็น 3 ระดับ กำหนดกรอบในการ

ดำเนินการรองรับสงครามไซเบอร์ในอนาคตไว้ 4 ด้าน แบ่งกรอบระยะเวลาออกเป็น 3 ระยะ เสนอแนะให้ปรับภารกิจในภาพรวมของหน่วยในกองทัพเพื่อการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกเป็น 2 รูปแบบคือ งานสนับสนุนการรบหลัก และงานในสายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ นำเสนอโครงสร้างหน่วยงานของกองทัพที่จะรองรับสงครามไซเบอร์อย่างเป็นรูปธรรมต่อไป

แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย พบว่าการดำเนินการในภาพรวมยังขาดการบูรณาการงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ บุคลากรมีจำนวนจำกัด เสนอแนะให้ สมช. เป็นหน่วยหลักรับผิดชอบการดำเนินการในภาพรวม เสนอแนะให้ตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต ผลักดันหน่วยงาน National CERT ให้เป็นศูนย์ปฏิบัติการระดับประเทศ

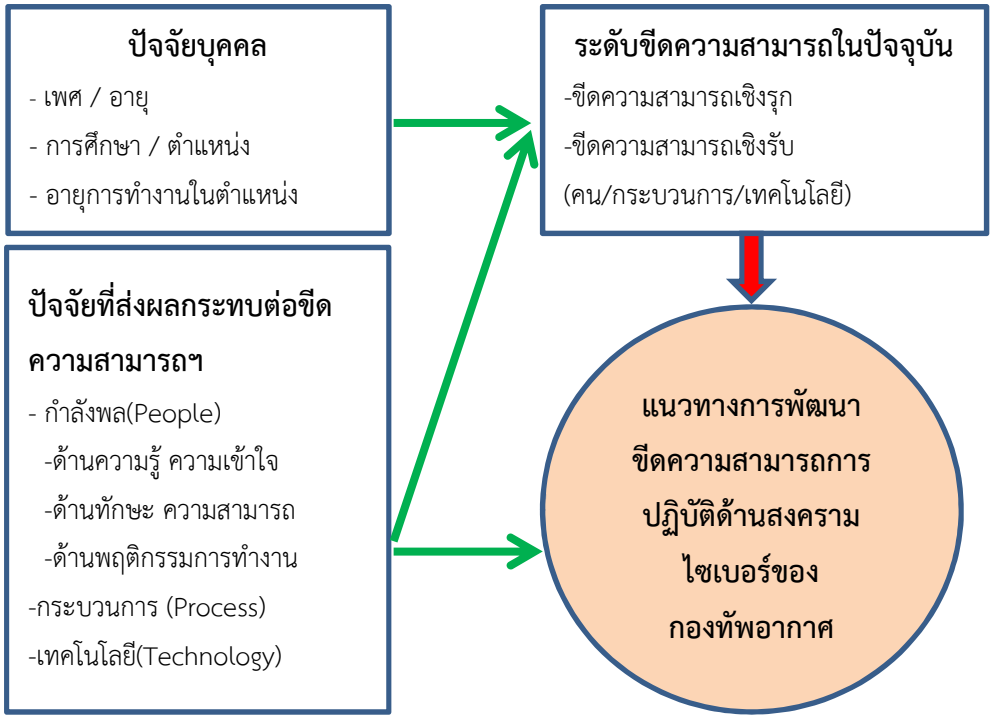
กองทัพอากาศ สาเหตุหลักของการเกิดภัยคุกคามด้านไซเบอร์ของกองทัพอากาศเกิดจากปัจจัยภายใน อาทิ กำลังพลที่รู้เท่าไม่ถึงการณ์และขาดความตระหนักรู้ และสาเหตุรองคือระบบหรือเทคโนโลยีที่ใช้งานเช่น ช่องโหว่ในซอฟต์แวร์ ไวรัสหรือเวิร์ม ต่อมาเป็นสาเหตุจากปัจจัยภายนอกเช่น เกิดจากแฮกเกอร์ เกิดจากการก่ออาชญากรรมและเกิดจากการก่อการร้าย ผลของการวิจัยสามารถนำไปใช้เป็นแนวทางกำหนดยุทธศาสตร์ และนโยบายเชิงรุกของกองทัพอากาศด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนวทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือ มีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ และมีความยั่งยืน บนพื้นฐานการพึ่งพาตนเอง

ระดับความพร้อมด้านบุคลากรของการรักษาความมั่นคงปลอดภัยเครือข่ายข้อมูลสารสนเทศต่างๆ มีค่าน้อยที่สุด และระดับความเสี่ยงด้านบุคลากรก็มีค่าสูงที่สุด ประกอบกับข้อมูลที่ได้รับพบว่า บุคลากรของกองทัพอากาศส่วนใหญ่ร้อยละ 96 ไม่เคยเข้ารับการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายข้อมูลสารสนเทศเลย ดังนั้น การที่กองทัพอากาศจะพัฒนาไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) ได้อย่างมีประสิทธิภาพและสมบูรณ์แบบนั้น ควรให้ความสนใจในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยระดับสากล ISO 27001 ผู้บังคับบัญชาทุกระดับต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยสารสนเทศและสร้างความตระหนักให้บุคลากรในทุกหน่วยงาน ได้รับรู้ถึงกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ถูกต้อง ควรจัดให้มีการฝึกอบรมบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้มีความรู้ มีทักษะ มีความชำนาญและมีความสามารถในการรับมือกับเหตุการณ์ ความเสี่ยง และภัยคุกคามด้านสารสนเทศต่างๆ ที่อาจจะเกิดขึ้นในอนาคตได้

กรอบแนวความคิดในการวิจัย

พิจารณาจากปัจจัยส่วนบุคคลที่เกี่ยวข้อง ปัจจัยที่ส่งผลต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ และระดับขีดความสามารถของหน่วยในปัจจุบัน โดยนำข้อมูลที่ได้จากการรวบรวมแล้วนำมาวิเคราะห์ให้ได้แนวทางในการพัฒนาขีดความสามารถของการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศต่อไป ดังแผนภาพที่ 2-2

แผนภาพที่ 2-2 กรอบแนวความคิดในการวิจัย



บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยแบบผสมผสาน (Mixed Method Procedures) ประกอบด้วย การวิจัยเชิงคุณภาพ (Qualitative research) และการวิจัยเชิงปริมาณ (Quantitative Research) เป็นการศึกษาเพื่อค้นหาแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยศึกษาจากวรรณกรรมที่เกี่ยวข้อง และจากการสัมภาษณ์เชิงลึกและการสนทนากลุ่มระหว่างผู้บริหารหน่วยรวมทั้งผู้เชี่ยวชาญและผู้ทรงคุณวุฒิภายในกองทัพอากาศ เพื่อนำมากำหนดเป็นแนวทางที่เหมาะสมในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยมีรายละเอียดของการวิจัยดังต่อไปนี้

ขั้นตอนการดำเนินการวิจัย

1. ศึกษาแนวคิด ทฤษฎีการจัดการและการบริหารองค์การที่มีประสิทธิภาพ
2. ศึกษารูปแบบ ทฤษฎีหลักการทำสงครามรูปแบบต่างๆ และแนวคิดเกี่ยวกับภัยคุกคามรูปแบบใหม่ในวรรณกรรมที่เกี่ยวข้อง
3. สัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ทรงคุณวุฒิที่เป็นผู้บริหารระดับสูง ผู้บริหารระดับกลางของหน่วยที่เกี่ยวข้องด้านการสื่อสารและการปฏิบัติด้านสงครามไซเบอร์ และจัดการสนทนากลุ่ม (Focus Group) ระหว่างผู้บริหารและผู้เชี่ยวชาญ
4. วิเคราะห์ผลที่ได้จากแบบสอบถามผู้ที่เกี่ยวข้องกับการปฏิบัติด้านสงครามไซเบอร์
5. วิเคราะห์ผลที่ได้จากวรรณกรรมที่เกี่ยวข้อง จากการสัมภาษณ์และจากการสนทนากลุ่ม
6. วิเคราะห์แนวทางเพื่อพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
7. สรุปแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

แหล่งข้อมูล

1. ขอบเขตพื้นที่

1.1 หน่วยขึ้นตรงกองทัพอากาศในที่ตั้งดอนเมือง กรุงเทพมหานคร เฉพาะที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารประกอบด้วยกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ดำเนินการเลือกจากการสุ่มตัวอย่าง

1.2 หน่วยขึ้นตรงกองทัพอากาศนอกที่ตั้งดอนเมืองและต่างจังหวัด ประกอบด้วย กองบิน 10 กองบินและ 1 โรงเรียนการบิน ดำเนินการเลือกจากการสุ่มตัวอย่าง

2. ผู้ให้ข้อมูลสำคัญ

2.1 ผู้บังคับบัญชาชั้นสูงของกองทัพอากาศ

2.2 ผู้บังคับบัญชาระดับเจ้ากรมหรือรองเจ้ากรมที่รับผิดชอบงานระบบเทคโนโลยีสารสนเทศและระบบสื่อสารกองทัพอากาศ

การเก็บรวบรวมข้อมูล

การสัมภาษณ์ ผู้วิจัยสัมภาษณ์ด้วยตนเอง โดยการบันทึกข้อมูลด้วยการจดบันทึก และหรือบันทึกด้วยเครื่องบันทึกเสียง และ/หรือภาพเคลื่อนไหว

การสนทนากลุ่ม ผู้วิจัยได้จัดสนทนากลุ่มและบันทึกข้อมูลด้วยการจดบันทึก

การแจกแบบสอบถาม โดยแจกจ่ายไปยังผู้ปฏิบัติงานที่เกี่ยวข้องโดยตรง ดำเนินการเก็บรวบรวมข้อมูลจากแบบสอบถามด้วยตนเองและรับคืนพร้อมตรวจสอบความสมบูรณ์ของการกรอกแบบสอบถาม

เครื่องมือที่ใช้ในการวิจัย

การวิจัยนี้จะเก็บรวบรวมข้อมูลจากการศึกษาวรรณกรรมที่เกี่ยวข้องโดยผู้ดำเนินการวิจัย และดำเนินการการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ (In-depth Interview) โดยใช้แนวคำถามปลายเปิดแบบมีโครงสร้าง หลังจากนั้นจะใช้วิธีการวิเคราะห์เนื้อหา (Content analysis) ในการวิเคราะห์ข้อมูลที่ได้จากทั้ง 2 แหล่ง

1. การสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ (In-depth Interview)

เป็นการสัมภาษณ์ผู้บริหารระดับสูง ผู้บริหารระดับกลาง และผู้ที่มีความรู้ความชำนาญด้านการสื่อสารและการปฏิบัติด้านสงครามไซเบอร์ จากบุคลากรภายในกองทัพอากาศ จำนวน 10 คน ดังมีรายชื่อต่อไปนี้ (บางท่านไม่สะดวกในการให้สัมภาษณ์แต่ตอบคำถามตามแบบสัมภาษณ์)

1.1 พล.อ.อ.จอม รุ่งสว่าง	เสนาธิการทหารอากาศ
1.2 พล.อ.ท.พิชัย เขม้นจันทร์	เจ้ากรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ
1.3 พล.อ.ต.จิโรจ บำรุงลาภ	ผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.4 พล.อ.ต.ชาวลา ราชวงศ์	ผู้อำนวยการสำนักระบบบัญชาการและควบคุมกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.5 น.อ.ทรงพล พรหมวา	รองผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.6 น.อ.อัศวิน รุจาคม	รองผู้อำนวยการสำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

1.7 น.อ.รศ.ดร.ประสงค์ ปราณีตพลกรัง	รองศาสตราจารย์ กองการศึกษา โรงเรียนนายเรืออากาศ
1.8 น.อ.วิสุทธิ์ สมภักดี	ผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.9 น.อ.อมร ชมเชย	รองผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.10 น.อ.นิวัต เนียมพลอย	รองผู้อำนวยการ กองนโยบายและแผน สำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

2. แนวคำถามสำหรับการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ (In-depth Interview)

ตารางที่ 3-1 แนวคำถามสำหรับสัมภาษณ์เชิงลึกผู้บริหารระดับสูง ผู้บริหารระดับกลางและผู้เชี่ยวชาญ

วัตถุประสงค์การวิจัย	ตัวแปรการวิจัย	คำสัมภาษณ์
1. วิเคราะห์ขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ	- กำลังพล - กระบวนการ - เทคโนโลยี - การจัดองค์กร - วิสัยทัศน์ หลักนิยม	1. ความคิดเห็นเกี่ยวกับการปฏิบัติต่างๆด้านสงครามไซเบอร์ ซึ่งเป็นภารกิจใหม่ของกองทัพอากาศและการจัดหน่วยรับผิดชอบงานด้านนี้
2. วิเคราะห์ปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ	- กำลังพล - กระบวนการ - เทคโนโลยี - การจัดองค์กร - งบประมาณ	2. ความคิดเห็นเกี่ยวกับปัจจัยที่มีผลกระทบต่อการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วยขึ้นตรงและหน่วยอื่นๆ เช่น กำลังพล เครื่องมือ การบริหารจัดการ งบประมาณ เป็นต้น
3. วิเคราะห์แนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ	- กำลังพล - กระบวนการ - เทคโนโลยี - การจัดองค์กร - วิสัยทัศน์ หลักนิยม นโยบายและงบประมาณ	3. ความคิดเห็นในการปรับปรุงและพัฒนาการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วยให้มีประสิทธิภาพ เช่น กำลังพล เครื่องมือ การบริหารจัดการ งบประมาณ เป็นต้น

3. การทดสอบความเที่ยงตรงของเครื่องมือที่ใช้ในการวิจัย

3.1 ความเที่ยงตรงตามเนื้อหา (Content Validity)

ผู้วิจัยได้ดำเนินการทดสอบความเที่ยงตรงตามเนื้อหา (Content Validity) ของแบบสอบถาม โดยใช้ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (Item-Objective Congruence Index : IOC) และการทดสอบความเชื่อมั่น (Reliability) ของแบบสอบถาม จากนั้นนำไปเก็บข้อมูลโดยเก็บรวบรวมข้อมูล เมื่อสร้างแบบสอบถามเสร็จเรียบร้อยแล้ว นำไปให้ผู้ทรงคุณวุฒิจำนวน 5 ท่านพิจารณาความเที่ยงตรง (Validity) ของเครื่องมือ โดยหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์หรือ IOC ตามวิธีของโรวิเนลลิและแฮมบิลตัน (ศรัยกร บุษยะมา. 2545) ซึ่งคะแนนแบ่งออกเป็น 3 ระดับดังต่อไปนี้คือ

แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 1
ไม่แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 0
แน่ใจว่าไม่มีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ -1

หลังจากนั้นจึงนำแบบสอบถามส่งให้ผู้ทรงคุณวุฒิประเมินความสอดคล้องของข้อคำถามกับวัตถุประสงค์ และนำมาหาค่าความสอดคล้องโดยใช้สูตรในสมการ 3.1

$$IOC = \frac{\sum R}{n}$$

เมื่อ R = ผลคูณของคะแนนกับจำนวนผู้ทรงคุณวุฒิ
n = จำนวนผู้ทรงคุณวุฒิ

โดยเปรียบเทียบกับเกณฑ์มาตรฐานความเที่ยงตรงของเคิลเคนดอล, กรูเบอร์และจอร์นสัน ซึ่งได้เสนอมาตรการการประเมินผลดังชีความสอดคล้องของแบบสอบถามกับจุดประสงค์ไว้ดังนี้

ค่าเฉลี่ย 0.00 – 0.49 ความสอดคล้องอยู่ในระดับต่ำ
ค่าเฉลี่ย 0.50 – 0.69 ความสอดคล้องอยู่ในระดับยอมรับ
ค่าเฉลี่ย 0.70 – 0.79 ความสอดคล้องอยู่ในระดับดี
ค่าเฉลี่ย 0.80 – 1.00 ความสอดคล้องอยู่ในระดับดีมาก

ในที่นี้ผู้ทรงคุณวุฒิจำนวน 5 ท่าน ที่ทำการประเมินได้แก่

1. น.อ.ดร.นภัทร์ แก้วนาค ตำแหน่ง อาจารย์อาวุโส วิทยาลัยการทัพอากาศ
2. รศ.ดร.พงษ์ หรดาล ตำแหน่ง อธิการบดี มหาวิทยาลัยราชภัฏพระนคร
3. ดร.พิลาศพงษ์ ทรัพย์เสริมศรี ตำแหน่ง ผู้อำนวยการหลักสูตรวิทยาศาสตรมหาบัณฑิตสาขาวิชาระบบสารสนเทศคอมพิวเตอร์ มหาวิทยาลัยศรีปทุม
4. น.อ.ผศ.ดร พาห์รณ สงวนโภคัย ตำแหน่ง ผู้อำนวยการ กองวิชาคณิตศาสตร์และคอมพิวเตอร์ โรงเรียนนายเรืออากาศ
5. น.อ.รศ.ดร.สัลยุทธ์ สว่างวรรณ ตำแหน่ง รองศาสตราจารย์ กองการศึกษา โรงเรียนนายเรืออากาศ

3.2 ความเชื่อมั่น (Reliability)

การทดสอบความเชื่อมั่นของแบบสอบถามการวิจัยครั้งนี้ เป็นการหาค่าความคงที่ภายใน (Internal Consistency) ของแบบสอบถาม เพราะใช้แบบสอบถามเพียงครั้งเดียว วิธีการคำนวณจะใช้วิธีการของ ครอนบาซ แอลฟา (บุญเรียง ขจรศิลป์, 2547) (Cronbach's Alpha) หรือเรียกสั้นๆ ว่า แอลฟา (Alpha) ดังสมการที่ 3.2

$$\sim = \left(\frac{k}{k-1}\right)\left[1-\frac{\sum_{i-1}^{k} S_i^2}{S^2}\right]$$

เมื่อ

$\sim$ หมายถึงสัมประสิทธิ์ความเที่ยงหรือสัมประสิทธิ์แอลฟาของเครื่องมือ

K หมายถึง จำนวนข้อคำถาม

S_i^2 หมายถึง ความแปรปรวนของข้อมูลแต่ละข้อ

S^2 หมายถึง ความแปรปรวนของข้อมูลที่วัดได้จากแบบวัดทั้งฉบับของผู้ถูกวัดทั้งหมด

ค่าแอลฟาที่ได้จะแสดงถึงระดับความคงที่ของแบบสอบถาม โดยจะมีค่าระหว่าง $0 \leq \sim \leq 1$ ค่าความเชื่อมั่นของเครื่องมือที่ใช้ในการวิจัย มีค่าความเชื่อมั่นตั้งแต่ 0.80 ขึ้นไป ถือว่ามีค่าความเชื่อมั่นสูง (ธีรวุฒิ เอกะกุล, 2545, หน้า 183)

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลสำหรับการวิจัยจะแบ่งออกเป็น 3 ส่วน คือ ส่วนแรกเป็นข้อมูลที่ได้จากการศึกษาวรรณกรรมจะใช้การวิเคราะห์เนื้อหา (Content analysis) ส่วนที่สองเป็นข้อมูลที่ได้จากการส่งแบบสอบถามตรงไปยังผู้ปฏิบัติงานที่เกี่ยวข้องกับการปฏิบัติด้านสารสนเทศ ส่วนที่สามเป็นข้อมูลที่ได้จากความคิดเห็นของผู้บริหารระดับสูง ผู้บริหารระดับกลางและผู้เชี่ยวชาญ ที่สนทนาหรือตอบแบบสัมภาษณ์เพื่อตอบคำถามแบบปลายเปิด จะใช้การวิเคราะห์เนื้อหาเช่นกัน หลังจากนั้นจึงสรุปเป็นแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

1. การวิเคราะห์ข้อมูลเชิงปริมาณ (Quantitative Analysis) โดยนำแบบสอบถามที่เก็บรวบรวมมาตรวจสอบและลงรหัสในแบบสอบถามทุกข้อ และนำข้อมูลที่ลงรหัสไปวิเคราะห์ข้อมูลโดยใช้โปรแกรมสำเร็จรูปเพื่อการวิจัยทางสังคมศาสตร์ (Statistical Package for the Social Science : SPSS) ในการประมวลและจัดทำตารางวิเคราะห์ทางสถิติเพื่อนำเสนอข้อมูลและสรุปผลการวิจัย ซึ่งสามารถประมวลผลโดยใช้สถิติ ดังนี้

1.1 ส่วนที่ 1 การวิเคราะห์การนำเสนอข้อมูลทั่วไป ได้แก่ เพศ อายุ ระดับการศึกษา เป็นต้น โดยใช้สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ย ร้อยละ และ ส่วนเบี่ยงเบนมาตรฐาน

1.2 ส่วนที่ 2 การวิเคราะห์ความถี่ เกี่ยวกับความรู้ ความเข้าใจ ทักษะ ความสามารถ ความพึงพอใจ เกี่ยวกับการปฏิบัติด้านสารสนเทศและด้านสงครามไซเบอร์กองทัพอากาศ โดยแบ่งระดับคำตอบเป็น 5 ระดับตาม Likert Scale ดังนี้

ระดับปัจจัยที่ส่งผลต่อความรู้ ความสามารถ ความพอใจ	**คะแนน**
น้อยที่สุด	1
น้อย	2
ปานกลาง	3
มาก	4
มากที่สุด	5

จากการให้คะแนนตาม Likert Scale ข้างต้น สามารถกำหนดค่าน้ำหนักคะแนนได้โดยคิดจากสูตรการหาค่าพิสัย ได้ตามสูตร ดังนี้

$$\frac{\text{ค่าพิสัย}}{\text{จำนวนช่วงชั้น}} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนช่วงชั้น}}$$

$$= \frac{5-1}{5}$$

$$= \mathbf{0.80}$$

ดังนั้นจึงสามารถแบ่งคะแนนค่าเฉลี่ยเพื่อการแปลผลได้ดังนี้

ช่วงคะแนน 4.21-5.00 หมายถึง มีระดับความรู้ ความสามารถ มากที่สุด
ช่วงคะแนน 3.41-4.20 หมายถึง มีระดับความรู้ ความสามารถ มาก
ช่วงคะแนน 2.61-3.40 หมายถึง มีระดับความรู้ ความสามารถ ปานกลาง
ช่วงคะแนน 1.81-2.60 หมายถึง มีระดับความรู้ ความสามารถ น้อย
ช่วงคะแนน 1.00-1.80 หมายถึง มีระดับความรู้ ความสามารถ น้อยมาก

1.3 ส่วนที่ 3 วิเคราะห์ประเด็นเกี่ยวกับข้อเสนอแนะเพื่อเป็นแนวทางในการพัฒนาขีดความสามารถในการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

2. การวิเคราะห์ข้อมูลเชิงคุณภาพ(Qualitative Analysis) ประกอบด้วยขั้นตอนต่างๆ ตามลำดับ ได้แก่

ขั้นตอนที่ 1 การตรวจสอบข้อมูล
ขั้นตอนที่ 2 การทำดัชนีข้อมูล
ขั้นตอนที่ 3 การทำข้อสรุปชั่วคราวและการกำจัดข้อมูล
ขั้นตอนที่ 4 การสร้างบทสรุปและพิสูจน์บทสรุป

ซึ่งหลังจากที่ผู้วิจัยได้เก็บรวบรวมข้อมูลแล้ว จะต้องตรวจสอบข้อมูลและการวิเคราะห์ข้อมูล โดยกระทำไปพร้อมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูลใช้แนวคิดทฤษฎีเป็นกรอบในการวิเคราะห์โดยวิธีการหลักที่ใช้มี 2 วิธี คือ วิธีแรกเป็นการวิเคราะห์ข้อมูลโดยการตีความสร้างข้อสรุปแบบอุปนัย ซึ่งได้จากการสังเกตและการสัมภาษณ์ที่ได้จดบันทึกไว้จากสิ่งที่เป็นรูปธรรมหรือ

ปรากฏการณ์ที่มองเห็น วิธีที่สอง เป็นการวิเคราะห์ข้อมูลโดยการวิเคราะห์เนื้อหา ซึ่งได้จากการศึกษาเอกสาร ต้องคำนึงถึงบริบท หรือสภาพแวดล้อมของข้อมูลเอกสารที่นำมาวิเคราะห์ประกอบด้วยว่ามีการเปลี่ยนแปลงไปอย่างไร

3. การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม

ใช้การสรุปประเด็นต่างๆ โดยนำข้อมูลที่ได้จากผู้ให้ข้อมูลสำคัญ และข้อมูลที่ได้จากการสนทนากลุ่มมาเปรียบเทียบและตรวจสอบความแน่นอนของข้อมูล (Data Triangulation) เพื่อยืนยันความน่าเชื่อถือของข้อมูลและวิเคราะห์ข้อมูลด้วยการสรุป

บทที่ 4
ผลการวิจัย

การวิจัยเรื่อง “แนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ” การวิจัยแบบผสมผสาน (Mixed Method Procedures) ประกอบด้วยการวิจัยเชิงคุณภาพ (Qualitative research) และการวิจัยเชิงปริมาณ (Quantitative Research) โดยในบทนี้ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยใช้เทคนิคการวิเคราะห์เนื้อหา (Content analysis) โดยข้อมูลที่นำมาวิเคราะห์ได้จากการเก็บรวบรวมข้อมูลจาก 3 ส่วน คือ ส่วนแรก จากแบบสอบถามที่ส่งไปยังหน่วยเกี่ยวข้องที่ปฏิบัติด้านสารสนเทศและด้านไซเบอร์ ส่วนที่สอง จากหนังสือ ตำรา วารสาร เว็บไซต์ ยุทธศาสตร์กองทัพอากาศ นโยบายผู้บัญชาการทหารอากาศ งานวิจัยที่เกี่ยวข้อง และส่วนที่สามจากข้อมูลที่ได้รับจากการสัมภาษณ์เชิงลึก (In-depth interview) ผู้บริหารระดับสูง ระดับกลาง และผู้เชี่ยวชาญด้านการสื่อสารและการปฏิบัติด้านสงครามไซเบอร์ และจากการสนทนากลุ่ม เพื่อนำมาสรุปเป็นแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ ตามกระบวนการวิจัยที่ได้เสนอไว้ในบทที่ 3 เพื่อนำไปสู่การวิเคราะห์และสรุปผลการวิจัยในลำดับต่อไป

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลนำมาจาก 3 ส่วน คือส่วนแรกจากแบบสอบถามที่ส่งไปยังหน่วยขึ้นตรงของกองทัพอากาศที่ปฏิบัติงานด้านสารสนเทศและด้านไซเบอร์ ส่วนที่สองเป็นข้อมูลจากเอกสาร ระเบียบ คำสั่ง หลักนิยม วรรณกรรม และงานวิจัยที่เกี่ยวข้อง และส่วนที่สามเป็นข้อมูลจากการสัมภาษณ์ผู้บริหารระดับสูง ผู้บริหารระดับกลางและจากการสนทนากลุ่ม จากนั้นจึงนำข้อมูลมาวิเคราะห์โดยใช้เทคนิคการวิเคราะห์เนื้อหา (Content analysis) โดยมุ่งเน้นข้อมูลเกี่ยวกับตัวแปรอิสระในการวิจัย ซึ่งประกอบด้วย ตัวแปรแรกคือปัจจัยที่ส่งผลกระทบต่อการปฏิบัติด้านสงครามไซเบอร์ แบ่งออกเป็น 3 องค์ประกอบย่อย คือ กำลังพล (ความรู้ ทักษะ ความเชี่ยวชาญในการทำงาน พฤติกรรมในการทำงาน) การบริหาร/การจัดการ และเทคโนโลยี ตัวแปรที่สองคือระดับขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ตัวแปรย่อยคือ กำลังพล (ความรู้ ทักษะ ความเชี่ยวชาญในการทำงาน พฤติกรรมในการทำงาน) การบริหาร/การจัดการ และ เทคโนโลยี จากการวิเคราะห์สามารถสรุปผลได้ดังนี้

1. วิเคราะห์จากแบบสอบถาม

1.1 ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตารางที่ 4-1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ข้อมูลบุคคล	รายละเอียด	จำนวน	ร้อยละ
เพศ	ชาย	201	91
	หญิง	22	9
อายุ	25-35 ปี	100	44.8
	36-46 ปี	59	26.5
	47 ปีขึ้นไป	64	28.7
วุฒิการศึกษา	ต่ำกว่าปริญญาตรี	44	19.7
	ปริญญาตรี	145	65
	สูงกว่าปริญญาตรี	34	15.2
ระดับชั้นยศ	จ.อ.- พ.อ.อ.(พิเศษ)	71	34.5
	ร.ต.- รอ.	61	27.4
	น.ต.-น.อ.	77	34.6
	น.อ.(พิเศษ) ขึ้นไป	8	3.6
ตำแหน่ง	ระดับกรม	9	4
	ระดับสำนัก	6	2.7
	ระดับกอง	44	19.7
	ระดับแผนก	108	48.4
	ระดับฝ่าย	45	20.2
	ลูกจ้าง/พนักงานราชการ	8	3.6
	อื่นๆ	3	1.3
อายุการปฏิบัติงานในตำแหน่ง	น้อยกว่า 5 ปี	129	57.8
	6-10 ปี	42	18.8
	11-15 ปี	24	10.8
	16-20	10	4.5
	21 ปีขึ้นไป	18	8.1

ผู้วิจัยได้ตรวจสอบคุณภาพของแบบสอบถามด้วยการหาค่าดัชนีความคล้อยตามวัตถุประสงค์(Index of Item Objective Congruence :IOC) และการหาความเชื่อมั่นด้วยการหาค่าสัมประสิทธิ์แอลฟ่าของครอนบัค(Cronbach’s Alpha Coefficient) ซึ่งแบบสอบถามสำหรับการวิจัยนี้มีค่าสัมประสิทธิ์แอลฟ่าของครอนบัคเท่ากับ 0.9407

จากตารางการบันทึกข้อมูลพบว่ากำลังพลส่วนใหญ่เป็นเพศชายร้อยละ 91 อายุเฉลี่ย 41 ปี โดยส่วนใหญ่มีอายุอยู่ระหว่าง 25-35 ปี ทั้งนี้ภาพรวมอายุเฉลี่ยน้อยกว่า 35 ปีจะมีมากที่สุดซึ่ง

เป็นห้วงของวัยทำงาน นอกนั้นจะเป็นห้วงของระดับผู้บริหารที่มีอายุมากกว่า 35 ปีขึ้นไปจะมีจำนวนไม่แตกต่างกันมากนัก ในจำนวนนี้มีผู้จบปริญญาตรีมากที่สุด ร้อยละ 65 ระดับต่ำกว่าปริญญาตรี และสูงกว่าปริญญาตรีมีจำนวนใกล้เคียงกัน ระดับชั้นยศที่เป็นกำลังหลักปฏิบัติงานจะมีตั้งแต่ จ.อ.-น.อ. โดยจะพบว่าผู้ปฏิบัติงานในระดับแผนกจะมีมากที่สุด รองมาเป็นระดับกองและระดับฝ่ายที่น่ากังวลก็คือผู้ปฏิบัติที่มีอายุงานน้อยกว่า 5 ปีมีจำนวนมาก ซึ่งหมายถึง กำลังพลมีความรู้ แต่ทักษะ และประสบการณ์หรือความชำนาญในการปฏิบัติงานยังมีไม่เพียงพอ

1.2 ส่วนที่ 2 ความรู้ ความเข้าใจ ทักษะ ความพึงพอใจในการปฏิบัติงาน

จากการวิเคราะห์แบบสอบถามส่วนที่สองโดยใช้สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ยเลขคณิต ค่าเบี่ยงเบนมาตรฐาน จากนั้นนำผลที่ได้มาเปรียบเทียบกับช่วงที่แบ่งไว้ 5 ช่วงคือ

ความรู้ ทักษะ ความสามารถ	คะแนน
มากที่สุด	4.21-5.00
มาก	3.41-4.20
ปานกลาง	2.61-3.40
น้อย	1.81-2.60
น้อยมาก	1.00-1.80

ตารางที่ 4-2 ความรู้ ความเข้าใจ ทักษะ ความพึงพอใจในการปฏิบัติงาน

รายละเอียด	$\bar{X}$	S.D.	แปลความ
1. ความรู้ ความเข้าใจเกี่ยวกับการปฏิบัติด้านสารสนเทศและสงครามไซเบอร์			
1.1 เข้าใจความหมายของคำว่า สงครามสารสนเทศ	3.48	.948	มาก
1.2 เข้าใจความหมายของคำว่า สงครามไซเบอร์	3.40	.976	ปานกลาง
1.3 เข้าใจถึงภัยคุกคามและอันตรายจากสงครามไซเบอร์และสงครามสารสนเทศ	3.50	.934	มาก
1.4 เข้าใจภัยคุกคามและอันตรายการจากไวรัส มัลแวร์ หนอนคอมพิวเตอร์	3.63	.986	มาก
1.5 เข้าใจถึงความเสียหายที่เกิดจากการแฮกเกอร์ หรือ นักเจาะระบบคอมพิวเตอร์	3.68	.950	มาก
1.6 มีความรู้เกี่ยวกับการป้องกันไวรัส มัลแวร์ หนอนคอมพิวเตอร์	3.31	.987	ปานกลาง
1.7 มีความรู้เกี่ยวกับการใช้คอมพิวเตอร์ให้ทำงานอื่นนอกเหนือจากงานประจำ	3.49	.999	มาก
1.8 มีความเข้าใจวิธีการกำหนดความรู้ความสามารถของบุคคลในการปฏิบัติงาน	3.45	.852	มาก
รวม	3.49	.924	มาก

ตารางที่ 4-2 ความรู้ ความเข้าใจ ทักษะ ความพึงพอใจ (ต่อ)

รายละเอียด	$\bar{X}$	S.D.	แปลความ
2. ทักษะการปฏิบัติงานด้านสารสนเทศและสงครามไซเบอร์			
2.1 มีความสามารถในการติดตั้งและกำหนดค่าต่างๆ ของระบบเครือข่าย	2.89	1.028	ปานกลาง
2.2 มีความสามารถในการค้นหาและกำจัดไวรัสคอมพิวเตอร์	3.07	1.073	ปานกลาง
2.3 มีความสามารถในการใช้โปรแกรมเจาะระบบคอมพิวเตอร์หรือเครือข่าย	2.46	1.145	ปานกลาง
2.4 มีความสามารถในการเขียนโปรแกรมเจาะระบบ หรือโปรแกรมไวรัส	2.22	1.229	น้อย
2.5 มีความสามารถในการเขียนโปรแกรมคอมพิวเตอร์หรือเขียนเว็บเพจ	2.43	1.326	ปานกลาง
2.6 มีความสามารถในการเรียนรู้และถ่ายทอดความรู้ให้กับผู้อื่นได้เป็นอย่างดี	2.81	1.185	ปานกลาง
2.7 ระดับขีดความสามารถของบุคคลในหน่วยในการป้องกันระบบเครือข่ายและข้อมูล	2.82	1.037	ปานกลาง
2.8 ระดับขีดความสามารถของหน่วยในการป้องกันระบบเครือข่ายและข้อมูล	2.93	1.069	ปานกลาง
รวม	2.70	1.093	ปานกลาง
3. ความคิด ทัศนคติ แรงจูงใจและความต้องการส่วนตัวของบุคลล			
3.1 ต้องการให้ตำแหน่งที่เกี่ยวกับสงครามไซเบอร์มีค่าตอบแทนพิเศษตามความสามารถ	3.75	.966	มาก
3.2 ต้องการให้จัดอบรมเพื่อให้เข้าใจเกี่ยวกับการปฏิบัติด้านสงครามไซเบอร์	4.04	.850	มาก
3.3 ต้องการเอกสารและข่าวสารที่เกี่ยวข้องกับสงครามไซเบอร์อย่างต่อเนื่องเป็นปัจจุบัน	3.91	.973	มาก
3.4 ต้องการให้จัดฝึกการปฏิบัติเกี่ยวกับสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ	3.93	.956	มาก
3.5 ต้องการสร้างขวัญกำลังใจ แรงจูงใจ จนท.ที่ปฏิบัติงานด้านสงครามไซเบอร์	3.91	.964	มาก
3.6 ต้องการให้มีหน่วยงานรับผิดชอบงานสงครามไซเบอร์ในหน่วยขึ้นตรงทุกหน่วย	3.78	1.114	มาก
3.7 ต้องการให้หมุนเวียนกำลังพลในการปฏิบัติงานด้านสงครามไซเบอร์	3.61	1.088	มาก
รวม	3.85	.959	มาก

ตารางที่ 4-2 (ต่อ) ความรู้ ความเข้าใจ ทักษะ ความพึงพอใจ

รายละเอียด	$\bar{x}$	S.D.	แปลความ
4. ความพึงพอใจ ในการปฏิบัติงานในที่ทำงาน			
4.1 มีความพอใจในสถานที่ทำงาน	3.79	.864	มาก
4.2 มีความพอใจในระบบรักษาความปลอดภัยเครือข่ายของหน่วย	3.44	.898	มาก
4.3 มีความพอใจในระบบป้องกันไวรัสคอมพิวเตอร์ที่ใช้อยู่ในเครื่อง	3.36	.910	ปานกลาง
4.4 มีความพอใจในระเบียบและคำแนะการปฏิบัติด้านสงครามไซเบอร์ของหน่วย	3.26	.924	ปานกลาง
4.5 ตำแหน่งของท่านตรงกับอัตราที่ ทอ. กำหนดไว้ให้บรรจุในหน่วย	3.64	1.096	มาก
4.6 ตำแหน่งปัจจุบันให้ความรู้ความเข้าใจต่อการปฏิบัติงานด้านสงครามไซเบอร์มาก	2.95	1.169	ปานกลาง
รวม	3.41	.936	มาก
5. ความพึงพอใจของท่านต่อภาพรวมของหน่วยงาน	3.68	.950	มาก

ผลการวิเคราะห์ข้อมูลพบว่า กำลังมีความรู้ ความเข้าใจเกี่ยวกับการปฏิบัติด้านสารสนเทศและสงครามไซเบอร์ อยู่ในเกณฑ์เฉลี่ยดีมาก แต่ทักษะ ประสบการณ์ ความเชี่ยวชาญในการปฏิบัติงานด้านสารสนเทศและสงครามไซเบอร์ อยู่ในระดับปานกลางค่อนมาทางน้อย โดยเฉพาะความรู้และทักษะในการปฏิบัติการเชิงรุกมีค่าเฉลี่ยน้อย ในส่วนของความคิด ทัศนคติ แรงจูงใจและความต้องการส่วนตัวของบุคลล รวมทั้งความพึงพอใจในการปฏิบัติงานในที่ทำงาน อยู่ในระดับดีมาก แสดงว่ากองทัพให้ความสำคัญในเรื่องกระบวนการและสิ่งอำนวยความสะดวกในการปฏิบัติงานรวมทั้งการให้สวัสดิการด้านต่างๆที่ดีแก่กำลังพล

1.3 ส่วนที่ 3 ข้อคิดเห็นและข้อเสนอแนะ เป็นคำถามแบบปลายเปิด จำนวน 5 ข้อ สรุปผลการวิเคราะห์ได้ดังนี้

1.3.1 ด้านกำลังพล พบว่าขาดแคลนกำลังพลที่มีความรู้ความสามารถด้านไซเบอร์ ควรสนับสนุนบุคลากรที่มีความรู้ความชำนาญเฉพาะด้านปฏิบัติงานด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับให้เหมาะสมกับภารกิจของแต่ละหน่วยงาน เปิดตำแหน่ง น.สารสนเทศมากขึ้น ส่งเสริมให้บุคลากรไปศึกษาและอบรมต่างประเทศ ติดตามเทคโนโลยีที่ทันสมัยตลอดเวลา ตั้งหน่วยงานแยกออกมาเพื่อทำงานด้านนี้โดยเฉพาะและควรเพิ่มค่าตอบแทนให้กับบุคลกรที่ปฏิบัติงานด้านไซเบอร์ มีการหมุนเวียนกำลังพลบรรจุในตำแหน่งนี้ บุคลากรที่รับเข้าใหม่ต้องมีความรู้ด้านไซเบอร์มีจิตสำนึกในการรักษาความปลอดภัยด้านไซเบอร์

1.3.2 ด้านเครื่องมือ พบว่าเครื่องมือ อุปกรณ์มีไม่เพียงพอในการทำงาน และไม่ทันสมัย ควรมีระบบไฟฟ้าสำรองที่ตอบสนองได้ทันทีที่ไฟฟ้าหลักขัดข้อง ควรมีระเบียบเกี่ยวกับอุปกรณ์คอมพิวเตอร์ ทอ.เพื่อกำหนดรายละเอียดที่จำเป็นในการจัดซื้อ มีโปรแกรมที่ถูกกฎหมายใช้งานในหน่วยงาน ทอ.ด้วย

1.3.3 ด้านการบริหาร พบว่า โครงสร้างยังไม่ตอบสนองการปฏิบัติงาน ควรเป็นหน่วยขึ้นตรงกับ ผบ.หน่วย และมีผู้รับผิดชอบที่ชัดเจน การบริหารงานยังไม่เป็นระบบ ควรเพิ่มแผนกปฏิบัติการให้เพียงพอกับภารกิจที่ได้รับ

1.3.4 ด้านงบประมาณ พบว่าควรสนับสนุนงบประมาณให้เพียงพอกับการปฏิบัติงานด้านไซเบอร์และสงครามรูปแบบใหม่ ทั้งเชิงรุกและเชิงรับ

1.3.5 ด้านอื่นๆ พบว่า กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศควรเป็นหน่วยที่ดูแลด้านสงครามไซเบอร์ เพียงหน่วยเดียวและวางระบบป้องกันให้กับทุกหน่วยงานใน ทอ. ส่งเสริมการใช้อุปกรณ์และโปรแกรมที่ถูกกฎหมาย ควรมีแผนแม่บทของสงครามไซเบอร์เฉพาะด้านการรักษาข้อมูลที่มีชั้นความลับ หน่วยงานยังขาดโปรแกรมการเข้ารหัสทำให้การเก็บข้อมูลหรือการประมวลผล การดูแลเป็นไปด้วยความลำบากส่งผลให้ผู้ใช้งานไม่สามารถรับส่งข้อมูลสำคัญได้ทันเวลา และควรมีการฝึกปฏิบัติร่วมกับหน่วยงานอื่น ๆ ทั้งภายใน และภายนอกหน่วย หรือในระดับประเทศ

2. วิเคราะห์จากวรรณกรรมและผลงานวิจัยที่เกี่ยวข้อง

2.1 การจัดองค์กรและการบริหารองค์กรให้มีให้มีประสิทธิภาพ พบว่า ควรพิจารณาถึงโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อม และควรเป็นองค์กรแห่งการเรียนรู้ และควรให้ความสำคัญกับพฤติกรรมของผู้ปฏิบัติงานในองค์กร เนื่องจากการบริหารเป็นกระบวนการทำงานให้สำเร็จโดยใช้บุคคลอื่น พฤติกรรมของบุคคลในองค์กรจึงมีความสำคัญต่อการเพิ่มผลผลิตและประสิทธิผลขององค์กร สำหรับการบริหารองค์กรให้มีคุณภาพควรใช้หลักการ Deming Circle คือ Plan-Do-Check-Action เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม การตรวจสอบที่นำไปสู่การแก้ไขปรับปรุง ทำให้ปัญหาที่เกิดขึ้นแล้วไม่เกิดซ้ำ หรือลดความรุนแรงของปัญหา ถือเป็นการนำความผิดพลาดมาใช้ให้เกิดประโยชน์มีความเหมาะสมกับการปฏิบัติงานด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ นอกจากนั้นเพื่อป้องกันความเสียหายจากการปฏิบัติงานควรนำระบบการบริหารความเสี่ยง(Risk Management) เข้ามาช่วยในการบริหารงาน ผลที่ได้คือข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ดังนั้นทุกองค์กรควรจะจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารองค์กรให้มีประสิทธิภาพอีกทางหนึ่งด้วย อีกทั้งควรนำระบบสมรรถนะ (Competency Model) มาใช้ในการพัฒนาองค์กร เพราะจะทำให้บุคลากรในทุกตำแหน่งทราบถึงความรู้ ความสามารถของตนเอง และทราบว่าจะต้องพัฒนาและฝึกฝนอย่างไรจึงจะทำให้มีขีดความสามารถเพิ่มขึ้น เมื่อวางแผนดำเนินการอย่างเป็นระบบจะทำให้องค์การนั้นมีบุคลากรที่มีประสิทธิภาพและทำให้ผลประกอบการหรือผลการปฏิบัติภารกิจต่างๆ มีประสิทธิภาพตามมา

การนำระบบสมรรถนะมาใช้ในการบริหารองค์กรนับว่ามีประโยชน์อย่างยิ่งในยุคปัจจุบัน เพราะเป็นการสร้างบุคลากรให้มีความรู้ ความสามารถ ทัศนคติ ที่จะปฏิบัติหน้าที่ให้ประสบความสำเร็จและเกิดประสิทธิภาพกับองค์กรอย่างสูงสุด และผู้บริหารองค์กรจำเป็นต้องมีสมรรถนะ

ด้านการบริหารอันประกอบด้วย การมีวิสัยทัศน์ การวางแผน ภาวะผู้นำ การแก้ปัญหาและการตัดสินใจ สุดท้ายต้องมีความสามารถในการบริหารความเปลี่ยนแปลงที่อาจเกิดขึ้นได้ทุกเวลาอีกด้วย

สภาพแวดล้อมในการทำงานเป็นสิ่งสำคัญที่จะทำให้บรรยากาศการทำงานภายในองค์มีประสิทธิภาพ เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอก ซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร ประกอบด้วย โครงสร้างการทำงานที่ดี มีระบบรางวัลตอบแทนที่เหมาะสม มีความเป็นอิสระในการทำงาน มีความอบอุ่นมีการสนับสนุนช่วยเหลือกันและกัน มีการยอมรับความขัดแย้ง ยอมรับฟังความคิดเห็นผู้อื่น และสุดท้ายต้องมีความรักในหมู่คณะด้วย

2.2 ภัยคุกคามรูปแบบใหม่ พบว่า แนวโน้มภัยคุกคามรูปแบบใหม่จะเป็นภัยที่มีความซับซ้อน หลากหลายมิติร่วมกัน และจะทวีความรุนแรงขึ้นเรื่อยๆ ภัยคุกคามนี้จะส่งผลกระทบต่อโครงสร้างของสังคมไทยโดยตรง ทั้งนี้การป้องกันและแก้ไขภัยคุกคามรูปแบบใหม่ในปัจจุบันมีลักษณะต่างคนต่างทำ ไม่มีองค์กรที่ชัดเจนรับผิดชอบบูรณาการ นโยบาย ยุทธศาสตร์ และการแปลงนโยบายไปสู่การปฏิบัติที่ชัดเจน ทำให้ไม่สามารถป้องกัน ยับยั้ง และแจ้งเตือนภัยล่วงหน้าได้อย่างมีระบบตั้งแต่ก่อนเกิดเหตุการณ์ และเมื่อเกิดเหตุการณ์ภัยที่ร้ายแรงสังคมไทยอาจจะต้องตกอยู่ในสภาวะระส่ำระสาย เสียขวัญ จนขยายวงกว้างไปสู่ความมั่นคงด้านอื่นๆ ในสถานการณ์วิกฤตร้ายแรงเช่นนี้มีความจำเป็นอย่างยิ่งที่กองทัพไทย ซึ่งเป็นกลไกทางด้านความมั่นคงของรัฐบาล ที่มีขีดความสามารถและศักยภาพสูงในการจัดการกับปัญหาความมั่นคงในลักษณะภัยคุกคามรูปแบบใหม่ที่เป็นองค์รวม จะได้เตรียมปรับบทบาทและโครงสร้างการจัดของกองทัพให้เหมาะสม เพื่อเผชิญกับภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างเร่งด่วน เฉียบพลันในอนาคต อันจะทำให้กองทัพได้เป็นที่พึ่งและมีคุณค่ามากยิ่งขึ้นต่อสังคมไทย

2.3 ภัยคุกคามด้านไซเบอร์ พบว่า โดยสภาพและลักษณะของภัยคุกคามมีการเปลี่ยนแปลงไปจากเดิมอย่างมาก ตลอดจนมีรูปแบบในการโจมตีเป้าหมายที่หลากหลาย มีรูปแบบมากมายในการปฏิบัติโดยไม่ต้องใช้กำลังพลมากมาย จนทำให้ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามแทบไม่ทัน ดังนั้นแนวความคิดและแนวทางในการป้องกันระบบและทรัพย์สินขององค์กรให้ได้ประสิทธิผล (effectiveness) จำเป็นอย่างยิ่งที่จะต้องปรับความคิดและปรับกลยุทธ์ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป กำลังพลเพียงคนเดียวกับเครื่องมือที่ทันสมัยก็สามารถทำสงครามไซเบอร์ได้ องค์กรต้องเตรียมตัวรับมือกับภัยคุกคามรูปแบบใหม่ ที่มาทางไซเบอร์ โดยผ่านช่องทาง Social Network, Mobile Devices หรือ Cloud Services และเพื่อลดระดับความรุนแรงที่อาจเกิดขึ้นควรนำหลักการในระบบมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เพราะเป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก นอกจากนั้นถ้าเราต้องการให้ระบบขององค์กรมั่นคงปลอดภัย เราควร “ลดเวลาในการตรวจจับลง” (decrease Detect time) และ “ลดเวลาในการตอบสนองลง” (decrease React time) ด้วยเช่นกัน และพบว่ามี 4 ปัจจัยที่เราต้องนำมาพิจารณาในการวางแผนกลยุทธด้านความมั่นคงปลอดภัย (Security Strategy) ได้แก่ Protection (การป้องกัน) Detection (การตรวจจับ) Reaction (การตอบสนอง) และTime (เวลา) สำหรับการ

ป้องกันที่ได้ผลอีกทางหนึ่งคือ ต้องมีการอัพเดทข้อมูลต่างๆของฝ่ายเราเป็นประจำ นานาชาติต้องมีมาตรการเตรียมความพร้อม เพื่อรับมือกับการโจมตีทางไซเบอร์ มียุทธศาสตร์ที่ครอบคลุมสงครามไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียมหรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม

การแก้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศนั้น ควรมีมุมมอง 3 ด้านได้แก่ People, Process and Technology การปรับกระบวนการโดยการปฏิบัติตามมาตรฐาน ISO/IEC 27001:2013 เป็นการแก้ปัญหาที่ Process และ Technology แต่ปัจจัยสำคัญอยู่ที่ “มนุษย์” หรือ “People” ดังนั้นการเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศทั่วไป และการให้ความรู้ด้านภัยสารสนเทศ จึงเป็นเรื่องจำเป็นที่องค์กรต้องทำเป็นประจำทุกปี เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูงได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติ มีความพร้อมต่อการรับมือ “Incident” ต่างๆที่จะเกิดขึ้น นอกจากนี้กลไกกระบวนการและเทคนิคในการตรวจจับความผิดปกติในระบบ แบบ Real-Time ก็มีความจำเป็นเช่นกัน เพราะฉะนั้นเราจึงต้องเตรียมพร้อมกับเหตุการณ์ที่ไม่พึงประสงค์อยู่ตลอดเวลา ก็จะช่วยให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของเรามีประสิทธิผลมากขึ้น

2.4 ความพร้อมการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า กองทัพยังไม่ได้กำหนดหลักเกณฑ์และวิธีการที่ใช้ในการวัดความพร้อมด้านนี้ เนื่องจากเป็นหน่วยงานที่ตั้งขึ้นมาใหม่อยู่ระหว่างการเตรียมการโดยจะใช้กระบวนการบริหารที่เหมาะสมและการบริหารความเสี่ยงรวมทั้งระบบสมรรถนะเข้ามาช่วยในการปฏิบัติงาน แต่งานด้านสารสนเทศอื่นๆ กองทัพอากาศได้จัดทำยุทธศาสตร์การพัฒนาและกลยุทธ์ในการดำเนินงานด้านเทคโนโลยีสารสนเทศไว้เรียบร้อยแล้ว ยังขาดยุทธศาสตร์ในการปฏิบัติด้านสงครามไซเบอร์และการกำหนดหน้าที่ความรับผิดชอบให้กับหน่วยเกี่ยวข้องเท่านั้น ปัจจุบันกองทัพอากาศได้วางระบบเครือข่ายสารสนเทศไปยังหน่วยต่างๆ ทั่วประเทศ สามารถบริหารจัดการระบบเครือข่ายและสามารถใช้เป็นระบบสารสนเทศของกองทัพได้ดีในระดับหนึ่ง แต่การป้องกันระบบเครือข่ายและข้อมูลที่อยู่ในระบบเครือข่าย ยังมีความเสี่ยงมากจากการถูกบุกรุก เนื่องจากมีการปรับโครงสร้างการจัดหน่วยใหม่เมื่อเดือนสิงหาคม 2557 ทำให้การดำเนินงานด้านไซเบอร์ยังไม่เรียบร้อยเท่าที่ควร อีกทั้งขาดกำลังพลที่มีความรู้ความสามารถและทักษะในด้านสงครามไซเบอร์ในทุกระดับ นอกจากนี้เครื่องมือที่ต้องใช้งานมีสภาพเก่าและไม่เพียงพอ จึงทำให้ระบบสารสนเทศของกองทัพอากาศ ถูกกระทำทางไซเบอร์อยู่เสมอ และต้องใช้เวลานานในการกู้ระบบกลับคืนมาให้เป็นปกติ การที่กองทัพอากาศจะพัฒนาไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) ได้อย่างมีประสิทธิภาพและสมบูรณ์แบบนั้น ผู้บังคับบัญชาทุกระดับต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และสร้างความตระหนักให้บุคลากรในทุกหน่วยงาน ได้รับรู้ถึงกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ถูกต้อง ควรจัดให้มีการฝึกอบรมบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้มีความรู้ มีทักษะ มีความชำนาญและมีความสามารถในการรับมือกับเหตุการณ์ ความเสี่ยง และภัยคุกคามด้านสารสนเทศต่างๆ ที่อาจจะเกิดขึ้นในอนาคตได้ และควรมีระบบการตรวจจับและแจ้งเตือนภัยเมื่อถูกกระทำทางไซเบอร์พร้อมทั้งแนวทางป้องกัน ทั้งนี้งบประมาณก็ยังเป็นปัจจัยที่สำคัญในการเตรียมความพร้อมด้านนี้

2.5 ปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์พบว่า กำลังพลเป็นปัจจัยหลัก กล่าวคือ ขาดกำลังพลที่มีความรู้ มีทักษะ และความเชี่ยวชาญ รวมทั้งงบประมาณที่มีไม่เพียงพอสนับสนุนกิจการด้านนี้ โดยเฉพาะหน่วยนอกที่ตั้งดอนเมืองเป็นจุดอ่อนอย่างยิ่งในการถูกโจมตีทางไซเบอร์ ปัจจัยรองลงมาคือ การบริหารจัดการระบบงาน และเครื่องมือ อุปกรณ์ที่ช่วยในการปฏิบัติงาน รวมถึงเทคโนโลยีที่นำมาใช้ยังไม่เพียงพอไม่ทันสมัย อีกทั้งงบประมาณที่มีจำกัดไม่พอสนับสนุนเหล่านี้ล้วน เป็นผลกระทบโดยตรงต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ สาเหตุหลักของการเกิดภัยคุกคามด้านไซเบอร์ของกองทัพอากาศเกิดจากปัจจัยภายใน เช่น กำลังพลที่รู้เท่าไม่ถึงการณ์และขาดความตระหนักรู้ และสาเหตุรองคือระบบหรือเทคโนโลยีที่ใช้งานเช่น ช่องโหว่ในซอฟต์แวร์ ไวรัสหรือเวิร์ม ต่อมาเป็นสาเหตุจากปัจจัยภายนอกเช่น เกิดจากแฮกเกอร์เกิดจากการก่ออาชญากรรมและเกิดจากการก่อการร้าย อย่างไรก็ตามกองทัพอากาศสามารถนำผลการวิจัยที่เกี่ยวข้องด้านไซเบอร์นี้ไปใช้เป็นแนวทางในการกำหนดยุทธศาสตร์และนโยบายเชิงรุกของกองทัพอากาศด้านความมั่นคงปลอดภัยทาง ไซเบอร์ได้โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนวทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือมีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ และมีความยั่งยืนบนพื้นฐานการพึ่งพาตนเอง

3. วิเคราะห์จากการสัมภาษณ์เชิงลึก

จากคำถามการสัมภาษณ์เชิงลึกจำนวน 5 ข้อ สามารถสรุปผลได้ดังนี้

3.1 ความเห็นเกี่ยวกับการปฏิบัติต่างๆ ด้านสงครามไซเบอร์ ซึ่งเป็นภารกิจใหม่ที่หน่วยงานต้องรับมือในปัจจุบัน สรุปได้ว่า มีความสำคัญอย่างยิ่งต่อการปฏิบัติภารกิจของกองทัพ เป็นภารกิจที่ต้องกระทำหลีกเลี่ยงไม่ได้ โดยจะต้องทำให้เกิดความได้เปรียบในทุกด้าน และเป็นปัจจัยสร้างผลกระทบต่อระบบบัญชาการและควบคุมในสงครามยุคใหม่ หน่วยต้องปรับตัวให้มีความพร้อมตลอดเวลาเพื่อรับมือกับสงครามไซเบอร์ตั้งแต่ในยามปกติ และคำนึงถึงการปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2550 ฉบับนี้ด้วยเพราะมีผลต่อการปฏิบัติการเชิงรุก ในการปฏิบัติการเชิงรับต้องป้องกันให้เข้มแข็งมากที่สุดและเปิดเผย ส่วนการปฏิบัติเชิงรุกจะกระทำเพื่อป้องกันผลประโยชน์ของชาติเท่านั้นและมีชั้นความลับด้วย

3.2 ความเห็นเกี่ยวกับปัจจัยที่มีผลกระทบต่อการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วยในปัจจุบัน สรุปได้ว่า ปัจจัยด้านกำลังพล ที่มีความรู้ด้านสงครามไซเบอร์ มีจำนวนไม่เพียงพอ ที่มีอยู่ที่ขาดความรู้ ความสามารถ ทักษะและความชำนาญในการปฏิบัติ รองลงมาคือเครื่องมือและอุปกรณ์ที่ไม่ทันสมัย ไม่เพียงพอ โปรแกรมบางอย่างหมดอายุการใช้งาน รองลงมาคือการจัดสรรงบประมาณด้านนี้ไม่เพียงพอ และสุดท้ายคือการบริหารจัดการไม่ชัดเจน เช่น ยังไม่มีแผนแม่บทด้านสงครามไซเบอร์ ต้องมีความชัดเจนในแผนยุทธศาสตร์ด้านสงครามไซเบอร์ อีกทั้งการกำหนดภารกิจ การสร้างองค์ความรู้ และโครงสร้างการจัดหน่วยงานที่ต้องสอดคล้องกับภารกิจด้วย

3.3 ความเห็นเกี่ยวกับการปรับปรุงและพัฒนาการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วยให้มีประสิทธิภาพเพิ่มขึ้น สรุปได้ว่า ควรพัฒนาที่กำลังพลเป็นอันดับแรก ด้วยการอบรมให้มีความรู้ ความสามารถเทียบเท่ากับระดับสากลเพื่อให้รับมือกับสงครามไซเบอร์ได้ และต้องสร้างให้ทุก

คนมีจิตสำนึก มีความตระหนักในการรักษาความปลอดภัยด้านไซเบอร์ จัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วย ส่งเสริมด้านสวัสดิการความเป็นอยู่และควรเพิ่มค่าตอบแทนพิเศษให้ กับผู้ปฏิบัติงานด้านสงครามไซเบอร์โดยมีข้อกำหนดว่าต้องผ่านการทดสอบและผ่านการอบรมหลักสูตรที่ได้มาตรฐานมีใบประกาศนียบัตรรับรองจึงจะได้รับค่าตอบแทนพิเศษ รองลงมาคือการกำหนดเป้าหมายที่เราจะไปหรืออยากจะเป็นต้องมีความชัดเจน แล้วจึงนำมากำหนดภารกิจ การจัดหน่วย การสร้างองค์ความรู้ที่ต้องการ แล้วจึงสรรหาทรัพยากรต่อไป อีกทั้งควรจัดทำแผนแม่บทด้านสงครามไซเบอร์เพื่อใช้เป็นแนวทางในการดำเนินงาน และควรกำหนดผู้มีอำนาจในการอนุมัติให้ปฏิบัติการตอบโต้ทางไซเบอร์เชิงรุกเพื่อป้องกันการกระทำจากฝ่ายตรงข้าม

3.4 ความเห็นเกี่ยวกับการปฏิบัติเพื่อมิให้กำลังพลที่มีความรู้ความสามารถและทักษะ ด้านสงครามไซเบอร์ลาออกจากกองทัพ สรุปได้ว่า ต้องกำหนดเส้นทางการเจริญเติบโตที่ชัดเจน เปิดโอกาสให้เท่าเทียมกัน เพื่อให้กำลังพลมีความมั่นใจในวิชาชีพ มีความเจริญก้าวหน้า มีค่าตอบแทนพิเศษในอัตราที่เหมาะสม เนื่องจากมีภาระงานที่ต้องติดตามอย่างต่อเนื่องตลอดเวลา ส่งเสริมให้มีการแสดงออกซึ่งความสามารถที่มีอยู่ ทำการฝึกอบรมให้กำลังพลก้าวทันเทคโนโลยีอยู่เสมอ ผู้ปฏิบัติงานไซเบอร์ไม่จำเป็นต้องมีตำแหน่งอยู่ในกองทัพก็สามารถทำงานให้กองทัพได้ ควรมีหลักสูตรการเรียนการสอนในสายวิทยาการ การเพิ่มพูนความรู้ให้กับหน่วยเกี่ยวข้องอย่างต่อเนื่องเพื่อให้มีการทำงานทดแทนกันได้

3.5 ข้อเสนอแนะอื่นๆ สรุปได้ว่า ต้องสร้างจิตสำนึก มุ่งเน้นตั้งแต่ผู้บังคับบัญชาลงไปทุกระดับ ให้มีความรู้และเข้าใจถึงผลเสียหายเมื่อถูกกระทำทางไซเบอร์ นอกจากนั้นเห็นควรให้พิจารณาด้านกฎหมายที่เกี่ยวข้องด้วยทั้งในประเทศและระหว่างประเทศในกรณีที่ต้องปฏิบัติการเชิงรุก มีข้อกำหนดระเบียบที่คุ้มครองการปฏิบัติการด้านไซเบอร์ให้กับผู้ปฏิบัติงานตามคำสั่งที่ถูกต้องจากผู้บังคับบัญชา หน่วยงานที่ปฏิบัติด้านนี้ควรตั้งเป็นหน่วยงานอิสระ ไม่ต้องมีตำแหน่งหรือชั้นยศ ไม่ถูกจำกัดด้วยระเบียบของทางราชการมากเกินไป

4. วิเคราะห์จากผลการสนทนากลุ่ม

สรุปผลจากการสนทนากลุ่ม ได้ดังนี้

4.1 สมรรถนะหรือ ขีดความสามารถในการปฏิบัติการด้านสงครามไซเบอร์ ควรมีความหมายว่า ความสามารถในการโจมตีอีกฝ่ายหนึ่งโดยใช้จุดอ่อนของระบบที่ตรวจพบเพื่อเข้ามาทำลายหรือรบกวนขัดขวางกระบวนการทำงานทุกแบบของฝ่ายตรงข้าม รวมทั้งโครงสร้างพื้นฐานของชาติที่ใช้เครือข่ายคอมพิวเตอร์เป็นเครื่องมือสำคัญในการขับเคลื่อนการปฏิบัติงานโดยหวังผลสัมฤทธิ์ให้เกิดผลกระทบต่อระบบเศรษฐกิจ สังคม และความมั่นคงของชาติ อาจเป็นการกระทำทั้งระดับบุคคล องค์กร กลุ่มอาชญากร หรือเครือข่ายก่อการร้าย ที่มาจากภายในและภายนอกประเทศ

4.2 การประเมิน สมรรถนะหรือขีดความสามารถในการปฏิบัติการด้านสงครามไซเบอร์ กองทัพอากาศควรดำเนินการประเมินสมรรถนะใน 2 ลักษณะคือ การประเมินตามหลักวิชาการ และการประเมินจากการฝึกและปฏิบัติจริง การประเมินแต่ละแบบต้องระบุถึง กำลังพล (ความรู้ ความสามารถ ทักษะ ทัศนคติ) กระบวนการบริหาร/จัดการ(นโยบายที่ชัดเจนต่อเนื่อง ระเบียบปฏิบัติ การจัดการความรู้ การบริหารความเสี่ยง มาตรฐานการรักษาความปลอดภัยระบบสารสนเทศ การตรวจสอบระบบหาจุดอ่อน จุดแข็ง งบประมาณที่พอเพียง) และเทคโนโลยี(การออกแบบระบบที่แข็งแรง คงทน รวมทั้ง อุปกรณ์หรือเครื่องมือที่ทันสมัย เพียงพอ ทำงานในแบบ

เสมือนจริงมากที่สุด) ทั้งนี้เพื่อความสะดวกและรวดเร็วในเบื้องต้นสามารถนำหลักการที่กำหนดโดย ITU และมาตรฐานการรักษาความปลอดภัย ISO/IEC 27001-2013 มาใช้เป็นแนวทางในการประเมินได้ และผู้ที่ทำการประเมินจะต้องมีความรู้เกี่ยวกับระบบดังกล่าวเป็นอย่างดีด้วย

4.3 แนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ สรุปได้ว่า ต้องพัฒนาที่ กำลังพล กระบวนการบริหาร/จัดการ และเทคโนโลยี ซึ่งสามารถสรุปในภาพรวมได้ 3 ขั้นตอนดังนี้

ขั้นที่ 1 การจัดการทรัพยากรเพื่อการปฏิบัติด้านไซเบอร์ การบริหารจัดการทรัพยากรมนุษย์ที่มีอยู่ โดยเฉพาะกำลังพลที่มีความรู้ความสามารถด้านไอที ให้สามารถปฏิบัติการด้านสงครามไซเบอร์ได้ตามหลักการ Network Centric Warfare

ขั้นที่ 2 การเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โดยการพัฒนาปรับปรุงระบบเครือข่ายให้มีความปลอดภัย การตรวจสอบทางเทคนิคและการประเมินความเสี่ยงระบบเครือข่าย การกำหนดมาตรฐานการเชื่อมต่อเครือข่าย การพัฒนาบุคลากรให้ก้าวทันเทคโนโลยีด้านการรักษาความปลอดภัยระบบเครือข่าย

ขั้นที่ 3 การเสริมสร้างขีดความสามารถการปฏิบัติการไซเบอร์ โดยการพัฒนาขีดความสามารถเชิงรุก เพื่อให้มีความพร้อมในการปฏิบัติการกรณีจำเป็น เช่น การจัดตั้งเครือข่ายพันธมิตร ด้านไซเบอร์กับมหาวิทยาลัย สถาบันการศึกษา องค์กร/บุคคลภายนอกกองทัพอากาศ เพื่อให้มีความพร้อมและสามารถปฏิบัติการไซเบอร์ได้ในสถานการณ์จำเป็น

4.4 แนวทางการได้มาและรักษาบุคลากรที่มีสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ สรุปได้ว่า แสวงหาจากภายในกองทัพและจากภายนอกกองทัพ ด้วยการจัดกิจกรรมแข่งขันความสามารถด้านไซเบอร์ หรือจากการฝึกอบรมพิเศษต่างๆที่ให้ความรู้ด้านไซเบอร์ ปรับปรุงกฎ ระเบียบให้ทันสมัย ปรับหลักสูตรการเรียนการสอนในสายวิยาการต่างๆ ให้มีเรื่องสงครามไซเบอร์อยู่ด้วยเพื่อสร้างความตระหนักรู้และช่วยกันรักษาความปลอดภัยไซเบอร์ ควรแบ่งกลุ่มการปฏิบัติงานเป็นกำลังพลในเครื่องแบบและพลเรือน (กำลังพลสมทบ) ให้มีการทำงานเป็นคาบเวลา ในด้านการรักษาบุคลากรให้อยู่ในกองทัพนั้นควรกำหนดเส้นทางการเจริญเติบโตที่ชัดเจนว่าสามารถไปถึงระดับใด ให้เกียรติให้ความสำคัญต่อการปฏิบัติหน้าที่ และมีค่าตอบแทนพิเศษให้ในอัตราที่เหมาะสม โดยต้องมีขีดความสามารถตามมาตรฐานกำหนดมีการประเมินทุกปี หากพิจารณาตามหลักวิชาการแล้วสามารถกำหนดเป็นแนวทางได้ 4 ขั้นตอนคือ (1) การวางแผนทรัพยากรมนุษย์ (2) การสรรหาและการคัดเลือก (3) การพัฒนาทรัพยากรมนุษย์ (4) การบริหารค่าตอบแทน

4.5 รูปแบบในการปฏิบัติเชิงรุกและเชิงรับด้าน Cyber Warfare ของกองทัพอากาศ สรุปได้ว่าการปฏิบัติเชิงรุก ต้องกระทำในทางลับที่สุดเท่านั้น ต้องมีบัญชีเป้าหมาย ต้องมีระเบียบและกำหนดหน้าที่ให้ชัดเจนว่าใครต้องทำอะไรอย่างไร แก้ไขกฎ ระเบียบที่ล้าสมัยให้สามารถอำนวยความสะดวกในการปฏิบัติเชิงรุกของบุคลากรได้ ที่สำคัญต้องกำหนดในหลักนิยมและยุทธศาสตร์ให้ชัดเจน รวมทั้งพิจารณาจัดตั้งเครือข่ายความร่วมมือทางไซเบอร์ สร้างให้ทุกคนมีจิตสำนึกในการรักษาความปลอดภัยไซเบอร์ สำหรับการปฏิบัติเชิงรับ ต้องตรวจสอบและปรับปรุงเครือข่ายให้มีความปลอดภัย มีความแข็งแรง คงทนต่อการบุกรุกและทำลาย ใช้มาตรฐานการรักษา

ความปลอดภัยมาเป็นแนวทางในการปฏิบัติ พัฒนากำลังพลให้มีความสามารถและทักษะ ก้าวทันเทคโนโลยีด้านการรักษาความปลอดภัยเครือข่าย

4.6 กองทัพควรใช้นวัตกรรมการป้องกัน Cyber Warfare แบบใดจึงจะเหมาะสมและยั่งยืน สรุปได้ว่า ต้องเรียนรู้เทคโนโลยีให้ครบวงจร ตั้งแต่ Hardware ไปจนถึง Cyber concept ต้องควบคุมและประยุกต์ใช้งานได้ มีโปรแกรมที่เหมาะสมใช้งาน จัดให้มีระบบจำลองยุทธด้านไซเบอร์ (Cyber Range) เพื่อแก้ปัญหาด้านบุคลากรและแก้ปัญหาระบบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์แบบเดิมที่เน้นไปที่ “See and Hear” แต่ไม่ได้เน้นที่ “Do” หรือ “Practice” นอกจากนี้ยังต้องมีการจัดระบบการเรียนรู้ (KM) มีเครื่องมือที่ทันสมัย ตรวจสอบให้พร้อมใช้งานอยู่เสมอ จัดให้มีศูนย์รักษาความปลอดภัยทางไซเบอร์เพื่อคอยตรวจจับผู้บุกรุก มีการฝึกอย่างจริงจัง สนับสนุนการวิจัยที่ทำให้ระบบมีความแข็งแรง คงทน อีกทั้งการลดเวลาในการตรวจจับและการตอบสนองเพื่อให้การป้องกันมีประสิทธิภาพ

4.7 ปัจจัยที่มีผลกระทบต่อการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศคือ กำลังพล เครื่องมือและอุปกรณ์ งบประมาณ นโยบาย กฎระเบียบและการมีจิตสำนึกรวมทั้งทัศนคติที่ดีที่สำคัญที่สุดคือนโยบายของผู้บริหารต้องมีความชัดเจนและต่อเนื่อง โดยมีรายละเอียดของปัจจัยดังนี้

4.7.1 ภาวะผู้นำ (Leadership) ต้องมีนโยบายที่ชัดเจนต่อเนื่อง

4.7.2 กำลังพลและวัฒนธรรมองค์กร (Personal & Culture) กำลังพลมีความรู้มีทักษะและความสามารถสูง มีขวัญกำลังใจดี และมีบรรยากาศที่ดีในการทำงานและสถานที่ทำงาน

4.7.3 การศึกษาและการฝึกอบรม (Education/Training) มีการฝึกอบรมให้ความรู้ การจัดการความรู้ มีการฝึกอย่างต่อเนื่องสม่ำเสมอทั้งในที่บังคับการและในพื้นที่การฝึก (ปฏิบัติจริง)

4.7.4 การจัดหน่วยงาน (Organization) โครงสร้างหน่วยที่ทำงานได้สะดวกรวดเร็ว ลดเวลาในการตรวจจับและการตอบสอง มีเส้นทางการเจริญเติบโตของกำลังพลที่ชัดเจน

4.7.5 หลักนิยม (Doctrine) มีกำหนดหัวข้อการทำสงครามไซเบอร์ไว้ในหลักนิยมมีหลักการและแนวทาง อีกทั้งมียุทธศาสตร์การพัฒนาที่ชัดเจน มีแผนแม่บทรองรับ หน่วยสามารถแปลงนโยบายไปสู่การปฏิบัติได้อย่างถูกต้อง

4.7.6 เทคโนโลยี (Technology/Material) ต้องทันสมัยและเพียงพอ ต้องวางแผนให้สามารถนำเทคโนโลยีมาใช้ประโยชน์ได้ในทุกส่วนที่ปฏิบัติงานมีการวางแผนจัดหาทดแทนตามวงรอบของเทคโนโลยีที่เปลี่ยนแปลงไปและให้ทันกับความต้องการและภัยคุกคามที่เกิดขึ้น

4.7.7 เครื่องอำนวยความสะดวก (Facilities) อุปกรณ์หรือเครื่องมือทุกชนิดที่ใช้ในการปฏิบัติต้องมีพร้อมใช้งานอยู่เสมอทั้งภายในหน่วยงานและสนับสนุนหน่วยอื่นๆ สามารถใช้ได้กับเทคโนโลยีสมัยใหม่ เพื่อให้การปฏิบัติงานด้านไซเบอร์มีประสิทธิภาพ

สรุปผลการวิจัย

ผู้วิจัยได้นำข้อมูลทั้งหมดที่ผ่านการวิเคราะห์แล้วมาสังเคราะห์ตรวจสอบความซ้ำซ้อนของผลที่ได้จากการวิเคราะห์ และนำมาพิจารณาเปรียบเทียบกับทฤษฎี แนวคิดรวมทั้งเอกสารผลงานวิจัยที่เกี่ยวข้อง แบบสอบถามและการสัมภาษณ์เชิงลึกและสรุปผลการสนทนากลุ่มอีกครั้งหนึ่ง ทำให้ทราบผลที่ได้รับจากการวิจัยดังนี้

1. ทำให้ทราบขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่ามีขีดความสามารถในการปฏิบัติเชิงรุกอยู่ในระดับต่ำ แต่การปฏิบัติเชิงรับอยู่ในระดับปานกลาง สาเหตุจากกำลังพลยังขาดทักษะและประสบการณ์ในการปฏิบัติด้านสงครามไซเบอร์ กำลังพลที่เชี่ยวชาญด้านสงครามไซเบอร์มีจำนวนน้อย เครื่องมือที่มีใช้งานไม่ทันสมัยไม่ทันเทคโนโลยีและไม่เพียงพอที่จะใช้ในการปฏิบัติทั้งเชิงรุกและเชิงรับ ไม่มีระบบการแจ้งเตือนภัยเมื่อถูกกระทำทางไซเบอร์

2. ทำให้ทราบปัจจัยที่มีผลกระทบต่อการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า ปัจจัยที่มีผลกระทบประกอบด้วย (1) กำลังพล เป็นปัจจัยหลักที่ส่งผลกระทบมากที่สุด เพราะกิจกรรมทุกอย่างจะดำเนินไปได้ต้องอาศัยกำลังพลเป็นผู้ปฏิบัติและเป็นผู้ควบคุม (2) กระบวนการบริหาร/จัดการ เป็นปัจจัยรองลงมาที่มีผลกระทบ จะต้องบริหารจัดการทั้งกำลังพล เครื่องมือเครื่องใช้และงบประมาณให้สามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ (3) เทคโนโลยี เป็นอีกปัจจัยหนึ่งที่มีผลกระทบ เนื่องจากเทคโนโลยีก้าวหน้าไปอย่างรวดเร็วแต่การเตรียมบุคลากรของหน่วยต่างๆ ยังตามไม่ทันและไม่เพียงพอ (4)งบประมาณ เป็นปัจจัยสำคัญอีกข้อหนึ่งที่ต้องมีให้กับหน่วยอย่างเพียงพอและต่อเนื่องจึงจะทำให้ระบบการปฏิบัติต่างๆ ขับเคลื่อนไปอย่างมีประสิทธิภาพ และ (5) ผู้บริหารระดับสูงของหน่วย เป็นปัจจัยหลักอีกข้อหนึ่งที่จะทำให้การปฏิบัติดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ ผู้บริหารที่ดีต้องมีเทคนิคและนำภาวะผู้นำมาใช้ในการบริหารงานด้วย

3. ทำให้ทราบแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า ต้องพัฒนากำลังพลให้มีความเข้าใจและมีความรู้ด้านสงครามไซเบอร์เป็นอันดับแรก อีกทั้งทำให้กำลังพลมีขวัญกำลังใจที่ดีในการปฏิบัติงานร่วมกัน กำหนดเส้นทางการเจริญเติบโตให้ชัดเจน ต่อจากนั้นจึงปรับปรุงพัฒนากระบวนการบริหารจัดการ รวมทั้งกฎ ระเบียบ ที่ใช้เป็นแนวทางในการปฏิบัติหาแนวทางในการ “ลดเวลาในการตรวจจับลง” (decrease Detect time) และ “ลดเวลาในการตอบสนองลง” (decrease React time) จะทำให้ระบบขององค์กรมั่นคงปลอดภัยจากสงครามไซเบอร์และควรนำกระบวนการบริหารงาน P-D-C-A (Plan, Do, Check, Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลกเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม ในด้านเทคโนโลยีควรจัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วย นำหลักการในระบบมาตรฐาน ISO/IEC 27001-2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร จัดให้มีศูนย์รักษาความปลอดภัยทางไซเบอร์เพื่อคอยตรวจจับผู้บุกรุกและระบบแจ้งเตือนภัยไซเบอร์ไปยังหน่วยและผู้เกี่ยวข้องเมื่อกองทัพถูกกระทำทางไซเบอร์ จัดตั้งนักรบไซเบอร์ของกองทัพอากาศ

เพื่อให้ใช้ปฏิบัติภารกิจด้านไซเบอร์และปรับปรุงให้ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ สำหรับงบประมาณ ต้องให้การสนับสนุนอย่างเพียงพอและต่อเนื่อง เพื่อให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ สิ่งสำคัญที่จะขาดมิได้คือผู้บริหารระดับสูงต้องมีความรู้และเข้าใจในการปฏิบัติการไซเบอร์และการทำสงครามไซเบอร์ อีกทั้งให้ความสำคัญในการปฏิบัติและให้การสนับสนุนอย่างต่อเนื่องทุกขั้นตอน สุดท้ายคือควรนำระบบสมรรถนะมาใช้ในการบริหารจัดการ นำระบบจัดการความรู้มาใช้เพื่อพัฒนากำลังให้มีความรู้ มีทักษะเพิ่มขึ้นเรื่อยๆ ที่จะขาดมิได้คือควรนำกระบวนการบริหารความเสี่ยงมาช่วยในการวางแผนและควบคุมการปฏิบัติ สุดท้ายต้องมีกระบวนการประเมินผลการปฏิบัติงานทุกวงรอบอย่างน้อยปีละสามครั้งเพื่อให้มั่นใจว่ากองทัพจะสามารถรับมือกับภัยคุกคามด้านไซเบอร์และการทำสงครามไซเบอร์ได้อย่างมีประสิทธิภาพ

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

สรุป

การวิจัยเรื่อง “แนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ” การวิจัยแบบผสมผสาน (Mixed Method Procedures) ประกอบด้วยการวิจัยเชิงคุณภาพ (Qualitative research) และการวิจัยเชิงปริมาณ (Quantitative Research) ดำเนินการค้นคว้าวรรณกรรมและงานวิจัยที่เกี่ยวข้อง พร้อมทั้งข้อมูลที่ได้จากแบบสอบถาม จากการสัมภาษณ์ผู้บริหารระดับสูง ระดับกลางและผู้เชี่ยวชาญ รวมทั้งมีการจัดสนทนากลุ่ม เพื่อให้ทราบคำตอบจากวัตถุประสงค์ของการวิจัยที่ตั้งไว้ สรุปได้ดังนี้

1. วัตถุประสงค์ของการวิจัย

1.1 เพื่อศึกษาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

1.2 เพื่อศึกษาปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

1.3 เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ

2. ผลที่ได้จากการวิจัย จากการศึกษาตามกระบวนการวิจัยในแต่ละขั้นตอน เป็นการศึกษาที่ใช้กรอบแนวคิดในการวิเคราะห์ และสังเคราะห์ข้อมูลที่เกี่ยวข้อง สรุปได้ดังนี้

2.1 ทำให้ทราบขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า มีขีดความสามารถในการปฏิบัติเชิงรุกอยู่ในระดับต่ำ แต่การปฏิบัติเชิงรับอยู่ในระดับปานกลาง ซึ่งมีสาเหตุดังนี้

2.1.1 กำลังพล พบว่า ความรู้ด้านไซเบอร์ไม่เพียงพอ ขาดทักษะและประสบการณ์ในการปฏิบัติการเชิงรุกด้านสงครามไซเบอร์ ผู้เชี่ยวชาญด้านสงครามไซเบอร์มีจำนวนน้อยมาก หน่วยปฏิบัติบรรจุกำลังพลไม่ตรงตามอัตราที่กำหนด กำลังพลขาดทักษะและความชำนาญด้านไซเบอร์ ผู้ปฏิบัติส่วนใหญ่เป็นข้าราชการที่บรรจุใหม่อายุราชการส่วนใหญ่น้อยกว่า 10 ปี จึงส่งผลให้ขาดประสบการณ์ด้านนี้ ส่วนผู้ที่มีประสบการณ์มากและเชี่ยวชาญสูงจะเป็นผู้บริหารระดับกลางและระดับสูงส่วนมากมีอายุราชการมากกว่า 20 ปี การผลิตกำลังพลทดแทนและการฝึกให้มีทักษะและความชำนาญอยู่ระหว่างดำเนินการคาดว่าอีก 2 ปีจึงจะสามารถมีขีดความสามารถตามที่กองทัพกำหนด

2.1.2 กระบวนการบริหาร/จัดการ พบว่า การจัดองค์กรยังไม่มีความสะดวกและรวดเร็วในการปฏิบัติงาน มีสายการปฏิบัติที่ยาวเกินไป รวมทั้งภารกิจและหน้าที่ที่ต้องปฏิบัติของหน่วยเกี่ยวข้องยังไม่ชัดเจนว่าต้องทำอะไร อย่างไรเกี่ยวกับสงครามไซเบอร์ อีกทั้งหลักนิยม นโยบายขาดความชัดเจนและความต่อเนื่อง รวมทั้งแนวทางและระเบียบปฏิบัติหรือกฎหมายที่เกี่ยวข้องด้านไซเบอร์ที่ยังไม่ครอบคลุมการปฏิบัติทั้งเชิงรุกและเชิงรับ ขาดความสมบูรณ์ในแผนยุทธศาสตร์

กองทัพอากาศและไม่มีแผนแม่บทด้านสงครามไซเบอร์ นอกจากนั้นยัง ไม่มีระบบการแจ้งเตือนภัยไปยังหน่วยต่างๆ เมื่อกองทัพถูกกระทำทางไซเบอร์

2.1.3 เทคโนโลยี ที่มีใช้ในปัจจุบันไม่ทันสมัย เครื่องมือหรืออุปกรณ์ต่างๆ ที่จำเป็นในการปฏิบัติงานเชิงรุกและเชิงรับมีไม่เพียงพอ ถึงแม้จะมีการนำหลักการมาตรฐานการรักษาความปลอดภัยเครือข่ายสารสนเทศมาใช้งานแต่ยังไม่สามารถป้องกันการบุกรุกเครือข่ายได้ดีเท่าที่ควร เทคโนโลยีได้ก้าวหน้าไปอย่างรวดเร็วแต่การเตรียมบุคลากรด้านนี้ยังตามไม่ทันและไม่เพียงพอ

2.2 ทำให้ทราบปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่าปัจจัยที่มีผลกระทบประกอบด้วย กำลังพล กระบวนการบริหาร/จัดการ เทคโนโลยี งบประมาณและความเอาใจใส่ของผู้บริหารระดับสูง ทัศนคติในการปฏิบัติงานร่วมกันมีรายละเอียดดังนี้

2.2.1 กำลังพล เป็นปัจจัยหลักที่ส่งผลกระทบมากที่สุด เพราะกิจกรรมทุกอย่างจะต้องมีคนเป็นผู้ควบคุมรับผิดชอบ หากกำลังพลขาดความรู้ ความสามารถ มีทักษะน้อยเกินไป อีกทั้งขาดความชำนาญในการปฏิบัติก็จะส่งผลให้ภารกิจไม่บรรลุผลสำเร็จ นอกจากนั้นกำลังพลควรจะต้องมีภาวะผู้นำและจิตสำนึกที่ดีต่อเพื่อนร่วมงานและต่อองค์กร รวมทั้งมีการสร้างบรรยากาศที่ดีในที่ทำงาน

2.2.2 กระบวนการบริหาร/จัดการ เป็นปัจจัยรองลงมาที่มีผลกระทบเนื่องมาจากการจัดองค์กรที่ไม่เอื้ออำนวยความสะดวกและรวดเร็วในการปฏิบัติ รวมทั้งภารกิจหน้าที่ที่ต้องปฏิบัติของหน่วยเกี่ยวข้องยังไม่ชัดเจนว่าต้องทำอะไร อย่างไรเกี่ยวกับสงครามไซเบอร์ อีกทั้งหลักนิยม นโยบาย หลักการ แนวทางและระเบียบปฏิบัติหรือกฎหมายที่เกี่ยวข้องด้านไซเบอร์ที่ไม่ครอบคลุมการปฏิบัติทั้งเชิงรุกและเชิงรับ ขาดความสมบูรณ์ในแผนยุทธศาสตร์กองทัพอากาศและไม่มีแผนแม่บทด้านสงครามไซเบอร์ ที่สำคัญคืองบประมาณต้องเพียงพอและต่อเนื่อง อีกทั้งผู้บริหารระดับสูง เป็นปัจจัยหลักที่สำคัญ ที่ต้องมีความรู้และเข้าใจในงานด้านนี้พร้อมทั้งให้การสนับสนุนอย่างจริงจังและต่อเนื่อง

2.2.3 เทคโนโลยี เป็นปัจจัยอีกอย่างหนึ่งที่มีผลกระทบ อันเนื่องมาจากเทคโนโลยีที่นำมาใช้ในการทำสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับไม่ทันสมัยและเครื่องมือหรืออุปกรณ์ต่างๆ ที่จำเป็นไม่เพียงพอ ถึงแม้จะมีการนำหลักการในระบบมาตรฐานการรักษาความปลอดภัยเครือข่ายสารสนเทศมาใช้งานแต่ยังไม่สามารถป้องกันการบุกรุกเครือข่ายได้ดีเท่าที่ควร เทคโนโลยีได้ก้าวหน้าไปอย่างรวดเร็วแต่การเตรียมบุคลากรด้านนี้ยังตามไม่ทันและไม่เพียงพอ

2.3 ทำให้ทราบแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า กองทัพอากาศควรพัฒนาในด้านต่างๆ ดังนี้

2.3.1 ด้านกำลังพล ต้องพัฒนาให้มีความรู้ความสามารถ มีทักษะและความเชี่ยวชาญด้านสงครามไซเบอร์ ส่งเสริมให้กำลังพลได้แสดงออกซึ่งความรู้ความสามารถที่มีอยู่ สร้างนักรบไซเบอร์กองทัพอากาศเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ รวมทั้งพิจารณากำหนดค่าตอบแทนพิเศษให้กับผู้ที่บรรจุเป็นนักรบไซเบอร์ของกองทัพในอัตราที่เหมาะสม ส่งเสริมให้มีการฝึกร่วมกันทั้งภายในและภายนอกกองทัพ และเฝ้าติดตามเทคโนโลยีที่ทันสมัยอยู่เสมอ ปลูกฝังให้มีภาวะผู้นำและมี

ทัศนคติที่ดีต่อองค์กร ต่อเพื่อนร่วมงาน รวมทั้งให้มีจิตสำนึกในการรักษาความปลอดภัยด้านไซเบอร์ร่วมกัน

2.3.2 ด้านการบริหาร/จัดการ ควรปรับปรุงหลักนิยมกองทัพอากาศ โดยกำหนดให้มีหลักการและแนวทางการปฏิบัติด้านสงครามไซเบอร์ พร้อมทั้งปรับปรุงแผนยุทธศาสตร์กองทัพอากาศให้ชัดเจนในหัวข้อการกำหนดเป้าหมายที่สำคัญของการปฏิบัติด้านสงครามไซเบอร์ และต้องจัดทำแผนแม่บทด้านสงครามไซเบอร์รองรับแผนยุทธศาสตร์เพื่อเป็นแนวทางในการดำเนินงานด้านสงครามไซเบอร์ให้หน่วยเกี่ยวข้อง ปรับปรุงโครงสร้างการจัดหน่วยและกำหนดภารกิจให้กับหน่วยอย่างชัดเจนว่าต้องรับผิดชอบอะไรและต้องทำอะไรในงานด้านนี้ และบรรจุกำลังพลที่มีความรู้ความสามารถด้านไซเบอร์ให้กับหน่วยปฏิบัติให้ตรงตามอัตราที่กำหนด เพื่อให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้ นอกจากนั้นควรนำกระบวนการบริหารงาน Deming Circle ที่ใช้หลักการ Plan-Do-Check- Act เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม นำกระบวนการจัดการความรู้ (Knowledge Management) มาใช้ในการถ่ายโอนความรู้อย่างเป็นระบบ เป็นการสร้างทรัพย์สินทางปัญญาของหน่วย เพื่อให้กำลังพลมีความรู้ที่ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ นำกระบวนการบริหารจัดการความเสี่ยง(Risk Management) เข้ามาช่วยในการบริหารงาน เพื่อให้ได้ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด ปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ให้ทุกหน่วยจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารหน่วยให้มีประสิทธิภาพ และนำระบบสมรรถนะ (Competency Model) มาใช้ในการพัฒนาองค์กรเพราะจะทำให้บุคลากรในทุกตำแหน่งทราบถึงความรู้ ความสามารถของตนเอง และทราบว่าจะต้องพัฒนาและฝึกฝนอย่างไรจึงจะทำให้มีขีดความสามารถเพิ่มขึ้น และจัดให้มีระบบจำลองยุทธด้านไซเบอร์ หรือที่เรียกว่า “Cyber Range” เพื่อแก้ปัญหาด้านบุคลากรและการเรียนรู้การสอนโดยเน้นไปที่ “Do” หรือ “Practice” มากกว่าการ “See and Hear” และที่สำคัญต้องมีการประเมินผลการปฏิบัติงานอย่างน้อยปีละสองครั้งเพื่อติดตามความพร้อมของหน่วยและกำลังพลให้สามารถปฏิบัติภารกิจได้ตลอดเวลา สุดท้ายคือผู้บริหารระดับสูงจะต้องมีความรู้ในด้านนี้และเอาใจใส่อย่างจริงจัง ให้การสนับสนุนอย่างต่อเนื่องทุกระดับ

2.3.3 ด้านเทคโนโลยี ควรจัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วยให้พอเพียงตามความจำเป็นและเหมาะสมกับภารกิจที่หน่วยได้รับ นำหลักการในระบบมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เพราะเป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก รวมทั้งจัดให้มีระบบแจ้งเตือนภัยไปยังหน่วยและผู้เกี่ยวข้องเมื่อกองทัพถูกกระทำทางไซเบอร์ เพื่อให้หน่วยและผู้เกี่ยวข้องเพิ่มการระวังป้องกันมิให้ระบบถูกโจมตีจากไซเบอร์ นอกจากนั้นจำเป็นต้องจัดหาอาวุธไซเบอร์ที่ทันสมัยเพื่อให้นักรบไซเบอร์ของกองทัพอากาศใช้ปฏิบัติภารกิจด้านไซเบอร์ และปรับปรุงให้ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ ให้การสนับสนุนการวิจัยและนำผลการวิจัยมาใช้งานเพื่อทำให้ระบบมีความ

แข็งแรง คงทน สามารถลดเวลาในการตรวจจับและการตอบสนองอันจะทำให้การป้องกันมีประสิทธิภาพ

2.3.4 ด้านงบประมาณ ควรให้ความสำคัญกับภารกิจด้านสงครามไซเบอร์ ด้วยการสนับสนุนงบประมาณให้เพียงพอและต่อเนื่อง เพื่อให้หน่วยเกี่ยวข้องสามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ และส่งเสริมให้หน่วยจัดหาโปรแกรมที่ถูกกฎหมายและทันสมัยมาใช้งาน เพื่อให้สามารถตรวจจับและป้องกันการบุกรุกหรือการทำสงครามไซเบอร์ได้เป็นอย่างดี

อภิปรายผล

ผลการวิจัยที่ได้เป็นแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยแนวทางดังกล่าวนี้สอดคล้องกับแนวความคิด ทฤษฎีและผลงานวิจัยที่เกี่ยวข้องตามที่ได้กล่าวไว้แล้วในบทที่ 2 เช่น ระบบสมรรถนะในการบริหารองค์กร (อาภรณ์ ภู่วิทยพันธุ์ (2552:17-18)) การให้ความสำคัญกับบรรยากาศภายในองค์กร (สเตียร์ส (Steers, 1977)) การพัฒนาไปสู่องค์กรสมัยใหม่ที่เน้นการจัดความรู้เป็นสำคัญ อีกทั้งการบริหารความเสี่ยงที่ต้องนำมาพิจารณาภัยคุกคามรูปแบบใหม่ที่ต้องให้ความสำคัญในการจัดการ การจัดหน่วยและการบริหารหน่วยที่รับผิดชอบงานด้านสงครามไซเบอร์ของกองทัพอากาศที่จัดตั้งขึ้นมาใหม่ อีกทั้งผลงานวิจัยของนาวาอากาศเอก รศ.ดร.ประสงค์ ประณีตพลกรัง เรื่องแผนยุทธศาสตร์การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ ผลงานวิจัยของ นาวาอากาศโท จตุชัย แพงจันทร์ เรื่องรูปแบบการปฏิบัติการสงครามไซเบอร์ และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง และผลงานวิจัยของนาวาอากาศโท วัชรพงศ์ ธรรมรักษ์ เรื่องการบริหารจัดการเครือข่ายการรักษาความปลอดภัยด้านสารสนเทศและด้านไซเบอร์ ซึ่งสามารถนำมาพิจารณาร่วมกันและวิเคราะห์ เพื่อใช้เป็นแนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศได้อย่างดี มีความเหมาะสมที่จะนำไปใช้เพื่อพัฒนาบุคลากร การบริหารองค์กร การจัดองค์กร และการพัฒนาขีดความสามารถของระบบอาวุธยุทโธปกรณ์ ให้มีความพร้อมที่จะปฏิบัติการด้านสงครามไซเบอร์และพร้อมรับมือกับภัยคุกคามรูปแบบใหม่ได้ทุกรูปแบบ และสามารถรองรับเทคโนโลยีที่ใช้ระบบเครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพ โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนวทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือ มีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับได้อย่างมีประสิทธิภาพ มีความมั่นคงยั่งยืนและสามารถพึ่งพาตนเองได้

ประโยชน์ที่ได้จากการวิจัย นอกจากจะทำให้มีความเข้าใจอย่างถูกต้อง ได้ทราบองค์ประกอบและได้ทราบแนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ทำให้เกิดแบบแผนการพัฒนาการปฏิบัติด้านสงครามไซเบอร์อย่างเป็นรูปธรรม เพื่อสอดรับวิสัยทัศน์ที่จะก้าวไปสู่ความเป็นกองทัพอากาศชั้นนำในภูมิภาคอาเซียน (One of the best Air Forces in ASEAN) และเป็นไปตามนโยบายของผู้บัญชาการทหารอากาศในด้านการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อเสนอแนะ

โดยสรุปข้อเสนอแนะของการวิจัยสามารถแจกแจงได้เป็น 2 ด้าน ได้แก่ ข้อเสนอแนะการต่อยอดงานวิจัยที่สนับสนุนมุมมองในเชิงนโยบาย และข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป โดยมีรายละเอียดดังนี้

1. ข้อเสนอแนะการต่อยอดงานวิจัยที่สนับสนุนมุมมองในเชิงนโยบาย

1.1 ด้านกำลังพล

1.1.1 ฝึกอบรมให้กำลังพลก้าวทันเทคโนโลยีอยู่เสมอ มีความรู้ ความสามารถเทียบเท่ากับระดับสากลเพื่อให้รับมือกับสงครามไซเบอร์ได้ และฝึกปฏิบัติจริงด้านสงครามไซเบอร์เพื่อให้กำลังพลมีความรู้เท่าทันสถานการณ์และสามารถแก้ไขปัญหาได้อย่างรวดเร็ว ปลูกฝังให้มีภาวะผู้นำในทุกระดับ

1.1.2 จัดให้มีการฝึกร่วมระหว่างหน่วยงานภายในและภายนอกกองทัพอากาศเพื่อเพิ่มพูนทักษะและประสบการณ์ อีกทั้งสามารถติดตามเทคโนโลยีใหม่ๆ ที่นำมาใช้ในการทำสงครามไซเบอร์ ส่งเสริมให้มีการแสดงออกซึ่งความสามารถที่มีอยู่

1.1.3 ปลูกฝังให้กำลังพลทุกระดับมีจิตสำนึก มีความตระหนักในการรักษาความปลอดภัยด้านไซเบอร์ ให้มีความรู้และเข้าใจถึงผลเสียหายเมื่อถูกกระทำทางไซเบอร์ทั้งเรื่องของราชการและเรื่องส่วนตัว

1.1.4 พิจารณาเพิ่มค่าตอบแทนพิเศษให้กับผู้ปฏิบัติงานด้านสงครามไซเบอร์โดยมีข้อกำหนดว่าต้องผ่านการทดสอบและผ่านการอบรมหลักสูตรที่ได้มาตรฐานมีใบประกาศนียบัตรรับรองจากองค์กรที่ได้มาตรฐานหรือเป็นที่ยอมรับทั่วไปจึงจะได้รับค่าตอบแทนพิเศษ

1.1.5 กำหนดเส้นทางการเจริญเติบโตที่ชัดเจนของกำลังพล เปิดโอกาสให้เท่าเทียมกัน เพื่อให้กำลังพลมีความมั่นใจในวิชาชีพ มีความเจริญก้าวหน้าอย่างต่อเนื่อง

1.1.6 ควรมีหลักสูตรการเรียนการสอนในสายวิทยาการ การเพิ่มพูนความรู้ให้กับหน่วยเกี่ยวข้องอย่างต่อเนื่องเพื่อให้มีการทำงานทดแทนกันได้

1.1.7 การรับสมัครกำลังพลเข้ามาใหม่จะต้องกำหนดคุณสมบัติให้มีความรู้ด้านไซเบอร์ มีจิตสำนึกในการรักษาความปลอดภัยด้านไซเบอร์ มีทัศนคติที่ดีต่อองค์กรและเพื่อนร่วมงาน และกำลังพลที่รับเข้ามาไม่จำเป็นต้องบรรจุเป็นทหาร ไม่จำเป็นต้องทำงานในหน่วย สามารถปฏิบัติงานนอกหน่วย เช่น ที่บ้าน ที่บริษัทซึ่งส่งไปแฝงตัวอยู่ในระบบต่างๆ ในภาคเอกชน เพื่อใช้เป็นเครื่องมือในการติดตาม ตรวจสอบ และส่งข้อมูลให้กับส่วนกลาง มีอัตราค่าตอบแทนที่เหมาะสมตามความสามารถในการปฏิบัติงานที่ประเมินผลผ่านค่ามาตรฐาน

1.1.8 กำหนดแนวทางในการคัดเลือกกำลังพลที่มีความรู้ความสามารถด้านไซเบอร์เพื่อสร้างนักรบไซเบอร์ของกองทัพอากาศ โดยให้ปฏิบัติอยู่กับหน่วยต่างๆ ในกองทัพอากาศและนอกกองทัพอากาศ โดยมีภารกิจการปฏิบัติด้านสงครามไซเบอร์ตามที่กำหนด และจัดหาอาวุธไซเบอร์ให้กับนักรบเหล่านั้นอย่างเหมาะสมและเพียงพอ

1.2 ด้านการบริหารจัดการ

1.2.1 ปรังปรุงหลักนิยมกองทัพอากาศโดยกำหนดให้มีหลักการและแนวทางการปฏิบัติด้านสงครามไซเบอร์ ปรับปรุงแผนยุทธศาสตร์ของกองทัพอากาศ ให้มีเป้าหมายหลักและรองที่ต้องการอย่างชัดเจนเกี่ยวกับการปฏิบัติด้านสงครามไซเบอร์ และจัดทำแผนแม่บทด้านสงครามไซเบอร์รองรับแผนยุทธศาสตร์ดังกล่าว กำหนดแนวทางการปฏิบัติและหน่วยที่ต้องปฏิบัติให้ชัดเจนทั้งเชิงรุกและเชิงรับ เพื่อเป็นแนวทางให้หน่วยเกี่ยวข้องนำไปวางแผนในการปฏิบัติและขอรับการสนับสนุนงบประมาณต่อไป

1.2.2 ปรับปรุงโครงสร้างการจัดหน่วย ทั้งฝ่ายอำนวยการและหน่วยปฏิบัติให้มีหน่วยงานรองรับ มีกำลังพลบรรจุให้ตรงตามอัตราที่กำหนดอย่างเพียงพอและมีคุณภาพ ผู้ปฏิบัติงานด้านไซเบอร์ไม่จำเป็นต้องมีตำแหน่งอยู่ในกองทัพก็สามารถทำงานให้กองทัพได้ การกำหนดภารกิจ การสร้างองค์ความรู้และโครงสร้างการจัดหน่วยงานต้องสอดคล้องกับภารกิจ ซึ่งหน่วยงานด้านสงครามไซเบอร์ควรเป็นหน่วยอิสระที่ขึ้นตรงต่อผู้บัญชาการทหารอากาศ หัวหน้าหน่วยควรได้รับมอบอำนาจในการสั่งการปฏิบัติด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับในเบื้องต้น เพื่อป้องกันการกระทำจากฝ่ายตรงข้าม และเป็นหน่วยที่ปฏิบัติงานภายใต้ศูนย์ปฏิบัติการกองทัพอากาศเพื่อพิจารณาให้ข้อเสนอแนะการปฏิบัติด้านสงครามไซเบอร์ต่อผู้บัญชาการทหารอากาศ

1.2.3 นำปัจจัย 4 ข้อมาพิจารณาวางแผนกลยุทธด้านความมั่นคงปลอดภัย (Security Strategy) ได้แก่ Protection (การป้องกัน) Detection (การตรวจจับ) Reaction (การตอบสนอง) และTime (เวลา) ด้วยการ “ลดเวลาในการตรวจจับ” (decrease Detect time) และ “ลดเวลาในการตอบสนอง” (decrease React time) จะทำให้ระบบรักษาความปลอดภัยขององค์กรมั่นคงปลอดภัยจากสงครามไซเบอร์

1.2.4 ต้องมีการอัพเดทข้อมูลต่างๆ ของฝ่ายเราเป็นประจำ ต้องมีมาตรการเตรียมความพร้อมเพื่อรับมือกับการโจมตีทางไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม

1.2.5 นำกระบวนการบริหารงานให้มีคุณภาพ ของ Deming Circle คือ Plan-Do-Check- Act เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม การตรวจสอบที่นำไปสู่การแก้ไขปรับปรุงทำให้ปัญหาที่เกิดขึ้นแล้วไม่เกิดซ้ำ หรือลดความรุนแรงของปัญหา ถือเป็นการนำความผิดพลาดมาใช้ให้เกิดประโยชน์มีความเหมาะสมกับการปฏิบัติงานด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ

1.2.6 นำกระบวนการบริหารความเสี่ยง(Risk Management) เข้ามาช่วยในการบริหารงาน เพื่อให้ได้ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด ปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ให้ทุกหน่วยจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารหน่วยให้มีประสิทธิภาพ

1.2.7 นำระบบสมรรถนะ(Competency Model) มาใช้ในการพัฒนาองค์กร เพราะจะทำให้บุคลากรในทุกตำแหน่งทราบถึงความรู้ ความสามารถของตนเอง และทราบว่าจะต้องพัฒนาและฝึกฝนอย่างไรจึงจะทำให้มีขีดความสามารถเพิ่มขึ้น

1.2.8 นำกระบวนการจัดการความรู้ (Knowledge Management) มาใช้เพื่อการถ่ายโอนความรู้อย่างเป็นระบบ เป็นการสร้างทรัพย์สินทางปัญญาของหน่วย เพื่อให้กำลังพลมีความรู้ที่ทันสมัยอยู่เสมอ

1.2.9 กำหนดหลักเกณฑ์และแนวทางในการวัดขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของหน่วย เพื่อให้หน่วยมีความพร้อมรับมือกับภัยคุกคามรูปแบบใหม่อยู่เสมอ และใช้เป็นข้อมูลในการปรับปรุงพัฒนาและวางแผนของบประมาณสนับสนุนต่อไป

1.2.10 จัดให้มีระบบจำลองยุทธด้านไซเบอร์ หรือที่เรียกว่า “Cyber Range” เพื่อแก้ปัญหาด้านบุคลากรและการเรียนรู้การสอนโดยเน้นไปที่ “Do” หรือ “Practice” มากกว่าการ “See and Hear”

1.2.11 ผู้บริหารชั้นสูงของหน่วยทุกระดับ ต้องศึกษาและเข้าใจในการปฏิบัติด้านไซเบอร์และการทำสงครามไซเบอร์ พร้อมทั้งให้การสนับสนุนการปฏิบัติทุกมิติอย่างจริงจังและต่อเนื่อง

1.3 ด้านเทคโนโลยี

1.3.1 จัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วย ให้พอเพียงตามความจำเป็นและเหมาะสมกับภารกิจที่หน่วยได้รับ

1.3.2 นำหลักการในระบบมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เพราะเป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก

1.3.3 จัดให้มีระบบแจ้งเตือนภัยไปยังหน่วยและผู้เกี่ยวข้องเมื่อกองทัพถูกกระทำทางไซเบอร์เพื่อให้หน่วยและผู้เกี่ยวข้องเพิ่มการระวังป้องกันมิให้ระบบถูกโจมตีจากไซเบอร์

1.3.4 พิจารณาจัดหาอาวุธไซเบอร์ที่ทันสมัย เพื่อให้นักรบไซเบอร์ของกองทัพอากาศใช้ปฏิบัติภารกิจด้านไซเบอร์ และปรับปรุงให้ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ

1.4 ด้านงบประมาณ

1.4.1 ให้ความสำคัญกับภารกิจด้านสงครามไซเบอร์ ด้วยการสนับสนุนงบประมาณให้เพียงพอ เพื่อให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ

1.4.2 ให้การสนับสนุนงบประมาณเพื่อให้หน่วยใช้โปรแกรมที่ถูกกฎหมายและใช้โปรแกรมที่ทันสมัย สามารถตรวจจับและป้องกันการทำสงครามไซเบอร์ได้เป็นอย่างดี

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ผู้วิจัยขอเสนอแนวทางการทำวิจัยต่อยอดในประเด็นที่เกี่ยวข้องกับสงครามไซเบอร์และความมั่นคงปลอดภัยไซเบอร์ ดังนี้

2.1 สมรรถนะ (Competency) ของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์สำหรับข้าราชการทั่วไปและข้าราชการที่ทำงานในตำแหน่งเฉพาะที่เกี่ยวข้องกับไซเบอร์ในกองทัพอากาศควรเป็นอย่างไร

2.2 การพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ให้เพียงพอต่อความต้องการของกองทัพอากาศควรมียุทธศาสตร์อย่างไร

2.3 การกำหนดตำแหน่งและมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยด้านไซเบอร์และด้านสงครามไซเบอร์สำหรับสนับสนุนการมุ่งสู่ AEC และการเป็นกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force: NCAF) รวมทั้งการเป็นกองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Force in ASEAN) ควรมียุทธศาสตร์อย่างไร

2.4 การวิจัยในเชิงการสร้างนวัตกรรมด้านเทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ ควรเป็นอย่างไร

2.5 การตระหนักรู้ของข้าราชการในกองทัพอากาศต่อความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ควรเป็นอย่างไร

2.6 การจัดสรรงบประมาณด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ในกองทัพอากาศเท่าใดถึงจะเพียงพอและเหมาะสม

2.7 ระดับความเสี่ยงด้านไซเบอร์ในกองทัพอากาศเป็นอย่างไร

2.8 สภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ในกองทัพอากาศเป็นอย่างไร

2.9 ทัศนคติและความร่วมมือของข้าราชการในกองทัพอากาศต่อความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์เป็นอย่างไร

บรรณานุกรม

ภาษาไทย

หนังสือ

กลาโหม, กระทรวง. แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม ฉบับที่ 2 พ.ศ.2551-2554. กรุงเทพฯ : กระทรวงกลาโหม, 2551.

กองทัพไทย. แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย และกองบัญชาการกองทัพไทย พ.ศ.2557-2561. กรุงเทพฯ : กองทัพไทย, 2557.

กองทัพอากาศ. แผนพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ พ.ศ.2557-2562. กรุงเทพฯ : กองทัพอากาศ, 2557.

กองทัพอากาศ. ยุทธศาสตร์กองทัพอากาศ พ.ศ.๒๕๕๑-๒๕๖๒ (ฉบับปรับปรุง พ.ศ.๒๕๕๒). 2552.

จตุชัย แพงจันทร์, นาวาอากาศตรี. Master in Security 2nd Edition. นนทบุรี: ไอดีซี พรีเมียร์, 2553.

จตุชัย แพงจันทร์. Master in Security 2nd Edition. อินโฟเพรส,บริษัท ไอดีซีพรีเมียร์ จำกัด, 2553.

จตุชัย แพงจันทร์. เจาะระบบ Network 3rd Edition. นนทบุรี: ไอดีซีฯ, 2555.

เทคโนโลยีสารสนเทศและการสื่อสาร, กระทรวง. (ร่าง)แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ของประเทศไทย พ.ศ.2557-2561. กรุงเทพฯ : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2557.

พูลศิริ พรหมกูล. การสำรวจความต้องการใช้ทรัพยากรสารสนเทศของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา. กรุงเทพฯ, 2555.

ริชาร์ด เอ. คลาร์ก และ โรเบิร์ต คเนค. CYBER WAR. กรุงเทพฯ : สำนักพิมพ์มติชน, 2555.

สุชาดา กีระนันทน์. เทคโนโลยีสารสนเทศสถิติ:ข้อมูลในระบบสารสนเทศ. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย., 2541.

สุเมธ จิตภักดีบดินทร์. ก้าวสู่นักทดสอบและป้องกันการเจาะระบบ. กรุงเทพฯ : สำนักพิมพ์ EZ-GENIUS., 2556.

ฐานข้อมูลอิเล็กทรอนิกส์

กองทัพเรือ. “แนวทางการใช้งานระบบสารสนเทศ”.(ออนไลน์). เข้าถึงได้จาก : http://www.Logis.navy.mi.th/data/loganalyse/it_appr.pdf, 2557.

กองทัพเรือ. “ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยสารสนเทศ พ.ศ.2554”.(ออนไลน์). เข้าถึงได้จาก : http://www.ctbdc.navy.mi.th/it_ctbdc/rabiabnavy_ 2554.pdf, 2554.

กองทัพอากาศ. “นโยบายผู้บัญชาการทหารอากาศ พุทธศักราช 2558”. (ออนไลน์). เข้าถึงได้จาก http://imgcdn.rtaf.mi.th/web/rtafpolicy/RTAF_Policy_58.pdf , 2558.

กองทัพอากาศ. “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ”. (ออนไลน์). เข้าถึงได้จาก:http://imgcdn.rtaf.mi.th/2556/admin/RTAF_25561102015313.pdf, 2557.

“การจัดการความเสี่ยง”. (ออนไลน์). เข้าถึงได้จาก : http://ermthailand.blogspot.com/p/erm-coso.html,2558.

ดารารัตน์ เข็มจร. “ความท้าทายใหม่ของการบริหารทรัพยากรมนุษย์”. (ออนไลน์). เข้าถึงได้จาก. http://gotoknow.org/blog/d, 2558.

ไทยรัฐ, หนังสือพิมพ์. “อัพเดทกองทัพไทย รับสงครามไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก http://www.thairath.co.th/content/382273, 2558.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์๖องค์การมหาชน,สำนักงาน). (ออนไลน์). เข้าถึงได้จาก : http://www.etda.or.th, 2557.

พิสิฏฐ์ สินธุวงศานนท์. “ระบบโทรคมนาคม”. (ออนไลน์). เข้าถึงได้จาก.https://www.gotoknow.org/posts/282028, 2558.

เมธา สุวรรณสาร. “การจัดการความเสี่ยง © 2013 Information Technology Governance.” (ออนไลน์). เข้าถึงได้จาก : http://th.wikipedia.org/wiki/การจัดการความเสี่ยง, 2558

ฤทธี อินทราวุธ, พ.อ. “กองทัพบกกับความมั่นคงปลอดภัยด้านไซเบอร์ของชาติ”.(ออนไลน์).เข้าถึงได้จาก http://km.rta.mi.th/newkm/index.php/menu-km6/4-army-and-national-cyber-security, 2557.

“วงจรการบริหารงานคุณภาพ Henri Fayol”. (ออนไลน์). เข้าถึงได้จาก: http://adisony.blogspot.com/2012/10/henri-fayol.html , 2558.

“วงจรการบริหารงานคุณภาพ Edwards Deming”. (ออนไลน์). เข้าถึงได้จาก : http://adisony.blogspot.com/2012/10/edward-deming.html, 2558.

ศูนย์รักษาความปลอดภัยคอมพิวเตอร์.(ออนไลน์). เข้าถึงได้จาก : http://csc.mod.go.th/about, 2557.

เอกสารวิจัย

จตุชัย แพงจันทร์, นาวาอากาศโท. “รูปแบบการปฏิบัติการสงครามไซเบอร์ และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, 2555.

จักรกฤษณ์ ธรรมมาวิชัย, นาวาอากาศตรี. “การเตรียมกำลังทางอากาศใน Network Centric Operations.” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, 2550.

บุญมี บุญเอี่ยม, “ศึกษาการนำอิทธิบาท 4 ไปใช้ในการทำงานของพนักงานศูนย์ควบคุมการบินภูเก็ต บริษัท วิทยุการบินแห่งประเทศไทย จำกัด”. วิทยานิพนธ์การศึกษามหาบัณฑิต, มหาวิทยาลัยทักษิณ, 2544.

ประสงค์ ปราณีตพลกรัง, นาวาอากาศเอก ดร. “แผนยุทธศาสตร์การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ สถาบันวิชาการทหารอากาศชั้นสูง กองบัญชาการฝึกศึกษาทหารอากาศ, 2557.

วัชรพงศ์ ธรรมรักษ์, นาวาอากาศโท. “ตัวแบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) สำหรับกองทัพอากาศ” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, 2554.

วิโรจน์ ธันวรักษ์กิจ,พลเรือตรี. “แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย” เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2556.

สุชาติ ผ่องพุฒิ ,พลตรี. “แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย” เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2556.

อมร ชมเชย, นาวาอากาศโท. “ระบบการรักษาความปลอดภัยด้านระบบสารสนเทศกองทัพอากาศให้พร้อมรับกับ Digital Air Force และ Network Centric Warfare.” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, 2551.

อำพน ธรรมโชติ, “การพัฒนาประสิทธิภาพการทำงานของพนักงาน การไฟฟ้าส่วนภูมิภาค จังหวัดเพชรบุรี”. วิทยานิพนธ์บริหารธุรกิจมหาบัณฑิต, สาขาการจัดการทั่วไป, มหาวิทยาลัยราชภัฏสวนดุสิต, 2548.

ภาษาต่างประเทศ

Journal

L. Gulick and J. Urwick, Papers on the Science of Administration, (New York : Institute of Public Administration, 1973).

Price, Alan. Human Resource Management, In a Business Context, 2 edition (London: Thomson Learning, 2004).

“The New Economics”. The MIT Press; 2nd edition (August 11, 2000).

U.S. Headquarters, Department of the Army. “Signal Support to Theater Operations”. (Field Manual No.11-45, April12,2004)

Databases on the Internet

“Information system”. (Online). Available : // en.wikipedia. org/ wiki/Information_system Laudon, K.C. & Laudon, J.P.(2001). Essentials of management information systems: Organization and technology in the enterprise. 4th ed. Upper Saddle River, NJ: Prentice Hall. 2005.

Net-Security. “Lack of computer security experts weighs heavy on U.S. cyber defense” .(online).Avialable:http://www.net-security.org/secworld.php?id=9611,2010.

Routine Collection of Capture Fishery Data. “Annex 5 Glossary”. (Online). Available : //www.fao.org/documents/ show_cdr.asp?url_file=/DOCREP/003/ X2465E/x2465e0h.htm, 2005.

“Siam Intelligence”. (ออนไลน์). เข้าถึงได้จาก : http://www.siamintelligence.com/obama cyber-security-order/, 2556.

TELECOM JOURNAL. “Cyber Security ต้องรู้ก่อนเข้าสู่ Digital Econommy”. (ออนไลน์). เข้าถึงได้จาก : http://www.nstda.or.th/news/19700-cyber-security, 2557.

The United States Department of Defense. “Special Report:The Cyber Domain”. (online).Avialable:http://www.defense.gov/home/features/2013/0713_cyberdomain, 2013.

US-CERT. “The National Strategy to Secure Cyberspace”. (online). Avialable : http:// www.us-cert.gov/sites/default/files/publications/crberspace_strategy.pdf, 2003.

Van Vliet, V. William Edwards Deming. Retrieved [insert date] from ToolsHero: http://www.toolshero.com/william-edwards-deming/, 2009.

ภาคผนวก

ผนวก ก.
รายชื่อผู้ให้สัมภาษณ์เชิงลึกและการสนทนากลุ่ม

1. รายชื่อผู้ให้การสัมภาษณ์เชิงลึก

1.1 พล.อ.อ.จอม รุ่งสว่าง	เสนาธิการทหารอากาศ
1.2 พล.อ.ท.พิชัย เขม้นจันทร์	เจ้ากรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ
1.3 พล.อ.ต.จิโรจ บำรุงลาภ	ผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.4 พล.อ.ต.ชาวลา ราชวงศ์	ผู้อำนวยการสำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.5 น.อ.ทรงพล พรหมวา	รองผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.6 น.อ.อัศวิน รุจาคม	รองผู้อำนวยการสำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.7 น.อ.รศ.ดร.ประสงค์ ปราณีตพลกรัง	กองวิชาคณิตศาสตร์และคอมพิวเตอร์ กองการศึกษา โรงเรียนนายเรืออากาศ
1.8 น.อ.วิสุทธิ์ สมภักดี	ผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.9 น.อ.อมร ชมเชย	รองผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.10 น.อ.นิวัต เนียมพลอย	รองผู้อำนวยการ กองนโยบายและแผน สำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

2. รายชื่อผู้เข้าร่วมการสนทนากลุ่ม (Focus Group)

2.1 น.อ.ประยูร ธรรมาธิวัฒน์	รองผู้อำนวยการ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.2 น.อ.ทรงพล พรหมวา	รองผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.3 น.อ.รศ.ดร.ประสงค์ ปราณีตพลกรัง	รองศาสตราจารย์ กองการศึกษา โรงเรียนนายเรืออากาศ
2.4 น.อ.วิสุทธิ์ สมภักดี	ผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.5 น.อ.นิวัต เนียมพลอย	รองผู้อำนวยการ กองนโยบายและแผน สำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.6 น.อ.สุรชาติ จันทรเสนีย์	ผู้อำนวยการกองกรรมวิธีข้อมูล สำนักบริหารงบประมาณ สำนักปลัดบัญชีทหารอากาศ
2.7 น.อ.วิชัย ดีชัย	นายทหารฝ่ายเสนาธิการ ประจำ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.8 น.อ.สกล ทองใบใหญ่	นายทหารเทคโนโลยีการรักษาความปลอดภัยคอมพิวเตอร์ ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
2.9 น.อ.อภิชาติ บุตรสาทร	รองผู้อำนวยการกองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
2.10 น.อ.ผศ. ดร. พาห์รณ สงวนโภคัย	ผู้อำนวยการกองวิชาคณิตศาสตร์และคอมพิวเตอร์ โรงเรียนนายเรืออากาศ

2.11 น.อ.ดร.สุธี จันทรพันธุ์ อาจารย์ภาควิชาคอมพิวเตอร์ กอง การศึกษา โรงเรียนนายเรืออากาศ

2.12 ร.อ.พายัพ ศิรินาม อาจารย์ภาควิชาคอมพิวเตอร์ กอง การศึกษา โรงเรียนนายเรืออากาศ

3. หัวข้อที่ใช้ในการสัมภาษณ์เชิงลึก มีรายละเอียดดังนี้

3.1 ท่านมีความเห็นอย่างไร เกี่ยวกับการปฏิบัติต่างๆ ด้านสงครามไซเบอร์ ซึ่งเป็นภารกิจใหม่ที่หน่วยงานต้องรับมือในปัจจุบัน

3.2 ท่านมีความเห็นอย่างไร เกี่ยวกับปัจจัยที่มีผลกระทบต่อการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วยในปัจจุบัน เช่น กำลังพล เครื่องมือ/อุปกรณ์ การบริหารจัดการ และงบประมาณ เป็นต้น

3.3 ท่านมีความเห็นอย่างไร ในการปรับปรุงและพัฒนาการปฏิบัติงานด้านสงครามไซเบอร์ของหน่วย ให้มีประสิทธิภาพเพิ่มขึ้น เช่น กำลังพล เครื่องมือ/อุปกรณ์ การบริหารจัดการ/การฝึก และงบประมาณ เป็นต้น

3.4 ท่านมีความเห็นว่าควรปฏิบัติอย่างไร เพื่อมิให้กำลังพลที่มีความรู้ความสามารถและทักษะด้านสงครามไซเบอร์ลาออกจากกองทัพ

3.5 ข้อเสนอแนะเพิ่มเติม

4. หัวข้อที่ใช้ในการสนทนากลุ่ม มีรายละเอียดดังนี้

4.1 ท่านคิดว่า สมรรถนะหรือ ขีดความสามารถในการปฏิบัติการด้านสงครามไซเบอร์ควรมีความหมายอย่างไร

4.2 ท่านคิดว่า กองทัพควรใช้วิธีการอย่างไร ในการประเมินสมรรถนะ หรือขีดความสามารถในการปฏิบัติการด้านสงครามไซเบอร์

4.3 แนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ ควรเป็นอย่างไร

4.4 แนวทางการได้มาและรักษาบุคลากรที่มีสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ควรเป็นอย่างไร

4.5 รูปแบบในการปฏิบัติเชิงรุกและเชิงรับด้าน Cyber Warfare ของกองทัพควรเป็นแบบใดจึงจะใช้ได้ผล

4.6 กองทัพควรใช้นวัตกรรมการป้องกัน Cyber Warfare แบบใดจึงจะเหมาะสมและยั่งยืน

4.7 ปัจจัยความสำเร็จต่อการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ควรมีอะไรบ้าง

ผนวก ข.
แบบสอบถาม
“แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ”

คำชี้แจงแบบสอบถาม

1. แบบสอบถามฉบับนี้มีจุดมุ่งหมาย เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถด้านสงครามไซเบอร์ของกองทัพอากาศ

2. แบบสอบถามฉบับนี้ แบ่งออกเป็น 3 ตอน คือ 1. แบบสอบถามเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม 2. แบบสอบถามความรู้ ความเข้าใจการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและสงครามไซเบอร์ 3. ข้อเสนอแนะเพิ่มเติมเกี่ยวกับการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์

3. แบบสอบถามฉบับนี้ใช้สำหรับการศึกษาวิจัยเท่านั้น การตอบแบบสอบถามนี้จะไม่มีผลกระทบต่อท่านแต่อย่างใด แต่จะเป็นประโยชน์ในกระบวนการทำงานของบุคลากรของหน่วยงาน

4. โปรดเติมเครื่องหมาย ✓ และกรอกข้อความให้สมบูรณ์

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. เพศ ☐ ชาย ☐ หญิง

2. อายุ ☐ 25-35 ปี ☐ 36-46 ปี ☐ 47 ปีขึ้นไป

3. วุฒิการศึกษา ☐ ต่ำกว่าปริญญาตรี ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ระดับชั้นยศ ☐ จ.อ.- พ.อ.อ.(พิเศษ) ☐ ร.ต.-ร.อ. ☐ น.ต.-น.อ. ☐ น.อ.(พิเศษ) ขึ้นไป

5. ตำแหน่งปัจจุบัน

☐ ระดับกรม ☐ ระดับสำนัก ☐ ระดับกอง

☐ ระดับแผนก ☐ ระดับฝ่าย ☐ พนักงานราชการ/ลูกจ้าง

☐ อื่นๆ โปรดระบุ.....

6. อายุการทำงานในตำแหน่งนี้ ☐ น้อยกว่า 5 ปี ☐ 6-10 ปี ☐ 11-15 ปี ☐ 16-20 ปี ☐ 21 ปีขึ้นไป

ส่วนที่ 2 ความรู้ ความเข้าใจ ทักษะ ความพึงพอใจในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและสงครามไซเบอร์

ระดับ 5 = มากที่สุดหรือดีมาก 4 = มากหรือดี 3 = ปานกลางหรือพอใช้ 2 = น้อย 1 = น้อยที่สุดหรือต้องปรับปรุงแก้ไข

รายละเอียด	**ระดับความรู้ ความสามารถ ความพอใจ**

	5	4	3	2	1
1. ความรู้ ความเข้าใจเกี่ยวกับการปฏิบัติด้านสารสนเทศและสงครามไซเบอร์					
1.1 เข้าใจความหมายของคำว่า สงครามสารสนเทศ และ					
1.2 เข้าใจความหมายของคำว่า สงครามไซเบอร์					
1.3 เข้าใจถึงภัยคุกคามและอันตรายจากสงครามไซเบอร์และ					
1.4 เข้าใจภัยคุกคามและอันตรายการจากไวรัส มัลแวร์ หนอน					
1.5 เข้าใจถึงความเสียหายที่เกิดจากการแฮกเกอร์ หรือ นัก					
1.6 มีความรู้เกี่ยวกับการป้องกันไวรัส มัลแวร์ หนอน					
1.7 มีความรู้เกี่ยวกับการใช้คอมพิวเตอร์ให้ทำงานอื่น					
1.8 มีความเข้าใจวิธีการกำหนดความรู้ความสามารถของบุคคล					
2. ทักษะการปฏิบัติงานด้านสารสนเทศและสงครามไซเบอร์					
2.1 มีความสามารถในการติดตั้งและกำหนดค่าต่างๆของระบบ					
2.2 มีความสามารถในการค้นหาและกำจัดไวรัสคอมพิวเตอร์					
2.3 มีความสามารถในการใช้โปรแกรมเจาะระบบคอมพิวเตอร์					
2.4 มีความสามารถในการเขียนโปรแกรมเจาะระบบ หรือ					
2.5 มีความสามารถในการเขียนโปรแกรมคอมพิวเตอร์หรือ					
2.6 มีความสามารถในการเรียนรู้และถ่ายทอดความรู้ให้กับผู้อื่น					
2.7 ระดับขีดความสามารถของบุคคลในหน่วยในการป้องกัน					
2.8 ระดับขีดความสามารถของหน่วยในการป้องกันระบบ					
3. ความคิด ทัศนคติ แรงจูงใจและความต้องการส่วนตัวของบุคลล					
3.1 ต้องการให้ตำแหน่งที่เกี่ยวกับสงครามไซเบอร์มี					
3.2 ต้องการให้จัดอบรมเพื่อให้เข้าใจเกี่ยวกับการปฏิบัติด้าน					
3.3 ต้องการเอกสารและข่าวสารที่เกี่ยวข้องกับสงครามไซเบอร์					
3.4 ต้องการให้จัดฝึกการปฏิบัติเกี่ยวกับสงครามไซเบอร์ทั้งเชิง					
รุกและเชิงรับ					
รายละเอียด	**ระดับความรู้ ความสามารถ ความพอใจ**				
	5	4	3	2	1
3.5 ต้องการสร้างขวัญกำลังใจ แรงจูงใจ จนท.ที่ปฏิบัติงานด้าน					
3.6 ต้องการให้มีหน่วยงานรับผิดชอบงานสงครามไซเบอร์ใน					
3.7 ต้องการให้หมุนเวียนกำลังพลในการปฏิบัติงานด้าน					

4. ความพึงพอใจ ในการปฏิบัติงานในที่ทำงาน					
4.1 มีความพอใจในสถานที่ทำงาน					
4.2 มีความพอใจในระบบรักษาความปลอดภัยเครือข่ายของ					
4.3 มีความพอใจในระบบป้องกันไวรัสคอมพิวเตอร์ที่ใช้อยู่ใน					
4.4 มีความพอใจในระเบียบและคำแนะการปฏิบัติด้านสงคราม					
4.5 ตำแหน่งของท่านตรงกับอัตราที่ ทอ. กำหนดไว้ให้บรรจุใน					
4.6 ตำแหน่งปัจจุบันให้ความรู้ความเข้าใจต่อการปฏิบัติงาน					
5. ความพึงพอใจของท่านต่อภาพรวมของหน่วยงาน					

ส่วนที่ 3 ข้อเสนอแนะ

สิ่งที่ท่านต้องการให้มีการปรับปรุงแก้ไข

3.1 ด้านกำลังพล

.....

3.2 ด้านเครื่องมือ เครื่องใช้และสิ่งอำนวยความสะดวกในการปฏิบัติงาน

.....

3.3 ด้านการบริหารหน่วย การจัดการ โครงสร้างหน่วย

.....

3.4 ด้านงบประมาณ

.....

3.5 ด้านอื่นๆ

.....

ขอขอบพระคุณที่กรุณาตอบ
แบบสอบถาม
น.อ.ประยูร ธรรมาธิวัฒน์
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร รุ่นที่ 57
ผู้ทำการวิจัย

ประวัติย่อผู้วิจัย

ชื่อ	นาวาอากาศเอก ประยูร ธรรมาธิวัฒน์
วัน เดือน ปีเกิด	18 มีนาคม 2504
การศึกษา	โรงเรียนเตรียมทหาร รุ่นที่ 21
	โรงเรียนนายเรืออากาศ รุ่นที่ 28
	ศิษย์การบินโรงเรียนการการบิน รุ่นที่ 78
	โรงเรียนนายทหารอากาศชั้นผู้บังคับฝูง รุ่นที่ 70
	โรงเรียนเสนาธิการทหารอากาศ รุ่นที่ 38
	วิทยาลัยการทัพอากาศ รุ่นที่ 41
ประวัติการทำงาน	1. หัวหน้าแผนกอำนวยการ กองบิน 1 (นครราชสีมา)
โดยย่อ	2. ผู้บังคับฝูงบิน 102 กองบิน 1 (L-39)
	3. นายทหารฝ่ายเสนาธิการ กองยุทธการ กรมยุทธการทหารอากาศ
	4. รองผู้บังคับการ กองบิน 23 (อุดรธานี)
	5. นายทหารฝ่านเสนาธิการ ประจำเสนาธิการทหารอากาศ
	6. ผู้อำนวยการกองปฏิบัติกิจพิเศษ กรมยุทธการทหารอากาศ
	7. ผู้บังคับการกองบิน 41 (เชียงใหม่)
	8. ฝ่ายเสนาธิการ ประจำกรมเทคโนโลยีสารสนเทศและ การสื่อสารทหารอากาศ
ตำแหน่งปัจจุบัน	รองผู้อำนวยการ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศ และการสื่อสารทหารอากาศ

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

ผู้วิจัย นาวาอากาศเอกประยูร ธรรมาธิวัฒน์ หลักสูตร วปอ. รุ่นที่ 57

ตำแหน่ง รองผู้อำนวยการ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ความเป็นมาและความสำคัญของปัญหา

ในอดีตที่ผ่านมา เมื่อมีปัญหาที่เกิดขึ้นระหว่างประเทศไม่ว่าเรื่องใดก็ตาม เมื่อใช้การเจรจาด้าน การทูตไม่ประสบผลสำเร็จ สุดท้ายต้องจบด้วยการใช้กำลังทางทหารเข้าทำการต่อสู้กัน ฝ่ายใดมีศักยภาพและขีดความสามารถหรือมีสมรรถนะดีกว่าจะเป็นฝ่ายได้ชัยชนะและทำให้ได้มาซึ่งผลประโยชน์แห่งชาติของประเทศนั้นๆ ขีดความสามารถดังกล่าวประกอบด้วยจำนวนกำลังพล จำนวนอาวุธยุทโธปกรณ์ที่ใช้ เทคโนโลยีขั้นสูง ยุทธศาสตร์และยุทธวิธีการรบที่ใช้เทคโนโลยีขั้นสูงเข้าช่วยอำนวยความสะดวกในการบัญชาการและควบคุมการรบ ทุกวันนี้ทุกประเทศต่างมีกำลังพล อาวุธและการส่งกำลังบำรุงที่ไม่แตกต่างกันมากนักแต่สิ่งที่แตกต่างกันคือเทคโนโลยีที่นำมาช่วยอำนวยความสะดวกในการรบ

ปัจจุบันกิจการวิทยาศาสตร์และเทคโนโลยีได้มีการพัฒนาในทุกๆด้านอย่างรวดเร็วแต่ละประเทศจึงลงทุนพัฒนาและนำเทคโนโลยีเข้ามาใช้งานทั้งภาคเอกชนและภาคราชการ ซึ่งจะเห็นได้ว่าเทคโนโลยีสารสนเทศสมัยใหม่ได้เข้ามามีบทบาทในทุกกิจการซึ่งจะเชื่อมโยงเป็นโครงข่ายที่เกื้อหนุนซึ่งกันและกัน หากกิจการใดมีเหตุทำให้ต้องหยุดชงักหรือบกพร่องในการปฏิบัติ จะส่งผลให้กิจการอื่นๆ เกิดขัดข้องและหยุกชงักตามไปด้วย จากเหตุดังกล่าวจึงนำมาสู่แนวคิดการทำสงครามสมัยใหม่ที่ทำการรบโดยไม่ต้องใช้กำลังทางทหาร แต่ทำการรบโดยใช้การกระทำให้ระบบสารสนเทศและระบบเครือข่ายที่เกี่ยวข้องเกิดข้อขัดข้องไม่สามารถให้บริการได้และต้องใช้เวลานานในการซ่อมบำรุงเพื่อให้สามารถนำกลับมาใช้งานได้ตามปกติส่งผลเสียหายต่อเศรษฐกิจของประเทศ เสียหายต่อบุคคลและองค์กรซึ่งการกระทำดังกล่าวเป็นส่วนหนึ่งของการทำสงครามไซเบอร์ (Cyber Warfare)

กองทัพอากาศเป็นกองทัพที่ต้องใช้เทคโนโลยีขั้นสูงในการปฏิบัติภารกิจให้บรรลุวัตถุประสงค์ โดยใช้กำลังพลน้อยแต่ได้ประสิทธิภาพมาก จึงได้ศึกษาและนำระบบเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเป็นส่วนหนึ่งในการปฏิบัติงาน เรียกว่า “การปฏิบัติที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations)” ซึ่งในระบบดังกล่าวจะประกอบด้วยเครือข่ายสารสนเทศ เครือข่ายการสื่อสารโทรคมนาคม ที่จะต้องเชื่อมโยงระบบเข้าด้วยกันเพื่อให้สามารถติดต่อรับส่งข้อมูลทุกประเภทได้อย่างรวดเร็ว ถูกต้องและเชื่อถือได้ พร้อมที่จะให้ผู้บังคับบัญชาสั่งใช้กำลังทางอากาศได้ตลอดเวลา หากมีการกระทำที่ทำให้เครือข่ายดังกล่าวขัดข้องไม่สามารถรับส่งข้อมูลได้จะทำให้การสั่งใช้กำลังทางอากาศมีข้อขัดข้องทันที การกระทำที่มีผลให้ระบบเครือข่ายดังกล่าวขัดข้อง

หรือชำรุดเสียหายไม่สามารถใช้การได้ถือได้ว่าเป็นส่วนหนึ่งของการทำสงครามไซเบอร์ (Cyber Warfare) ในปัจจุบันทุกหน่วยงานทั่วโลกได้ให้ความสำคัญในเรื่องนี้เป็นอย่างยิ่ง โดยจัดตั้งหน่วยงานขึ้นมากำกับดูแลโดยเฉพาะ

จากหลายเหตุการณ์ที่ผ่านมาพบว่าภัยคุกคามจากไซเบอร์ทำให้ระบบเครือข่ายและระบบสารสนเทศของกองทัพอากาศมีข้อขัดข้องในการรับส่งข้อมูลอยู่เสมอ ทั้งในที่ตั้งดอนเมืองและต่างจังหวัด การทำสงครามไซเบอร์จะไม่มีการแจ้งเตือนล่วงหน้าแต่จะแอบกระทำอย่างเงียบๆ ค่อยเป็นค่อยไป กองทัพอากาศก็เป็นเป้าหมายหนึ่งที่ถูกกระทำอยู่เรื่อยมาและเจ้าหน้าที่ได้ทำการแก้ไขให้ระบบสามารถกลับมาทำงานได้ตามปกติ ซึ่งต้องใช้เวลาพอสมควร การทำสงครามไซเบอร์ดังกล่าวที่ตรวจพบประกอบด้วยการแอบเจาะระบบเครือข่าย การปล่อยไวรัสเข้าระบบเครือข่าย การเปลี่ยนแปลงระบบเครือข่ายให้ทำงานผิดพลาดในการรับส่งข้อมูล เป็นต้น การกระทำดังกล่าวสร้างความเสียหายต่อการปฏิบัติภารกิจในภาพรวมของกองทัพเป็นอย่างมาก ทำให้ทราบว่าระบบการป้องกันและการปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ ยังมีศักยภาพและประสิทธิภาพไม่ดีเท่าที่ควร จึงเห็นสมควรที่ต้องปรับปรุง แก้ไขและพัฒนาเพื่อให้การปฏิบัติงานด้านสงครามไซเบอร์มีขีดความสามารถหรือมีศักยภาพเพิ่มขึ้น

ผู้วิจัยมีหน้าที่รับผิดชอบการปฏิบัติด้านระบบบัญชาการและควบคุมและการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ทั้งสองด้านมีความสำคัญเท่าเทียมกันในการใช้กำลังกองทัพอากาศเพื่อป้องกันประเทศและช่วยเหลือประชาชน แต่ปัจจุบันผู้วิจัยให้ความสนใจเกี่ยวกับการปฏิบัติด้านสงครามไซเบอร์เป็นอันดับต้น จึงมีความตั้งใจทำการวิจัยในเรื่องนี้ซึ่งจะทำให้กองทัพอากาศได้ทราบแนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ให้มีศักยภาพและมีประสิทธิภาพดียิ่งขึ้น

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
2. เพื่อศึกษาปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ
3. เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ

ขอบเขตของการวิจัย

การศึกษาเรื่องแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ผู้วิจัยได้กำหนดขอบเขตของการวิจัยดังต่อไปนี้

1. ขอบเขตประชากร ประกอบด้วยข้าราชการของกองทัพอากาศและหน่วยขึ้นตรงของกองทัพอากาศที่ปฏิบัติงานด้านเครือข่ายสารสนเทศ สงครามไซเบอร์ ระบบสื่อสารที่ปฏิบัติงานในปี 2557 ถึง 2558 โดยการสุ่มตัวอย่าง

2. ขอบเขตตัวแปร เป็นการศึกษาแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยมีตัวแปรที่ใช้ในการวิจัยดังนี้

2.1 ปัจจัยด้านบุคคล ได้แก่ เพศ ช่วงอายุ ระดับการศึกษา ระดับชั้นยศ และตำแหน่งปัจจุบัน รวมทั้งอายุการปฏิบัติตั้งแต่เข้ารับราชการถึงปัจจุบัน

2.2 ตัวแปรอิสระ ได้แก่ ปัจจัยที่ส่งผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ประกอบด้วย ความรู้ ความเข้าใจ ทักษะและความสามารถในการปฏิบัติงานด้านสงครามไซเบอร์ การรักษาความปลอดภัยและงบประมาณ

2.3 ตัวแปรตาม ได้แก่ ระดับขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ประกอบด้วย ขีดความสามารถเชิงรุกและเชิงรับ(กำลังพล/กระบวนการ/เทคโนโลยี)

3. ขอบเขตพื้นที่ กองทัพอากาศ

4. ผู้ให้ข้อมูลสำคัญ ประกอบด้วยผู้บังคับบัญชาชั้นสูงของกองทัพอากาศ ผู้บริหารระดับสูงที่ควบคุมกำกับดูแลการปฏิบัติด้านสงครามไซเบอร์ ด้านระบบสื่อสารและด้านระบบเครือข่ายสารสนเทศ

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยแบบผสมผสาน (Mixed Method Procedures) ประกอบด้วยการวิจัยเชิงคุณภาพ (Qualitative research) ด้วยการสัมภาษณ์เชิงลึกและเทคนิคการสนทนากลุ่มระหว่างผู้บริหารหน่วยรวมทั้งผู้เชี่ยวชาญและผู้ทรงคุณวุฒิภายในกองทัพอากาศ และการวิจัยเชิงปริมาณ(Quantitative Research) ด้วยการแจกแบบสอบถาม พร้อมกับได้ศึกษาจากวรรณกรรมที่เกี่ยวข้อง เพื่อนำมากำหนดเป็นแนวทางที่เหมาะสมในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ

การเก็บรวบรวมข้อมูล การสัมภาษณ์ ผู้วิจัยสัมภาษณ์ด้วยตนเอง โดยบันทึกข้อมูลด้วยการจดบันทึก และหรือบันทึกด้วยเครื่องบันทึกเสียง และ/หรือภาพเคลื่อนไหว การแจกแบบสอบถาม โดยแจกจ่ายไปยังผู้ปฏิบัติงานที่เกี่ยวข้องโดยตรง ดำเนินการเก็บรวบรวมข้อมูลจากแบบสอบถามตนเองและรับคืนพร้อมตรวจสอบความสมบูรณ์ของการกรอกแบบสอบถาม และการจัดประชุมสนทนากลุ่ม (Focus Group) โดยบันทึกข้อมูลด้วยการจดบันทึก

การวิเคราะห์ข้อมูล หลังจากที่ผู้วิจัยได้เก็บรวบรวมข้อมูลแล้ว จะต้องตรวจสอบข้อมูลและการวิเคราะห์ข้อมูล โดยกระทำไปพร้อมกับการเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูลใช้แนวคิดทฤษฎีเป็นกรอบในการวิเคราะห์โดยวิธีการหลักที่ใช้มี 2 วิธี คือ วิธีแรกเป็นการวิเคราะห์ข้อมูลโดยการตีความสร้างข้อสรุปแบบอุปนัย ซึ่งได้จากการสังเกตและการสัมภาษณ์ที่ได้จดบันทึกไว้จากสิ่งที่เป็นรูปธรรมหรือปรากฏการณ์ที่มองเห็น วิธีที่สอง เป็นการวิเคราะห์ข้อมูลโดยการวิเคราะห์เนื้อหาซึ่งได้จากการศึกษาเอกสารต้องคำนึงถึงบริบทหรือสภาพแวดล้อมของข้อมูลเอกสารที่นำมาวิเคราะห์ประกอบด้วยว่ามีการเปลี่ยนแปลงไปอย่างไร การวิเคราะห์ข้อมูลการสัมภาษณ์และการสนทนากลุ่มใช้การสรุปประเด็นต่างๆ โดยนำข้อมูลที่ได้จากผู้ให้ข้อมูลสำคัญมาเปรียบเทียบและตรวจสอบความแน่นอนของข้อมูล (Data Triangulation) เพื่อยืนยันความน่าเชื่อถือของข้อมูลและวิเคราะห์ข้อมูลด้วยการสรุป

ผลการวิจัย

จากการศึกษาตามกระบวนการวิจัยในแต่ละขั้นตอน เป็นการศึกษาที่ใช้กรอบแนวคิดในการวิเคราะห์ และสังเคราะห์ข้อมูลที่เกี่ยวข้อง สรุปผลที่ได้จากการวิจัยดังนี้

1. ทำให้ทราบขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า มีขีดความสามารถในการปฏิบัติเชิงรุกอยู่ในระดับต่ำ แต่การปฏิบัติเชิงรับอยู่ในระดับปานกลาง ซึ่งมีสาเหตุดังนี้

1.1 กำลังพล พบว่า ความรู้ด้านไซเบอร์ไม่เพียงพอ ขาดทักษะและประสบการณ์ในการทำสงครามไซเบอร์ ผู้เชี่ยวชาญด้านสงครามไซเบอร์มีจำนวนน้อยมาก หน่วยปฏิบัติบรรจุกำลังพลไม่มีทักษะและความชำนาญด้านไซเบอร์ ผู้ปฏิบัติส่วนใหญ่เป็นข้าราชการที่บรรจุใหม่อายุราชการยังน้อย จึงขาดประสบการณ์ด้านนี้ ส่วนผู้ที่มีประสบการณ์มากและเชี่ยวชาญจะเป็นผู้บริหารระดับกลางและสูง การผลิตกำลังพลทดแทนและการฝึกให้มีทักษะและความชำนาญอยู่ระหว่างดำเนินการ

1.2 กระบวนการบริหาร/จัดการ พบว่า การจัดองค์กรยังไม่มีความสะดวกและรวดเร็วในการปฏิบัติงาน รวมทั้งภารกิจและหน้าที่ที่ต้องปฏิบัติของหน่วยเกี่ยวข้องยังไม่ชัดเจนว่าต้องทำอะไร อย่างไรเกี่ยวกับสงครามไซเบอร์ อีกทั้งหลักนิยม นโยบาย ขาดความชัดเจนและต่อเนื่อง รวมทั้งแนวทางและระเบียบปฏิบัติหรือกฎหมายที่เกี่ยวข้องด้านไซเบอร์ที่ยังไม่ครอบคลุมการปฏิบัติทั้งเชิงรุกและเชิงรับ ขาดความสมบูรณ์ในแผนยุทธศาสตร์กองทัพอากาศและไม่มีแผนแม่บทด้านสงครามไซเบอร์ นอกจากนั้นยัง ไม่มีระบบการแจ้งเตือนภัยไปยังหน่วยต่างๆ เมื่อกองทัพถูกกระทำทางไซเบอร์

1.3 เทคโนโลยี ที่มีใช้ในปัจจุบันไม่ทันสมัย เครื่องมือหรืออุปกรณ์ต่างๆ ที่จำเป็นในการปฏิบัติงานเชิงรุกและเชิงรับมีไม่เพียงพอ ถึงแม้จะมีการนำมาตรฐานการรักษาความปลอดภัยเครือข่ายสารสนเทศมาใช้งานแต่ยังไม่สามารถป้องกันการบุกรุกเครือข่ายได้ดีเท่าที่ควร เทคโนโลยีได้ก้าวหน้าไปอย่างรวดเร็วแต่การเตรียมบุคลากรด้านนี้ยังตามไม่ทันและไม่เพียงพอ

2. ทำให้ทราบปัจจัยที่มีผลกระทบต่อขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่าปัจจัยที่มีผลกระทบประกอบด้วย กำลังพล กระบวนการบริหาร/จัดการ เทคโนโลยี งบประมาณและทัศนคติในการปฏิบัติงานร่วมกัน รายละเอียดดังนี้

2.1 กำลังพล เป็นปัจจัยหลักที่ส่งผลกระทบมากที่สุด เพราะกิจกรรมทุกอย่างจะต้องมีคนเป็นผู้ควบคุมรับผิดชอบ หากกำลังพลขาดความรู้ ความสามารถ มีทักษะน้อยเกินไป อีกทั้งขาดความชำนาญในการปฏิบัติก็จะส่งผลให้ภารกิจไม่บรรลุผลสำเร็จ นอกจากนั้นยังต้องมีภาวะผู้นำและจิตสำนึกที่ดีต่อเพื่อนร่วมงานและต่อองค์กร การสร้างบรรยายกาศที่ดีในที่ทำงาน

2.2 กระบวนการบริหาร/จัดการ เป็นปัจจัยรองลงมาที่มีผลกระทบ เนื่องมาจากการจัดองค์กรที่ไม่เอื้ออำนวยความสะดวกและรวดเร็วในการปฏิบัติ รวมทั้งภารกิจหน้าที่ที่ต้องปฏิบัติของหน่วยเกี่ยวข้องยังไม่ชัดเจนว่าต้องทำอะไร อย่างไรเกี่ยวกับสงครามไซเบอร์ อีกทั้งหลักนิยม นโยบาย หลักการ แนวทางและระเบียบปฏิบัติหรือกฎหมายที่เกี่ยวข้องด้านไซเบอร์ที่ไม่ครอบคลุมการ

ปฏิบัติทั้งเชิงรุกและเชิงรับ ขาดความสมบูรณ์ในแผนยุทธศาสตร์กองทัพอากาศและไม่มีแผนแม่บทด้านสงครามไซเบอร์ ที่สำคัญคืองบประมาณต้องเพียงพอและต่อเนื่อง

2.3 เทคโนโลยี เป็นปัจจัยอีกอย่างหนึ่งที่มีผลกระทบ อันเนื่องมาจากเทคโนโลยีที่นำมาใช้ในการทำสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับไม่ทันสมัยและเครื่องมือหรืออุปกรณ์ต่างๆ ที่จำเป็นไม่เพียงพอ ถึงแม้จะมีการนำมาตรฐานการรักษาความปลอดภัยเครือข่ายสารสนเทศมาใช้งาน แต่ยังไม่สามารถป้องกันการบุกรุกเครือข่ายได้ดีเท่าที่ควร เทคโนโลยีได้ก้าวหน้าไปอย่างรวดเร็วแต่การเตรียมบุคลากรด้านนี้ยังตามไม่ทันและไม่เพียงพอ

3. ทำให้ทราบแนวทางการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ของกองทัพอากาศ พบว่า กองทัพอากาศควรพัฒนาในด้านต่างๆ ดังนี้

3.1 ด้านกำลังพล ต้องพัฒนาให้มีความรู้ความสามารถ มีทักษะและความเชี่ยวชาญด้านสงครามไซเบอร์ ส่งเสริมให้กำลังพลได้แสดงออกซึ่งความรู้ความสามารถที่มีอยู่สร้างนักรบไซเบอร์กองทัพอากาศเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ รวมทั้งพิจารณากำหนดค่าตอบแทนพิเศษให้กับผู้ที่บรรจุเป็นนักรบไซเบอร์ของกองทัพในอัตราที่เหมาะสม ส่งเสริมให้มีการฝึกร่วมกันทั้งภายในและภายนอกกองทัพ และเฝ้าติดตามเทคโนโลยีที่ทันสมัยอยู่เสมอ ปลูกฝังให้มีทัศนคติที่ดีต่อองค์กรและเพื่อนร่วมงานและให้มีจิตสำนึกในการรักษาความปลอดภัยทางไซเบอร์ร่วมกัน

3.2 ด้านการบริหาร/จัดการ ควรปรับปรุงหลักนิยมกองทัพอากาศให้มีการปฏิบัติด้านสงครามไซเบอร์ และปรับปรุงแผนยุทธศาสตร์กองทัพอากาศให้กำหนดเป้าหมายที่ชัดเจนกับการปฏิบัติด้านสงครามไซเบอร์ และจัดทำแผนแม่บทด้านสงครามไซเบอร์รองรับแผนยุทธศาสตร์เพื่อเป็นแนวทางในการดำเนินงานด้านสงครามไซเบอร์ให้หน่วยเกี่ยวข้อง ปรับปรุงโครงสร้างการจัดหน่วยและกำหนดภารกิจให้กับหน่วยอย่างชัดเจนว่าต้องรับผิดชอบอะไรและต้องทำอะไรในงานด้านนี้ และบรรจุกำลังพลที่มีความรู้ ความสามารถด้านไซเบอร์ให้กับหน่วยปฏิบัติ เพื่อให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้ นอกจากนั้นควรนำกระบวนการบริหารงาน Deming Circle ที่ใช้หลักการ Plan-Do-Check- Act เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม นำกระบวนการจัดการความรู้ (Knowledge Management) มาใช้ในการถ่ายโอนความรู้อย่างเป็นระบบ เป็นการสร้างทรัพย์สินทางปัญญาของหน่วย เพื่อให้กำลังพลมีความรู้ที่ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ นำกระบวนการบริหารจัดการความเสี่ยง (Risk Management) เข้ามาช่วยในการบริหารงาน เพื่อให้ได้ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด ปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ให้ทุกหน่วยจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารหน่วยให้มีประสิทธิภาพ และนำระบบสมรรถนะ (Competency Model) มาใช้ในการพัฒนาองค์กรเพราะจะทำให้บุคลากรในทุกตำแหน่งทราบถึงความรู้ ความสามารถของตนเอง และทราบว่าจะต้องพัฒนาและฝึกฝนอย่างไรจึงจะทำให้มีขีดความสามารถเพิ่มขึ้น และจัดให้มีระบบจำลองยุทธด้านไซเบอร์ หรือที่เรียกว่า “Cyber Range” เพื่อแก้ปัญหาด้านบุคลากรและการเรียนรู้การสอนโดยเน้นไปที่ “Do” หรือ “Practice” มากกว่าการ “See and Hear”

3.3 ด้านเทคโนโลยี ควรจัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วย ให้พอเพียงตามความจำเป็นและเหมาะสมกับภารกิจที่หน่วยได้รับ นำระบบมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เพราะเป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก รวมทั้งจัดให้มีระบบแจ้งเตือนภัยไปยังหน่วยและผู้เกี่ยวข้องเมื่อกองทัพถูกกระทำทางไซเบอร์ เพื่อให้หน่วยและผู้เกี่ยวข้องเพิ่มการระวังป้องกันมิให้ระบบถูกโจมตีจากไซเบอร์ นอกจากนั้นจำเป็นต้องจัดหาอาวุธไซเบอร์ที่ทันสมัย เพื่อให้นักรบไซเบอร์ของกองทัพอากาศใช้ปฏิบัติภารกิจด้านไซเบอร์ และปรับปรุงให้ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ นอกจากนั้นควรให้การสนับสนุนการวิจัยและนำผลการวิจัยมาใช้งานเพื่อทำให้ระบบมีความแข็งแรง คงทน สามารถลดเวลาในการตรวจจับและการตอบสนองอันจะทำให้การป้องกันมีประสิทธิภาพ

3.4 ด้านงบประมาณ ควรให้ความสำคัญกับภารกิจด้านสงครามไซเบอร์ ด้วยการสนับสนุนงบประมาณให้เพียงพอและต่อเนื่อง เพื่อให้หน่วยเกี่ยวข้องสามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ และส่งเสริมให้หน่วยจัดหาโปรแกรมที่ถูกกฎหมายมาใช้งานและใช้โปรแกรมที่ทันสมัย สามารถตรวจจับและป้องกันการทำสงครามไซเบอร์ได้เป็นอย่างดี

อภิปรายผล

ผลการวิจัยที่ได้เป็นแนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ โดยแนวทางดังกล่าวนี้สอดคล้องกับแนวความคิด ทฤษฎีและผลงานวิจัยที่เกี่ยวข้องตามที่ได้กล่าวไว้แล้วในบทที่ 2 เช่น ระบบสมรรถนะในการบริหารองค์กร (อาภรณ์ ภู่วิทยพันธุ์ (2552:17-18)) การให้ความสำคัญกับบรรยากาศภายในองค์กร(สเตียร์ส (Steers, 1977)) การพัฒนาไปสู่องค์กรสมัยใหม่ที่เน้นการจัดความรู้เป็นสำคัญ อีกทั้งการบริหารความเสี่ยงที่ต้องนำมาพิจารณา ภัยคุกคามรูปแบบใหม่ที่ต้องให้ความสำคัญในการจัดการ การจัดหน่วยและการบริหารหน่วยที่รับผิดชอบงานด้านสงครามไซเบอร์ของกองทัพอากาศที่จัดตั้งขึ้นมาใหม่ อีกทั้งผลงานวิจัยของ นาวาอากาศเอก รศ.ดร.ประสงค์ ประณีตพลกรัง เรื่องแผนยุทธศาสตร์การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ ผลงานวิจัยของนาวาอากาศโท จตุชัย แพงจันทร์ เรื่องรูปแบบการปฏิบัติการสงครามไซเบอร์ และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง และผลงานวิจัยของนาวาอากาศโท วัชรพงศ์ ธรรมรักษ์ เรื่อง ที่ดำเนินการวิจัยเกี่ยวกับการบริหารจัดการเครือข่าย การรักษาความปลอดภัยด้านสารสนเทศและด้านไซเบอร์ ซึ่งสามารถนำมาพิจารณาร่วมกันและวิเคราะห์ เพื่อใช้เป็นแนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศได้อย่างดี มีความเหมาะสมที่จะนำไปใช้เพื่อพัฒนาบุคลากร การบริหารองค์กร การจัดองค์กร และการพัฒนาขีดความสามารถของระบบอาวุธยุทโธปกรณ์ ให้มีความพร้อมที่จะปฏิบัติการด้านสงครามไซเบอร์และพร้อมรับมือกับภัยคุกคามรูปแบบใหม่ได้ทุกรูปแบบ และสามารถรองรับเทคโนโลยีที่ใช้ระบบเครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพ โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนว

ทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือ มีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ มีความยั่งยืนและสามารถพึ่งพาตนเองได้ ประโยชน์ที่ได้จากการวิจัย นอกจากจะทำให้มีความเข้าใจอย่างถูกต้อง ได้ทราบองค์ประกอบและได้ทราบแนวทางในการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ ทำให้เกิดแบบแผนการพัฒนาการปฏิบัด้านสงครามไซเบอร์อย่างเป็นรูปธรรม เพื่อสอดรับวิสัยทัศน์ที่จะก้าวไปสู่ความเป็นกองทัพอากาศชั้นนำในภูมิภาคอาเซียน (One of the best Air Forces in ASEAN)

ข้อเสนอแนะ

โดยสรุปข้อเสนอแนะของการวิจัยสามารถแจกแจงได้เป็น 2 ด้าน ได้แก่ ข้อเสนอแนะการต่อยอดงานวิจัยที่สนับสนุนมุมมองในเชิงนโยบาย และข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป โดยมีรายละเอียดดังนี้

1. ข้อเสนอแนะการต่อยอดงานวิจัยที่สนับสนุนมุมมองในเชิงนโยบาย

1.1 ด้านกำลังพล

1.1.1 ฝึกอบรมให้กำลังพลก้าวทันเทคโนโลยีอยู่เสมอ มีความรู้ ความสามารถเทียบเท่ากับระดับสากลเพื่อให้รับมือกับสงครามไซเบอร์ได้ และฝึกปฏิบัติจริงด้านสงครามไซเบอร์เพื่อให้กำลังพลมีความรู้เท่าทันสถานการณ์และสามารถแก้ไขปัญหาได้อย่างรวดเร็ว

1.1.2 จัดให้มีการฝึกร่วมระหว่างหน่วยงานภายในและภายนอกกองทัพอากาศเพื่อเพิ่มพูนทักษะและประสบการณ์ อีกทั้งสามารถติดตามเทคโนโลยีใหม่ๆ ที่นำมาใช้ในการทำสงครามไซเบอร์ ส่งเสริมให้มีการแสดงออกซึ่งความสามารถที่มีอยู่

1.1.3 ปลูกฝังให้กำลังพลทุกระดับมีจิตสำนึก มีความตระหนักในการรักษาความปลอดภัยด้านไซเบอร์ ให้มีความรู้และเข้าใจถึงผลเสียหายเมื่อถูกกระทำทางไซเบอร์ทั้งเรื่องของราชการและเรื่องส่วนตัว

1.1.4 พิจารณาเพิ่มค่าตอบแทนพิเศษให้กับผู้ปฏิบัติงานด้านสงครามไซเบอร์โดยมีข้อกำหนดว่าต้องผ่านการทดสอบและผ่านการอบรมหลักสูตรที่ได้มาตรฐานมีใบประกาศนียบัตรรับรองจากองค์กรที่ได้มาตรฐานหรือเป็นที่ยอมรับทั่วไปจึงจะได้รับค่าตอบแทนพิเศษ

1.1.5 กำหนดเส้นทางการเจริญเติบโตที่ชัดเจนของกำลังพล เปิดโอกาสให้เท่าเทียมกัน เพื่อให้กำลังพลมีความมั่นใจในวิชาชีพ มีความเจริญก้าวหน้าอย่างต่อเนื่อง

1.1.6 ควรมีหลักสูตรการเรียนการสอนในสายวิทยาการ การเพิ่มพูนความรู้ให้กับหน่วยเกี่ยวข้องอย่างต่อเนื่องเพื่อให้มีการทำงานทดแทนกันได้

1.1.7 การรับสมัครกำลังพลเข้ามาใหม่จะต้องกำหนดคุณสมบัติให้มีความรู้ด้าน ไซเบอร์ มีจิตสำนึกในการรักษาความปลอดภัยด้านไซเบอร์ มีทัศนคติที่ดีต่อองค์กรและเพื่อนร่วมงาน

1.1.8 กำหนดแนวทางในการคัดเลือกกำลังพลที่มีความรู้ความสามารถด้านไซเบอร์เพื่อสร้างนักรบไซเบอร์ของกองทัพอากาศ โดยให้ปฏิบัติอยู่กับหน่วยต่างๆ ในกองทัพอากาศและนอกกองทัพอากาศ โดยมีภารกิจการปฏิบัติด้านสงครามไซเบอร์ตามที่กำหนด และจัดหาอาวุธไซเบอร์ให้กับนักรบเหล่านั้นอย่างเหมาะสมและเพียงพอ

1.2 ด้านการบริหารจัดการ

1.2.1 ปรังปรุงหลักนิยมกองทัพอากาศ ปรับปรุงแผนยุทธศาสตร์ของกองทัพอากาศ ให้มีเป้าหมายหลักและรองที่ต้องการอย่างชัดเจนเกี่ยวกับการปฏิบัติด้านสงครามไซเบอร์ และจัดทำแผนแม่บทด้านสงครามไซเบอร์รองรับแผนยุทธศาสตร์ดังกล่าว กำหนดแนวทางการปฏิบัติและหน่วยที่ต้องปฏิบัติให้ชัดเจนทั้งเชิงรุกและเชิงรับ เพื่อเป็นแนวทางให้หน่วยเกี่ยวข้องนำไปวางแผนในการปฏิบัติและขอรับการสนับสนุนงบประมาณต่อไป

1.2.2 ปรับปรุงโครงสร้างการจัดหน่วย ทั้งฝ่ายอำนวยการและหน่วยปฏิบัติให้มีหน่วยงานรองรับ มีกำลังพลบรรจุให้ตรงตามอัตราที่กำหนดอย่างเพียงพอและมีคุณภาพ ผู้ปฏิบัติงานด้านไซเบอร์ไม่จำเป็นต้องมีตำแหน่งอยู่ในกองทัพก็สามารถทำงานให้กองทัพได้ การกำหนดภารกิจ การสร้างองค์ความรู้และโครงสร้างการจัดหน่วยงานต้องสอดคล้องกับภารกิจ ซึ่งหน่วยงานด้านสงครามไซเบอร์ควรเป็นหน่วยอิสระที่ขึ้นตรงต่อผู้บัญชาการทหารอากาศ หัวหน้าหน่วยควรได้รับมอบอำนาจในการสั่งการปฏิบัติด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับในเบื้องต้น เพื่อป้องกันการกระทำจากฝ่ายตรงข้าม และเป็นหน่วยที่ปฏิบัติงานภายใต้ศูนย์ปฏิบัติการกองทัพอากาศเพื่อพิจารณาให้ข้อเสนอแนะการปฏิบัติด้านสงครามไซเบอร์ต่อผู้บัญชาการทหารอากาศ

1.2.3 นำปัจจัย 4 ข้อมาพิจารณาวางแผนกลยุทธด้านความมั่นคงปลอดภัย (Security Strategy) ได้แก่ Protection (การป้องกัน) Detection (การตรวจจับ) Reaction (การตอบสนอง) และTime (เวลา) ด้วยการ “ลดเวลาในการตรวจจับ” (decrease Detect time) และ “ลดเวลาในการตอบสนอง” (decrease React time) จะทำให้ระบบรักษาความปลอดภัยขององค์กรมั่นคงปลอดภัยจากสงครามไซเบอร์

1.2.4 ต้องมีการอัพเดทข้อมูลต่างๆของฝ่ายเราเป็นประจำ ต้องมีมาตรการเตรียมความพร้อมเพื่อรับมือกับการโจมตีทางไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม

1.2.5 นำกระบวนการบริหารงานให้มีคุณภาพ ของ Deming Circle คือ Plan-Do-Check- Act เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้นและแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม การตรวจสอบที่นำไปสู่การแก้ไขปรับปรุงทำให้ปัญหาที่เกิดขึ้นแล้วไม่เกิดซ้ำ หรือลดความรุนแรงของปัญหา ถือเป็นการนำความผิดพลาดมาใช้ให้เกิดประโยชน์มีความเหมาะสมกับการปฏิบัติงานด้านสงครามไซเบอร์ทั้งเชิงรุกและเชิงรับ

1.2.6 นำกระบวนการบริหารความเสี่ยง(Risk Management) เข้ามาช่วยในการบริหารงาน เพื่อให้ได้ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด ปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ให้ทุกหน่วยจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารหน่วยให้มีประสิทธิภาพ

1.2.7 นำระบบสมรรถนะ (Competency Model) มาใช้ในการพัฒนาองค์กร เพราะจะทำให้บุคลากรในทุกตำแหน่งทราบถึงความรู้ ความสามารถของตนเอง และทราบว่าจะต้องพัฒนาและฝึกฝนอย่างไรจึงจะทำให้มีขีดความสามารถเพิ่มขึ้น

1.2.8 นำกระบวนการจัดการความรู้ (Knowledge Management) มาใช้เพื่อการถ่ายโอนความรู้อย่างเป็นระบบ เป็นการสร้างทรัพย์สินทางปัญญาของหน่วย เพื่อให้กำลังพลมีความรู้ที่ทันสมัยอยู่เสมอ

1.2.9 กำหนดหลักเกณฑ์และแนวทางในการวัดขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของหน่วย เพื่อให้หน่วยมีความพร้อมรับมือกับภัยคุกคามรูปแบบใหม่อยู่เสมอ และใช้เป็นข้อมูลในการปรับปรุงพัฒนาและวางแผนของบประมาณสนับสนุนต่อไป

1.2.10 จัดให้มีระบบจำลองยุทธด้านไซเบอร์ หรือที่เรียกว่า “Cyber Range” เพื่อแก้ปัญหาด้านบุคลากรและการเรียนรู้การสอนโดยเน้นไปที่ “Do” หรือ “Practice” มากกว่าการ “See and Hear”

1.3 ด้านเทคโนโลยี

1.3.1 จัดหาเครื่องมือและอุปกรณ์ที่ทันสมัยให้กับหน่วย ให้พอเพียงตามความจำเป็นและเหมาะสมกับภารกิจที่หน่วยได้รับ

1.3.2 นำระบบมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เพราะเป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก

1.3.3 จัดให้มีระบบแจ้งเตือนภัยไปยังหน่วยและผู้เกี่ยวข้องเมื่อกองทัพถูกกระทำทาง ไซเบอร์เพื่อให้หน่วยและผู้เกี่ยวข้องเพิ่มการระวังป้องกันมิให้ระบบถูกโจมตีจากไซเบอร์

1.3.4 พิจารณาจัดหาอาวุธไซเบอร์ที่ทันสมัย เพื่อให้นักรบไซเบอร์ของกองทัพอากาศใช้ปฏิบัติภารกิจด้านไซเบอร์ และปรับปรุงให้ทันสมัยก้าวทันเทคโนโลยีอยู่เสมอ

1.4 ด้านงบประมาณ

1.4.1 ให้ความสำคัญกับภารกิจด้านสงครามไซเบอร์ ด้วยการสนับสนุนงบประมาณให้เพียงพอ เพื่อให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ

1.4.2 ให้การสนับสนุนงบประมาณเพื่อให้หน่วยใช้โปรแกรมที่ถูกกฎหมายและใช้โปรแกรมที่ทันสมัย สามารถตรวจจับและป้องกันการทำสงครามไซเบอร์ได้เป็นอย่างดี

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ผู้วิจัยขอเสนอแนวทางการทำวิจัยต่อยอดในประเด็นที่เกี่ยวข้องกับสงครามไซเบอร์และความมั่นคงปลอดภัยไซเบอร์ ดังนี้

2.1 สมรรถนะ (Competency) ของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์สำหรับข้าราชการทั่วไปและข้าราชการที่ทำงานในตำแหน่งเฉพาะที่เกี่ยวข้องกับไซเบอร์ในกองทัพอากาศควรเป็นอย่างไร

2.2 การพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ให้เพียงพอต่อความต้องการของกองทัพอากาศควรมียุทธศาสตร์อย่างไร

2.3 การกำหนดตำแหน่งและมาตรฐานวิชาชีพด้านความมั่นคงปลอดภัยด้านไซเบอร์และด้านสงครามไซเบอร์สำหรับสนับสนุนการมุ่งสู่ AEC และการเป็นกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force: NCAF) รวมทั้งการเป็นกองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Force in ASEAN) ควรมียุทธศาสตร์อย่างไร

2.4 การวิจัยในเชิงการสร้างนวัตกรรมด้านเทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์ ควรเป็นอย่างไร

2.5 การตระหนักรู้ของข้าราชการในกองทัพอากาศต่อความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ควรเป็นอย่างไร

2.6 การจัดสรรงบประมาณด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ในกองทัพอากาศเท่าใดถึงจะเพียงพอและเหมาะสม

2.7 ระดับความเสี่ยงด้านไซเบอร์ในกองทัพอากาศเป็นอย่างไร

2.8 สภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์ในกองทัพอากาศเป็นอย่างไร

2.9 ทัศนคติและความร่วมมือของข้าราชการในกองทัพอากาศต่อความมั่นคงปลอดภัยไซเบอร์และด้านสงครามไซเบอร์เป็นอย่างไร