แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ

โดย

นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง
รองผู้อำนวยการสำนักนโยบายและแผน
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
กองทัพอากาศ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 59
ประจำปีการศึกษา พุทธศักราช 2559 - 2560

บทคัดย่อ

เรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ
ลักษณะวิชา การทหาร
ผู้วิจัย นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง **หลักสูตร** วปอ. **รุ่นที่** 59

ระบบเทคโนโลยีสารสนเทศมีความสำคัญต่อการปฏิบัติภารกิจทางทหารเป็นอย่างยิ่ง ถึงแม้จะมีการดำเนินการอย่างมีประสิทธิภาพ แต่ก็จะมีความเสี่ยงที่เกิดจากความผิดพลาดของระบบ หรือถูกโจมตีทางไซเบอร์จากผู้ไม่หวังดี ซึ่งบุคลากรเป็นปัจจัยหนึ่งที่มีผลต่อการปฏิบัติภารกิจ จึงมีความจำเป็นต้องพัฒนาเพิ่มขีดความสามารถเพื่อรองรับเทคโนโลยีที่เปลี่ยนแปลงตลอดเวลา ในการวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ โดยวิธีการวิจัยเชิงคุณภาพด้วยการรวบรวมและวิเคราะห์ข้อมูลจากเอกสารที่เกี่ยวข้อง รวมถึงการสัมภาษณ์ผู้บังคับบัญชาและผู้ปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ และกำหนดขอบเขตการวิจัยเฉพาะในกองทัพอากาศ

ผลการวิจัยพบว่าขีดความสามารถการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติเชิงรับอยู่ในระดับดีและการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง มีนโยบาย กระบวนการ แผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติเกือบทุกด้าน แต่ยังขาดแนวความคิดการปฏิบัติการด้านไซเบอร์ รวมถึงมีระบบและอุปกรณ์ที่ทันสมัยมีประสิทธิภาพ ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านไซเบอร์ คือ บุคลากร ซึ่งมีไม่เพียงพอ ขาดความรู้ และทักษะในการปฏิบัติงานด้านไซเบอร์ ระบบการจัดการความรู้มีข้อมูลไม่ครบถ้วน และโครงสร้างการจัดหน่วยสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น ดังนั้น เพื่อให้การปฏิบัติด้านไซเบอร์ของกองทัพอากาศมีขีดความสามารถเพิ่มขึ้น ต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวน ให้มีความรู้ ความสามารถ มีทักษะ พร้อมที่จะปฏิบัติภารกิจด้านไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งบรรจุบุคลากรเพิ่มเติมให้เหมาะสมกับภารกิจที่ได้รับ รวมถึงเร่งดำเนินการจัดทำแนวความคิดการปฏิบัติการด้านไซเบอร์เพื่อให้บุคลากรนำไปเป็นแนวทางการปฏิบัติภารกิจ ทบทวนแผนงานให้ทันสมัยและครอบคลุมการปฏิบัติ และควรจัดทำระบบการจัดการความรู้ให้มีข้อมูลถูกต้องครบถ้วน หากมีภารกิจด้านไซเบอร์มากขึ้นจากปัจจุบันควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติภารกิจด้วย

คำนำ

กองทัพอากาศได้กำหนดยุทธศาสตร์ในการพัฒนากองทัพด้วยการเป็น “กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ซึ่งจะทำให้กองทัพอากาศมีฐานข้อมูลข่าวสารในลักษณะดิจิทัล และมีระบบเทคโนโลยีสารสนเทศที่สามารถตอบสนองต่อการปฏิบัติภารกิจของกองทัพอากาศได้อย่างมีประสิทธิภาพ กองทัพอากาศจึงนำเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ช่วยในการปฏิบัติภารกิจให้สามารถติดต่อและรับ-ส่งข้อมูลข่าวสารได้อย่างรวดเร็วและมีประสิทธิภาพ โดยเฉพาะในระบบการควบคุมและบังคับบัญชา การพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารมารองรับการปฏิบัติภารกิจในด้านต่าง ๆ มีประโยชน์เป็นอย่างยิ่ง แต่ก็มีโทษอย่างมหันต์เช่นกัน โดยเฉพาะเมื่อมีการนำมาสร้างเป็นภัยคุกคามด้านไซเบอร์ส่งผลกระทบต่อการปฏิบัติภารกิจในระบบคอมพิวเตอร์ เครือข่าย ฐานข้อมูล และความมั่นคงของประเทศ

กองทัพอากาศให้ความสำคัญในเรื่องการปฏิบัติด้านไซเบอร์เป็นอย่างยิ่ง จึงจัดตั้งหน่วยงานขึ้นมารับผิดชอบ โดยกำหนดให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศจัดตั้งกองสงครามไซเบอร์ขึ้นมาเพื่อรับผิดชอบการปฏิบัติด้านไซเบอร์โดยตรง เนื่องจากเป็นหน่วยงานใหม่บุคลากรที่ปฏิบัติงานในระบบยังไม่มีทักษะและแนวทางการปฏิบัติงานที่ชัดเจน ผู้วิจัยจึงมีความสนใจทำวิจัยเพื่อให้ได้แนวทางในการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศให้มีประสิทธิภาพสูงขึ้น

นาวาอากาศเอก

(ณรงค์เวตย์ เรืองจวง)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 59
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีความสำคัญต่อการปฏิบัติภารกิจทุกรูปแบบ ซึ่งกองทัพอากาศ นำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ในการปฏิบัติภารกิจเช่นกัน การดำเนินการในอดีตที่ผ่านมา การเก็บรวบรวมข้อมูลด้านต่าง ๆ ของกองทัพอากาศจะดำเนินการที่หน่วยซึ่งกว่าจะส่งมาให้ผู้บังคับบัญชาทราบและตัดสินตกลงใจต้องใช้เวลานาน เมื่อเทคโนโลยีมีการพัฒนาอย่างทันสมัยและมีความรวดเร็วยิ่งขึ้น กองทัพอากาศจึงนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติภารกิจการเตรียมกำลังกองทัพอากาศ การป้องกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพอากาศ โดยเฉพาะการป้องกันทางอากาศและด้านการสนับสนุนภายในกองทัพ รวมถึงสนับสนุนหน่วยงานความมั่นคงอื่นภายนอกกองทัพอีกด้วย การประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศทำให้ใช้เวลาในการดำเนินการสั้นลง รวมถึงสามารถจัดเก็บข้อมูลได้อย่างรวดเร็ว และสามารถจัดเก็บเป็นข้อมูลอิเล็กทรอนิกส์ในระบบสารสนเทศของกองทัพอากาศได้เป็นจำนวนมาก แต่ด้วยวิวัฒนาการทางเทคโนโลยีในรูปแบบดิจิทัลทั้ง ระบบอุปกรณ์ เครือข่ายทางสาย ไร้สาย และทางอินเทอร์เน็ต มีการใช้งานมากขึ้นและมีการพัฒนาอย่างรวดเร็ว จึงเป็นปัจจัยสำคัญที่ก่อให้เกิดจุดอ่อนในขณะปฏิบัติงานและถูกผู้ไม่หวังดีนำวิธีการทางไซเบอร์มาล้วงข้อมูลหรือโจมตีโครงสร้างระบบสารสนเทศและเครือข่าย เพื่อสร้างความได้เปรียบทางด้านข้อมูลของบุคคล หน่วยงาน หรือองค์กรต่าง ๆ ซึ่งกองทัพอากาศได้ถูกโจมตีทางไซเบอร์โจมตีเว็บเพจและเข้าถึงข้อมูลอยู่เนือง ๆ นับเป็นภัยอย่างยิ่งต่อความมั่นคงในการปฏิบัติภารกิจของกองทัพอากาศ กระทรวงกลาโหมและความมั่นคงของชาติ โดยแนวโน้มจะมีความรุนแรงมากขึ้นตามลำดับ

กองทัพอากาศได้เล็งเห็นผลที่เกิดขึ้น จึงกำหนดให้มีการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร กระบวนการทำงานบุคลากรและหน่วยงานของกองทัพอากาศ ให้สามารถปฏิบัติภารกิจได้อย่างครบถ้วน ถูกต้อง ปลอดภัย ทันตอสถานการณ และได้ขอปรับโครงสร้างกองทัพอากาศใน พ.ศ.๒๕๕๗ โดยมีการปรับอัตราภายในกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ที่เป็นหน่วยขึ้นตรงกองทัพอากาศให้มีหน้าที่ พิจารณาดำเนินการด้านเทคโนโลยีสารสนเทศและสงครามสารสนเทศ ซึ่งดำเนินการในงานด้านฝ่ายเสนาธิการ การจัดทำแผนแม่บท แผนงาน โครงการ งบประมาณ กิจการบัญชาการและควบคุม เทคโนโลยีสารสนเทศและการสงครามไซเบอร์ และได้จัดตั้งหน่วยเพิ่มขึ้น คือ กองสงครามไซเบอร์ เพื่อรับผิดชอบงานด้านสงครามไซเบอร์โดยตรง มีหน้าที่กำหนดแนวทางและมาตรการในการป้องกันและการรักษาความปลอดภัยระบบสารสนเทศ เป็นหน่วยขึ้นตรงสำนักระบบบัญชาการและควบคุมกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ โดยหน่วยงานนี้เป็นหน่วยงานใหม่ได้รับการบรรจุบุคลากรจากหน่วยขึ้นตรงกองทัพอากาศตามความจำเป็นที่เหมาะสมและหาได้ในขณะนั้น ซึ่งบุคลากรดังกล่าวมีพื้นฐานความรู้และความสามารถแตกต่างกัน ทำให้

การปฏิบัติภารกิจในหน้าที่ด้านสงครามไซเบอร์มีขีดจำกัด การจัดหาระบบและอุปกรณ์มาใช้งาน ไม่สามารถดำเนินการได้ทันตามเวลาที่เหมาะสม การฝึก อบรม การถ่ายทอดความรู้ ความสามารถ ไม่อาจดำเนินการได้อย่างมีประสิทธิภาพ ระบบโปรแกรม อุปกรณ์และสถานที่ทำงานยังไม่สมบูรณ์ อาจจะทำให้ไม่สามารถรับมือต่อการปฏิบัติของผู้ไม่หวังดีได้

ผู้วิจัยมีหน้าที่รับผิดชอบในการจัดทำแผนงาน/โครงการด้านเทคโนโลยีสารสนเทศและสงครามสารสนเทศ การจัดการความรู้ การบริหารการฝึกและศึกษา จำพวกทหารสารสนเทศและสงครามอิเล็กทรอนิกส์ ซึ่งบุคลากรจำพวกดังกล่าวปฏิบัติหน้าที่ในตำแหน่ง นายทหาร/เจ้าหน้าที่เทคโนโลยีสารสนเทศและการสื่อสารภายในหน่วย โดยก่อนบรรจุเข้ารับราชการมีความรู้ความสามารถตามวุฒิการศึกษาก่อนเข้ารับราชการ ผู้วิจัยจึงมีความสนใจและตั้งใจทำวิจัย ปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านสงครามสารสนเทศไซเบอร์ การให้ความรู้ การฝึกอบรม และการศึกษา ของบุคลากร โดยเฉพาะด้านสงครามไซเบอร์ในภาพรวม เพื่อให้กองทัพอากาศทราบถึงปัญหา ข้อจำกัด ปัจจัยที่เกี่ยวข้องและแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและข้อจำกัด การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
2. เพื่อศึกษาปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
3. เพื่อเสนอแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

ขอบเขตของการวิจัย

การวิจัยครั้งนี้จะศึกษาและวิเคราะห์ถึงปัญหา ข้อจำกัด ปัจจัยที่เกี่ยวข้องในการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ โดยเฉพาะอย่างยิ่ง การพัฒนาบุคคลากรและปัจจัยที่เกี่ยวข้องกับการปฏิบัติภารกิจด้านไซเบอร์ ซึ่งผู้วิจัยได้กำหนดขอบเขตของการวิจัย ดังนี้

1. ขอบเขตประชากร

ประชากรที่ใช้ในการวิจัยครั้งนี้ประกอบด้วยข้าราชการชั้นสัญญาบัตรของกองทัพอากาศที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยขึ้นตรงกองทัพอากาศที่ปฏิบัติงานในระหว่างปี พ.ศ.2559 ถึง พ.ศ.2560 โดยมีผู้ให้ข้อมูลสำคัญ ประกอบด้วย ผู้บังคับบัญชาชั้นสูงของกองทัพอากาศ และผู้บังคับบัญชาและผู้ปฏิบัติหน้าที่ของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ และเป็นการศึกษาในเรื่องการเตรียมบุคลากรในการปฏิบัติด้านไซเบอร์

2. ขอบเขตพื้นที่ กองทัพอากาศ
3. ขอบเขตระยะเวลาการวิจัย ตั้งแต่เดือน ธ.ค.59 ถึงเดือน มิ.ย.60

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาและวิเคราะห์จากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไปด้านไซเบอร์ นโยบายระดับชาติ นโยบายระดับกองทัพ นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของกองทัพอากาศ และการปฏิบัติงานด้านไซเบอร์ ดังนี้

1. รวบรวมเอกสารที่เกี่ยวข้อง เช่น ตำรา วารสาร บทความ เอกสารทางวิชาการ นโยบายที่เกี่ยวข้อง ตลอดจนค้นคว้าทางอินเทอร์เน็ต เป็นต้น
2. สัมภาษณ์ผู้บังคับบัญชา ผู้เชี่ยวชาญ และผู้ปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ

ประโยชน์ที่ได้รับจากการวิจัย

1. ทราบถึงสภาพปัญหาข้อจำกัดการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
2. ทราบถึงปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
3. ข้อเสนอแนะแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์กองทัพอากาศ

คำจำกัดความ

การพัฒนาบุคลากร	หมายถึง	การเพิ่มประสิทธิภาพด้านทักษะ ความชำนาญในการทำงาน ตลอดจนปรับเปลี่ยนทัศนคติของบุคลากรทุกระดับให้เป็นไปในทิศทางเดียวกัน การเพิ่มประสิทธิภาพบุคลากรสามารถทำได้ด้วยวิธีการฝึกอบรม ปฐมนิเทศ การศึกษาส่งไปดูงานต่างประเทศสัมมนาทั้งในและนอกสถานที่ เพื่อบุคลากรจะสามารถปฏิบัติงานได้อย่างเต็มที่ และมุ่งไปสู่ความสำเร็จตามเป้าหมายขององค์กร
เทคโนโลยีสารสนเทศ	หมายถึง	การประยุกต์ใช้ความรู้ทางด้านคอมพิวเตอร์และอุปกรณ์โทรคมนาคม เพื่อทำการ จัดเก็บ ค้นหา จัดส่ง กระจายออก ติดตาม รวบรวม และจัดการข้อมูลต่าง ๆ
หัวหน้าสายวิทยาการ	หมายถึง	หน่วยขึ้นตรงกองทัพอากาศซึ่งรับผิดชอบกำลังพลในเหล่าทหารและจำพวกทหาร หรือรับผิดชอบกำลังพลในจำพวกทหารที่รับผิดชอบ
จำพวกทหารเทคโนโลยีสารสนเทศ	หมายถึง	ผู้ที่มีความรู้ความสามารถในหน้าที่ทางด้านระบบสารสนเทศ สงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ที่เกี่ยวกับการบริหารจัดการและปฏิบัติการเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ ระบบ

		เทคโนโลยีภูมิสารสนเทศระบบบัญชาการและควบคุม สงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์
สงครามไซเบอร์	หมายถึง	การใช้คอมพิวเตอร์และอินเทอร์เน็ตในการ (Cyber Warfare) ทำสงคราม เช่น การโจมตีเว็บหรือบล็อกเว็บ โฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมือง ผ่านอินเทอร์เน็ต การเจาะข้อมูลลับ โดยแฮ็กเกอร์ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ การทำลายอุปกรณ์การทหารที่ใช้คอมพิวเตอร์ควบคุม เป็นต้น
ไซเบอร์ (Cyber)	หมายถึง	คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง
การโจมตีทางไซเบอร์	หมายถึง	การโจมตีต่อฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานมิติทางไซเบอร์ของฝ่ายตรงข้าม รวมถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้ามด้วย

บทที่ 2
แนวคิด ทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

การทำวิจัย เรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ ผู้ศึกษาได้ศึกษาจากเอกสาร แนวความคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการปฏิบัติการด้านไซเบอร์ เพื่อเป็นกรอบแนวทางในการศึกษาค้นคว้า โดยใช้แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ดังกล่าวมาเป็นกรอบแนวทางการศึกษา ดังนี้

1. แนวคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กรและองค์กรสมัยใหม่
2. ไซเบอร์ กับการรักษาความปลอดภัย และการปฏิบัติการสงครามไซเบอร์
3. สงครามไซเบอร์ (Cyber Warfare)
4. งานที่เกี่ยวข้อง
5. ยุทธศาสตร์กองทัพอากาศ
6. การพัฒนาบุคลากรของกองทัพอากาศ

แนวคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กรและองค์การสมัยใหม่

1. สมรรถนะในองค์กร

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 ความสามารถหลักที่คาดหวังให้พนักงานทุกคนทุกระดับองค์กรจะต้องมี องค์การบางแห่งเรียกสมรรถนะหลัก ซึ่งเป็นสิ่งที่ทำให้เป้าหมาย วิสัยทัศน์ และภารกิจขององค์การประสบความสำเร็จ ทั้งนี้สมรรถนะหลักที่ถูกปฏิบัติเหมือน ๆ กันในองค์กรจะนำไปสู่การสร้างนวัตกรรมองค์กร (Corporate Culture) หลักปฏิบัติที่สืบทอดต่อไปยังพนักงานคนอื่น ๆ ต่อไปได้

1.2.2 สมรรถนะทางการบริหาร (Managerial Competency) หมายถึง ความสามารถในการบริหารจัดการงานที่คาดหวังกับกลุ่มพนักงาน แยกตามระดับตำแหน่งงาน ถ้าตำแหน่งงานเหมือนกันคาดหวังว่าจะมีสมรรถนะประเภทนี้เหมือนกัน เช่น ผู้จัดการฝ่าย ไม่ว่าจะเป็นฝ่ายใด ๆ ก็ตามจะต้องมีสมรรถนะในเรื่อง วิสัยทัศน์เชิงกลยุทธ์ การวางแผนงาน การบริหารการเปลี่ยนแปลง การสร้างเครือข่ายที่เหมือนกัน พบว่าการกำหนดสมรรถนะทางการบริหารนั้นจะกำหนดขึ้นจากบทบาทหน้าที่และความรับผิดชอบหลักที่เหมือนกันตามระดับตำแหน่งงาน และจำนวนข้อของสมรรถนะทางการบริหารจะต้องมีจำนวนไม่มาก

1.2.3 สมรรถนะตามหน้าที่ (Function Competency) หมายถึง ความสามารถในงานเฉพาะด้านที่แตกต่างกันไปในแต่ละหน่วยงาน พบว่า การกำหนดสมรรถนะตามหน้าที่ขึ้นอยู่กับลักษณะงานที่รับผิดชอบ (Job Description) โดยพิจารณาว่าในแต่ละตำแหน่งงานคาดหวังความรู้ ทักษะและคุณลักษณะส่วนบุคคลในเรื่องใดบ้าง ซึ่งความสามารถเหล่านี้จะส่งผลการทำงานที่ผู้บังคับบัญชามอบหมายให้ประสบความสำเร็จ โดยสามารถวัดความสำเร็จของงานได้จากตัวชี้วัดผลงานหลัก (Key Performance Indicators) ดังนั้นจำนวนสมรรถนะตามหน้าที่จึงมีความแตกต่างกันไปในแต่ละหน่วยงาน โดยปกติแล้วจะมีไม่มากเช่นเดียวกันอยู่ระหว่าง 5 - 7 ข้อ นอกจากนี้ยังพบว่าการจัดแบ่งสมรรถนะตามหน้าที่นั้นสามารถแบ่งได้อีก 2 ประเภทย่อยได้แก่ (1) Common Function Competency เป็นความสามารถในงานที่เป็นเรื่องทั่ว ๆ ไปตำแหน่งงานอื่นในฝ่ายอื่น ๆ และ (2) Specific Function Competency เป็นความสามารถในงานทางเทคนิคเฉพาะด้านที่ต้องอาศัยความชำนาญและระยะเวลาในการเรียนรู้และฝึกฝน

1.3 องค์ประกอบที่สำคัญของสมรรถนะการเป็นผู้นำของผู้บริหารองค์กร

สมรรถนะทางการบริหาร (Managerial Competency : MC) หมายถึง สมรรถนะที่เป็นความสามารถทางการจัดการซึ่งสะท้อนให้เห็นถึงทักษะในการบริหารและจัดการงานต่าง ๆ กำหนดให้ต้องมีทั้งระดับผู้บริหารและระดับพนักงานปฏิบัติการ แต่จะแตกต่างกันตามบทบาทหน้าที่และความรับผิดชอบโดยแบ่งเป็นข้อย่อย ดังนี้

1.3.1 วิสัยทัศน์เชิงกลยุทธ์ (Strategic Visioning) ความเข้าใจถึงวิสัยทัศน์ พันธกิจ เพื่อกำหนดกลยุทธ์และยุทธศาสตร์การดำเนินงาน ตลอดจนการรวบรวมติดตามและวิเคราะห์กลยุทธ์การดำเนินงานต่าง ๆ

1.3.2 การวางแผนงาน (Planning) ความรู้ ความเข้าใจ แนวคิด หลักการ กระบวนการ วิธีการวางแผนและติดตามงานรวมทั้งการประมวลผลเพื่อประยุกต์ใช้ในการวางแผนและติดตามงานให้มีประสิทธิภาพและประเมินผลการปฏิบัติงานตามแผนที่กำหนดขึ้น

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

1.3.4 การแก้ไขปัญหาและตัดสินใจ (Problem Solving and Decision Making) ความสามารถในการวิเคราะห์สาเหตุและผลกระทบของปัญหา พร้อมทั้งสามารถวิเคราะห์และค้นหาการแก้ไขปัญหาได้หลากหลายวิธี สามารถตัดสินใจแก้ไขปัญหาได้อย่างเหมาะสมกับสถานการณ์และเกิดประโยชน์สูงสุดแก่องค์การ

1.3.5 บริหารการเปลี่ยนแปลง (Change Management) การวิเคราะห์และการคาดการณ์การเปลี่ยนแปลงที่เกิดภายในองค์กรและหน่วยงานรวมทั้งการคิดหาเครื่องมือ และวิธีการใหม่มาใช้ในองค์กร

2. แนวความคิดและทฤษฎีเกี่ยวกับบรรยากาศขององค์กร

2.1 ความหมายของบรรยากาศขององค์กร

ผู้วิจัยได้ศึกษาและสรุปความหมายของบรรยากาศองค์กรจากนักวิชาการด้านทรัพยากรมนุษย์หลายท่าน เพื่อนำมาใช้ประโยชน์ในการปรับปรุงและพัฒนาองค์กรให้เหมาะสมกับลักษณะการทำงานที่เป็นมาตรฐาน ซึ่งสรุปได้ว่า บรรยากาศองค์กร หมายถึง สภาพแวดล้อมในการทำงานที่เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอกซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร

2.2 แนวคิดเกี่ยวกับบรรยากาศองค์กร

สเตียร์ส (Steers, 1977) ได้แบ่งองค์ประกอบของบรรยากาศองค์การไว้ 6 ด้าน ดังนี้

2.2.1 โครงสร้างการทำงาน (Task Structure) จากการสำรวจความรู้สึกนึกคิดของพนักงานในองค์กรเห็นว่า โครงสร้างในการทำงานเป็นอุปสรรคหรือบั่นทอนต่อจิตใจในการทำงานหรือไม่ ตัวอย่างโครงสร้างในการทำงานที่เป็นอุปสรรค เช่น การรวบอำนาจในการบังคับบัญชา ระบบงบประมาณที่ค่อนข้างเข้มงวด กฎระเบียบที่ไม่ยืดหยุ่นและกรรมวิธีในการทำงานมีขั้นตอนที่ยุ่งยากซับซ้อน เป็นต้น

2.2.2 ระบบรางวัลตอบแทน (Reward Systems) ต้องวิเคราะห์ว่าเป็นระบบที่มีความยุติธรรมและเพียงพอต่อมาตรฐานการครองชีพหรือไม่

2.2.3 ความเป็นอิสระ (Autonomy) หมายถึง ความรู้สึกของพนักงานที่เห็นว่าเขามีอิสระและได้รับอนุญาตจากองค์กรให้สามารถแสดงออกซึ่งความคิดสร้างสรรค์งานใหม่ ๆ 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 “ส่วนราชการมีหน้าที่พัฒนาความรู้ในส่วน

ราชการเพื่อให้มีลักษณะเป็นองค์กรแห่งการเรียนรู้อย่างสม่ำเสมอ โดยต้องรับรู้ข้อมูลข่าวสารและสามารถประมวลผลความรู้ในด้านต่าง ๆ เพื่อนำมาประยุกต์ใช้ในการปฏิบัติราชการได้อย่างถูกต้อง รวดเร็วและเหมาะสมกับสถานการณ์ รวมทั้งต้องส่งเสริมและพัฒนาความรู้ความสามารถสร้างวิสัยทัศน์ และปรับเปลี่ยนทัศนคติของข้าราชการในสังกัดให้เป็นบุคลากรที่มีประสิทธิภาพและมีการเรียนรู้ร่วมกัน" จากภาวะปัจจัยต่าง ๆ จึงทำให้เกิดความปรารถนาที่จะสร้างและพัฒนาองค์กรให้เป็นองค์การสมัยใหม่ บุคลากรสามารถเพิ่มพูนความรู้ความสามารถได้อย่างต่อเนื่องและสามารถสร้างผลงานได้ตามความปรารถนา อีกทั้งเป็นแหล่งสร้างความคิดทางปัญญา โดยการเรียนรู้ที่จะเรียนรู้ร่วมกัน ดังนั้นองค์กรสมัยใหม่ควรจะมีลักษณะสำคัญคือ ต้องเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง 5 ระบบขององค์กรแห่งการเรียนรู้ ได้แก่ การเรียนรู้ (Learning) องค์กร (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology) ให้เป็นตัวขับเคลื่อนและพัฒนาองค์การ เพราะการเรียนรู้ประเภทนี้ไม่สามารถจะเกิดขึ้นและไม่สามารถคงอยู่ได้หากปราศจากความเข้าใจและการพัฒนาระบบย่อยที่สัมพันธ์กัน

4. การพัฒนาบุคลากร

การพัฒนาบุคลากร หมายถึง กระบวนการที่จะเสริมสร้างและเปลี่ยนแปลงผู้ปฏิบัติงานในด้านต่าง ๆ เช่น ความรู้ความสามารถ ทักษะ อุปนิสัย ทัศนคติ และวิธีการในการทำงานที่จะนำไปสู่ประสิทธิภาพในการทำงาน (สมาน รังสิโยกฤษณ, 2542 : 80) การฝึกอบรมหรือการพัฒนาบุคลากร เป็นการเสริมสร้างความรู้ความเข้าใจ และความชำนาญให้แก่พนักงานในองค์การจนสามารถก่อให้เกิดการเปลี่ยนแปลงในพฤติกรรมและทัศนคติที่ค่อนข้างจะถาวรอันจะอำนวยประโยชน์ให้พนักงานปฏิบัติงานได้อย่างมีประสิทธิภาพมากขึ้น และทำให้มีความเจริญก้าวหน้าในการทำงาน (สุปราณี ศรีฉัตราภิมุข, 2542 : 1) กระบวนการที่ได้ออกแบบไว้อย่างมีเป้าหมายเพื่อให้ผู้ปฏิบัติงานได้มีโอกาสเรียนรู้โดยการฝึกอบรม การศึกษา และการพัฒนาเป็นการเพิ่มพูนความรู้และศักยภาพในการทำงาน รวมทั้งปรับพฤติกรรมของผู้ปฏิบัติงานให้พร้อมที่จะปฏิบัติหน้าที่ที่รับผิดชอบให้เกิดประโยชน์สูงสุดต่อองค์การ และมีโอกาสก้าวหน้าในตำแหน่งที่สูงขึ้น มักพบปัญหาและอุปสรรคของการพัฒนาบุคลากร โดยปัญหาและอุปสรรคในการพัฒนาบุคลากรในองค์การใด ๆ ไว้ 5 ประการ สรุปได้ดังนี้

4.1 ปัญหาด้านเจ้าหน้าที่ที่ดำเนินการพัฒนาบุคลากร เนื่องจากลักษณะงานด้านพัฒนาบุคลากรในองค์การโดยทั่วไปแล้ว เป็นงานที่ช่วยเหลือสนับสนุนการดำเนินงานของเจ้าหน้าที่สายงานหลักเป็นส่วนใหญ่ ดังนั้นบุคลากรโดยทั่วไปจึงมักจะพอใจทำงานในสายงานหลักมากกว่าสายงานช่วยเหลือสนับสนุน

4.2 ปัญหาด้านวิทยากร วิทยากรที่มีคุณสมบัติดีและเหมาะสมยังมีอยู่น้อยมาก ส่วนใหญ่วิทยากรในโครงการพัฒนาบุคลากรในปัจจุบันมักขาดคุณสมบัติการเป็นผู้ฝึกสอนที่ดีแต่จะมีลักษณะเป็นผู้บรรยายหรือผู้บอกเล่าถึงประสบการณ์ในการทำงานของตนมากกว่า ผู้รับการพัฒนาจึงได้รับความรู้แปลกใหม่น้อยมาก อีกทั้งยังขาดการเลือกวิธีการและเทคนิคในการพัฒนาได้อย่างถูกต้องเหมาะสมด้วย

4.3 ปัญหาด้านตัวบุคลากรที่เข้ารับการพัฒนา แบ่งออกเป็น 4 ลักษณะ คือ

4.3.1 ผู้เข้ารับการพัฒนาจำนวนหนึ่งไม่เข้าใจในวัตถุประสงค์ที่แท้จริงของการพัฒนาว่า พัฒนาแล้วจะได้รับประโยชน์อย่างไรบ้าง แต่เข้ารับการพัฒนาเพราะได้รับคำสั่งจากผู้บังคับบัญชา

4.3.2 ผู้เข้ารับการพัฒนาบางคนมีทัศนคติที่ไม่ดีต่อการพัฒนาบุคลากร กล่าวคือคิดว่าเป็นเรื่องของเด็กนักเรียนในห้องเรียนซึ่งไม่เหมาะกับผู้ใหญ่ที่ทำงานแล้ว อีกทั้งคิดว่าเป็นการเสียเวลาเสียเงินโดยเปล่าประโยชน์และก็มีหน้าที่งานทำอยู่แล้วก็ไม่มีความจำเป็นต้องเข้ารับการพัฒนาอีกแต่อย่างใด

4.3.3 บุคลากรบางคนมีทัศนคติในทางอนุรักษ์นิยม พอใจที่จะประพฤติปฏิบัติตามแนวทางเดิมที่เคยยึดถือปฏิบัติมาช้านานแล้วและไม่ยอมรับจนถึงขนาดต่อต้าน

4.3.4 บุคลากรบางคนมีทัศนคติมองโลกในแง่ร้ายอยู่เสมอ ไม่เชื่อว่าวิทยากรจะมีความรู้ความสามารถมากเพียงพอที่จะมาฝึกสอนตนได้ และไม่เชื่อว่าเนื้อหาสาระของโปรแกรมการพัฒนาบุคลากรจะดีพอที่จะยอมรับคำแนะนามาใช้ปฏิบัติได้

4.3.4 ปัญหาด้านสถานที่และอุปกรณ์ที่ใช้ในการพัฒนาบุคลากร การพัฒนาบุคลากรจะประสบผลสำเร็จได้โดยง่าย ถ้ามีสิ่งอำนวยความสะดวกด้านต่าง ๆ อย่างพร้อมมูล โดยเฉพาะอย่างยิ่งสถานที่และอุปกรณ์เครื่องใช้ต่าง ๆ แต่การจัดหาสิ่งอำนวยความสะดวกเหล่านี้ต้องลงทุนสูง อุปกรณ์บางชิ้นมีราคาแพงมาก องค์การบางแห่งก็ไม่สามารถหาซื้อมาได้ครบถ้วน

4.3.5 ปัญหาด้านผู้บริหารหรือหัวหน้าหน่วยงานของผู้เข้ารับการพัฒนา บุคลากรนักบริหารบางคนมีทัศนคติที่คับแคบ ไม่เห็นความสำคัญของการพัฒนาบุคลากรจึงไม่ให้การสนับสนุน บางคนก็สำคัญผิดว่าการพัฒนาบุคลากรแก้ไขปัญหาได้ฉับพลัน เมื่อไม่สามารถแก้ปัญหาได้รวดเร็วทันใจตามที่ต้องการก็ต่อต้าน ประการสุดท้ายนักบริหารบางคนคิดว่ามีความรู้ความสามารถมากกว่าเจ้าหน้าที่ที่จัดการพัฒนาบุคลากรจึงเป็นผู้สั่งการและดำเนินการต่าง ๆ เองจึงอาจก่อให้เกิดปัญหามากมาย (วรนารถ แสงมณี, 2543 : 134-136)

5. การจัดการความรู้ (Knowledge Management)

5.1 Dave Snowden (2002) ได้กล่าวว่า การจัดการความรู้ หมายถึง การรวบรวมองค์ความรู้ที่อยู่กระจัดกระจายทั้งในตัวบุคคลหรือเอกสารมาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ นำความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานให้เกิดประสิทธิภาพอันจะส่งผลให้องค์กรมีความสามารถในเชิงแข่งขันสูงสุด (การจัดการความรู้, ออนไลน์, 2002)

5.2 ชนิดของความรู้ (Types of knowledge) แบ่งเป็น 3 ประเภท ประกอบด้วย (1) ความรู้ที่อยู่ในตัวคน (Tacit Knowledge) หมายถึง ความรู้ ประสบการณ์ พรสวรรค์ต่าง ๆ ที่ผู้นั้นมีอย่างเชี่ยวชาญ (2) ความรู้ที่ชัดแจ้ง (Explicit Knowledge) ได้แก่ ความรู้ที่ถ่ายทอดออกมาอยู่ในรูปของหนังสือ วารสาร สื่อโสตทัศนวัสดุ (3) ความรู้ที่ชัดเจนแน่นอน (Implicit) เป็นความรู้ที่ชัดแจ้งและผ่านการถกเถียงและสรุปผลว่าเป็นความรู้ที่เหมาะสมกับวัตถุประสงค์ที่ต้องการมากที่สุด

5.3 กระบวนการจัดการความรู้ (Demarest, 1997) ได้อธิบายถึงกระบวนการในการจัดการความรู้ไว้ 5 ขั้นตอน ได้แก่ กระบวนการสร้างความรู้ (Construction) กระบวนการ

รวบรวมความรู้ (Embodiment) กระบวนการเผยแพร่ความรู้ (Dissemination) กระบวนการใช้ความรู้หรือนำความรู้ไปใช้ (Use) และกระบวนการจัดการองค์ความรู้ (Management)

5.4 การจัดการความรู้มีประโยชน์ คือ ช่วยประหยัดเวลาในการปฏิบัติงานและช่วยในการตัดสินใจเพื่อแก้ไขปัญหาได้ถูกต้อง ช่วยในการคิดผลิตสิ่งใหม่ ๆ ช่วยพัฒนาทักษะของผู้ปฏิบัติงาน ส่งเสริมให้เกิดเครือข่ายและการปฏิบัติการณ์ของกลุ่มเพราะมีชุมชนนักปฏิบัติ ช่วยขับเคลื่อนกลยุทธ์ขององค์กร รับรู้ปัญหาขององค์กรได้อย่างรวดเร็ว ช่วยแพร่กระจายแนวปฏิบัติที่ดีระหว่างหน่วยงานในองค์กรช่วยสร้างคู่มือ/แนวปฏิบัติในการทำงานสำหรับหน่วยงานที่มีสาขามากจะช่วยให้สามารถปฏิบัติงานเหมือนกันหรืองานในหน้าที่เดียวกันได้ไม่แตกต่างกัน ช่วยทำให้ผลผลิตและการบริการดีขึ้น ช่วยให้เกิดการแลกเปลี่ยนความคิดข้ามสายงานทำให้เกิดการพัฒนาและสร้างนวัตกรรมใหม่ ๆ ช่วยเพิ่มความสามารถในการแข่งขันให้กับองค์กร ช่วยบันทึกความรู้ไว้ให้กับองค์กร (กรณีคนลาออกจากราชการ หรือเกษียณอายุราชการ) ช่วยลดช่องว่างทางความคิดระหว่างพนักงานเก่ากับพนักงานใหม่ ช่วยถ่ายโอนความรู้จากรุ่นไปสู่รุ่น และช่วยตอบสนองความต้องการของลูกค้าได้ตรงจุด

การจัดองค์กรที่เหมาะสม มีบรรยากาศองค์กรที่ดี และให้บุคลากรมีส่วนร่วมในการปฏิบัติงาน รวมถึงมีการจัดการความรู้ให้บุคลากรอย่างสม่ำเสมอเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงานจะทำให้เกิดประสิทธิภาพภายในองค์กรให้สามารถบรรลุวัตถุประสงค์ตามที่ต้องการ

ไซเบอร์กับการรักษาความปลอดภัยและการปฏิบัติการ (Cyber with Security and Operations) (ไซเบอร์กับการรักษาความปลอดภัยและการปฏิบัติการ, ออนไลน์, 2556)

1. ความหมายของ Cyber

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” ไซเบอร์เนติกส์ (Cybernetics) เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์ หรือระบบกลไกที่ทำงานคล้ายคลึงกัน วิชานี้เปรียบเทียบความคล้ายคลึง และต่างกันระหว่างสิ่งมีชีวิตกับสิ่งไม่มีชีวิต และยึดหลักการพื้นฐานทางด้านการสื่อสารและการควบคุมที่สามารถอธิบายการทำงานของทั้งสิ่งมีชีวิตและสิ่งไม่มีชีวิตได้

2. การรักษาความปลอดภัยของไซเบอร์ (Cyber Security)

Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรมและความผิดพลาดต่าง ๆ ซึ่งความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ การละเมิดการป้องกัน

ข้อมูลส่วนตัว, การรบกวนการทำงานหรือการดำเนินธุรกรรม และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

2.1 มาตรการในการรักษาความปลอดภัยไซเบอร์

มาตรการในการรักษาความปลอดภัยไซเบอร์จึงมีระบบในการรักษาความปลอดภัยที่หลากหลาย ทำให้มาตรการรักษาความปลอดภัยที่ใช้ในห้วงไซเบอร์จึงสามารถนำไปประยุกต์ใช้ร่วมกับมาตรการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ เช่น เทคนิค Authentication ใช้ในการตรวจสอบและยืนยันตัวบุคคล หรืออุปกรณ์ปลายทางที่มีการติดต่อสื่อสารระหว่างกัน เทคนิค Automated theorem proving และเครื่องมือในการตรวจสอบอื่น ๆ สามารถทำให้กลไกที่ใช้งานระบบรักษาความปลอดภัยตามความต้องการที่ได้กำหนดไว้ เทคนิค Chain of Trust สามารถถูกใช้ในการทำให้ซอฟต์แวร์ที่ถูกใช้งานผ่านการตรวจสอบและยืนยันจากผู้ออกแบบระบบ เทคนิคการรหัส (Cryptographic) สามารถถูกใช้ในการป้องกันข้อมูลระหว่างการส่งข้อมูลระหว่างระบบ ลดโอกาสความเป็นไปได้ในการลักลอบเปิดเผยและแก้ไขข้อมูลระหว่างการรับ-ส่ง อุปกรณ์ Firewall สามารถป้องกันระบบจากการรุกรานแบบ online โดยการกำหนดการผ่านเข้าออกของ Data Package ผ่านเส้นทางการจราจรบนเครือข่ายที่กำหนด ตามที่ผู้ดูแลระบบได้ออกแบบไว้ เป็นต้น

2.2 การปฏิบัติการในห้วงไซเบอร์ (Cyberspace Operations)

การดำเนินกลยุทธ์ภายใต้ขอบเขตในห้วงไซเบอร์ เป็นสิ่งนำมาซึ่งขีดความสามารถในการปฏิบัติการด้านต่าง ๆ ของ ทอ.สหรัฐ ได้แก่ การบัญชาการ การควบคุม การติดต่อสื่อสาร การปฏิบัติด้านคอมพิวเตอร์ การข่าวกรอง การเฝ้าตรวจ และการลาดตระเวน ปัจจุบันการทำงานของระบบการค้าระหว่างประเทศ อุตสาหกรรมพื้นฐาน และการป้องกันประเทศที่ทันสมัยขึ้นอยู่กับอิสรภาพของการใช้งานทรัพยากรภาคพื้น ภาคทะเล ภาคอากาศ ห้วงอวกาศ และห้วงไซเบอร์ โดยเฉพาะพลังอำนาจห้วงไซเบอร์มีอิทธิพลและส่งผลกระทบต่อกับการปฏิบัติในส่วนอื่น ๆ การควบคุมในห้วงไซเบอร์โดยรวมกับการปฏิบัติภารกิจ เป็นความต้องการพื้นฐานก่อนสิ่งอื่นใดของการปฏิบัติทุกภารกิจทางทหารที่มีประสิทธิภาพ ขณะที่เราชื่นชอบกำลังที่พร้อมด้วยขีดความสามารถด้านไซเบอร์ เรายังคงต้องตระหนักถึงขีดความสามารถและความพยายามที่ไม่สมมาตรในห้วงไซเบอร์ของศัตรูของเราเช่นกัน ดังนั้น เราต้องดำรงพันธะด้านการศึกษา การฝึกอบรม และการจัดหายุทโธปกรณ์ให้กับกำลังพล เพื่อความเหนือกว่าในการแข่งขันของห้วงไซเบอร์ต่อไป เมื่อพิจารณาแล้วการปฏิบัติการไซเบอร์ไม่เพียงแต่ส่งผลกระทบด้านการทหารเท่านั้น หากสามารถนำไปใช้ในความมั่นคงด้านอื่น ๆ (ด้านเศรษฐกิจ ด้านสังคม และวัฒนธรรม) ดังนั้น ในภาคธุรกิจที่จะต้องคงความได้เปรียบคู่แข่งทางการค้า และรักษาฐานลูกค้าเดิม ตลอดจนขยายฐานการตลาดใหม่อยู่ตลอดเวลา จำเป็นจะต้องพึ่งพาการปฏิบัติการในห้วงไซเบอร์เช่นเดียวกันกับด้านการทหาร การสงครามไซเบอร์ หรือ Cyber Warfare (CW) เป็นการใช้กรอบของไซเบอร์เป็นเครื่องมือเพื่อให้ได้มาซึ่งการครองความได้เปรียบในห้วงไซเบอร์ หรือ Cyberspace Superiority (ระดับขั้นในการควบคุมในห้วงไซเบอร์) โดยกำลังฝ่ายหนึ่งที่สามารถบังคับหรืออนุญาตให้การปฏิบัติการดำเนินการไปอย่างเชื่อมั่นและปลอดภัย โดยหน่วยกำลังที่ปฏิบัติบนพื้นที่ปฏิบัติการที่เกี่ยวข้อง การปฏิบัติการทางทหารที่ดำเนินการเพื่อขัดขวางการปฏิบัติงานระบบไซเบอร์และอาวุธของฝ่ายตรงข้าม รวมทั้ง เพื่อดำรงการปฏิบัติงานระบบไซเบอร์และอาวุธอย่างมีประสิทธิภาพของฝ่ายเราในการขัดกัน การปฏิบัติการ

ดังกล่าวรวมถึง การโจมตีทางไซเบอร์ (Cyber Attack) การป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากการสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions) ดังนี้

2.3 การโจมตีทางไซเบอร์ (Cyber Attack)

การโจมตีทางไซเบอร์ คือ การกระทำใด ๆ ที่ใช้คอมพิวเตอร์ เครือข่าย หรือระบบ รวมทั้งอุปกรณ์ที่เกี่ยวข้อง ซึ่งตั้งใจเป็นภัยคุกคาม ขัดขวาง หรือทำลายระบบ ทรัพยากร และการทำงานของไซเบอร์ที่สำคัญของศัตรู ผลกระทบที่ต้องการของการโจมตีทางไซเบอร์ไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมาย ตัวอย่างเช่น การโจมตีต่อระบบคอมพิวเตอร์ที่ต้องการลิดรอน หรือทำลายโครงสร้างพื้นฐานสาธารณูปโภค หรือขีดความสามารถของระบบบัญชาการและควบคุม (C2) การโจมตีทางไซเบอร์อาจจะต้องใช้พาหะตัวกลางในการดำเนินการ รวมทั้ง อุปกรณ์ต่อเชื่อมต่าง ๆ (Peripheral Devices) เครื่องส่งสัญญาณอิเล็กทรอนิกส์ (Electronic Transmitters) การเข้ารหัส (Embedded Code) หรือเจ้าหน้าที่ปฏิบัติงาน (Operators) กิจกรรมหรือผลกระทบของการโจมตีอาจจะเกิดขึ้นอย่างกระจัดกระจายเป็นวงกว้าง หรือเป็นเฉพาะพื้นที่ที่เป็นเป้าหมาย

2.4 การป้องกันทางไซเบอร์ (Cyber Defense)

การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในห้วงไซเบอร์ของหน่วยงานที่เกี่ยวข้อง ในการดำรงขีดความสามารถด้านการตรวจจับวิเคราะห์และลดภัยคุกคาม/จุดเสี่ยงต่าง ๆ และดำเนินกลยุทธ์ในการเอาชนะฝ่ายตรงข้าม เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ รวมถึงการปฏิบัติการเครือข่ายเชิงรุก (Proactive NetOps) การดำเนินการดังนี้

2.4.1 การป้องกันการโจมตีทางไซเบอร์ (Defensive Counter Cyber : DCC) เป็นมาตรการป้องกันต่าง ๆ ทั้งหมดที่ถูกออกแบบเพื่อตรวจจับ ระบุตัวตน สกัดกั้น และทำลาย หรือลดกิจกรรมอันตรายต่าง ๆ ที่พยายามเจาะ หรือโจมตีผ่านห้วงไซเบอร์

2.4.2 มาตรการเชิงรับ (Defensive Countermeasures) เป็นมาตรการในการใช้งานอุปกรณ์ และ/หรือเทคนิค ที่มีวัตถุประสงค์ต่อการทำให้การปฏิบัติของศัตรูด้อยประสิทธิภาพในเชิงการป้องกันระบบข้อมูลที่มีชั้นความลับ หรือระบบที่มีผลกระทบต่อการปฏิบัติการ

2.4.3 การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ (Cyber Operational Preparation of Environment : C-OPE)

การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ (C-OPE) เป็นการทำงานภายในห้วงไซเบอร์ในการวางแผนและเตรียมการให้กับการปฏิบัติการทางทหารที่ตามมา โดยอาจรวมถึงการกำหนดระบุข้อมูล การกำหนดตั้งค่าระบบ/เครือข่าย หรือโครงสร้างการเชื่อมต่อทางกายภาพกับระบบหรือเครือข่ายที่เกี่ยวข้อง เพื่อตรวจสอบช่องโหว่/จุดอ่อนของระบบ รวมถึงการกระทำเพื่อเพิ่มความมั่นใจการเข้าถึง และ/หรือการควบคุมระบบ เครือข่าย หรือข้อมูลในระหว่างการต่อสู้กับภัยคุกคามต่าง ๆ ทั้งนี้การเตรียมสภาพแวดการปฏิบัติการทางไซเบอร์ (C-OPE) ครอบคลุมการเปิดเผยเครือข่ายคอมพิวเตอร์ (Computer Network Exploitation: CNE)

การดำเนินการด้านไซเบอร์เป็นการดำเนินการในระบบเครือข่ายที่ใช้งานอย่างกว้างขวาง ต้องมีการรักษาความปลอดภัยและการปฏิบัติการห้วงไซเบอร์ที่ถูกต้องเหมาะสม ซึ่งเป็นการป้องกันระบบและข้อมูลที่สำคัญภายในองค์กรเพื่อไม่ให้ตกเป็นผลประโยชน์ของฝ่ายที่ไม่หวังดี หากมีส่วนใดส่วนหนึ่งโดนล้วงข้อมูลหรือทำลายข้อมูล องค์กรจะศูนย์เสียความเป็นเอกภาพในการบริหารงานภายในทันที

สงครามไซเบอร์ (Cyber Warfare)

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 การใช้คอมพิวเตอร์และอินเทอร์เน็ต ในการทำสงคราม เช่น การโจมตีเว็บ หรือบล็อคเว็บ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเทอร์เน็ตการเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ ทำให้ข้อมูลมีการเปลี่ยนแปลง การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก เป็นต้น

2. แนวคิดเกี่ยวกับการทำสงครามไซเบอร์

จุดกำเนิดแนวคิดของสงครามนี้ก่อตัวเป็นรูปร่างขึ้นจากนวนิยายชื่อนิวโรแมนเซอร์ (Neuromancer) ที่ชนะการประกวดจนถูกยกย่องเป็นวรรณกรรมประวัติศาสตร์ของแนวคิดใหม่จากผลงานเขียนของวิลเลียม กิ๊บสัน เป็นเรื่องราวของการนำเสนอ“ปัญญาประดิษฐ์”(Artificial Intelligence-AI) ในปี พ.ศ.2527 จนก่อให้เกิดแนวคิดต่อมาในการผลิตคอมพิวเตอร์โครงการที่ 3 ของโลกเพื่อให้ทำหน้าที่ทางด้านนี้และนำไปสู่คำนิยามของคำว่า “ไซเบอร์” ที่ชัดเจนเป็นรูปธรรมว่าไม่ใช่เพียงแต่ในความหมายของทางคอมพิวเตอร์ที่มักตีความคำว่า “ไซเบอร์” โดยนำไปรวมกับคำว่าไซเบอร์สเปซ (Cyberspace) มีความหมายว่าทุกแห่งทุกหนที่ไปได้ทั่ว ปัจจุบันไซเบอร์สเปซจะหมายถึง การอยู่ในเครือข่ายอินเทอร์เน็ตที่อยู่ทุกแห่งทุกหนที่ระบบอินเทอร์เน็ตเชื่อมต่อไปถึง เมื่อได้นำคำว่าไซเบอร์เนติกส์ (Cybernetics) ที่บัญญัติขึ้นโดย นอร์เบิร์ต วีเนอร์ นักคณิตศาสตร์ที่มีชื่อเมื่อ 48 ปีก่อนให้ความหมายว่า หมายถึง ระบบควบคุมการทำงานของเครื่องจักร หรือร่างกายที่สมบูรณ์ในตัวเอง และสามารถเรียนรู้ได้ภายในตัวของร่างกายด้วยระบบสื่อสารภายในหรือเชิงโทรจิตที่ติดกับตัวตน (Mindset) จึงมีการพิจารณาลักษณะสงครามไซเบอร์นี้เป็นสงครามความคิดที่ประยุกต์ใช้ระหว่างความคิดของความเป็นมนุษย์ที่มีตัวตนกับความเป็นเชิงมนุษย์หรือเลียนแบบมนุษย์ที่เรียกว่า

“ไซเบอร์ก” (Cyborg) การดำเนินการสงครามไซเบอร์มีแนวทางในการดำเนินที่แตกต่างและหลากหลาย ซึ่งได้แก่

2.1 การก่อการร้ายทางสารสนเทศ (Information Terrorism) เป็นลักษณะของการก่อความรุนแรง ความเสียหาย หรือก่อความไม่สงบบนระบบเครือข่ายที่เชื่อมต่อกัน

2.2 การโจมตีทางความหมาย (Semantic Attack) เป็นการใช้เทคนิคและความสามารถในการเป็นแฮกเกอร์แอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้าม เพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน เช่น การใช้แฮกเกอร์เจาะระบบตรวจจับของฝ่ายตรงข้ามแล้วทำการแก้ไขโปรแกรมให้ทำงานผิดผลาด โดยตรวจจับเครื่องบินฝ่ายเราได้แล้วแสดงเป็นเครื่องบินฝ่ายเดียวกันกับเครื่องบินฝ่ายตรงข้าม ทำให้ฝ่ายตรงข้ามไม่สามารถตรวจจับเครื่องบินของฝ่ายเราได้

3. ภัยคุกคามทางไซเบอร์

3.1 ประเภทของภัยคุกคามทางไซเบอร์ แบ่งออกเป็น 4 ประเภท ดังนี้

3.1.1 ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (Application-Based Threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่า มัลแวร์ (Malware) นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

3.1.2 ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-Based Threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพาเปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี

3.1.3 ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง

3.1.4 ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (Hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤติ สถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

3.2 ผู้ก่อเหตุทางไซเบอร์ คือ กลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม (นงรัตน์ สายเพชร, 2556) คือ (1) ประเทศที่มีความประสงค์ร้าย (2) ผู้ก่อการร้าย (3) สายลับภาคเอกชน/องค์กรอาชญากรรม (4) แฮกเกอร์ (Hackers) และ (5) แฮกทิวิส (Hacktivists)

3.3 ชนิดของภัยคุกคามจากไซเบอร์ สามารถจำแนกออกเป็น 2 กลุ่ม ได้แก่ การจำแนกตามประเภทของภัยคุกคาม และการจำแนกตามลักษณะ/ผลของภัยคุกคาม แต่ละกลุ่มมีรายละเอียดดังนี้

3.3.1 การจำแนกภัยคุกคามตามประเภทหน่วยงาน 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) โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server) ฟิชชิ่ง (Phishing) สตอร์มเวิร์ม (Storm Worm) และดีดอส (DDoS)

3.3.2 การจำแนกภัยคุกคามตามลักษณะ/ผลของภัยคุกคาม (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์ ผู้เขียนบทความเรื่องความเป็นมาของไทยเซิร์ตจากกระทรวงวิทย์ฯ สู่กระทรวง ICT ในเอกสาร Cyber Security Articles 2012 ของไทยเซิร์ต ได้แสดงรายละเอียดของภัยคุกคามจำแนกตามลักษณะ/ผลของภัยคุกคามจำนวน 8 ด้าน ประกอบด้วย เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (Fraud) ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) การเจาะระบบได้สำเร็จ (Intrusions) โค้ดมุ่งร้าย (Malicious code or malware) การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Information Security) และภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Others)

3.4 การรักษาความปลอดภัยไซเบอร์ (ปริญญา หอมเอนก.“Cyber Security”. แผ่นภาพ, 2557) ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนาและมีประยุกต์ใช้งานอย่างแพร่หลาย ข้อมูลสารสนเทศ การติดต่อสื่อสาร และการใช้งานคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ต่าง ๆ 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 ซึ่งเป็นมาตรฐานที่ยอมรับทั้งภาครัฐ

และเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก

สงครามไซเบอร์เป็นการปฏิบัติการในเครือข่ายที่สามารถทำลายข้อมูลหรือระบบคอมพิวเตอร์และอุปกรณ์อื่นที่อยู่บนเครือข่าย ซึ่งการรบแบบนี้จะไม่มีการเผชิญหน้าแบบการรบในอดีต ทำให้เกิดความวิตกกังวล และความสับสนในการปฏิบัติงาน หากเกิดขึ้นกับทางทหาร จะมีความเสี่ยงสูงมากเพราะรูปแบบการเข้าโจมตีในสงครามไซเบอร์ก่อให้เกิดผลกระทบต่อศักยภาพในการปฏิบัติการรบ ระบบควบคุม การออกคำสั่ง หรือข้อมูลมีความผิดพลาด จึงต้องมีการเตรียมพร้อมเพื่อรับมือกับสงครามไซเบอร์ตลอดเวลา

งานวิจัยที่เกี่ยวข้อง

1. บทวิเคราะห์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ปี พ.ศ. 2559
(แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ, ออนไลน์, 2559)

"The Information Security Forum" (ISF) เป็นองค์กรที่ไม่แสวงหากำไร มีสมาชิกประกอบด้วยองค์กรชั้นนำต่าง ๆ ทั่วโลก ได้จัดทำผลสำรวจ วิเคราะห์ และรายงาน "Threat Horizon Report" เพื่อพยากรณ์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ล่วงหน้าทุก ๆ 2 ปี โดยระบุประเด็นที่ส่งผลกระทบอย่างมีนัยสำคัญต่อองค์กร พร้อมทั้งแนวทางดำเนินการเพื่อป้องกันหรือช่วยลดผลกระทบที่อาจเกิดขึ้นจากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 โดย ISF ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทางไซเบอร์ยังคงต่อเนื่อง สู่ปลายขอบของความเชื่อถือที่องค์กรต้องรักษาไว้ให้ได้ รายงานได้ข้อสรุปหลักๆ ทั้งหมด 3 ประเด็น ได้แก่

1.1 ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (No-one Left to Trust in Cyberspace) การจารกรรมไซเบอร์ที่สนับสนุนโดยหน่วยงานภาครัฐจะกลายเป็นกระแสหลักการควบคุมอินเทอร์เน็ตภายในประเทศหรือภูมิภาค จะสร้างความยุ่งยากต่อธุรกิจเนื่องจากการแทรกแซงของภาครัฐ

1.2 ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ (Confidence in Accepted Solutions Crumbles) โดยผู้ให้บริการจะกลายเป็นช่องโหว่สำคัญ ระบบ Big Data จะกลายเป็นปัญหาหลัก และแอพพลิเคชั่นในมือถือ จะกลายเป็นช่องทางหลักที่ถูกเจาะข้อมูล และการเข้ารหัสข้อมูลในระบบจะไม่ได้ผล

1.3 ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Failure to Deliver the Cyber Resilience Promise) ผู้บริหาร ต้องรับรู้และถึงเวลาที่ต้องระบุข้อมูลวางแนวทางในการดำเนินการ ความแตกต่างด้านทักษะของบุคลากรจะมีช่องห่างกว้างมากขึ้น ความมั่นคงปลอดภัยสารสนเทศในปัจจุบันอาจจะไม่เหมาะสมและใช้ได้กับบุคลากรรุ่นใหม่

การจารกรรมทางไซเบอร์ (Cyber Espionage) จะทวีความเข้มข้นรุนแรงมากขึ้น ซึ่งผลการสำรวจและข้อมูลจากองค์กรชั้นนำ ได้สรุปผลการวิเคราะห์พฤติกรรม incidents จากภัยคุกคามต่าง ๆ ในรอบ 10 ปี คือ การจารกรรมทางไซเบอร์ (Cyber-Espionage) การโจมตีระบบ (DoS Attacks) โปรแกรมมุ่งร้ายเพื่อก่ออาชญากรรม (Crimeware) การโจมตีแอพพลิเคชั่นเว็บ (Web App Attacks) การเจาะระบบซื้อขาย (Point-of-Sale Intrusions) การดูดข้อมูลเพื่อทำปลอมบัตร (Payment Card

Skimmers) การขโมยหรือการทำให้สูญเสียทางกายภาพ (Physical Theft and Loss) ความผิดพลาดประเภทต่าง ๆ (Miscellaneous Errors) การใช้งานผิดวัตถุประสงค์จากคนในองค์กร (Insider Misuse) รวมถึงการจารกรรมไซเบอร์ด้วยโปรแกรมและซอฟต์แวร์ที่สนับสนุนพัฒนาขึ้นโดยภาครัฐ เพื่อติดตามพฤติกรรมกลุ่มเป้าหมายที่ต้องการจะมีวงกว้างมากขึ้น ดังนั้น แนวโน้มการควบคุมหรือแทรกแซงระบบอินเทอร์เน็ต หรือ อาจเรียกได้ว่าปิดประเทศด้านไซเบอร์ เฉพาะบางช่องทางที่ต้องการควบคุม จะมีให้เห็นมากขึ้น อย่างที่ประเทศจีนได้สร้างกำแพงเมืองจีนในโลกไซเบอร์อยู่ในขณะนี้ ทั้งเพื่อปกป้องพลเมืองตนเองไปที่จะผจญสื่อสารโลกภายนอก และป้องกันคนภายนอกเข้ามา ดังนั้น องค์กรทั่วโลกต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลง และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่

2. การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ : ความท้าทายของกองทัพบก (Cyber Security : A Challenge of Army) (ความท้าทายของกองทัพบก, ออนไลน์, 2557)

ปัจจุบันและแนวโน้มในอนาคตภัยคุกคามด้านไซเบอร์ นับวันจะทวีความเข้มข้นและความรุนแรงมากขึ้นตามลำดับ ทั้งนี้เป็นผลมาจากความเจริญก้าวหน้าด้านการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ (Cyber Attack) ซึ่งหลายคนอาจมองว่าเป็นภัยที่ไกลตัว รัฐบาลสหรัฐอเมริกา ได้ตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ดังกล่าว จึงได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology ; NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย (Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารความเสี่ยงไซเบอร์ (Cyber Risk Management) ที่มีผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย กลุ่มหน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม จำแนกเป็น 5 Functions (IPDRR : Identify, Protect, Detect, Respond, Recover) กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึงกลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ และข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม ซึ่งกองทัพบก ได้เล็งเห็นความสำคัญในด้านการรักษาความมั่งคงปลอดภัยไซเบอร์เช่นกัน จึงได้อนุมัติหลักการให้จัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Centre) ขึ้น การกำหนดกรอบความคิดในการปฏิบัติงาน (Framework) เพื่อสร้างหลักประกันความสำเร็จในการดำเนินการจึงเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่ง ทั้งนี้เพื่อใช้เป็นแนวทางการปฏิบัติงาน (Guide Line) ของเจ้าหน้าที่ศูนย์ไซเบอร์กองทัพบก และเจ้าหน้าที่อื่น ๆ ที่เกี่ยวข้อง รวมถึงการสร้างความสำนึกความตระหนัก และสร้างความรู้เข้าใจของกำลังพลทุกระดับชั้น โดยในชั้นต้นกรอบแนวทางการปฏิบัติงานของศูนย์ไซเบอร์กองทัพบก ยังคงยึดถือการดำเนินงานตามหลักหน้าที่พื้นฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and

Technology NIST) ทั้ง 5 ประการ (IPDRR : Identify, Protect, Detect, Respond, Recover) จึงต้องการบุคลากรที่จะมาปฏิบัติหน้าที่ โดยมีคุณลักษณะของงานประเภทสาขาต่าง ๆ ที่ต้องใช้ความรู้ ความสามารถ และประสบการณ์เฉพาะด้านที่แตกต่างและเหนือกว่าประเภทของงานสาขาด้านเทคโนโลยีสารสนเทศ (Information Technology : IT) ปกติประเภทสาขาต่าง ๆ ที่ต้องใช้ความรู้ ความสามารถและประสบการณ์เฉพาะด้านเป็นพิเศษในด้านไซเบอร์ เช่น การบริหารจัดการทรัพย์สิน (Asset Management : AM) การตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ (Environmental Scanning : ES) การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment : RA) การประเมินช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment : VA) การประกันความเสี่ยงด้านสารสนเทศ (Information Assurance : IA) การปฏิบัติการทดสอบเจาะระบบสารสนเทศ (Penetration Testing : Pen-Test) การบริหารจัดการความเสี่ยงระบบสารสนเทศ (Risk Management : RM) การเฝ้าระวัง ตรวจสอบ และวิเคราะห์ไซเบอร์ (Cyber Monitoring and Analysis) การปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations) การตรวจสอบระบบสารสนเทศ (IT Audit) การตรวจพิสูจน์หลักฐานทางดิจิตอล (Digital Forensics) การปฏิบัติการฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response ; CER) การปฏิบัติการกู้คืนระบบ (System Recovery ; SR) เป็นต้น

3. ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security

(สรุปภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security, ออนไลน์, 2559)

อาจารย์ปริญญา หอมเอนก สรุปแนวโน้มภัยคุกคามและทิศทางด้านความมั่นคงปลอดภัยในปี 2016 – 2018 ดังนี้

3.1 Cyber Security ไม่ใช่เรื่องเฉพาะฝ่าย IT อีกต่อไป หากเป็นเรื่องที่ต้องนำเข้าที่ประชุม “บอร์ดบริหาร” ขององค์กร

3.2 Microsoft ได้นำหลักการของ NIST Cybersecurity Framework มาใช้ใน Microsoft CDOC ได้แก่ Protect, Detect และ Respond

3.3 Cyber Threat Intelligence เป็นการเปลี่ยนวิธีการบริหารจัดการความมั่นคงปลอดภัยจาก “Reactive” เป็น “Proactive”

3.4 แฮ็คเกอร์จะมุ่งหน้าโจมตีไปยังเป้าหมายเฉพาะ แต่มีผลกระทบและสร้างความเสียหายสูงต่อองค์กร

3.5 การโจมตีของแฮ็คเกอร์จะมีลักษณะต่อเนื่องและฝังตัวเป็นระยะเวลานานกว่าองค์กรจะตรวจจับได้ว่าถูกแฮ็ค (Advanced Persistent Threats)

3.6 แฮ็คเกอร์พุ่งเป้าโจมตีองค์กรขนาดใหญ่ และมีรัฐบาลให้การสนับสนุนอยู่เบื้องหลัง (State-Sponsored Attack)

3.7 องค์กรจำเป็นต้องมีความสามารถในการตามล่าและติดตามแฮ็คเกอร์ในโลกจริงที่ไม่ใช่เพียงโลกไซเบอร์

และกล่าวเพิ่มเติมว่า “ปัจจุบันนี้แฮ็คเกอร์ระดับประเทศเขาไม่แฮ็คระบบหรือปล่อยมัลแวร์กันแล้ว แต่ใช้วิธีฝัง Backdoor มากับอุปกรณ์ IoT เช่น CCTV, IP Camera หรือ Router

ตั้งแต่แรกแทน ส่งผลให้แฮ็คเกอร์สามารถเข้าโจมตีระบบผ่านอุปกรณ์หรือสร้างกองทัพซอมบี้ไว้โจมตี DDoS แบบที่ปรากฏในข่าวล่าสุดได้ตามต้องการทันที”

ยุทธศาสตร์กองทัพอากาศ (ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2560)

1. ยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ.2560-พ.ศ.2579) (ฉบับเผยแพร่)

ยุทธศาสตร์กองทัพอากาศ 20 ปี ให้ความสำคัญกับการพัฒนากองทัพอากาศในทุกด้านอย่างเป็นระบบ ทั้งนี้ เพื่อให้กองทัพอากาศมีขีดความสามารถที่เพียงพอและเหมาะสมในการปฏิบัติภารกิจที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ โดยมีวัตถุประสงค์สำคัญ เพื่อปรับปรุงขอบเขตการพัฒนากองทัพอากาศให้สอดคล้องกับสภาวะแวดล้อมด้าน ความมั่นคงที่เปลี่ยนแปลงไปในปัจจุบันและที่คาดว่าจะเกิดขึ้นในกรอบระยะเวลา 20 ปีจากนี้ไปมีความสอดคล้องกับยุทธศาสตร์ชาติ ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม และยุทธศาสตร์ทหารกองทัพไทย ซึ่งยุทธศาสตร์ทหารกองทัพไทย 20 ปี กำหนดวัตถุประสงค์เพื่อเสริมสร้าง ความพร้อมรบของกองทัพไทยในการปฏิบัติภารกิจหลักในการป้องกันประเทศ พิทักษ์รักษาและเทิดทูนสถาบันพระมหากษัตริย์ รวมทั้งต้องสามารถสนับสนุนรัฐบาลในการแก้ไขปัญหาสำคัญของชาติ โดยใช้การปฏิบัติการร่วมเชิงรุก เสริมสร้างกองทัพให้เป็นกำลังอเนกประสงค์ที่มีความหลากหลาย พร้อมเผชิญภัยคุกคามทุกรูปแบบ ทั้งนี้ ยังคงยึดถือแนวคิดทางยุทธศาสตร์ จำนวน 3 แนวคิด ตามยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม 20 ปี โดยกำหนดวัตถุประสงค์เฉพาะทางทหารด้านสงครามไซเบอร์ คือ การปฏิบัติการในสงครามไซเบอร์ (Cyber Warfare) เพื่อให้กองทัพไทย มีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ (Cyber Domain) ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติ ตลอดจนสามารถบูรณาการและให้การสนับสนุนความมั่นคงไซเบอร์ (Cyber Security) ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ ซึ่งยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทยได้กำหนดแนวทางการปฏิบัติการทางทหารในมิติไซเบอร์ของกองทัพไทย ทั้งในการเตรียมกำลังและใช้กำลัง โดยแยกเป็น 3 ประเด็นยุทธศาสตร์ ได้แก่

1.1 ยุทธศาสตร์การป้องกันเชิงรุกสำหรับปฏิบัติการในมิติไซเบอร์ เสริมสร้างพลังอำนาจทางไซเบอร์ของกองทัพไทย (RTARF Cyber Power) เพื่อการปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้าม ทั้งที่เป็นรัฐ (State Actors) ไม่ใช่รัฐ (Non-State Actors) และสนับสนุนโดยรัฐ (State Sponsored Actors) ตลอดจนกลุ่มบุคคล หรือบุคคลใด ๆ ที่อาจเป็นภัยคุกคามทางไซเบอร์ (Cyber Threats) โดยมีความมุ่งหมายในการลดทอน ขัดขวาง ระงับ ยับยั้ง หรือปฏิบัติการเชิงรุกในลักษณะจำกัด (Limited Offensive Action) และการตอบโต้ (Counterattack) อย่างรวดเร็วกรณีถูกโจมตีทางไซเบอร์ ทั้งนี้ เพื่อความได้เปรียบต่อฝ่ายตรงข้ามตั้งแต่ในสภาวะปกติ และสร้างการตระหนักรู้ทางไซเบอร์ (Cyber Awareness) ที่จะนำไปสู่การตัดสินใจของระดับผู้บังคับบัญชาให้เท่าทันต่อสถานการณ์ต่าง ๆ

1.2 ยุทธศาสตร์การผนึกกำลังป้องกันประเทศสาหรับปฏิบัติการในมิติไซเบอร์ สร้างความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติไซเบอร์ของทุกภาคส่วนภายในประเทศอย่างเป็นระบบ

2. ยุทธศาสตร์กองทัพอากาศ

ยุทธศาสตร์กองทัพอากาศได้กำหนดบทบาท หน้าที่ และภารกิจด้านไซเบอร์ โดยกำหนดให้เป็น มิติไซเบอร์ (Cyber Domain) เทคโนโลยีสารสนเทศและการสื่อสารด้านเครือข่ายและอินเทอร์เน็ตได้รับ การพัฒนาอย่างรวดเร็ว รวมทั้งการเกิดขึ้นของภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบการจารกรรมข้อมูล และการโจมตีเพื่อทำลายล้าง ล้วนก่อให้เกิดผลกระทบและความเสียหายในวงกว้าง หลายประเทศมีการจัดตั้งหน่วยงานรับผิดชอบโดยตรง และกำหนดเป็นมิติหนึ่งในการปฏิบัติการด้านความมั่นคงของชาติ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ และยุทธศาสตร์ด้านสงครามไซเบอร์กองทัพไทย กำหนดให้เหล่าทัพต้องมีขีดความสามารถ ดังนี้ การป้องกันภัยคุกคามทางไซเบอร์ พัฒนาและใช้ประโยชน์จากขีดความสามารถทางไซเบอร์ในการปฏิบัติการทางทหาร ร่วมมือกับหน่วยงานภายในเพื่อการผนึกกำลังป้องกันประเทศ

กองทัพอากาศจึงจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ให้มี ความพร้อมในการเผชิญกับภัยคุกคามด้านไซเบอร์และสอดคล้องตามยุทธศาสตร์และนโยบาย ที่เกี่ยวข้อง นอกจากนี้การพัฒนาสู่กองทัพอากาศดิจิตอล (DAF) และกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (NCAF) จำเป็นต้องพัฒนาระบบเครือข่าย (Network) ให้มีความแข็งแรงและปลอดภัย และกำหนดกลยุทธเพื่อพัฒนาขีดความสามารถด้านสงครามไซเบอร์ มีวัตถุประสงค์เพื่อพัฒนาขีดความสามารถด้านสงครามไซเบอร์ของกองทัพอากาศ โดยพัฒนาโครงสร้างพื้นฐาน บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ และใช้ประโยชน์จากการปฏิบัติการทางไซเบอร์ในการขยายขีดความสามารถการปฏิบัติการทางทหาร รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือ กับหน่วยงานภายในประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์ มีกลยุทธ์ย่อยในการดำเนินการ ดังนี้

2.1 พัฒนาหลักนิยมการปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศทั้งเชิงรุกและเชิงรับ รวมทั้งปรับปรุงหลักนิยมของกองทัพอากาศในส่วนอื่น ๆ ที่เกี่ยวข้อง เพื่อใช้เป็นพื้นฐานในการปฏิบัติการ

2.2 พัฒนายุทโธปกรณ์ทางไซเบอร์ (Cyber Weapon) อย่างเป็นรูปธรรม ในการป้องกัน ติดตาม เฝ้าระวัง แจ้งเตือน และวิเคราะห์เหตุคุกคามทางไซเบอร์ (Cyber Incident Response) ตลอดจนการทำลายผู้ที่มีส่วนเกี่ยวข้องในการโจมตีทางไซเบอร์เพื่อเป็นการป้องปราม

2.3 พัฒนาระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก (Cyber Intelligence) เพื่อจัดทำบัญชีเป้าหมายทางไซเบอร์ โดยเฉพาะเป้าหมายภายในระบบโครงสร้างพื้นฐานวิกฤตของรัฐ ระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ทางทหาร และเป้าหมายที่มีความอ่อนไหว หรือมีความสำคัญทางยุทธศาสตร์ของฝ่ายตรงข้าม

2.4 พัฒนาระบบการฝึกศึกษาสาหรับการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศอย่างเป็นรูปธรรม รวมทั้งการฝึกจำลองยุทธ์ด้านไซเบอร์ และจัดให้มีการฝึกอย่างต่อเนื่องเพื่อพัฒนาบุคลากร และนักรบไซเบอร์ (Cyber Warrior)

2.5 พัฒนาระบบการจัดการความรู้ (Knowledge Management System) เพื่อให้เกิดการแลกเปลี่ยนและต่อยอดองค์ความรู้ด้านการปฏิบัติการไซเบอร์อย่างรวดเร็วและเป็นรูปธรรม

รวมทั้งการแลกเปลี่ยนองค์ความรู้ การฝึกศึกษา และการวิจัยและพัฒนากับหน่วยงานทั้งภายในและภายนอกกองทัพอากาศ

3. ร่างแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560 – 2564 (ร่างแผนแม่บทไซเบอร์, ออนไลน์, 2560)

เมื่อวันที่ 23 ส.ค.59 พล.ต.ฤทธี อินทราวุธ ผู้อำนวยการศูนย์เทคโนโลยีทางทหาร กองบัญชาการกองทัพบก แถลงผลการประชุมสภากลาโหม ที่มี พล.อ.ประวิตร วงษ์สุวรรณ รองนายกฯ และ รมว.กลาโหม เป็นประธาน ได้เห็นชอบ ร่างแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 โดยสรุปสาระสำคัญ คือ ร่างแผนแม่บทฯ นี้ จะครอบคลุมแผนงานหลัก 6 แผนงาน ได้แก่

1. แผนการจัดองค์กรด้านไซเบอร์ โดย กห. บก.ทท. และเหล่าทัพ ดำเนินการจัดตั้งหน่วยงานไซเบอร์/ ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง

2. แผนการป้องกันระบบโครงสร้างพื้นฐาน โดย กห. บก.ทท. และเหล่าทัพเตรียมจัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของตนขึ้นมาเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่จะมาโจมตีระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูลรวมทั้งการจัดตั้งทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านปลอดภัยไซเบอร์ได้อย่างรวดเร็ว และทันเวลา

3. แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกัน สะกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่าง ๆ รวมถึงการจัดให้มีการแข่งขันทักษะการปฏิบัติการไซเบอร์ (Cyber Contest) ทั้งนี้มิได้มุ่งหมายเพื่อสร้างนักรบไซเบอร์ (Cyber Warrior) หรือใช้เจ้าหน้าที่ดังกล่าวไปโจมตีหรือแฮ็กข้อมูลส่วนบุคคล ซึ่งเป็นการละเมิดกฎหมายทุกอย่างกระทำภายใต้กรอบกฎหมาย

4. แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโนโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตามความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวันจะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว

5. แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain)

6. แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ธุรกิจเอกชน และประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน และนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ที่มีพลังอำนาจที่ยิ่งใหญ่

โดยจะดำเนินการจัดตั้งศูนย์ไซเบอร์ในระดับกระทรวงกลาโหม โดยสำนักงานปลัดกระทรวงกลาโหม กรมเทคโนโลยีสารสนเทศและอวกาศ กห. (ทสอ.กห.) ภายในปีงบประมาณ 2560 โดยจะเชื่อมโยงกับการตั้งศูนย์ Cyber ของ กองบัญชาการกองทัพไทย และ 3 เหล่าทัพ มีขอบเขตอำนาจหน้าที่ ในการประสานนโยบายไซเบอร์กับระดับชาติ รวมทั้งรับผิดชอบด้านนโยบายยุทธศาสตร์ และปฏิบัติงานด้านไซเบอร์ในระดับยุทธศาสตร์ของกระทรวงกลาโหมในภาพรวม

จากการที่กองทัพอากาศจัดทำยุทธศาสตร์กองทัพอากาศ 20 ปี รองรับยุทธศาสตร์ของหน่วยเหนือ เพื่อเป็นแนวทางในการพัฒนากองทัพอากาศให้สอดคล้องกับสภาวะแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลง นั้น จะเห็นได้ว่า กองทัพอากาศให้ความสำคัญงานด้านไซเบอร์เป็นอย่างมาก และได้กำหนดการพัฒนาบุคลากรพร้อมให้จัดหาระบบที่เกี่ยวข้องมารองรับการปฏิบัติงานเพื่อป้องกันระบบต่าง ๆ ที่มีใช้งานในกองทัพอากาศให้ปลอดภัยจากภัยคุกคามอย่างเป็นรูปธรรม

การพัฒนาบุคลากรของกองทัพอากาศ

กองทัพอากาศได้จัดทำระเบียบกองทัพอากาศ ว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ พ.ศ.2552 (และที่แก้ไขเพิ่มเติม) เพื่อกำหนดเป็นแนวทางการบริหารกำลังพลในด้านต่างๆ เช่น การบรรจุเข้าตำแหน่ง การให้ความรู้ด้านการทหาร การให้ความรู้สายวิชาชีพ การฝึกงานในหน้าที่ เป็นต้น เพื่อพัฒนากำลังพลให้มีประสิทธิภาพ มีคุณสมบัติที่เหมาะสมกับตำแหน่งที่ตรงกับความรู้ความสามารถ มีประเด็นที่เกี่ยวข้องดังนี้

1. ความหมาย

1.1 “การแยกประเภทกำลังพล” หมายความว่า การจำแนกกำลังพลของกองทัพอากาศออกเป็นจำพวกทหาร สาขาจำพวก โดยคำนึงคุณสมบัติและลักษณะงานที่ปฏิบัติเหมาะสมที่สุด

1.2 “จำพวกทหาร” หมายความว่า กลุ่มกำลังพลที่มีคุณสมบัติคล้ายคลึงกันและเป็นไปตามที่กระทรวงกลาโหมกำหนด

1.3 “สาขาจำพวก” หมายความว่า กลุ่มกำลังพลที่แบ่งย่อยออกจากจำพวกทหารโดยมีคุณสมบัติและลักษณะงานเหมือนกัน

1.4 “ความชำนาญทหารอากาศ” หมายความว่า กลุ่มของลักษณะงานที่ต้องการคุณสมบัติพื้นฐานเดียวกันซึ่งแสดงโดยเลขหมายความชำนาญทหารอากาศ

1.5 “เลขหมายความชำนาญทหารอากาศ” หมายความว่า กลุ่มตัวเลขที่กำหนดขึ้นเพื่อใช้แสดงความชำนาญทหารอากาศ

1.6 “หลักสูตรที่กองทัพอากาศกำหนด” หมายความว่า หลักสูตรการฝึกศึกษาหรืออบรมที่กำหนดไว้ในผนวกการบรรยายลักษณะความชำนาญทหารอากาศของแต่ละเลขหมายความชำนาญทหารอากาศ หรือหลักสูตรภายนอกกองทัพอากาศที่กองทัพอากาศรับรองให้เทียบเท่าหลักสูตรดังกล่าว

1.7 “คุณสมบัติ” หมายความว่า คุณสมบัติของกำลังพลทางการศึกษา การฝึก ประสบการณ์ และปัจจัยอื่น ๆ ที่กำลังพลจำเป็นต้องมีหรือควรมีตามที่กำหนดไว้

1.8 “หน่วยหัวหน้าสายวิทยาการ” หมายความว่า หน่วยขึ้นตรงกองทัพอากาศ ซึ่งรับผิดชอบกำลังพลในเหล่าทหาร หรือรับผิดชอบกำลังพลในจำพวกทหารตามที่กำหนด

2. ความสัมพันธ์ของการแยกประเภทกำลังพลกับระบบงานอื่น

การแยกประเภทกำลังพลกองทัพอากาศมีความสัมพันธ์กับระบบงานอื่นคือ อัตรากองทัพอากาศ การบรรจุ การย้าย การศึกษา การฝึกงานในหน้าที่ และการทะเบียนประวัติ

2.1 หลักเกณฑ์การแยกประเภทกำลังพล

2.1.1 การกำหนดเหล่าทหาร นายทหารสัญญาบัตร และนายทหารประทวน เมื่อได้รับการบรรจุเข้ารับราชการและแต่งตั้งยศ จะได้รับการกำหนดเหล่าทหารตามคุณสมบัติพื้นฐานของกำลังพล และเป็นไปตามที่กระทรวงกลาโหมกำหนด

2.1.2 การแต่งตั้งเลขหมายความชำนาญทหารอากาศ ให้กระทำได้เมื่อกำลังพลผู้นั้นยังไม่ได้รับการแต่งตั้งเลขหมายความชำนาญทหารอากาศนั้นมาก่อน ดังนี้

2.1.2.1 การแต่งตั้งเลขหมายความชำนาญทหารอากาศหลัก

นายทหารสัญญาบัตร ผู้ที่ได้รับการบรรจุเข้ารับราชการและแต่งตั้งยศเป็นนายทหารสัญญาบัตร หรือนายทหารประทวนที่ได้รับการเลื่อนยศเป็นนายทหารสัญญาบัตร จะได้รับการแต่งตั้งเลขหมายความชำนาญทหารอากาศหลัก ตรงตามเลขหมายความชำนาญทหารอากาศหน้าที่ของตำแหน่งที่บรรจุ

นายทหารประทวน ผู้ที่ได้รับการบรรจุเข้ารับราชการและแต่งตั้งยศเป็นนายทหารประทวนจะได้รับการแต่งตั้งเลขหมายความชำนาญทหารอากาศหลักให้ตรงตามเลขหมายความชำนาญทหารอากาศหน้าที่ของตำแหน่งที่บรรจุ

2.1.2.2 การแต่งตั้งเลขหมายความชำนาญทหารอากาศรอง

นายทหารสัญญาบัตร หรือนายทหารประทวน เมื่อได้รับการแต่งตั้งเลขหมายความชำนาญทหารอากาศหลักแล้ว สามารถแต่งตั้งเลขหมายความชำนาญทหารอากาศรองที่เหมาะสมได้อีกไม่เกินสองเลขหมาย การแต่งตั้งให้กระทำได้เมื่อมีคุณสมบัติอย่างใดอย่างหนึ่งตามที่กำหนดไว้ ได้แก่ มีพื้นฐานการศึกษาตามหลักสูตรที่กองทัพอากาศกำหนด หรือ สำเร็จการฝึกอบรมตามหลักสูตรที่กองทัพอากาศกำหนด

2.1.3 การเลื่อนระดับความชำนาญ ให้กระทำได้เมื่อกำลังพลผู้นั้นได้รับหมายเลขความชำนาญทหารอากาศมาแล้ว

2.1.3.1 นายทหารสัญญาบัตร

ผู้ที่มีประสบการณ์เพิ่มขึ้นครบถ้วนตามเลขหมายความชำนาญทหารอากาศที่มีระดับความชำนาญที่สูงกว่า และอยู่ในจำพวกทหาร สาขาจำพวก อย่างเดียวกัน หรือผู้ที่เร็จการศึกษาตามหลักสูตรที่กองทัพอากาศกำหนดให้เลื่อนระดับความชำนาญได้เฉพาะเลขหมายความชำนาญทหารอากาศหลัก หรือเลขหมายความชำนาญทหารอากาศรอง ซึ่งตรงกับเลขหมายความชำนาญทหารอากาศหน้าที่ของตำแหน่งที่กำลังพลผู้นั้นบรรจุอยู่เท่านั้น

2.1.3.2 นายทหารประทวน

ผู้ที่สำเร็จการฝึกอบรมตามหลักสูตรที่กองทัพอากาศกำหนด หรือผู้ที่ผ่านการฝึกงานในหน้าที่ตามเลขหมายความชำนาญทหารอากาศที่มีระดับความชำนาญที่สูงกว่าและอยู่ในจำพวกทหาร สาขาจำพวก อย่างเดียวกัน หรือผู้ที่ผ่านการทดสอบความรู้ความสามารถจากหน่วยหัวหน้าสายวิทยาการ เพื่อเลื่อนระดับความชำนาญ ให้เลื่อนระดับความชำนาญได้ตั้งแต่วันที่ผ่านการฝึกงานในหน้าที่ หรือวันที่ผ่านการทดสอบความรู้ความสามารถตามแต่กรณี

จากการที่กองทัพอากาศได้จัดทำระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ ขึ้นมาเพื่อเป็นแนวทางในการบริหารกำลังพลนั้น เห็นได้ว่าการเข้าบรรจุในตำแหน่งที่สูงขึ้น จะมีการพัฒนากำลังพลโดยให้มีการศึกษาและฝึกงานในหน้าที่ให้กับกำลังพลในทุกระดับ รวมถึงยังมีการเพิ่มพูนความรู้ โดยมีทุนให้รับการศึกษาจากสถาบันภายนอกกองทัพ และบริษัทที่เกี่ยวข้องกับการปฏิบัติหน้าที่โดยตรง ทำให้กำลังพลมีโอกาสในการพัฒนาตนเองตามระยะเวลาที่เหมาะสม

สรุป

จากการรวบรวมข้อมูลเอกสาร แนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กรและองค์กรสมัยใหม่ และการปฏิบัติการด้านสงครามไซเบอร์ การรักษาความปลอดภัยและการปฏิบัติการด้านไซเบอร์ งานและบทความที่เกี่ยวข้อง ยุทธศาสตร์กองทัพอากาศ นโยบายผู้บังคับบัญชา และการพัฒนาบุคลากรตามระเบียบกองทัพอากาศ ว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ พ.ศ.2552 ทำให้ทราบถึงแนวทางการรวบรวมข้อมูลที่เกี่ยวข้องกับงานด้านไซเบอร์ การจัดองค์การ การบริหารความเสี่ยงที่อาจจะเกิดขึ้น การพัฒนาองค์การและการพัฒนาบุคลากร รวมถึงแนวทางการดำเนินการของกองทัพอากาศในส่วนที่เกี่ยวข้องกับแผนยุทธศาสตร์ แผนงาน โครงการ นโยบายผู้บังคับบัญชา การปฏิบัติงานด้านไซเบอร์ในปัจจุบันของกองทัพอากาศ โดยเฉพาะยุทธศาสตร์กองทัพอากาศที่จัดทำไว้เพื่อเป็นแนวทางการพัฒนากองทัพให้สอดคล้องกับสภาวะแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลง เพื่อป้องกันระบบที่มีใช้งานในกองทัพให้ปลอดภัยจากภัยคุกคามอย่างเป็นรูปธรรม ซึ่งผู้วิจัยจะใช้ให้เป็นประโยชน์ต่อการดำเนินการต่อไป

บทที่ 3
การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

การปฏิบัติภารกิจด้านไซเบอร์มีองค์ประกอบหลายส่วน ซึ่งแต่ละส่วนมีความจำเป็นต่อการปฏิบัติภารกิจอย่างยิ่งยวด ในภาพรวมของกองทัพอากาศสามารถแบ่งออกได้ ดังนี้

หน่วยงานรับผิดชอบและหน่วยงานที่เกี่ยวข้องกับด้านไซเบอร์ของกองทัพอากาศ

กองทัพอากาศได้กำหนดวิสัยทัศน์องค์กรในการที่จะเป็น “กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ในปี พ.ศ.2562 โดยกำหนดยุทธศาสตร์ในการขับเคลื่อนกองทัพอากาศ 12 ปี แบ่งออกเป็น 3 ช่วง ได้แก่ ช่วงที่ 1 (พ.ศ.2551 - 2554) การเป็นกองทัพอากาศดิจิทัล (Digital Air Force: DAF) ช่วงที่ 2 (พ.ศ.2555 - 2558) การเป็นกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force: NCAF) และช่วงที่ 3 (พ.ศ.2559 - 2562) ขับเคลื่อนไปสู่การเป็นกองทัพอากาศชั้นนำในภูมิภาคด้วยการปฏิบัติงานแบบใช้เครือข่ายเป็นศูนย์กลางเต็มรูปแบบ ในการปฏิบัติการรบและการปฏิบัติการที่ไม่ใช่การรบ เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทุกรูปแบบได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเอง โดยจุดเน้นสำคัญของประเด็นยุทธศาสตร์ คือ ยุทธศาสตร์ที่ว่าด้วยการเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศ ภายใต้การเสริมสร้างนภานุภาพตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) เพื่อให้การดำเนินการภายใต้ NCO เป็นไปอย่างมีประสิทธิภาพ จำเป็นต้องมีและดำรงไว้ซึ่งขีดความสามารถในการปฏิบัติงานที่สอดประสานกันระหว่างองค์ประกอบทั้ง 6 ส่วน เพื่อการตัดสินตกลงใจที่ถูกต้องและรวดเร็วของผู้บังคับบัญชาในระบบบัญชาการและควบคุม ก่อให้เกิดเป็นความได้เปรียบด้านอำนาจกำลังรบ ทั้งนี้ องค์ประกอบที่สำคัญในการดำรงไว้ซึ่งขีดความสามารถในการติดต่อสื่อสารอย่างเสรี ได้แก่ ระบบเครือข่าย ซึ่งจำเป็นต้องมีการรักษาความปลอดภัยจากภัยคุกคามทางไซเบอร์โดยเฉพาะภัยคุกคามในรูปของสงครามไซเบอร์ (Cyberwarfare) ซึ่งทวีจำนวนและมีระดับความรุนแรงเพิ่มมากขึ้นทุกขณะ อย่างเข้มงวดจริงจังทุกส่วนภายใต้ความร่วมมือจากบุคลากรทุกระดับ เนื่องจากหากระบบเครือข่ายไม่สามารถตอบสนองต่อความต้องการใช้งานได้ในเวลาที่ต้องการ ระบบบัญชาการและควบคุมก็จะไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ก่อให้เกิดความไม่สัมฤทธิ์ผลในการปฏิบัติในองค์รวม ดังนั้น จึงจำเป็นที่จะต้องหาแนวทางปฏิบัติเพื่อป้องกันภัยอันเกิดจากการทำสงครามไซเบอร์

จากการที่เทคโนโลยีสารสนเทศพัฒนาขึ้นอย่างรวดเร็ว ในปี 52 กองทัพอากาศ ได้จัดตั้งกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) เพื่อรับผิดชอบงานดังกล่าว มีหัวหน้าหน่วยในอัตรา พลอากาศตรี ซึ่งมีหน่วยขึ้นตรง คือ กองนโยบายและแผน กองเทคโนโลยีสารสนเทศ กองสื่อสารอิเล็กทรอนิกส์ กองสารสนเทศและการสื่อสารทหารอากาศ

ต่อมาในปี 57 การดำเนินการด้านไซเบอร์มีความรุนแรงมากขึ้น จึงมีการปรับ ทสส.ทอ. ให้มีความรับผิดชอบมากขึ้น และให้หัวหน้าหน่วยเป็นอัตรา พลอากาศโท โดยการจัดโครงสร้าง

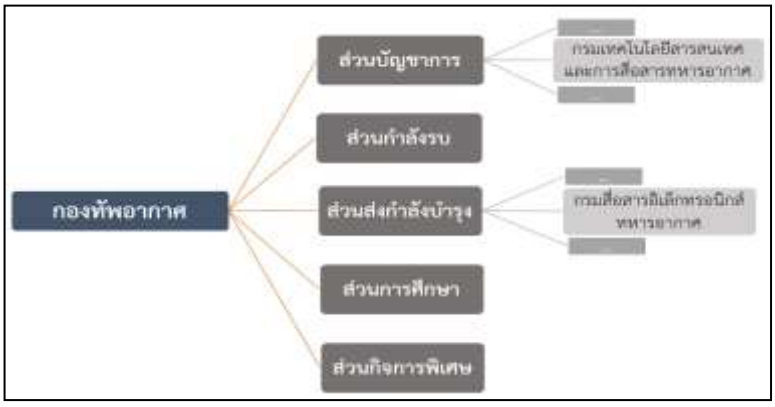
กองทัพอากาศ ตามพระราชกฤษฎีกาแบ่งส่วนราชการและกำหนดหน้าที่ส่วนราชการกองทัพอากาศ พ.ศ.2557 ดังนี้

แผนภาพที่ 3-1 โครงสร้างกองทัพอากาศ

ที่มา : เว็บไซต์กองทัพอากาศ (www.rtaf.mi.th)

ภายใต้โครงสร้างกองทัพอากาศ กำหนดให้ ทสส.ทอ.เป็นหน่วยงานฝ่ายสนาธิการรับผิดชอบเกี่ยวกับงานเชิงนโยบายด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการปฏิบัติการไซเบอร์และการปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ มี กองสงครามไซเบอร์ เป็นหน่วยงานรับผิดชอบด้านสงครามไซเบอร์ โดยมีหน่วยงานที่เกี่ยวข้อง คือ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) เป็นหน่วยงานสนับสนุนและซ่อมบำรุงที่รับผิดชอบเกี่ยวกับงานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบโทรคมนาคม และการติดต่อสื่อสารเชิงปฏิบัติ มีศูนย์คอมพิวเตอร์และกองสื่อสารโทรคมนาคม เป็นหน่วยงานรับผิดชอบ รวมถึงมีหน่วยขึ้นตรงของกองทัพอากาศที่จะต้องรับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีใช้งานด้วย

แผนภาพที่ 3-2 หน่วยรับผิดชอบและหน่วยเกี่ยวข้องด้านไซเบอร์



1. กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.)

มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนา และดำเนินการด้านระบบบัญชาการและควบคุม ระบบเครือข่าย เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ ปฏิบัติการสงครามอิเล็กทรอนิกส์ และปฏิบัติการสงครามไซเบอร์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศสงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์

การจัดหน่วย ประกอบด้วย ส่วนบังคับบัญชา แผนกธุรการ สำนักนโยบายและแผน และสำนักระบบบัญชาการและควบคุม

สำนักนโยบายและแผน ประกอบด้วย กองนโยบายและแผน กองสื่อสารอิเล็กทรอนิกส์ และกองเทคโนโลยีสารสนเทศ

สำนักระบบบัญชาการและควบคุม ประกอบด้วย กองระบบบัญชาการและควบคุม กองสงครามอิเล็กทรอนิกส์ และกองสงครามไซเบอร์ ประกอบด้วย แผนกสงครามไซเบอร์ แผนกกรรมวิธีข้อมูลสงครามไซเบอร์ แผนกรักษาความปลอดภัยระบบสารสนเทศ แผนกปฏิบัติการสงครามไซเบอร์ และแผนกประเมินผลการสงครามไซเบอร์ ปัจจุบันกองสงครามไซเบอร์ ได้รับอัตราอนุมัติกำลังพล จำนวน 59 อัตรา บรรจุจริง จำนวน 25 คน

มีขอบเขตความรับผิดชอบที่สำคัญ คือ การพิจารณา เสนอนโยบาย งานฝ่ายเสนาธิการด้านเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ ในขอบเขตเกี่ยวกับ ระบบบัญชาการและควบคุม ระบบเครือข่าย คลื่นความถี่ให้ครอบคลุมการปฏิบัติภารกิจของกองทัพอากาศทั้งภายในและภายนอกประเทศ เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ การสงครามอิเล็กทรอนิกส์และการสงครามไซเบอร์ บริหารจัดการในฐานะหัวหน้าสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์ เกี่ยวกับ การจัดการความรู้ การบริหารการฝึกและศึกษา การบริหารกำลังพลจำพวกทหารสารสนเทศและสงครามอิเล็กทรอนิกส์

แผนภาพที่ 3-3 การจัดหน่วยกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

2. กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.)

มีหน้าที่ วางแผนการปฏิบัติ อำนวยการ ประสานงาน ติดตาม กำกับการ พัฒนา และดำเนินการเกี่ยวกับกิจการสื่อสารอิเล็กทรอนิกส์ กิจการกระจายเสียงและกิจการโทรทัศน์ มาตรวิทยาและการพัสดุสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรา กิจการในสายวิทยาการด้านสื่อสารอิเล็กทรอนิกส์ มีหน้าที่ที่สำคัญ คือ ดำเนินกิจการสื่อสารอิเล็กทรอนิกส์ให้พร้อมในขอบเขตเกี่ยวกับการเตรียมกำลังตามยุทธศาสตร์กองทัพอากาศ แผนการใช้กำลังทางอากาศ การจัดทำแผนงาน โครงการ งบประมาณ ด้านสื่อสารอิเล็กทรอนิกส์ การกำหนดมาตรฐานข้อมูลคุณลักษณะเฉพาะ กรรมวิธีการปฏิบัติของพัสดุอุปกรณ์สายสื่อสารอิเล็กทรอนิกส์ การปฏิบัติการสื่อสารอิเล็กทรอนิกส์ เครือข่ายสื่อสารและสารสนเทศ โทรคมนาคม และสนับสนุนการปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ การส่งกำลังและการพัสดุสื่อสารอิเล็กทรอนิกส์ คอมพิวเตอร์ และการภาพการพัฒนากิจการสื่อสารอิเล็กทรอนิกส์ รวมทั้งประสานการซ่อมบำรุงและให้คำแนะนำทางเทคนิค

แผนภาพที่ 3-4 การจัดหน่วยกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.)

ที่มา : เว็บไซต์กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (www.comm.rtaf.mi.th)

สอ.ทอ.มีหน่วยรับผิดชอบที่เกี่ยวข้อง คือ ศูนย์คอมพิวเตอร์ มีหน้าที่ดำเนินการและปฏิบัติการเกี่ยวกับกิจการเทคโนโลยีสารสนเทศ การกรรมวิธีข้อมูล การสื่อสารข้อมูล การสงครามสารสนเทศ และการซ่อม สร้าง ผลิต ประกอบติดตั้ง ดัดแปลงบริภัณฑ์คอมพิวเตอร์ บริภัณฑ์เครือข่ายสื่อสารข้อมูลของกองทัพอากาศ ตลอดจนการควบคุมสถานภาพเครือข่ายสื่อสารข้อมูลและระบบสารสนเทศ ซึ่งศูนย์คอมพิวเตอร์นี้มีงานหลักด้านไซเบอร์ คือ การควบคุม กำกับดูแลการบริการ ระบบอุปกรณ์คอมพิวเตอร์และเครือข่ายสื่อสารข้อมูลของกองทัพอากาศ โดยจะต้องเฝ้าตรวจและเฝ้าระวังตรวจจับสิ่งแปลกปลอมเพื่อเฝ้าระวังโปรแกรมหวังร้ายที่จะเข้ามาในระบบของกองทัพอากาศ

และหาทางช่วยเหลือและแก้ไขเมื่อถูกโจมตีทางไซเบอร์จากผู้ไม่หวังดี ปัจจุบันศูนย์คอมพิวเตอร์ ได้รับอัตราอนุมัติกำลังพล จำนวน 215 อัตรา บรรจุจริง จำนวน 80 คน

3. หน่วยขึ้นตรงกองทัพอากาศ

มีนายเทคโนโลยีสารสนเทศเป็นผู้กำกับดูแลการใช้งานระบบสานสนเทศและการสื่อสารภายในหน่วย ปัจจุบันฝ่ายเทคโนโลยีสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศ ได้รับอัตราอนุมัติกำลังพล จำนวน 8 อัตรา บรรจุจริง จำนวน 4 คน

4. หน่วยที่กองทัพอากาศประสานและปฏิบัติงานร่วม

4.1 ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม เป็นหน่วยขึ้นตรง กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหมมีหน่วยในความรับผิดชอบ คือ กองแผนไซเบอร์ และกองปฏิบัติการไซเบอร์

4.2 กองบัญชาการกองทัพไทย ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย (เพื่อพลาง) เป็นหน่วยขึ้นตรงกับ กองบัญชาการกองทัพไทย มีหน่วยงานในความรับผิดชอบ คือ กองยุทธการและการข่าว กองปฏิบัติการ กองวิทยาการ กองสนับสนุน และกองธุรการ

4.3 ศูนย์ไซเบอร์ กองทัพบก เป็นหน่วยขึ้นตรงกองทัพบก มีหน่วยในความรับผิดชอบ คือ กองรักษาความมั่นคงปลอดภัยไซเบอร์ กองปฏิบัติการไซเบอร์ กองสนับสนุนการปฏิบัติการข่าวสาร และกองธุรการ

4.4 กองสงครามไซเบอร์ สำนักนโยบายและแผน กรมการสื่อสารและเทคโนโลยีสารสนเทศ กองทัพเรือ เป็นหน่วยขึ้นตรงกับสำนักนโยบายและแผน กรมการสื่อสารและเทคโนโลยีสารสนเทศ กองทัพเรือ มีหน่วยขึ้นตรง คือ แผนกวิเคราะห์และประเมินผล แผนกปฏิบัติการ และแผนกรักษาความมั่นคงปลอดภัย

4.5 หน่วยงานพิเศษอื่น ๆ ที่ประสานงานร่วมในการดำเนินการด้านสงครามไซเบอร์ มีหน่วยงานภายนอกที่กองทัพอากาศติดต่อและประสานการปฏิบัติงานร่วม ด้านไซเบอร์ ดังนี้ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสถาบันเทคโนโลยีป้องกันประเทศ (องค์กรมหาชน) (สทป.)

ปัจจัยที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์

1. วงรอบการปฏิบัติด้านไซเบอร์

หลักการทั่วไปด้านไซเบอร์ ประกอบด้วย วงรอบการปฏิบัติทางไซเบอร์และปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์ โดยวงรอบการปฏิบัติทางไซเบอร์ แบ่งออกเป็น วงรอบการป้องกันทางไซเบอร์ และวงรอบการโจมตีทางไซเบอร์ ดังนี้

1.1 วงรอบการป้องกันทางไซเบอร์ (Cyber Defense) วงรอบการป้องกันทางไซเบอร์ แบ่งการปฏิบัติออกเป็น 4 ขั้นตอน

1.1.1 การป้องกัน (Protect) หมายถึง การระวังป้องกันไม่ให้เกิดความเสียหายใด ๆ ขึ้นกับระบบสารสนเทศที่ใช้งานในส่วนที่รับผิดชอบ โดยถือปฏิบัติตามแนวทางหรือมาตรการต่าง ๆ ในการป้องกันระบบสารสนเทศ หรือปฏิบัติตาม กฎ ระเบียบ และข้อปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ ที่องค์กรกำหนด

1.1.2 การตรวจจับ (Detect) หมายถึง การเฝ้าระวังการถูกโจมตีหรือการถูกคุกคามทางไซเบอร์ ด้วยการสังเกตสิ่งผิดปกติใด ๆ ที่เกิดขึ้นในการใช้งานระบบสารสนเทศ หรือการใช้ซอฟต์แวร์ตลอดจนระบบตรวจจับอื่น ๆ ที่ช่วยในการตรวจจับสิ่งผิดปกติขณะที่ใช้งานและไม่ได้ใช้งานระบบ พร้อมทั้งรายงานเหตุการณ์ความผิดปกติที่ตรวจพบให้กับผู้รับผิดชอบที่เกี่ยวข้อง เพื่อให้สามารถตอบสนองและแก้ไขได้ทันท่วงที

1.1.3 การตอบสนอง (React) หมายถึง การปฏิบัติเพื่อแก้ไขปัญหาและระงับเหตุการณ์การล่วงละเมิดการรักษาความปลอดภัยทางไซเบอร์ที่เกิดขึ้นโดยทันที ตามมาตรการการปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ขยายผลกระทบต่อไปยังระบบสารสนเทศอื่นที่เกี่ยวข้อง

1.1.4 การฟื้นฟู (Recover) หมายถึง การปฏิบัติเพื่อฟื้นฟูระบบสารสนเทศที่ได้รับผลกระทบทั้งหมด ให้กลับคืนสู่สภาพปกติที่พร้อมใช้งานโดยเร็วที่สุด พร้อมทำการปรับปรุงกระบวนการป้องกันให้มีประสิทธิผลในการรักษาความปลอดภัยยิ่งขึ้น

1.2 วงรอบการโจมตีทางไซเบอร์ (Cyber Attack) วงรอบการโจมตีทางไซเบอร์แบ่งการปฏิบัติออกเป็น 5 ขั้นตอน ดังนี้

1.2.1 รวบรวมข้อมูลเป้าหมาย (Information Gathering) หมายถึง การรวบรวมข้อมูลเป้าหมายเกี่ยวกับโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์ และเครื่องมือที่ใช้ วิธีการใช้งาน และข้อมูลต่าง ๆ ของบุคลากร ที่อาจเป็นประโยชน์ในการโจมตี โดยทำการสืบค้นข้อมูลจากกระบวนการทางเทคนิคทุกวิธีที่สามารถปฏิบัติได้ รวมถึงการใช้วิธีวิศวกรรมสังคม (Social Engineering) ด้วย

1.2.2 ตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification) หมายถึง การตรวจสอบหาช่องโหว่หรือการวิเคราะห์ช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ เพื่อการโจมตีจากข้อมูลเป้าหมายที่รวบรวมได้

1.2.3 ปฏิบัติการโจมตี (Attack) หมายถึง การใช้อาวุธทางด้านไซเบอร์ทุกรูปแบบในการเข้าโจมตีระบบเป้าหมาย เพื่อให้เกิดผลตามที่คาดหวัง

1.2.4 เปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) หมายถึง การเปิดช่องโหว่ทิ้งไว้ในระบบที่เข้าโจมตี เพื่อใช้เป็นช่องทางสำหรับการเข้าปฏิบัติการครั้งต่อไป ด้วยวิธีการฝังทางลับ (Backdoor) ไว้ในระบบที่เป็นเป้าหมาย

1.2.5 ลบร่องรอยการโจมตี (Covering Tracks) หมายถึง การลบร่องรอยของการโจมตี หรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบ เพื่อไม่ให้สามารถสืบย้อนกลับมาถึงผู้โจมตีได้

2. ปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์

ตารางที่ 3-1 ปัจจัยที่มีผลกระทบต่อการปฏิบัติการไซเบอร์

ระบบสารสนเทศ				
Procedures	Peopleware	Technology		
		Data	Hardware	Software
นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง	บุคลากร	อุปกรณ์ เครื่องมือ และเทคโนโลยี		

การปฏิบัติการไซเบอร์ เป็นการปฏิบัติต่อระบบสารสนเทศภายใต้มิติของไซเบอร์ ซึ่งระบบสารสนเทศประกอบด้วย 3 องค์ประกอบ ได้แก่ ขั้นตอนการปฏิบัติ (Procedures) บุคลากร (Peopleware) และ เทคโนโลยี (Technology) (รวมถึงข้อมูล (Data) ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software)) ซึ่งมีปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์ ดังนี้

2.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง การปฏิบัติการไซเบอร์จะมีประสิทธิภาพได้ก็ต้องอาศัยรูปแบบ ขั้นตอน และกระบวนการปฏิบัติที่ดี ต้องมีการตั้งนโยบายและวางแผนการปฏิบัติต่าง ๆ มีการจัดลำดับความสำคัญของเป้าหมาย การกำหนดระยะเวลาการปฏิบัติ กำหนดผู้รับผิดชอบ งบประมาณที่จะใช้ มีการตรวจสอบและประเมินผลการปฏิบัติ ซึ่งสามารถนำผลการประเมินมาปรับปรุงกระบวนการปฏิบัติให้ดียิ่งขึ้นตามวงรอบแห่งการพัฒนาปรับปรุงคุณภาพแบบ PDCA (Plan Do Check และ Act) ซึ่งกองทัพอากาศมีการดำเนินการ ดังนี้

2.1.1 จัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.๒๕๕๒ โดยอ้างอิงจากมาตรฐาน ISO 27001 (2005) ซึ่งระเบียบนี้ให้ใช้บังคับข้าราชการ พนักงานราชการ ลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ มีความมุ่งหมายเพื่อกำหนดหลักการและมาตรการการป้องกันระบบสารสนเทศ รวมถึงให้แต่งตั้งคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศและนายทหารรักษาความปลอดภัยของหน่วยเพื่อดำเนินการอีกด้วย และกำหนดให้กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศตรวจสอบระบบสารสนเทศ

2.1.2 จัดทำนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ โดยมีวัตถุประสงค์เพื่อให้การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ของกองทัพอากาศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย รวมทั้งสอดคล้องกับกฎหมาย และกฎระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ด้วยการสร้างความมั่นคงปลอดภัยด้านบริหาร การสร้างความมั่นคงปลอดภัยด้านบุคลากร การสร้างความมั่นคงปลอดภัยด้านควบคุมการเข้าถึง การสร้างความมั่นคงปลอดภัยทางกายภาพ การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน และการตรวจสอบและการประเมินผลการปฏิบัติตามนโยบายและข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดแบบรายการ

ประเมินหน่วยงานด้านความมั่นคงปลอดภัยระบบสารสนเทศด้วย ซึ่ง ทสส.ทอ.ได้จัดเจ้าหน้าที่ผู้ตรวจสอบออกไปตรวจสอบหน่วยตามวงรอบที่กำหนด

2.1.3 โครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ มีวัตถุประสงค์ของโครงการเพื่อพัฒนาขีดความสามารถด้านสงครามไซเบอร์ในการป้องปรามการรุกรานจากภัยคุกคามทางไซเบอร์และการสังเกตการณ์ห้วงอวกาศของ ทอ. โดยกำหนดแผนงานในการจัดหาระบบป้องกันภัยทางไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแผนการฝึก ศึกษา อบรมของบุคลากรผู้ปฏิบัติงานด้านสงครามไซเบอร์

2.1.4 แผนแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศ พ.ศ.2560 - 2564 กำหนดให้เป็นแผนยุทธศาสตร์ในการพัฒนาระบบสงครามไซเบอร์ของ ทอ. มีวัตถุประสงค์เพื่อใช้เป็นกรอบและแนวทางในการพัฒนาระบบการปฏิบัติงานด้านสงครามไซเบอร์ของ ทอ. ประกอบด้วยด้านบุคลากร ด้านกระบวนการบริหารจัดการ และด้านเทคโนโลยีที่เกี่ยวข้องในการปฏิบัติการสงครามไซเบอร์ และเพื่อให้ผู้บริหารระดับสูงและผู้มีส่วนเกี่ยวข้อง ได้ทราบถึงเป้าหมายของโครงการ แผนงานและงบประมาณสำหรับการพัฒนาระบบการปฏิบัติงานด้านสงครามไซเบอร์ของ ทอ.

2.1.5 จัดการแข่งขัน Cyber Operations Contest โดยมีวัตถุประสงค์ให้ข้าราชการ ทอ.ในทุกระดับได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญในการดำรงขีดความสามารถของการรักษาความปลอดภัยในการใช้งานเครือข่าย และป้องกันการถูกโจมตีด้วยวิธีการต่าง ๆ ในยุคสงครามไซเบอร์ รวมถึงเพื่อสรรหาบุคลากรปฏิบัติงานด้านไซเบอร์

2.1.6 ประชุมประชาคมไซเบอร์ กองบัญชาการกองทัพไทย มีวัตถุประสงค์เพื่อให้ผู้ปฏิบัติงานในมิติไซเบอร์สามารถแลกเปลี่ยนองค์ความรู้ด้านไซเบอร์ร่วมกันอย่างสม่ำเสมอ อีกทั้งเพื่อการพัฒนาให้การปฏิบัติการร่วมในมิติไซเบอร์ของ ทท. เป็นรูปธรรมและเกิดความเข้าใจในกรอบแนวทางการปฏิบัติที่เป็นไปในทิศทางเดียวกัน

2.1.7 จัดทำแนวความคิดการปฏิบัติการไซเบอร์ของกองทัพอากาศ (อยู่ระหว่างดำเนินการ) มีวัตถุประสงค์ คือ เพื่อนำยุทธศาสตร์ของกองทัพอากาศไปปฏิบัติ เพื่อเป็นกรอบแนวทางในการจัดทำแผนงานที่เกี่ยวข้อง เพื่อใช้เป็นแนวทางในการพัฒนาสงครามไซเบอร์ และเพื่อสร้างความเข้าใจด้านแนวคิดในการดำเนินการให้บุคลากรกองทัพอากาศ

2.1.8 จัดตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของกองทัพอากาศ (อยู่ระหว่างดำเนินการ) จะกำหนดให้มีหน้าที่จัดการสอบสวนเมื่อมีเหตุการณ์ละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ จัดทำแผน Incident Response เผชิญเหตุ กำหนดมาตรการในการป้องกัน การรับมือและ ประสานเพื่อแก้ไขปัญหาภัยคุกคาม (Incident Coordination) การวิเคราะห์ปัญหาภัยคุกคาม (Threat Analysis) การพัฒนาบุคลากร (Security and Awareness Development) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics) ประสานงานหน่วยงานภายในและภายนอกกองทัพอากาศ

2.1.9 จัดให้มีการประชุมร่วมกับหน่วยงานภายนอกตามระยะเวลาที่กำหนดไว้ รวมถึงมีการประชุมร่วมกับต่างชาติในบางโอกาส

2.2 ปัจจัยด้านบุคลากร

ในการปฏิบัติการไซเบอร์บุคลากรถือว่าเป็นปัจจัยที่สำคัญ เพราะในทุก ๆ กระบวนการในการปฏิบัติการไซเบอร์จำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการปฏิบัติงานนั้น ๆ ทั้งการปฏิบัติการไซเบอร์เชิงรับ ที่ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว รวมทั้งสามารถกู้คืนระบบที่เสียหายให้กลับมาปฏิบัติงานได้โดยไม่กระทบต่อกระบวนการทำงานอื่น ๆ และการปฏิบัติการไซเบอร์เชิงป้องปรามที่ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการค้นหาจุดอ่อน ช่องโหว่ของระบบเป้าหมาย ซึ่งบุคลากรจะมีความสามารถในการปฏิบัติการไซเบอร์ได้ ก็ต้องได้รับการสนับสนุนและส่งเสริมในการพัฒนาองค์ความรู้ รวมทั้งการมีแรงจูงใจที่เหมาะสมเพื่อให้บุคลากรพัฒนาตนเองอยู่เสมอ เนื่องจากองค์ความรู้ด้านไซเบอร์มีการเปลี่ยนแปลงที่รวดเร็ว ซึ่งกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศดำเนินการตั้งแต่ พ.ศ.2557 ดังนี้

2.2.1 จัดให้มีหลักสูตรการฝึกศึกษาอบรม ในลักษณะของหลักสูตรการบรรยาย อบรม และปฏิบัติ ดังนี้

2.2.1.1 หลักสูตรสงครามไซเบอร์ สำหรับหลักสูตรจ่าอากาศ โรงเรียนจ่าอากาศ กรมยุทธศึกษาทหารอากาศ เป็นหลักสูตรสำหรับผู้จบการศึกษาจากโรงเรียนจ่าอากาศฯ และได้รับการบรรจุแต่งตั้งเข้ามาทำงานในกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ซึ่งดำเนินการมาแล้วจำนวน 2 รุ่น รวมจำนวน 18 คน

2.2.1.2 หลักสูตรสงครามไซเบอร์ หลักสูตรเสนาธิการทหารอากาศ โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ

2.2.1.3 หลักสูตรเจ้าหน้าที่เทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ หลักสูตรนายทหารเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อให้ผู้ที่เข้ามาบรรจุในตำแหน่งใหม่ รับทราบพื้นฐานงานด้านเทคโนโลยีสารสนเทศ งานสงครามอิเล็กทรอนิกส์ และงานด้านไซเบอร์ ดำเนินการมาแล้ว หลักสูตรละ 1 รุ่น มีผู้ผ่านหลักสูตรนายทหารเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ จำนวน 25 คน และหลักสูตรเจ้าหน้าที่เทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ จำนวน 33 คน

2.2.1.4 หลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ดำเนินการมาแล้ว 2 รุ่น จำนวน 44 คน

2.2.1.5 การเสริมสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ สำหรับการบรรยายพิเศษที่สถาบันการศึกษา/หน่วยงานต่าง ๆ

2.2.1.6 การอบรมเกี่ยวกับการประเมินและตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ให้กับผู้ปฏิบัติงานด้านรักษาความปลอดภัยระบบสารสนเทศ และจัดส่งผู้ตรวจสอบระบบสารสนเทศไปตรวจสอบการปฏิบัติงานภายในหน่วยด้วย

2.2.1.7 การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ เพื่อเสริมสร้างความตระหนักด้านความปลอดภัย ส่งให้เมล์อิเล็กทรอนิกส์ ของข้าราชการ พนักงานราชการ และลูกจ้างกองทัพอากาศ

2.2.1.8 ส่งบุคลากรเข้ารับการฝึกอบรม กับ บริษัทเอกชนและหน่วยงานภายนอก ด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์และสารสนเทศ

2.2.1.9 ส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานของรัฐ ทั้งในระดับปริญาตรีและโท ด้านเทคโนโลยีสารสนเทศ

2.2.1.10 จัดการฝึกอบรมการ ในการเลื่อนระดับความชำนาญให้กับข้าราชการชั้นประทวนที่มีคุณสมบัติครบเพื่อพิจารณา เลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น จำนวน 11 คน

2.2.2 การพิจารณาในการดำรงตำแหน่ง พิจารณาตามคุณสมบัติ ขั้นตอนระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ ซึ่งกำหนดให้ผู้ปฏิบัติงานด้านนี้มีเลขหมายความชำนาญหลัก และเลขหมายความชำนาญรอง กำหนดเป็นเลขหมาย 27 มีองค์ประกอบเพิ่มคือการกำหนดอายุการครองยศ ผ่านการฝึก ศึกษา และอบรมตามขั้นตอนของสายวิทยาการเทคโนโลยีสารสนเทศและการสื่อสาร สามารถเข้าตำแหน่งตามที่เลขหมายความชำนาญที่กำหนดไว้โดยจะเข้าตำแหน่งตามโครงสร้างที่ได้รับอนุมัติ

2.2.3 การฝึกอบรมกรณีที่มีการจัดหาระบบอุปกรณ์ใหม่ตามที่กองทัพอากาศจัดหาไว้ใช้งานตามสัญญาที่กำหนดไว้ และมีการจัดอบรมการใช้งานอุปกรณ์ที่มีใช้งานอยู่ให้กับบุคลากรที่บรรจุเข้ามาในหน่วย

2.3 ปัจจัยด้านเทคโนโลยี

เนื่องจากการปฏิบัติการไซเบอร์เป็นปฏิบัติการต่อระบบสารสนเทศ ที่เกิดจากเทคโนโลยี รวมทั้งปริมาณการใช้งานระบบสารสนเทศที่สูงขึ้นมาก ในปัจจุบันการอาศัยเพียงความรู้ความสามารถของบุคลากรไม่สามารถที่จะปฏิบัติงานได้อย่างมีประสิทธิภาพ จึงต้องอาศัยอุปกรณ์เครื่องมือ และเทคโนโลยีที่ทันสมัยและมีประสิทธิภาพที่ดีมาช่วยสนับสนุนในการปฏิบัติกองทัพอากาศได้ดำเนินการจัดหา ระบบเทคโนโลยีทั้งเชิงรุกและเชิงรับ ดังนี้

2.3.1 ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ซึ่งรับผิดชอบระบบอุปกรณ์ระบบสารสนเทศเป็นส่วนรวม ระบบการบริหารจัดการภายในหน่วย มีการดำเนินการตามขั้นตอนการบริหารความมั่นคงปลอดภัยสารสนเทศ 1.การวางแผน (Plan) (ขอบเขต นโยบาย ความเสี่ยง) 2.การลงมือทำ (Do) 3.การตรวจสอบ (Check) 4.การปรับปรุงแก้ไข (Act) 5.ข้อกำหนดทางด้านเอกสาร การควบคุมเอกสารและบันทึก 6.ความรับผิดชอบของฝ่ายบริหาร 7.การจัดสรรทรัพยากร 8.การฝึกอบรม การรับรู้และความสามารถ 9.การตรวจประเมินภายใน (Internal audit) 10.การทบทวนโดยฝ่ายบริหาร 11.การปรับปรุงอย่างต่อเนื่อง (Continual improvement) 12.การปฏิบัติการแก้ไข (Corrective action) 13.การปฏิบัติการป้องกัน (Preventive action) และ 14.รายการควบคุม (Controls) จนกระทั่งได้รับ มาตรฐาน ISO 27001:2013 โดยมีระบบที่จำเป็น ดังนี้

2.3.1.1 ระบบบริหารจัดการเครือข่าย (Network Management System) พร้อมศูนย์ปฏิบัติการเครือข่าย (Network Operations Center: NOC) ซึ่งใช้ในการบริหารจัดการเครือข่ายคอมพิวเตอร์และจัดการทรัพยากรในเครือข่ายสารสนเทศของกองทัพอากาศ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด โดยเฉพาะเครือข่ายระบบสารสนเทศเพื่อการรบ (CIS) โดยต้องทำการเก็บรวบรวมและวิเคราะห์ข้อมูลเพื่อนำมาใช้ตัดสินใจต่อการบริหารจัดการเครือข่ายได้

และจะต้องมีขีดความสามารถในการทำงานของระบบทั้ง 5 ส่วน คือ การจัดการระบบความผิดพลาดของเครือข่าย การจัดการคุณสมบัติของอุปกรณ์ของเครือข่าย การจัดการรูปแบบของเครือข่าย การจัดการระบบบัญชีของเครือข่าย และการจัดการระบบความปลอดภัยของเครือข่าย

2.3.1.2 ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (Intrusion Detection System: IDS/Intrusion Prevention System: IPS) ทั้งแบบทำงานในเครือข่าย (Network-based) และแบบทำงานเฉพาะเครื่อง (Host-based) พร้อมห้องปฏิบัติการ ซึ่งใช้ในการตรวจสอบข้อมูลที่ส่งผ่านระบบเครือข่าย ด้วยการวิเคราะห์รูปแบบและพฤติกรรมของแพ็คเก็ตข้อมูล เพื่อค้นหาสิ่งที่ผิดปกติประกอบการวิเคราะห์เหตุการณ์บุกรุกเครือข่าย โดยจะต้องประกอบไปด้วย ๒ ส่วน ดังนี้ ระบบตรวจจับการบุกรุก (IDS) และ ระบบป้องกันการบุกรุก (IPS)

2.3.1.3 ระบบป้องกันไวรัสและมัลแวร์ (Anti-Virus/Malware System) ซึ่งใช้ป้องกันไวรัสและมัลแวร์ประเภทต่าง ๆ โดยทำหน้าที่ในการคอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์ต่าง ๆ ติดตั้งใช้งานกับเครื่องคอมพิวเตอร์ในระบบสารสนเทศของกองทัพอากาศ

2.3.1.4 ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention System: DLP) ซึ่งใช้ป้องกันการสูญหายของข้อมูลที่มีความสำคัญอันเกิดจากการส่งผ่านข้อมูลผ่านเครือข่าย ด้วยการจำแนกประเภทข้อมูลตามชั้นความลับและเฝ้าระวังการใช้หรือการเคลื่อนย้ายข้อมูลสำคัญเหล่านั้นให้ดำเนินไปตามข้อกำหนดหรือนโยบาย

2.3.1.5 ระบบบริหารจัดการอัตลักษณ์ (Identity Management System) ซึ่งใช้บริหารจัดการตัวตนของบุคลากร เช่น การสร้างและลบข้อมูลบัญชีผู้ใช้ และระบบควบคุมสิทธิการใช้ข้อมูลสารสนเทศ (Digital Right Management: DRM) ซึ่งใช้บริหารจัดการสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน

2.3.1.6 ระบบรักษาความปลอดภัยทางด้านกายภาพ (Physical Security System) ซึ่งใช้รักษาความปลอดภัยของบุคคล สถานที่ อุปกรณ์เครื่องมือ และทรัพยากรต่าง ๆ ในระบบเครือข่าย เช่น ระบบกล้องวงจรปิด ระบบประตูหมุนกั้น และระบบการควบคุมประตูเข้าออก (Door Access Control) เป็นต้น ติดตั้งใช้งานที่หน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศที่สำคัญของกองทัพอากาศ มีกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นผู้ดูแลรับผิดชอบ

2.3.1.7 ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรองกรณีเกิดภัยพิบัติ (Data Center and Disaster Recovery Site) พร้อมอาคารและสิ่งอำนวยความสะดวก ซึ่งใช้ในการจัดเก็บและบริหารจัดการข้อมูล พร้อมทั้งเป็นศูนย์สำรองข้อมูลสำหรับการกู้คืนข้อมูลสำรองในกรณีเกิดภัยพิบัติกับศูนย์ข้อมูลหลัก

2.3.1.8 ระบบจำลองการโจมตีในรูปแบบการระดมโจมตีเพื่อให้เครื่องแม่ข่ายปฏิเสธการให้บริการ (Distributed Denial of Service: DDoS) เพื่อทดสอบความมั่นคงปลอดภัยของเครือข่าย (DDoS Attack Simulation System) ซึ่งใช้ในการทดสอบการโจมตีและการรับมือกับการโจมตี และระบบป้องกันการโจมตีแบบ

2.3.1.9 ระบบบริหารแพทช์ (Patch Management System) ที่ใช้ในการปรับปรุงส่วนซอฟต์แวร์ต่าง ๆ ของระบบคอมพิวเตอร์และเครือข่ายให้มีความทันสมัยเพื่อลดช่องโหว่ในการถูกโจมตี

2.3.1.10 ระบบป้องกันภัยคุกคามแบบขั้นสูงและต่อเนื่อง (Advanced Persistent Threats) ที่ใช้ในการป้องกันภัยคุกคามขั้นสูงและต่อเนื่อง ที่มาจากทางการเชื่อมต่อทางเว็บไซต์และจดหมายอิเล็กทรอนิกส์ เป็นต้น เพื่อให้สามารถป้องกันการโจมตีจากนักเจาะระบบขั้นสูงหรือผู้ไม่ประสงค์ดีแบบดำเนินการโดยรัฐหรือได้รับการสนับสนุนจากรัฐ

2.3.1.11 ระบบรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์ (Secured E-Mail Gateway System) ซึ่งใช้ในการรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์

2.3.1.12 ระบบป้องกันภัยคุกคามสำหรับระบบเครื่องแม่ข่ายแบบคลาวด์ (Cloud Server Security System) ที่ใช้ในการรักษาความปลอดภัยของระบบเครื่องแม่ข่ายเสมือน

2.3.1.13 ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านการรักษาความปลอดภัยเครือข่าย (Security Information/Event Management: SIEM) พร้อมห้องปฏิบัติการ ซึ่งใช้รวบรวมและจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) พร้อมทั้งวิเคราะห์หาความสัมพันธ์ และบริหารจัดการกับภัยคุกคาม (Incident Management) ได้อย่างมีประสิทธิภาพ

2.3.2 กองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ จัดหาอุปกรณ์เพิ่มเติมเพื่อเสริมประสิทธิภาพ ดังนี้

2.3.2.1 ระบบเข้ารหัสข้อมูล (Data Encryption System) ซึ่งใช้เข้ารหัสข้อมูลสำคัญหรือข้อมูลที่มีชั้นความลับทั้งในระบบสารสนเทศเพื่อการยุทธและระบบสารสนเทศเพื่อการสนับสนุน ที่ให้ความปลอดภัยสูงทั้งด้านความปลอดภัย (Confidentiality) และความครบถ้วนถูกต้อง (Integrity) ของข้อมูล ตามมาตรฐานสากล โดยประกอบ แบบกุญแจสมมาตร (Symmetric Key) และแบบกุญแจอสมมาตร (Asymmetric Key) พร้อมจัดให้มีโครงสร้างสถาปัตยกรรมกุญแจสาธารณะ (Public Key Infrastructure: PKI) ในส่วนของกองทัพอากาศ

2.3.2.2 ระบบพิสูจน์ตัวตนของผู้ใช้งานแบบหลายองค์ประกอบ (Multi-factor User Authentication) ซึ่งใช้ในการพิสูจน์เพื่อยืนยันตัวตนของผู้ใช้งานในการเข้าใช้งานระบบสารสนเทศ โดยเฉพาะระบบสารสนเทศเพื่อการยุทธที่ติดตั้งในอาคารปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations Center: NCOC) ด้วยการใช้ปัจจัยพิสูจน์ยืนยันอื่นเพิ่มเติมจากรหัสผ่าน (Password) ปกติ เช่น การใช้อุปกรณ์โทเค็น (Token) และการใช้ปัจจัยทางกายภาพของบุคคล (Biometric) ประกอบในการพิสูจน์ยืนยันตัวตนผู้ใช้งาน เป็นต้น

2.3.2.3 ระบบจำลองยุทธทางไซเบอร์ (Cyber Range) พร้อมห้องฝึกปฏิบัติการและห้องฝึกอบรม ซึ่งใช้ในการฝึกอบรมการปฏิบัติการทางไซเบอร์ ที่สามารถจำลองสถานการณ์ของระบบเครือข่ายคอมพิวเตอร์ภายใต้สภาวะแวดล้อมภัยคุกคามในปัจจุบันได้ตามความต้องการ และต้องสามารถรองรับต่อการจำลองสถานการณ์ภัยคุกคามจริงแบบอื่นที่อาจเกิดขึ้นในอนาคตได้ด้วย โดยสามารถใช้งานได้จากการเชื่อมต่อโดยตรงและจากระยะไกล (Remote Access) ติดตั้งใช้งานที่กองสงครามไซเบอร์ฯ มีกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เป็นผู้ดูแลรับผิดชอบ

2.3.2.4 ระบบเครือข่ายเพื่อการซ่อนพราง (Anonymity Network) ซึ่งใช้สำหรับปกปิดร่องรอยของการใช้งานบนอินเทอร์เน็ต เพื่อป้องกันไม่ให้ผู้อื่นสามารถย้อนรอยเส้นทางกลับมายังผู้ปฏิบัติได้โดยง่าย

2.3.2.5 ระบบบริหารจัดการช่องโหว่ในระบบคอมพิวเตอร์และเครือข่าย (Vulnerability Management System) ซึ่งใช้ตรวจสอบเพื่อหาช่องโหว่ในระบบคอมพิวเตอร์และเครือข่าย โดยสามารถบอกระดับความเสี่ยงของช่องโหว่ที่พบ และแนะนำวิธีการแก้ไขปัญหาช่องโหว่นั้น ๆ ได้

2.3.2.6 ระบบปฏิบัติการด้านการรักษาความปลอดภัยเชิงรุก (Offensive Security Operating System) ซึ่งเป็นระบบปฏิบัติการคอมพิวเตอร์แบบพิเศษที่มีบรรจุเครื่องมือต่าง ๆ สำหรับใช้ในการตรวจสอบ วิเคราะห์ และโจมตีทางไซเบอร์

2.3.2.7 ระบบตรวจสอบ/ตรวจพิสูจน์หลักฐานทางไซเบอร์ (Cyber Forensic System) พร้อมห้องปฏิบัติการ ซึ่งใช้ในการสืบสวนข้อมูลทางอิเล็กทรอนิกส์ เก็บหลักฐานสำคัญทางดิจิทัล (Digital Forensics) ในรูปแบบต่าง ๆ ทั้งที่อยู่ในระบบคอมพิวเตอร์และอุปกรณ์ที่สามารถจัดเก็บข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ เช่น โทรศัพท์แบบพกพา กล้องถ่ายรูป อุปกรณ์รับสัญญาณดาวเทียม อุปกรณ์จัดเก็บข้อมูล และเครื่องเล่นเกม เป็นต้น ในกรณีเกิดเหตุการณ์หรือภัยคุกคามทางไซเบอร์

2.3.2.8 ระบบยุทธภัณฑ์ทางไซเบอร์ (Cyber Weapon System) ซึ่งใช้ในการออกแบบ วิจัยและพัฒนา (Research and Development) เพื่อผลิตยุทธภัณฑ์ทางไซเบอร์ เช่น โปรแกรมประสงค์ร้าย (Malware) และซอฟต์แวร์สำหรับใช้ในการปฏิบัติการทางไซเบอร์อื่น ๆ เป็นต้น

2.3.2.9 ระบบควบคุมและรักษาความมั่นคงปลอดภัยอุปกรณ์แบบเคลื่อนที่ (Mobile Device Security Management) ซึ่งใช้ในการควบคุมและรักษาความมั่นคงปลอดภัยของการใช้อุปกรณ์แบบเคลื่อนที่

2.3.2.10 ระบบข่าวกรองทางไซเบอร์ (Cyber Intelligence System) ซึ่งใช้ในการรวบรวม ประมวลผล แลกเปลี่ยน และจัดเก็บข่าวกรองทางไซเบอร์ โดยสามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลกับระบบข่าวกรองทางไซเบอร์ของหน่วยงานที่เกี่ยวข้องอื่น ๆ ได้

3. ประสิทธิภาพ

3.1 โครงสร้างหลักของกรอบการดำเนินงานอธิบายวงจรต่อเนื่องของขบวนการทางธุรกิจซึ่งทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ดังนี้

3.1.1 การกำหนด การศึกษา ทำความเข้าใจวิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถการจัดการทรัพย์สิน สภาพแวดล้อมทางธุรกิจ การดำเนินงานภาครัฐ การประเมินความเสี่ยง กลยุทธ์การจัดการความเสี่ยง

3.1.2 การป้องกัน ควบคุม และดำเนินงานตามมาตรการป้องกันที่เหมาะสมเพื่อป้องกันหรือจำกัดระดับของภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์การควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล กระบวนการป้องกันข้อมูล การดูแลรักษาเทคโนโลยีที่ใช้ในป้องกัน

3.1.3 การตรวจจับการเฝ้าระวัง หรือมีการตรวจสอบติดตามอย่างต่อเนื่องเพื่อการเตือนภัยกับเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันที และสามารถควบคุมสถานการณ์ได้ความผิดปกติและเหตุการณ์ต่างๆ การสังเกตการณ์อย่างต่อเนื่อง และกระบวนการตรวจสอบ

3.1.4 การรับมือ กิจกรรมการรับมือกับเหตุการณ์ต่างๆ ที่เกิดขึ้นการวางแผนรับมือ การสื่อการ การวิเคราะห์ การลดความเสี่ยง และปรับปรุงแก้ไข

3.1.5 การคืนสภาพ แผนความต่อเนื่องทางธุรกิจเพื่อรองรับการดำเนินงานต่อเนื่อง แผนการกู้คืนขีดความสามารถภายหลังจากการโดนคุกคามทางไซเบอร์การวางแผนฟื้นฟู การปรับปรุง การสื่อสาร

3.2 กองทัพอากาศดำเนินการตามขั้นตอนดังกล่าวมีการดำเนินการอย่างครบถ้วน โดยเฉพาะการดำเนินการของศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ซึ่งรับผิดชอบระบบอุปกรณ์ระบบสารสนเทศเป็นส่วนรวม ได้รับมาตรฐาน ISO 27001(2013) ใน พ.ศ.2558 แต่เป็นในเชิงการป้องกันระบบเท่านั้น ส่วนในเชิงป้องปราม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ได้ทำการจัดการแข่งขัน Cyber Operations Contest และ มีการฝึกปฏิบัติในระบบจำลองยุทธทางไซเบอร์ (Cyber Range) ด้วย จึงถือได้ว่ากองทัพอากาศมีประสิทธิภาพด้านไซเบอร์ในระดับกลาง

4. ข้อจำกัดและปัญหา

4.1 ข้อจำกัด

4.1.1 ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งานนั้น ส่วนใหญ่ติดตั้งที่กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ แต่เนื่องด้วยมีข้อจำกัดด้านสถานที่ที่ไม่เพียงพอต่อการติดตั้งอุปกรณ์บางส่วนจึงนำมาติดตั้งใช้งานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ซึ่งควรจะติดตั้งใช้งานภายในพื้นที่เดียวกันเพื่อสะดวกต่อการปฏิบัติงานของบุคลากร

4.1.2 ระบบเทคโนโลยีที่จัดหามาใช้งานนั้นมีราคาสูง และต้องมีลิขสิทธิ์จากบริษัทผู้ผลิตอีกด้วย จึงต้องใช้งบประมาณมากขึ้น รวมถึงกองทัพอากาศต้องจัดหาระบบอื่นมาใช้งานในการปฏิบัติภารกิจด้วย ทำให้งบประมาณที่ได้รับมีข้อจำกัดไม่เพียงพอต่อการดำเนินการ

4.2 ปัญหา

4.2.1 ปัจจัยด้านนโยบาย แผน และการปฏิบัติที่เกี่ยวข้อง

4.2.1.1 การดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ ดำเนินการได้ไม่ครบถ้วน บุคลากรบางส่วนละเลยไม่ปฏิบัติตามทำให้ไวรัสและมัลแวร์เข้ามาในระบบ

4.2.1.2 ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 โดยอ้างอิงจากมาตรฐาน ISO 27001(2005) นั้นใช้งานมานานแล้ว อาจไม่ครอบคลุมการปฏิบัติ

4.2.1.3 คู่มือการปฏิบัติเมื่อถูกโจมตีระบบสารสนเทศและการสื่อสารมีการจัดทำใช้งานที่กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศแล้ว แต่ไม่มีการแจกจ่ายให้หน่วยเกี่ยวข้อง

4.2.1.4 คู่มือการใช้งานอุปกรณ์ในเบื้องต้น มีแต่ไม่ครอบคลุมการใช้งาน โดยเฉพาะเทคโนโลยีที่จัดหามาใช้งานใหม่

4.2.2 ปัจจัยด้านบุคลากร

4.2.2.1 บุคลากร ระดับกำลังพลหลักด้านไซเบอร์ วิทยากรอบรมให้ความรู้ด้านไซเบอร์ (Instructor) ผู้เฝ้าระวังระบบคอมพิวเตอร์เครือข่ายและความปลอดภัยทางไซเบอร์ ผู้ตรวจสอบการรักษาความปลอดภัยระบบสารสนเทศ ขาดทักษะในการปฏิบัติภารกิจ

4.2.2.2 หลักสูตรการศึกษาเฉพาะด้านจากนอกหน่วย ยังขาดงานด้านที่สำคัญ เช่น ด้านการเก็บหลักฐานเมื่อถูกโจมตี เป็นต้น

4.2.2.3 ไม่มีนักพัฒนาโปรแกรมเชิงป้องปราม

4.2.3 ปัจจัยด้านเทคโนโลยี

4.2.3.1 เทคโนโลยีพัฒนาเปลี่ยนแปลงตลอดเวลาทำให้ต้องมีการติดตามและจัดหามาไว้ใช้งาน

4.2.3.2 ระบบการจัดการความรู้ (Knowledge Management System) ยังไม่ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพ

สรุป

การดำเนินการด้านไซเบอร์มีปัจจัยที่เกี่ยวข้องหลักทั้ง 3 ด้าน คือ ด้านนโยบาย แผนงานและการปฏิบัติที่เกี่ยวข้อง ด้านบุคลกรและด้านเทคโนโลยีนั้น จะต้องมีการดำเนินการให้ถูกต้องเหมาะสมครบถ้วน รวมถึงต้องมีหน่วยงานที่รับผิดชอบในการกำหนดแนวทางการปฏิบัติ กำกับดูแล ตรวจสอบ รวบรวมปัญหาและข้อขัดข้องพร้อมแนวทางการแก้ไข เพื่อให้เกิดประสิทธิภาพในการปฏิบัติงานในการป้องกันและป้องปรามด้านไซเบอร์ดังกล่าว

บทที่ 4
การพัฒนาขีดความสามารถการปฏิบัติภารกิจด้านไซเบอร์

การวิจัยเรื่องแนวทางการพัฒนาขีดความสามารถบุคลากรด้านสงครามไซเบอร์ของกองทัพอากาศ เป็นการวิจัยเชิงคุณภาพ โดยบทนี้ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยศึกษาวิเคราะห์จากเอกสารทางวิชาการ หลักการปฏิบัติสงครามไซเบอร์ บทความด้านไซเบอร์ ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ เพื่อนำไปสู่การวิเคราะห์และการสรุปผลการวิจัยในลำดับต่อไป

การวิเคราะห์ข้อมูลจากประเด็นคำถามในการสัมภาษณ์

จากคำถามในการสัมภาษณ์ผู้บังคับบัญชาและผู้ปฏิบัติหน้าที่ด้านไซเบอร์ของกองทัพอากาศ จำนวน 5 ข้อ สามารถสรุปผลได้ดังนี้

1. การดำเนินการด้านไซเบอร์ ตามวงรอบการป้องกันทางไซเบอร์

การดำเนินการตามวงรอบการป้องกันทางไซเบอร์ ด้านการป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟู โดยการดำเนินการดังกล่าว กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศดำเนินการตามขั้นตอนแล้ว โดยการจัดหาระบบ อุปกรณ์ มีการควบคุมระบบที่เหมาะสม มีระบบรักษาความปลอดภัยอย่างมั่นคง มีการจัดทำแผนงานรองรับและแผนการบริหารความเสี่ยงในภาพรวมทั้งหมด จนได้รับมาตรฐาน ISO 27001(2013) รวมถึง กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ จัดทำแผนงานและระเบียบการปฏิบัติให้ผู้เกี่ยวข้องดำเนินการจึงมีความเห็นว่ากองทัพอากาศมีขีดความสามารถด้านไซเบอร์ในระดับดี

2. การดำเนินการด้านไซเบอร์ตามวงรอบการโจมตีทางไซเบอร์

การดำเนินการด้านไซเบอร์ตามวงรอบการโจมตีทางไซเบอร์ ด้านการรวบรวมข้อมูลเป้าหมาย การตรวจสอบหาช่องโหว่ของระบบ การปฏิบัติการโจมตี การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป และการลบร่องรอยการโจมตี นั้นกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศรับผิดชอบในการปฏิบัติ มีข้อจำกัดในการดำเนินการหลายด้าน เนื่องจากไม่มีเป้าหมายที่เป็นภัยอย่างชัดเจนที่จะให้ดำเนินการ แต่มีการจัดหาระบบอุปกรณ์ที่เกี่ยวข้องมาฝึกใช้งาน โดยเฉพาะนำระบบจำลองยุทธทางไซเบอร์มาฝึกให้กับบุคลากรกองทัพอากาศ จึงมีความเห็นว่ากองทัพอากาศมีขีดความสามารถด้านไซเบอร์ในระดับปานกลาง

3. โครงสร้างหน่วยงานด้านไซเบอร์

โครงสร้างเกิดขึ้นใน พ.ศ.2557 ภารกิจที่ได้รับในปัจจุบัน หน่วยสามารถตอบสนองต่อภารกิจได้อย่างจำกัด ดังนี้

3.1 หน่วยงานด้านสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศ ส่วนมากเป็นระดับฝ่ายซึ่งจะปฏิบัติภารกิจที่ได้รับตามความรับผิดชอบภายในหน่วย และประสานการปฏิบัติงานร่วมกับกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศที่เป็นงานหน่วยหลักและหน่วยงานอื่น

ที่เกี่ยวข้อง โครงสร้างอัตราที่ได้รับจึงเพียงพอสำหรับภารกิจเริ่มต้นใหม่เท่านั้น หากมีภารกิจเพิ่มเติมควรปรับโครงสร้างให้สอดคล้องด้วย

3.2 กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเป็นโครงสร้างที่ยกระดับความสำคัญขึ้นมาจากเดิม แต่โครงสร้างกองสงครามไซเบอร์ในปัจจุบันมีผู้อำนวยการกอง ชั้นยศนาวาอากาศเอก (เงินเดือน ระดับ น.5) เป็นผู้บังคับบัญชารับผิดชอบ งานที่ดำเนินการเป็นงานฝ่ายเสนาธิการและผู้ปฏิบัติงานด้านไซเบอร์โดยตรง การดำเนินการและกำกับดูแลการฝึกด้านไซเบอร์ รวมถึงต้องไปบรรยายให้สถานศึกษาและหน่วยเกี่ยวข้อง พร้อมกับปฏิบัติงานร่วมกับ เหล่าทัพ กองบัญชาการกองทัพไทย กระทรวงกลาโหมหน่วยราชการและหน่วยงานอื่น ซึ่งโครงสร้างยังสามารถรองรับภารกิจได้ หากมีภารกิจเพิ่มเติมควรปรับโครงสร้างให้เหมาะสม

3.3 ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นหน่วยที่จัดตั้งมานานเป็นหน่วยงานที่จะต้องปรนิบัติดูแลระบบเทคโนโลยีสารสนเทศทั้งปวงของกองทัพอากาศ บุคลากรมีคุณภาพและปฏิบัติงานได้อย่างมีประสิทธิภาพมีโครงสร้างที่เหมาะสมกับภารกิจที่ได้รับ

4. บุคลากร

บุคลากรมีประสิทธิภาพในระดับปานกลาง เนื่องจากเทคโนโลยีสารสนเทศมีการพัฒนาตลอดเวลา การได้รับระบบสารสนเทศเพิ่มเติมนั้นบุคลากรจะต้องเรียนรู้ในการใช้งานและแก้ไขข้องบกพร่องที่อาจจะเกิดขึ้น ซึ่งระบบเดิมคงใช้งานอยู่ทำให้มีภาระกรรมที่เพิ่มขึ้น ทำให้มีความต้องการบุคลากรที่มีทักษะมาปฏิบัติงาน และมีปัจจัยหลายอย่างที่ทำให้บุคลากรไม่อยู่ในระบบ เช่น ย้ายไปดำรงตำแหน่งที่สูงขึ้น เกษียณอายุราชการ ลาออก เป็นต้น จำนวนบุคลากรลดลงจึงมีความจำเป็นต้องจัดหาบุคลากรมาทดแทน การพัฒนาบุคลากรต้องดำเนินการอย่างต่อเนื่องเพื่อให้ทันต่อการปฏิบัติ

5. สถานที่ทำงาน

สถานที่ทำงานหน่วยสารสนเทศของหน่วยขึ้นตรงของกองทัพอากาศถึงแม้จะเป็นหน่วยที่จัดตั้งขึ้นใหม่แต่มีความพร้อมในการปฏิบัติหน้าที่ บุคลากรสามารถใช้งานได้อย่างเหมาะสม ส่วนสถานที่ทำงานกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศยังไม่เพียงพอที่จะรองรับการปฏิบัติงานด้านไซเบอร์ ซึ่งผู้บังคับบัญชาระดับสูงได้กำหนดพื้นที่เพิ่มเติมให้แล้ว อยู่ระหว่างการดำเนินการปรับปรุง และสถานที่ทำงานศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ มีพื้นที่คับแคบไม่เพียงพอต่อการติดตั้งระบบเทคโนโลยีสารสนเทศ เนื่องจากมีการจัดหาระบบเทคโนโลยีสารสนเทศเพิ่มเติมตลอดเวลา การติดตั้งระบบภายในอาคารไม่เพียงพอ ซึ่งได้ขอรับการสนับสนุนจากผู้บังคับบัญชาในการสร้างอาคารใหม่แล้ว อยู่ในระหว่างการดำเนินการของหน่วยเกี่ยวข้อง

การวิเคราะห์ข้อมูลหน่วยงานรับผิดชอบ

1. หน่วยงานรับผิดชอบกองทัพอากาศใช้เทคโนโลยีสารสนเทศเป็นองค์ประกอบในการปฏิบัติงานจำนวนมาก รวมถึงหน่วยรับผิดชอบดำเนินการจำกัด

1.1 กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (หัวหน้าหน่วยชั้นยศ นาวาอากาศเอก) มีหน่วยงานที่รับผิดชอบ ประกอบด้วย แผนกสงครามไซเบอร์ แผนกกรรมวิธีข้อมูลสงครามไซเบอร์ แผนกรักษาความปลอดภัยระบบสารสนเทศ แผนกปฏิบัติการสงครามไซเบอร์ และแผนกประเมินผลการสงครามไซเบอร์ ปัจจุบันบรรจุบุคลากร จำนวน 24 คน ปฏิบัติงานจริงด้านไซเบอร์ ดังนี้ การวางแผนดำเนินการด้านไซเบอร์ การประชุมร่วมกับหน่วยภายในและภายนอก เป็นผู้ตรวจสอบเทคโนโลยีด้านไซเบอร์พร้อมทั้งสรุปรายงานให้ผู้บังคับบัญชาทราบ เป็นวิทยากรให้การอบรมหลักสูตรที่เกี่ยวข้องปฏิบัติงานในศูนย์ปฏิบัติการกองทัพอากาศ จัดทำรายละเอียดแผนงานเพื่อขอรับการสนับสนุนงบประมาณ จัดการแข่งขัน Cyber Operations Contest จัดการอบรมหลักสูตรด้านการรักษาความปลอดภัย การประชุมร่วมและแลกเปลี่ยนองค์ความรู้กับหน่วยภายในและภายนอก สร้างความตระหนักรู้ด้านความปลอดภัยสารสนเทศให้แก่ข้าราชการกองทัพอากาศ เข้าร่วมการฝึกด้านไซเบอร์กับหน่วยงานที่เกี่ยวข้อง ซึ่งเมื่อวิเคราะห์แล้วจำนวนบุคลากรที่ได้รับการบรรจุไม่เพียงพอต่อการปฏิบัติงานส่งผลต่อการพัฒนาผู้ตรวจสอบและผู้ที่เป็นวิทยากรและการตรียมรับเทคโนโลยีที่จัดหามาใช้งาน ซึ่งมีความต้องการไม่น้อยกว่า 36 คน หรือประมาณร้อยละ 60 ของอัตราอนุมัติกำลังพลของหน่วย ส่วนวงรอบการปฏิบัติงานด้านไซเบอร์ จะประกอบด้วย วงรอบการป้องกัน (การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟู) และวงรอบการป้อมปราม (การโจมตีทางไซเบอร์) (การรวบรวมข้อมูลเป้าหมาย การตรวจสอบหาช่องโหว่ การปฏิบัติการโจมตี การเปิดช่องโหว่ และการลบรอยการโจมตี) เมื่อวิเคราะห์แล้วแผนกที่มีอยู่ของกองสงครามไซเบอร์ฯ จะมีไม่ครบถ้วนกับวงรอบการปฏิบัติงาน การเจริญเติบโตของบุคลากรตามสายงานจะดำเนินการอย่างไม่เหมาะสม เมื่อมีโอกาสสมควรทบทวนโครงสร้างดังกล่าว

1.2 ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (หัวหน้าหน่วยชั้นยศ นาวาอากาศเอก) มีหน่วยงานที่รับผิดชอบ คือ แผนกจัดดำเนินงาน กองกรรมวิธีข้อมูล กองสื่อสารข้อมูล กองซ่อมบริภัณฑ์คอมพิวเตอร์ ฝ่ายคลังพัสดุ ปัจจุบันบรรจุบุคลากร จำนวน 70 คน ปฏิบัติงานบริหารการใช้งานระบบสารสนเทศและด้านไซเบอร์เชิงป้องกันทั้งปวง เช่น ระบบบริหารจัดการเครือข่าย ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบรักษาความปลอดภัยทางด้านกายภาพ ระบบรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์ ระบบป้องกันภัยคุกคามสำหรับระบบเครื่องแม่ข่ายแบบคลาวด์ เป็นต้น ซึ่งจะต้องมีบุคลากรเฝ้าตรวจ 24 ชั่วโมง รวมถึงมีการดำเนินการด้านกรรมวิธีข้อมูล การซ่อมอุปกรณ์ทั้งระบบ การแก้ปัญหาให้กับผู้บังคับบัญชาและหน่วยขึ้นตรงกองทัพอากาศ ปฏิบัติงานในศูนย์ปฏิบัติการกองทัพอากาศ เข้าร่วมการฝึกร่วมและผสมกับหน่วยงานภายนอก การประชุมร่วมและการแลกเปลี่ยนองค์ความรู้กับหน่วยภายในและภายนอกและต้องดูแลรักษาระบบฯ ในภาพรวมอีกด้วย ซึ่งเมื่อพิจารณาแล้วจำนวนบุคลากรที่ได้รับการบรรจุยังไม่เพียงพอต่อการปฏิบัติงาน ซึ่งมีความต้องการไม่น้อยกว่า 120 คน หรือประมาณร้อยละ 55 ของอัตราอนุมัติกำลังพล

ของหน่วย และรูปแบบงานที่รับผิดชอบมีหลากหลายทำให้บุคลากรขาดทักษะในการปฏิบัติงาน รวมถึงสถานที่ทำงานไม่เพียงพอต่อการติดตั้งระบบและอุปกรณ์ที่จัดหามาใช้งานเพิ่มเติม

1.3 หน่วยสารสนเทศและการสื่อสารประจำหน่วยขึ้นตรง ส่วนมากจะเป็นระดับฝ่าย (หัวหน้าหน่วยชั้นยศ นาวาอากาศตรี) รับผิดชอบงานระบบคอมพิวเตอร์ การดำเนินการตามแผนงานที่กำหนด การรักษาความปลอดภัยระบบฯ การตรวจสอบระบบฯ การแก้ไขปัญหาให้กับผู้บังคับบัญชาในหน่วยและการแก้ไขปัญหาเฉพาะหน้า รวมถึงต้องจัดทำคำขอรับการสนับสนุนเพื่อขอรับงบประมาณในส่วนที่เกี่ยวข้อง มีการบรรจุข้าราชการ เพียง 4 คน แต่มีเครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบไม่น้อยกว่า 250 เครื่อง ซึ่งมีความต้องการไม่น้อยกว่า 6 คน หรือประมาณร้อยละ 75 ของอัตราอนุมัติกำลังพลของหน่วย รวมถึงรูปแบบงานที่รับผิดชอบมีหลากหลายทำให้บุคลากรขาดทักษะในการปฏิบัติงาน และไม่เพียงพอต่อการปฏิบัติงาน

1.4 การสร้างแรงจูงใจในการปฏิบัติงาน เมื่อตรวจสอบโครงสร้างและอัตราที่ได้รับเงินประจำตำเหน่งประเภทวิชาชีพเฉพาะจะได้รับตั้งแต่นายทหารชั้นยศนาวาอากาศโท ซึ่งดำรงตำแหน่งระดับหัวหน้าแผนกขึ้นไป ซึ่งการปฏิบัติงานด้านไซเบอร์มีความสำคัญอย่างยิ่งโดยจะต้องใช้ความคิดและความสามารถเฉพาะด้านเพื่อไม่ให้มีการสมองไหลจากกองทัพ ควรมีการจูงใจเพื่อให้บุคลากรได้รับเงินเพิ่มพิเศษ มิฉะนั้นจะไม่มีบุคลากรเสียสละมาทำงานด้านนี้

การวิเคราะห์ปัจจัยที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์

1. วงรอบการปฏิบัติด้านไซเบอร์

จากหลักการทั่วไปด้านไซเบอร์ วงรอบการปฏิบัติทางไซเบอร์ แบ่งออกเป็น วงรอบการป้องกันทางไซเบอร์ และวงรอบการโจมตีทางไซเบอร์ ดังนี้

1.1 วงรอบการป้องกันทางไซเบอร์ แบ่งการปฏิบัติเป็น 4 ขั้นตอน ดังนี้ การป้องกัน คือ การระวังป้องกันไม่ให้เกิดความเสียหายขึ้นกับระบบสารสนเทศที่ใช้งาน การตรวจจับ คือ การเฝ้าระวังการถูกโจมตีหรือการถูกคุกคามทางไซเบอร์ด้วยการสังเกต การใช้ซอฟต์แวร์ ตลอดจนระบบตรวจจับอื่น ๆ ช่วยในการตรวจจับสิ่งผิดปกติที่เกิดขึ้นในการใช้งานระบบสารสนเทศ การตอบสนอง (React) คือ การปฏิบัติเพื่อแก้ไขปัญหาและระงับเหตุการณ์การล่วงละเมิดการรักษาความปลอดภัยทางไซเบอร์ที่เกิดขึ้นโดยทันที และการฟื้นฟู (Recover) คือ การปฏิบัติเพื่อฟื้นฟูระบบสารสนเทศที่ได้รับผลกระทบทั้งหมด ให้กลับคืนสู่สภาพปกติที่พร้อมใช้งานโดยเร็วที่สุด พร้อมทำการปรับปรุงกระบวนการป้องกันให้มีประสิทธิผลในการรักษาความปลอดภัยยิ่งขึ้น

การปฏิบัติตามวงรอบดังกล่าว ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศได้ยึดถือตามแนวทางนี้มาตลอด โดยมีระบบอุปกรณ์ โปรแกรมและบุคลากรในการปฏิบัติงานเฝ้าตรวจ หากมีการพบไวรัสและมัลแวร์จะดำเนินการป้องกันไม่ให้เข้ามาในระบบทันที หรือหากมีการโจมตีระบบแล้วมีผลกระทบจะมีแผนงานในการดำเนินการฟื้นฟูระบบตามขั้นตอนในปัจจุบันสามารถป้องกันระบบได้ในระดับหนึ่ง

กรณีบุคลากรภายในกองทัพมีการดำเนินการนำอุปกรณ์มาต่อเชื่อมระบบคอมพิวเตอร์ภายในหน่วย โดยไม่มีการตรวจสอบก่อนใช้งานรวมถึงคอมพิวเตอร์ที่ได้รับการเชื่อมต่อไม่มีโปรแกรมป้องกันแต่ไม่ทันสมัย อาจทำให้ระบบติดไวรัสและมัลแวร์ได้ ซึ่งระบบป้องกันที่มีอยู่จะ

ตรวจพบได้ช้าและอาจจะไม่ทันต่อเหตุการณ์ โดยบุคลากรของกองทัพอากาศต้องดำเนินการตามระเบียบจัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 และปฏิบัติตามแนวนโยบายและการปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกองทัพอากาศในทุกกรณี รวมถึงในระบบสารสนเทศที่สำคัญทางด้านยุทธการ ต้องดำเนินการให้เป็นระบบปิดโดยไม่ให้เชื่อมต่อกับระบบอินเทอร์เน็ตภายนอกได้ หากบุคลากรที่อยู่ในระบบมีการฝ่าฝืนต้องได้รับการลงทัณฑ์ตามระเบียบกองทัพอากาศที่กำหนดไว้

1.2 วงรอบการโจมตีทางไซเบอร์ วงรอบการโจมตีทางไซเบอร์ แบ่งการปฏิบัติออกเป็น 5 ขั้นตอน ดังนี้ การรวบรวมข้อมูลเป้าหมาย คือ การรวบรวมข้อมูลเป้าหมายเกี่ยวกับโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์และเครื่องมือที่ใช้ วิธีการใช้งาน และข้อมูลต่าง ๆ ของบุคลากร ที่อาจเป็นประโยชน์ในการโจมตี ตรวจสอบหาช่องโหว่ของระบบ คือ การตรวจสอบหาช่องโหว่หรือการวิเคราะห์ช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์เพื่อการโจมตีจากข้อมูลเป้าหมายที่รวบรวมได้ การปฏิบัติการโจมตี คือ การใช้อาวุธทางด้านไซเบอร์ทุกรูปแบบในการเข้าโจมตีระบบเป้าหมาย เพื่อให้เกิดผลตามที่คาดหวัง การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป คือ การเปิดช่องโหว่ทิ้งไว้ในระบบที่เข้าโจมตี เพื่อใช้เป็นช่องทางสำหรับการเข้าปฏิบัติการครั้งต่อไป การลบร่องรอยการโจมตี คือ การลบร่องรอยของการโจมตี หรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบเพื่อไม่ให้สามารถสืบย้อนกลับมาถึงผู้โจมตีได้

ในการโจมตีทางไซเบอร์นี้ยังไม่มีกฎหมายรองรับ จึงไม่มีการดำเนินการอย่างเป็นรูปธรรม แต่มีการฝึกบุคลากรของกองทัพอากาศ โดยการจัดจัดการแข่งขัน Cyber Operations Contest เพื่อให้บุคลากรมีความรู้ความเข้าใจและตระหนักถึงความสำคัญในการดำรงขีดความสามารถของการรักษาความปลอดภัยในการใช้งานเครือข่าย และป้องกันการถูกโจมตีทางไซเบอร์ รวมถึงมีการฝึกในระบบจำลองยุทธทางไซเบอร์เพิ่มเติมด้วย ซึ่งการฝึกดังกล่าวยังสามารถใช้วิธีการที่ได้รับมาตรวจสอบหาช่วงโหว่ระบบสารสนเทศที่มีใช้งาน เพื่อเตรียมตัวป้องกันระบบให้เกิดประสิทธิภาพอีกด้วย

เมื่อวิเคราะห์จากข้อมูลแล้ว การดำเนินการของกองทัพอากาศเป็นไปตามวงรอบการปฏิบัติ เมื่อวิเคราะห์ในภาพรวมทั้งด้านเชิงป้องกันและการโจมตี (เชิงป้องปราม) พบว่าบุคลากรจะมีความรู้แต่ไม่ครอบคลุมการดำเนินการเชิงป้องกันและยังขาดทักษะการปฏิบัติงาน ส่วนด้านการโจมตี (เชิงป้องปราม) เห็นควรให้มีการจัดหาอุปกรณ์ที่จำเป็นในการปฏิบัติงาน เพื่อเพิ่มประสิทธิภาพเชิงป้องกันและการโจมตี เช่น ด้านโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์และเครื่องมือที่ใช้ และขีดความสามารถด้านนิติวิทยาศาสตร์ เป็นต้น

2. ปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์

2.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง

การปฏิบัติการไซเบอร์ จะมี ต้องมีการตั้งนโยบายและวางแผนการปฏิบัติต่าง ๆ การกำหนดการปฏิบัติ กำหนดผู้รับผิดชอบ และมีการตรวจสอบและประเมินผลการปฏิบัติ นั้นสามารถวิเคราะห์ได้ดังนี้

2.1.1 ตามที่กองทัพอากาศจัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 และ เมื่อศึกษารายละเอียดตามที่กำหนด

หน้าที่และวิธีดำเนินการในระบบสารสนเทศแล้ว ยังครอบคลุมการปฏิบัติ เพียงแต่ให้ปรับแก้ไขเพิ่มเติมแบบรายการตรวจติดตาม การปฏิบัติตามระเบียบกองทัพอากาศว่าด้วยรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.2552 และขอให้ ผู้บังคับบัญชาและผู้ตรวจสอบการรักษาความปลอดภัยระบบสารสนเทศ ตรวจติดตามการปฏิบัติอย่างเคร่งครัด รวมถึงให้ตรวจติดตามการดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศด้วย

2.1.2 โครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแผนแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศ นั้นมีความชัดเจนในขั้นตอนกล่าวคือ สามารถใช้เป็นแนวทางในการพัฒนาระบบการปฏิบัติงานด้านสงครามไซเบอร์ของ ทอ. ซึ่งมีการกำหนดเป้าหมายด้านการดำเนินการ ด้านบุคลากร ด้านกระบวนการบริหารจัดการ ด้านเทคโนโลยี และด้านงบประมาณ ไว้ชัดเจนสามารถนำมาเป็นแนวทางการปฏิบัติงานได้

2.1.3 จัดการแข่งขัน Cyber Operations Contest นั้น สามารถดำเนินการได้ตามวัตถุประสงค์ ซึ่งมีประโยชน์ต่อการปฏิบัติภารกิจเป็นอย่างยิ่ง สามารถฝึกบุคลากรได้เป็นอย่างดี แต่มีบุคลากรจำนวนน้อยที่เป็นตัวแทนหน่วยเข้ามารับการแข่งขัน หากบุคลากรดังกล่าวกลับนำไปเผยแพร่วิธีการที่หน่วยด้วยวิธีใดก็ตามจะเป็นประโยชน์ต่อการปฏิบัติของบุคลากรที่ไม่ได้เข้าร่วมแข่งขันเป็นอย่างมาก อีกทั้งเป็นช่องทางที่จะสรรหาบุคลากรเข้ามาปฏิบัติงานอีกด้วย

2.1.4 การประชุมประชาคมไซเบอร์ การประชุมร่วมกับหน่วยงานภายนอกและการประชุมร่วมกับต่างชาติ นั้นมีประโยชน์ต่อการแลกเปลี่ยน ข้อมูล องค์ความรู้และวิธีการปฏิบัติ ซึ่งเป็นการเพิ่มประสิทธิภาพบุคลากรได้อีกทางหนึ่ง

2.1.5 การเตรียมการจัดตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของกองทัพอากาศนั้น เหมาะสมที่จะต้องจัดตั้ง เนื่องจากการดำเนินการด้านไซเบอร์จะเป็นการดำเนินการของบุคลากรภายในหน่วยขึ้นตรงของกองทัพอากาศทั้งหมด ซึ่งจะต้องให้ความร่วมมือเพื่อตอบสนองต่อภัยคุกคาม เห็นสมควรอย่างยิ่งที่จะต้องเร่งดำเนินการ รวมถึงให้เร่งการจัดทำแนวความคิดการปฏิบัติการไซเบอร์ของกองทัพอากาศและแผนเผชิญเหตุเมื่อระบบสารสนเทศถูกโจมตี

2.2 ปัจจัยด้านบุคลากร

ในการปฏิบัติการไซเบอร์บุคลากรถือว่าเป็นปัจจัยที่สำคัญ เพราะในทุกกระบวนการในการปฏิบัติการไซเบอร์จำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการปฏิบัติงาน ทั้งการปฏิบัติการไซเบอร์เชิงรับ ที่ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว รวมทั้งสามารถกู้คืนระบบที่เสียหายให้กลับมาปฏิบัติงานได้โดยไม่กระทบต่อกระบวนการทำงานอื่น ๆ และการปฏิบัติการไซเบอร์เชิงป้องปราม ที่ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการค้นหาจุดอ่อน ช่องโหว่ของระบบเป้าหมาย ซึ่งบุคลากรจะมีความสามารถในการปฏิบัติการไซเบอร์ได้ ก็ต้องได้รับการสนับสนุนและส่งเสริมในการพัฒนาองค์ความรู้ รวมทั้งการมีแรงจูงใจที่เหมาะสมเพื่อให้บุคลากรพัฒนาตนเองอยู่เสมอ เนื่องจากองค์ความรู้ด้านไซเบอร์มีการเปลี่ยนแปลงที่รวดเร็ว ซึ่งกองทัพอากาศมีการดำเนินการ ดังนี้

2.2.1 ดำเนินการด้านการฝึก ศึกษาและอบรมบุคลากรด้านไซเบอร์

2.2.1.1 หลักสูตรพื้นฐานรองรับผู้ปฏิบัติงานและผู้บริหาร ได้จัดทำหลักสูตรสงครามไซเบอร์ให้กับโรงเรียนจ่าอากาศ กรมยุทธศึกษาทหารอากาศ หลักสูตรสำหรับผู้จบการศึกษาจากโรงเรียนจ่าอากาศฯ หลักสูตรเจ้าหน้าที่เทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ หลักสูตรนายทหารเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ เพื่อให้ผู้ที่เข้ามาบรรจุในตำแหน่งใหม่ทราบ หลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศ และมีการให้ความรู้ผู้บริหารระดับกลาง คือหลักสูตรสงครามไซเบอร์สำหรับนักศึกษาโรงเรียนเสนาธิการทหารอากาศ โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ

2.2.1.2 หลักสูตรเฉพาะ การอบรมเกี่ยวกับการประเมินและตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ให้กับผู้ปฏิบัติงานด้านรักษาความปลอดภัยระบบสารสนเทศ

2.2.1.3 ส่งบุคลากรเข้ารับการฝึกอบรมกับบริษัทเอกชนและหน่วยงานภายนอก รวมถึงส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานของรัฐ

2.2.1.4 หลักสูตรเกี่ยวกับสร้างความชำนาญ จัดการฝึกอบรมการในการเลื่อนระดับความชำนาญให้กับข้าราชการที่มีคุณสมบัติครบเพื่อพิจารณา เลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น

2.2.1.5 ส่งบุคลากรเข้ารับการฝึกศึกษาและอบรมกับบริษัทเอกชนและหน่วยงานภายนอก รวมถึงส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานภาครัฐ

2.2.1.6 การสร้างจิตสำนึกและการแจ้งเตือน การเสริมสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ สำหรับการบรรยายพิเศษที่สถาบันการศึกษา หน่วยงาน และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อเสริมสร้างความตระหนักด้านความปลอดภัย ส่งให้ทางไปรษณีย์อิเล็กทรอนิกส์ของข้าราชการ พนักงานราชการ และลูกจ้างกองทัพอากาศ

2.2.1.7 การพิจารณาในการดำรงตำแหน่ง พิจารณาตามคุณสมบัติขั้นตอนระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ แต่ตำแหน่งดังกล่าวเป็นไปตามโครงสร้างที่กำหนดไว้ จึงพิจารณาได้ไม่เกินตำแหน่งตามโครงสร้าง

ตามที่กองทัพอากาศได้ดำเนินการที่ผ่านมานั้น สามารถให้ความรู้และความสามารถบุคลากรได้ในระดับหนึ่ง แต่ยังขาดความชำนาญในการปฏิบัติงาน จึงเห็นควรต้องมีการฝึกอบรมและทบทวนกันอย่างต่อเนื่อง รวมถึงต้องมีเอกสารคู่มือการปฏิบัติงานและการจัดองค์ความรู้ด้วย รวมถึงการบรรจุบุคลากรจากภายนอกหน่วยเพื่อเข้าดำรงตำแหน่งด้านไซเบอร์ต้องกำหนดคุณสมบัติของการศึกษาให้ชัดเจน

2.3 ปัจจัยด้านเทคโนโลยี

กองทัพอากาศได้ดำเนินการจัดหา ระบบเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องปราม ดังนี้ เทคโนโลยีทั้งเชิงป้องกัน เช่น ระบบบริหารจัดการเครือข่าย ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบป้องกันการรั่วไหลของข้อมูล ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรอง ระบบจำลองการโจมตีในรูปแบบการระดมโจมตีเพื่อให้เครื่องแม่ข่ายปฏิเสธการให้บริการ ระบบบริหารแพทช์ ระบบรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์

ระบบป้องกันภัยคุกคามสำหรับระบบเครื่องแม่ข่ายแบบคลาวด์ ระบบเข้ารหัสข้อมูล และระบบจำลองยุทธทางไซเบอร์ เป็นต้น ส่วนเทคโนโลยีเชิงป้องปราม เช่น ระบบเครือข่ายเพื่อการซ่อนพราง ระบบบริหารจัดการช่องโหว่ในระบบคอมพิวเตอร์และเครือข่าย ระบบปฏิบัติการด้านการรักษาความปลอดภัยเชิงรุก ระบบข่าวกรองทางไซเบอร์ เป็นต้น

การจัดหาเทคโนโลยีมาใช้งานในกองทัพ เป็นการจัดหาเทคโนโลยีตามวงรอบการปฏิบัติการด้านไซเบอร์ทั้งเชิงป้องกันและเชิงป้องปราม โดยมีการจัดหาตามแผนงานที่กำหนดไว้ในโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศ แต่จากการที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว จึงต้องมีการจัดเทคโนโลยีใหม่มาใช้งานอย่างต่อเนื่องเพื่อป้องกันช่วงโหว่ที่อาจจะเกิดขึ้น ซึ่งจะส่งผลกระทบต่อบุคลากรที่รับผิดชอบใช้งานและงบประมาณของกองทัพอากาศ

3. ประสิทธิภาพ

การดำเนินการอย่างมีประสิทธิภาพ มีการดำเนินการ ดังนี้

3.1 โครงสร้างหลักของกรอบการดำเนินงานอธิบายวงจรต่อเนื่องของขบวนการ ซึ่งทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ คือ

3.1.1 การกำหนด การศึกษา ทำความเข้าใจวิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยง การจัดการความเสี่ยง

3.1.2 การดำเนินงานตามมาตรการป้องกันที่เหมาะสม

3.1.3 การตรวจจับการเฝ้าระวัง เพื่อการเตือนภัยกับเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์พร้อมกระบวนการตรวจสอบ

3.1.4 การรับมือ กิจกรรมการรับมือกับเหตุการณ์ต่าง ๆ ที่เกิดขึ้น

3.1.5 การคืนสภาพ เพื่อรองรับการดำเนินงานต่อเนื่อง ตามแผนการกู้คืนขีดความสามารถภายหลังจากการโดนคุกคามทางไซเบอร์ มีการวางแผนฟื้นฟูและการปรับปรุงระบบ

3.2 กองทัพอากาศดำเนินการตามขั้นตอนดังกล่าวมีการดำเนินการอย่างต่อเนื่อง โดยเฉพาะการดำเนินการเชิงป้องกันของ ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ซึ่งรับผิดชอบระบบอุปกรณ์ระบบสารสนเทศเป็นส่วนรวมได้รับมาตรฐาน ISO 27001(2013) ใน พ.ศ. 2558 ประสิทธิภาพเชิงป้องกันจึงอยู่ในระดับปานกลาง ซึ่งหากมีเทคโนโลยีใหม่เกิดขึ้นอาจจะทำให้ระบบที่มีใช้งานอยู่โดยบุกรุกได้

ส่วนในเชิงป้องปราม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศได้ทำการจัดการแข่งขัน Cyber Operations Contest และ มีการฝึกปฏิบัติในระบบจำลองยุทธทางไซเบอร์ (Cyber Range) ด้วย แต่บุคลากรด้านนี้ยังขาดความรู้เฉพาะด้านและทักษะในการดำเนินการ หากจะมีการโจมตีระบบที่คาดว่าจะเป็นภัยคุกคามของฝ่ายเราอาจจะดำเนินการได้อย่างไม่มีประสิทธิภาพ จึงถือได้ว่ากองทัพอากาศมีประสิทธิภาพด้านไซเบอร์เชิงป้องปรามในระดับต่ำ ควรมีการเร่งสร้างบุคลากรเชิงป้องปรามอย่างเร่งด่วน

ข้อจำกัดและปัญหา

1. ข้อจำกัด

1.1 สถานที่ ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งานนั้น ส่วนใหญ่ติดตั้งที่กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ แต่เนื่องด้วยมีข้อจำกัดด้านอาคารสถานที่ที่ไม่เพียงพอต่อการติดตั้ง อุปกรณ์บางส่วนที่จัดหามาใช้งานใน ปี พ.ศ.2560 จึงนำมาติดตั้งใช้งานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเพื่อใช้งาน ในด้านเทคนิคสามารถรับส่งสัญญาณได้อย่างมีประสิทธิภาพ แต่จะต้องใช้บุคลากรเพิ่มมากขึ้น ทำให้การปฏิบัติงานไม่คล่องตัว ปัจจุบันกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ ได้ขอรับการสนับสนุนงบประมาณในการสร้างอาคารเพื่อเป็นสถานที่ติดตั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารเพิ่มเติมรวมถึงอุปกรณ์ด้านไซเบอร์ด้วย เมื่อสร้างอาคารเสร็จสิ้นแล้วเห็นควรนำอุปกรณ์เชิงป้องกันทั้งหมดติดตั้งใช้งานที่อาคารใหม่ เพื่อสะดวกต่อการปฏิบัติงานของบุคคลากร

1.2 งบประมาณ ระบบเทคโนโลยีที่จัดหามาใช้งานนั้นมีราคาสูง และต้องมีลิขสิทธิ์จากบริษัทผู้ผลิตอีกด้วย จึงต้องใช้งบประมาณมากขึ้น รวมถึงกองทัพอากาศต้องจัดหาระบบอื่นมาใช้งานในการปฏิบัติภารกิจด้วย ทำให้งบประมาณที่ได้รับมีข้อจำกัดไม่เพียงพอต่อการดำเนินการในภาพรวม โดยเทคโนโลยีและลิขสิทธิ์นั้นจะไม่สามารถหลีกเลี่ยงได้ ไม่ว่าจะเป็นการจัดหาในรูปแบบไหนและจากบริษัทใดใด ซึ่งเป็นข้อเสียเปรียบของผู้ใช้เทคโนโลยี จึงเห็นควรให้กองทัพอากาศพิจารณาจัดหาเทคโนโลยีอย่างเหมาะสมและตามความจำเป็นต้องใช้งาน

1.3 ด้านเทคโนโลยี เทคโนโลยีมีการพัฒนาตลอดเวลา โดยจะมีโปรแกรมและอุปกรณ์ที่มีประสิทธิภาพเพิ่มเติมตลอดเวลา หากไม่มีการจัดหามาใช้งานอาจทำให้เทคโนโลยีเดิมที่มีใช้งานถูกบุกรุกจากผู้ไม่หวังดีทำให้ข้อมูลที่มีอยู่ถูกทำลายหรือไม่สามารถใช้งานได้ จึงต้องมีการติดตามเทคโนโลยีตลอดเวลาและจำเป็นต้องจัดหามาไว้ใช้งานเพื่อป้องกันภัยที่อาจจะเกิดขึ้น

2. ปัญหา

จากการที่ผู้ตรวจสอบจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศไปทำการตรวจสอบตามหน่วยขึ้นตรงกองทัพอากาศ สามารถสรุปปัญหาที่เกี่ยวข้องได้ ดังนี้

2.1 ด้านนโยบาย แผน และการปฏิบัติที่เกี่ยวข้อง

2.1.1 การดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ ดำเนินการได้ไม่ครบถ้วน บุคลากรบางส่วนละเลยไม่ปฏิบัติตามทำให้ไวรัสและมัลแวร์ เข้ามาในระบบ การตรวจสอบของผู้รับผิดชอบอาจจะดำเนินการได้ไม่ทั่วถึงเพราะมีภาระกรรมมาก และมีบุคลากรในการดำเนินการไม่เพียงพอ

2.1.2 ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 นั้นใช้งานมามากว่า 5 ปี อาจไม่ครอบคลุมการปฏิบัติในปัจจุบันควรมีการตรวจสอบและเพิ่มเติมข้อกำหนดในการดำเนินการดังกล่าว

2.1.3 คู่มือการปฏิบัติเมื่อถูกโจมตีระบบสารสนเทศและการสื่อสารยังไม่มีการจัดทำ ในการดำเนินการตามระเบียบการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 นั้นกำหนดในภาพรวมว่าจะต้องดำเนินการอย่างไร มีรายละเอียดที่หน่วยจะต้องดำเนินการ

เช่น ลดความเสียหายเบื้องต้น สำรวจความเสียหาย ตรวจสอบสาเหตุและจุดอ่อน เป็นต้น แต่ไม่มีข้อแนะนำทางเทคนิคว่าจะดำเนินการอย่างไร เช่น ขั้นตอนการสำรวจความเสียหาย ตรวจสอบสาเหตุและจุดอ่อน เป็นต้น จึงเห็นควรให้ผู้รับผิดชอบดำเนินการจัดทำอย่างเร่งด่วน

2.1.4 คู่มือการใช้งานอุปกรณ์ในเบื้องต้น มีแต่ไม่ครอบคลุมการใช้งานโดยเฉพาะเทคโนโลยีที่จัดหามาใช้งานใหม่

2.2 ด้านบุคลากร

2.2.1 บุคลากร ระดับกำลังพลหลักด้านไซเบอร์ วิทยากรอบรมให้ความรู้ด้านไซเบอร์ (Instructor) ผู้เฝ้าระวังระบบคอมพิวเตอร์เครือข่ายและความปลอดภัยทางไซเบอร์ ผู้ตรวจสอบการรักษาความปลอดภัยระบบสารสนเทศ ขาดทักษะและความชำนาญในการปฏิบัติภารกิจ ซึ่งมีจำนวนไม่เพียงพอต่อการปฏิบัติงาน

2.2.2 การศึกษาเฉพาะด้านจากนอกหน่วย บุคลากรไม่มีความรู้และความสามารถงานด้านที่สำคัญด้านไซเบอร์ เช่น ด้านการเก็บหลักฐานทางนิติวิทยาเมื่อถูกโจมตี เป็นต้น

2.2.3 ไม่มีนักพัฒนาโปรแกรมประสงค์ร้ายหรือมัลแวร์ (งานเชิงป้องปราม) บุคลากรที่มีอยู่สามารถพัฒนาโปรแกรมใช้งานได้ในระดับหนึ่ง แต่ไม่สามารถโปรแกรมประสงค์ร้ายหรือมัลแวร์เพื่อใช้งบในเชิงป้องปรามได้

2.3 ด้านเทคโนโลยี

2.3.1 เทคโนโลยี พัฒนาเปลี่ยนแปลงตลอดเวลาทำให้ต้องมีการติดตามและจัดหามาไว้ใช้งาน

2.3.2 ระบบการจัดการความรู้ (Knowledge Management System) มีการดำเนินการแต่ไม่ครอบคลุมเทคโนโลยีที่มีใช้งาน องค์ความรู้ที่มีอยู่ส่วนใหญ่จะติดอยู่กับตัวบุคล แต่ไม่สามารถถ่ายทอดองค์ความรู้นั้นได้ทั้งหมดรวม รวมถึงขีดความสามารถของบุคลากรผู้รับการถ่ายทอดยังไม่มีทักษะในการดำเนินการ

แนวทางการพัฒนาบุคลากร

การพัฒนาบุคลากรทั่วไปมีวัตถุประสงค์เพื่อแก้ไขการปฏิบัติงานที่มีประสิทธิภาพต่ำ เพื่อเสริมสร้างสมรรถภาพในการทำงาน เพื่อเตรียมบุคลากรพร้อมจะรับตำแหน่งที่สูงขึ้น และเพื่อสร้างความเข้าใจให้เกิดการประสานงานและปฏิบัติงานร่วมกันได้อย่างมีประสิทธิภาพ โดยการพัฒนาบุคลากรกองทัพอากาศ มีการดำเนินการทั้งภายในกองทัพอากาศโดยเมื่อบรรจุเข้าดำรงตำแหน่งจะจัดให้มีการเข้ารับการศึกษาในหลักสูตรที่เกี่ยวข้องกับการปฏิบัติหน้าที่ รวมถึงมีการจัดอบรมระยะสั้นเพื่อให้ทราบถึงการเปลี่ยนแปลงเทคโนโลยีและวิธีการปฏิบัติ และมีการจัดส่งไปฝึกศึกษา อบรมจากหน่วยงานภายนอก บริษัทเอกชน และมหาวิทยาลัย เพื่อเพิ่มประสิทธิภาพ รวมถึงมีพิจารณาเข้าดำรงตำแหน่งที่สูงขึ้น ดังนี้

1. บุคลากร

จากการปฏิบัติงานสามารถวิเคราะห์การดำเนินการของบุคลากรเป็นระดับ ดังนี้

1.1 ผู้บังคับบัญชาชั้นสูง มีขีดความสามารถดำเนินการได้เป็นอย่างดี พร้อมทั้งสนับสนุนการดำเนินการในทุกด้าน ทำให้งานด้านไซเบอร์ดำเนินการได้อย่างต่อเนื่อง

1.2 ผู้บังคับบัญชาระดับหัวหน้าหน่วยขึ้นตรงกองทัพอากาศ มีความเข้าใจในการดำเนินการด้านไซเบอร์เป็นอย่างดี แต่ยังพบข้อบกพร่องด้านเทคโนโลยีในระบบ เห็นควรให้มีการควบคุมและกำกับดูแล การดำเนินงานด้านไซเบอร์ภายในหน่วยให้ปฏิบัติตามแผนงานให้เกิดประสิทธิภาพสูงสุด

1.3 ระดับผู้ปฏิบัติงาน มีประสิทธิภาพปฏิบัติงานได้ตามที่มีการสั่งการ หน้าที่และแผนงานกำหนดไว้ แต่ไม่สามารถแก้ไขปัญหาในส่วนที่เกิดขึ้นนอกเหนือจากนี้ได้ รวมถึงบุคลากรมีจำนวนไม่พอเพียงทำให้ไม่สามารถตรวจระบบได้อย่างทั่วถึง จึงเห็นควรให้มีการฝึกอบรมทบทวนขั้นตอนการดำเนินงานด้านไซเบอร์จากส่วนกลาง และทบทวนการดำเนินการต่างๆ ตามภารกิจและแผนงานที่เกี่ยวข้องและการดำเนินการตามเทคโนโลยีที่เปลี่ยนแปลง รวมถึงควรบรรจุเพิ่มเติมบุคลากรให้เหมาะสมกับภารกิจด้วย

1.4 ระดับผู้ตรวจสอบและผู้ที่เป็นวิทยากรให้การอบรม จำนวนผู้ตรวจสอบระบบและผู้ที่เป็นวิทยากรมีไม่เพียงพอ เห็นควรให้เร่งจัดการอบรมและพัฒนาคลากรที่เกี่ยวข้อง รวมถึงบุคลากรของหน่วยขึ้นตรงกองทัพอากาศให้มีขีดความสามารถในการตรวจสอบระบบได้อย่างมีประสิทธิภาพเพิ่มเติม อีกทั้งเห็นควรให้จัดส่งบุคลากรไปอบรมกับหน่วยงานภายนอก มหาวิทยาลัยหรือบริษัทที่เกี่ยวข้องตามความเหมาะสมกับภารกิจที่ได้รับ พร้อมทั้งและให้ผู้ตรวจสอบและผู้ที่เป็นวิทยากรจัดทำเอกสารเพื่อเป็นคู่มือดำเนินการด้วย และเห็นควรบรรจุบุคลากรเพิ่มเติมให้เหมาะสมกับภารกิจด้วย

1.5 ระดับผู้รับผิดชอบดูแลระบบ เห็นควรให้ มีการควบคุมและกำกับดูแลบุคลากรในการทบทวนขั้นตอนการปฏิบัติหน้าที่อย่างต่อเนื่อง รวมถึงเมื่อมีการจัดหาเทคโนโลยีใหม่มาใช้งานต้องจัดให้ผู้รับผิดชอบระบบศึกษาเรียนรู้เทคโนโลยีใหม่อย่างเต็มขีดความสามารถ พร้อมให้จัดทำคู่มือการใช้งานเทคโนโลยีเป็นเอกสารเพื่อถ่ายทอดให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง และควรเพิ่มบุคลากรให้เหมาะสมกับภารกิจด้วย

1.6 ระดับเจ้าหน้าที่ทำงานด้านการรักษาความปลอดภัยระบบสารสนเทศ นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศ สามารถดำเนินการตามขั้นตอนด้านไซเบอร์ที่กำหนดไว้ แต่ยังไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ เห็นควรให้ ผู้รับผิดชอบจัดการฝึกอบรม ทบทวนและพัฒนาการดำเนินการด้านไซเบอร์เพิ่มเติมอย่างต่อเนื่อง

2. การดำเนินการด้านการฝึกศึกษาอบรม

2.1 จัดทำสูตรพื้นฐานรองรับผู้ปฏิบัติงานและผู้บริหาร ได้แก่ หลักสูตรสงครามไซเบอร์สำหรับนักเรียนสูตรจ่าอากาศ โรงเรียนจ่าอากาศ กรมยุทธศึกษาทหารอากาศ และสำหรับผู้จบการศึกษาจากโรงเรียนจ่าอากาศฯ หลักสูตรเจ้าหน้าที่เทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ และหลักสูตรนายทหารเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ สำหรับบุคลากรที่ได้รับการบรรจุแต่งตั้งเข้ามาทำงานในกองทัพอากาศ หรือสำหรับบุคลากรที่จะเข้ามาปฏิบัติงานด้านสารสนเทศหลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศสำหรับบุคลากรเมื่อปฏิบัติงานได้ระยะหนึ่ง หลักสูตรสงครามไซเบอร์สำหรับนายทหารนักเรียนเสนาธิการทหารอากาศ โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ และมีการจัดอบรมสัมมนาให้กับผู้บังคับบัญชาตามระยะเวลาที่เหมาะสม

2.2 จัดทำหลักสูตรเฉพาะ การอบรมเกี่ยวกับการประเมินและตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ให้กับผู้ปฏิบัติงานด้านรักษาความปลอดภัยระบบสารสนเทศ

2.3 ส่งบุคลากรเข้ารับการฝึกอบรม มีการส่งบุคลากรเข้าฝึกศึกษาและอบรม กับบริษัทเอกชนและหน่วยงานภายนอก รวมถึงส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานของรัฐ ซึ่งเป็นการสร้างองค์ความรู้ ทักษะการปฏิบัติงานของบุคลากรอีกทางหนึ่ง รวมถึงเป็นการสร้างความสัมพันธ์ในการปฏิบัติงานร่วมกับบุคลากรของหน่วยงานภายนอกด้วย

2.4 จัดการฝึกอบรมการในการเลื่อนระดับความชำนาญ มีการจัดการฝึกอบรมให้กับบุคลากรที่มีคุณสมบัติครบถ้วนเพื่อพิจารณา เลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น ซึ่งดำเนินการได้อย่างครบถ้วนและเป็นไปตามขั้นตอนระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ ที่กำหนดในการความรู้ความชำนาญให้กับบุคลากร

2.5 สร้างจิตสำนึกและการแจ้งเตือน มีการเสริมสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ ในการบรรยายพิเศษที่สถาบันการศึกษา หน่วยงาน และมีการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ส่งให้ทางเมล์อิเล็กทรอนิกส์ของข้าราชการ พนักงานราชการและลูกจ้างกองทัพอากาศ

จากการที่กองทัพอากาศได้จัดทำหลักสูตรที่เกี่ยวข้องดังกล่าวดำเนินการมาเป็นอย่างมีระบบและต่อเนื่อง แต่อย่างไรก็ดีเทคโนโลยีพัฒนาอย่างรวดเร็ว จึงเห็นควรให้จัดเตรียมหลักสูตรเพิ่มเติมเพื่อรองรับเทคโนโลยีใหม่และทบทวนหลักสูตรที่ใช้ในการฝึกศึกษาและอบรมด้านไซเบอร์อย่างต่อเนื่อง รวมถึงพิจารณาสถานศึกษาภายนอกเพื่อส่งบุคลากรไปฝึกศึกษาและอบรมตามความเหมาะสม และให้มีการทบทวนการปฏิบัติงานให้กับนายทหารเทคโนโลยีสารสเทศและผู้ที่ปฏิบัติหน้าที่นายทหารรักษาความปลอดภัยระบบสารสนเทศอย่างต่อเนื่อง พร้อมทั้งสร้างจิตสำนึกและการแจ้งเตือนด้านไซเบอร์ทุกครั้งเมื่อมีโอกาส

3. ปัจจัยอื่น ๆ ที่เกี่ยวข้อง

เมื่อวิเคราะห์องค์ประกอบที่เกี่ยวข้องเห็นควรดำเนินการเพิ่มเติม ดังนี้

3.1 จัดทำและปรับปรุงการขั้นตอนวิธีการตรวจสอบระบบให้ทันสมัย รวมทั้งให้มีการสุ่มตรวจสอบระบบในภาพรวมหากพบข้อบกพร่องให้รับแจ้งหน่วยเกี่ยวข้อง เพื่อแก้ไขโดยด่วน หากพบบุคลากรละเมิดให้พิจารณาลงทัณฑ์ตามแนวทางที่กองทัพอากาศกำหนด

3.2 จัดให้มีการทบทวนความรู้และการปฏิบัติงาน และการดำเนินการตามแผนให้กับผู้รับผิดชอบและดูแลระบบที่อยู่ในความรับผิดชอบอย่างต่อเนื่อง พร้อมทั้งจัดทำคู่มือคำแนะนำการใช้งานระบบอุปกรณ์ที่มีอยู่และระบบอุปกรณ์ที่จัดหามาใหม่ เพื่อเป็นคู่มือการใช้งานและใช้ทบทวนบุคลากร

3.3 เร่งรัดการจัดทำแนวความคิดการปฏิบัติการไซเบอร์ของกองทัพอากาศและแผนเผชิญเหตุเมื่อระบบสารสนเทศถูกโจมตี

3.4 จัดทำข้อตกลงกับหน่วยงานและสถานศึกษาภายนอก เพื่อแลกเปลี่ยนด้านการฝึกศึกษา อบรม การวิจัยและพัฒนาด้านไซเบอร์ พร้อมทั้งให้การสนับสนุนงบประมาณด้านการวิจัยและพัฒนาการปฏิบัติการด้านไซเบอร์ให้กับบุคลากรและหน่วยในกองทัพ

3.5 พิจารณาจัดส่งบุคลากรไปอบรมภายนอกหน่วย จนกระทั่งได้ใบรับรองความสามารถ (Cyber Certification) ทั้งด้านเชิงป้องกันและเชิงป้องปราม และให้นำความรู้ความสามารถกลับมาถ่ายทอดให้กับบุคลากรภายในกองทัพ

3.6 ส่งเสริมบุคลากรเข้าร่วมการฝึก การฝึกร่วม/ผสม ทั้งในประเทศและต่างประเทศ และบุคลากรเข้าศึกษาอบรมดูงานในหน่วยงานที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ และร่วมการประชุมด้านไซเบอร์ในทุกระดับ

3.7 โครงสร้างการจัดหน่วย ปัจจุบันหน่วยรับผิดชอบด้านไซเบอร์โดยตรงจัดตั้งเป็นระดับกอง (กองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ) เห็นควรพิจารณาทบทวนเพื่อรองรับการปฏิบัติภารกิจที่จะเกิดขึ้นในอนาคต โดยให้มีแต่ละส่วนงานรับผิดชอบ คือ ส่วนธุรการ ส่วนแผน ส่วนงานป้องกัน ส่วนงานตรวจจับ ส่วนงานตอบสนอง ส่วนงานฟื้นฟู และส่วนงานป้องปราม

3.8 การสร้างแรงจูงใจ การสร้างแรงจูงให้ให้กับผู้ปฏิบัติงาน เห็นควรให้ผู้บังคับบัญชาผลักดันในการดำเนินการขอเงินเพิ่มพิเศษ เป็นค่าตอบแทนให้กับผู้ปฏิบัติงานด้านไซเบอร์ ซึ่งเป็นเงินเพิ่มพิเศษนอกจากเงินเดือนที่ได้รับในทุกระดับชั้น โดยจะต้องกำหนดตำแหน่ง คุณสมบัติและหลักสูตรการศึกษาที่ชัดเจนในการได้รับค่าตอบแทนด้วย.

3.9 ข้อจำกัดที่ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งานติดตั้งใช้งาน 2 สถานที่ ถึงแม้ทางเทคนิคจะดำเนินการได้ แต่ควรติดตั้งใช้งานภายในพื้นที่เดียวกันเพื่อสะดวกต่อการปฏิบัติงานของบุคคลากรในการเฝ้าตรวจโดยไม่ต้องใช้บุคลากรในการปฏิบัติงานเพิ่มขึ้น

3.10 สร้างระบบการจัดการความรู้ (Knowledge Management System) ให้ครอบคลุมเทคโนโลยีที่มีใช้งาน

สรุป

การวิเคราะห์ข้อมูล หน่วยงานรับผิดชอบ ปัจจัยที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ วงรอบการปฏิบัติทางไซเบอร์ (วงรอบการป้องกันทางไซเบอร์ และวงรอบการป้องปราม (โจมตีทางไซเบอร์) ปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์ (ขบวนการ นโยบาย แผนงาน, บุคลากรและเทคโนโลยี) ประสิทธิภาพ ข้อจำกัด (สถานที่ งบประมาณ เทคโนโลยี) ปัญหา (ด้านนโยบาย แผน และการปฏิบัติที่เกี่ยวข้อง, ด้านบุคลากร และด้านเทคโนโลยี) แนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้อง ซึ่งได้รับข้อมูลจากการรวบผลการดำเนินการที่ผ่านมาและจากผู้เกี่ยวข้องกับการปฏิบัติงานด้านไซเบอร์ และจากการสัมภาษณ์ผู้บังคับบัญชา ทำให้ได้รับทราบถึงผลการดำเนินการ ปัญหาและแนวทางการแก้ไขปัญหา พร้อมทั้งข้อเสนอแนะแนวทางการดำเนินการของกองทัพอากาศ ให้เกิดประสิทธิภาพตามขีดความสามารถและงบประมาณที่ได้รับ โดยเฉพาะการพัฒนาบุคลากรของกองทัพอากาศ

บทที่ 5
สรุปและข้อเสนอแนะ

สรุป

จากผลการศึกษาวิจัย จะเห็นได้ว่ากองทัพอากาศได้ตระหนักถึงความสำคัญการปฏิบัติงานด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามที่อาจจะเกิดขึ้น โดยการจัดตั้งหน่วยงานรับผิดชอบ จัดหาเทคโนโลยีสารสนเทศพร้อมอุปกรณ์และระบบป้องกันมาใช้ในการปฏิบัติภารกิจ จัดทำแผนงานในการดำเนินการที่เกี่ยวข้อง รวมถึงพัฒนาบุคลากรด้านสารสนเทศ พร้อมจัดให้มีการตรวจสอบระบบอย่างต่อเนื่อง สามารถตอบตามวัตถุประสงค์ได้ ดังนี้

1. สภาพปัญหาและข้อจำกัด การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

1.1 ปัญหาและข้อจำกัด

1.1.1 ปัญหา

1.1.1.1 บุคลากรบางส่วนละเลยไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ ทำให้มีช่องโหว่ในระบบ มีไวรัสและมัลแวร์เข้ามาในระบบทำความเสียหายให้กับคอมพิวเตอร์ โปรแกรมและข้อมูล

1.1.1.2 บุคลากรด้านไซเบอร์ มีจำนวนไม่เพียงพอและขาดทักษะในการปฏิบัติภารกิจ ทำให้ระบบอาจถูกโจมตีจากผู้ไม่หวังดี ควรฝึกอบรมทบทวนให้บุคลากรให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

1.1.1.3 การศึกษาเฉพาะด้านยังไม่ครอบคลุม หลักสูตรการศึกษายังขาดงานด้านที่สำคัญ เช่น ด้านการเก็บหลักฐานเมื่อถูกโจมตี เป็นต้น และ ไม่มีนักพัฒนาโปรแกรมประสงค์ร้าย ควรสนับสนุนงบประมาณและจัดบุคลากรเข้ารับการศึกษาตามหลักสูตร และเร่งผลิตบุคลากรให้พร้อมปฏิบัติงาน

1.1.1.4 ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 ใช้งานมามากกว่า 5 ปี อาจไม่ครอบคลุมการปฏิบัติ ควรเร่งทบทวนปรับแก้ไขเพิ่มเติม

1.1.1.5 ระบบการจัดการความรู้ ยังไม่ครอบคลุมเทคโนโลยี เห็นควรให้ผู้เกี่ยวข้องรวบรวมองค์ความรู้และนำเข้าระบบเพื่อให้สามารถสืบค้นและเป็นแนวทางในการปฏิบัติ

1.1.1.6 คู่มือการใช้งานอุปกรณ์ในเบื้องต้นมีแต่ไม่ครอบคลุมการใช้งานโดยเฉพาะเทคโนโลยีที่จัดหามาใช้งานใหม่ รวมถึงคู่มือการปฏิบัติเมื่อถูกโจมตีระบบสารสนเทศและการสื่อสารยังไม่มีการจัดทำแจกจ่ายให้หน่วยเกี่ยวข้อง ควรเร่งดำเนินการอย่างเร่งด่วน

1.1.2 ข้อจำกัด

1.1.2.1 ด้านสถานที่ ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งานติดตั้งใช้งาน 2 สถานที่ ถึงแม้ทางเทคนิคจะดำเนินการได้ แต่ควรติดตั้งใช้งานภายในพื้นที่เดียวกันเพื่อสะดวกต่อการปฏิบัติงานของบุคคลากรในการเฝ้าตรวจและไม่ต้องใช้บุคลากรในการปฏิบัติงานเพิ่มขึ้น

1.1.2.2 ด้านลิขสิทธิ์ ระบบเทคโนโลยีที่จัดหามาใช้งานต้องมีลิขสิทธิ์จากบริษัทผู้ผลิต ทำให้งบประมาณมากขึ้น

1.1.2.3 ด้านเทคโนโลยี เทคโนโลยีมีการพัฒนาตลอดเวลาทำให้ต้องติดตามและจัดหามาไว้ใช้งานเพื่อป้องกันช่องโหว่ที่อาจจะเกิดขึ้น ส่งผลกระทบต่องบประมาณในภาพรวมของกองทัพ

2. ปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

ปัจจัยการปฏิบัติการไซเบอร์ กองทัพอากาศมีการปฏิบัติตามองค์ประกอบ 3 องค์ประกอบ ดังนี้

2.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง

กองทัพอากาศมีการดำเนินการ จัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 จัดทำนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ จัดทำโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ จัดการแข่งขัน Cyber Operations Contest รวมถึงอยู่ระหว่างการจัดตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของกองทัพอากาศและจัดทำแนวความคิดการปฏิบัติการไซเบอร์ของกองทัพอากาศ

การดำเนินการตามแผนและขั้นตอนดังกล่าวหากสามารถดำเนินการได้ตามแผนจะทำให้ปฏิบัติภารกิจด้านนี้เป็นไปอย่างมีประสิทธิภาพ ส่วนที่มีผลมากคือ บุคลากรมักละเลยไม่ปฏิบัติตาม และไม่ได้รับการสนับสนุนงบประมาณตามแผนและโครงการที่กำหนดไว้ประสิทธิภาพในการปฏิบัติภารกิจจะไม่มีบรรลุตามวัตถุประสงค์

2.2 ปัจจัยด้านเทคโนโลยี

กองทัพอากาศได้ดำเนินการจัดหาระบบเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องปรามดังนี้ เทคโนโลยีทั้งเชิงป้องกัน เช่น ระบบบริหารจัดการเครือข่าย ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบป้องกันการรั่วไหลของข้อมูล ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรอง ระบบจำลองการโจมตีในรูปแบบการระดมโจมตีเพื่อให้เครื่องแม่ข่ายปฏิเสธการให้บริการ ระบบรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์ ระบบป้องกันภัยคุกคามสำหรับระบบเครื่องแม่ข่ายแบบคลาวด์ ระบบเข้ารหัสข้อมูล และระบบจำลองยุทธทางไซเบอร์ เป็นต้น เทคโนโลยีเชิงป้องปราม เช่น ระบบเครือข่ายเพื่อการซ่อนพราง ระบบบริหารจัดการช่องโหว่ในระบบคอมพิวเตอร์และเครือข่าย ระบบปฏิบัติการด้านการรักษาความปลอดภัยเชิงรุก ระบบข่าวกรองทางไซเบอร์ เป็นต้น

การจัดหาเทคโนโลยีมาใช้งานในกองทัพ มีการจัดหาตามแผนงานที่กำหนดไว้ตามโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศ แต่จากการที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว จึงต้องมีการจัดเทคโนโลยีใหม่

มาใช้งานอย่างต่อเนื่อง โดยจะส่งผลกระทบต่อบุคลากรที่รับผิดชอบใช้งานและงบประมาณของกองทัพอากาศ

2.3 ปัจจัยด้านบุคลากร

กองทัพอากาศมีการดำเนินการด้านความรู้เพื่อรองรับบุคลากร ดังนี้

2.3.1 หลักสูตรพื้นฐานรองรับผู้ปฏิบัติงานและผู้บริหาร หลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศเมื่อมีการจัดอบรมสัมมนาให้กับผู้บังคับบัญชา การอบรมเกี่ยวกับการประเมินและตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ให้กับผู้ปฏิบัติงานด้านรักษาความปลอดภัยระบบสารสนเทศ

2.3.2 ส่งบุคลากรเข้ารับการฝึกอบรม กับ บริษัทเอกชนและหน่วยงานภายนอก รวมถึงส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานของรัฐ

2.3.3 จัดการฝึกอบรมการในการเลื่อนระดับความชำนาญให้กับบุคลากรที่มีคุณสมบัติครบเพื่อพิจารณา เลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น รวมถึงการพิจารณาในการดำรงตำแหน่ง พิจารณาตามคุณสมบัติตามขั้นตอน แต่ตำแหน่งดังกล่าวเป็นไปตามโครงสร้าง และอัตรากำลังพลที่กำหนดไว้ จึงพิจารณาได้ไม่เกินตำแหน่งตามโครงสร้างดังกล่าว

2.3.4 การสร้างจิตสำนึกและการแจ้งเตือน มีการเสริมสร้างจิตสำนึกด้านการรักษาความปลอดภัยทางไซเบอร์ ในการบรรยายพิเศษที่สถาบันการศึกษา หน่วยงาน และมีการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ส่งให้ทางเมล์อิเล็กทรอนิกส์ ของข้าราชการ พนักงานราชการและลูกจ้างกองทัพอากาศ

ตามที่กองทัพอากาศได้ดำเนินการที่ผ่านมานั้น สามารถให้ความรู้และความสามารถบุคลากรได้ในระดับหนึ่ง แต่ยังขาดทักษะและความชำนาญในการปฏิบัติงาน จึงเห็นควรต้องมีการฝึกอบรมและทบทวนอย่างต่อเนื่อง รวมถึงต้องมีเอกสารคู่มือการปฏิบัติงานและการจัดองความรู้ด้วย พร้อมทั้งควรส่งบุคลากรไปฝึกศึกษาอบรมจากหน่วยงานภายนอกตามความเหมาะสม

3. แนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการภารกิจด้านไซเบอร์ของกองทัพอากาศ

3.1 การพัฒนาบุคลากร

การพัฒนาบุคลากรกองทัพอากาศ มีข้อเสนอแนะในการดำเนินการ ดังนี้

3.1.1 บุคลากร

3.1.1.1 ผู้บังคับบัญชาระดับหัวหน้าหน่วยขึ้นตรงกองทัพอากาศมีความเข้าใจในการดำเนินการด้านไซเบอร์เป็นอย่างดี แต่ควรมีควบคุมและกำกับดูแล การดำเนินงานด้านไซเบอร์ภายในหน่วยให้ปฏิบัติตามแผนงานให้เกิดประสิทธิภาพสูงสุด

3.1.1.2 ระดับผู้ปฏิบัติงาน มีประสิทธิภาพปฏิบัติงานได้ตามที่มีการสั่งการ หน้าที่และแผนงานกำหนดไว้ แต่ไม่สามารถแก้ไขปัญหาในส่วนที่เกิดขึ้นนอกเหนือจากนี้ได้ จึงเห็นควรให้มีการฝึกอบรมทบทวนขั้นตอนการดำเนินงานด้านไซเบอร์อย่างต่อเนื่อง

3.1.1.3 ระดับผู้ตรวจสอบและผู้ที่เป็นวิทยากรให้การอบรม จำนวนผู้ตรวจสอบระบบมีไม่เพียงพอ เห็นควรให้เร่งจัดการอบรมและพัฒนาคลากรที่เกี่ยวข้องให้มีขีดความสามารถในการตรวจสอบระบบได้อย่างมีประสิทธิภาพเพิ่มเติม อีกทั้งเห็นควรให้จัดส่งไป

อบรมกับหน่วยงานภายนอก มหาวิทยาลัย หรือบริษัทที่เกี่ยวข้อง และให้ผู้ตรวจสอบและวิทยากรจัดทำเอกสารเพื่อเป็นคู่มือดำเนินการด้วย

3.1.1.4 ระดับผู้รับผิดชอบดูแลระบบ เห็นควรให้ มีการควบคุมและกำกับดูแลบุคลากร ในการทบทวนขั้นตอนการปฏิบัติหน้าที่อย่างต่อเนื่อง พร้อมให้จัดทำคู่มือการใช้งานเทคโนโลยีเป็นเอกสารเพื่อถ่ายทอดให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง

3.1.1.5 ระดับเจ้าหน้าที่ทำงานด้านการรักษาความปลอดภัยระบบสารสนเทศ นายทหารรักษาความปลอดภัยระบบสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศ สามารถดำเนินการตามขั้นตอนด้านไซเบอร์ที่กำหนดไว้ แต่ยังไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ เห็นควรให้ผู้รับผิดชอบจัดการฝึกอบรม ทบทวนและพัฒนาการดำเนินการด้านไซเบอร์เพิ่มเติม พร้อมทั้งเข้ารับการฝึกกับระบบจำลองยุทธทางไซเบอร์อย่างต่อเนื่อง

3.1.1.6 การบรรจุกำลังพลให้หน่วย ในภาพรวมควรบรรจุกำลังพลทุกระดับให้เพียงพอต่อการปฏิบัติภารกิจโดยไม่น้อยกว่า ร้อยละ 60 ของอัตราอนุมัติกำลังพล และต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจนว่าต้องการบุคลากรที่มีคุณวุฒิและความรู้ความสามารถที่ตรงกับการปฏิบัติงาน

3.1.2 การดำเนินการด้านหลักสูตรและที่เกี่ยวข้อง

3.1.2.1 จัดเตรียมหลักสูตรและทบทวนหลักสูตรที่ใช้ในการฝึกศึกษาและอบรมด้านไซเบอร์อย่างต่อเนื่อง รวมถึงพิจารณาสถานศึกษาภายนอกเพื่อส่งบุคลากรไปฝึกศึกษาและอบรมให้เหมาะสมกับตามความเหมาะสม

3.1.2.2 จัดทำและปรับปรุงการตรวจสอบระบบให้ทันสมัย รวมทั้งให้มีการสุ่มตรวจสอบระบบในภาพรวมหากพบข้อบกพร่องให้แจ้งหน่วยเกี่ยวข้องทราบ เมื่อพบบุคลากรกระทำผิดให้พิจารณาลงทัณฑ์ตามแนวทางที่กองทัพอากาศกำหนด

3.1.2.3 จัดให้มีการทบทวนความรู้และการปฏิบัติงาน และการดำเนินการตามแผนที่เกี่ยวข้องให้กับผู้รับผิดชอบและดูแลระบบที่อยู่ในความรับผิดชอบอย่างต่อเนื่อง

3.1.2.4 จัดทำข้อตกลงกับหน่วยงานและสถานศึกษาภายนอก เพื่อแลกเปลี่ยนด้านการฝึกศึกษา อบรม การวิจัยและพัฒนาด้านไซเบอร์ พร้อมทั้งให้การสนับสนุนงบประมาณด้านการวิจัยและพัฒนาการปฏิบัติการด้านไซเบอร์ให้กับบุคลากรและหน่วยในกองทัพ

3.1.2.5 พิจารณาจัดส่งบุคลากรไปอบรมภายนอกหน่วย จนกระทั่งได้ใบรับรองความสามารถ (Cyber Certification) และให้นำความรู้ความสามารถกลับมาถ่ายทอดให้กับบุคลากรภายในกองทัพ

3.1.2.6 ส่งเสริมบุคลากรเข้าร่วมการฝึก การฝึกร่วม/ผสม และบุคลากรเข้าศึกษาอบรมดูงานในประเทศและต่างประเทศ และร่วมการประชุมด้านไซเบอร์ในทุกระดับ

3.2 ปัจจัยที่เกี่ยวข้อง

3.2.1 โครงสร้างการจัดหน่วย ปัจจุบันหน่วยรับผิดชอบด้านไซเบอร์โดยตรงจัดตั้งเป็นระดับกอง (กองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ) เห็นควรพิจารณาให้ปรับขยายอัตราเพื่อรองรับการปฏิบัติภารกิจที่จะเกิดขึ้นในอนาคต

3.2.2 การจัดทำแผนและแนวทางการปฏิบัติงานให้ครอบคลุมการปฏิบัติงาน ปรับปรุงแผนที่เกี่ยวข้อง รวมถึงแนวทางการตรวจสอบระบบที่กำหนดไว้ในแผนให้ทันสมัยครอบคลุมการปฏิบัติงาน ควรจัดทำแผนและคู่มือการปฏิบัติเมื่อมีเหตุการณ์แจกจ่ายให้หน่วยเกี่ยวข้อง อีกทั้งควรจัดทำคู่มือการใช้งานระบบอุปกรณ์และโปรแกรมที่มีใช้งานอยู่และที่จะจัดหามาใหม่เพิ่มเติมเมื่อได้รับระบบ

3.2.3 การสร้างแรงจูงใจ การสร้างแรงจูงให้ให้กับผู้ปฏิบัติภารกิจ เห็นควรให้ผู้บังคับบัญชาผลักดันในการดำเนินการขอเงินเพิ่มพิเศษ เป็นค่าตอบแทนให้กับผู้ปฏิบัติงานด้านไซเบอร์

3.2.4 ระบบและอุปกรณ์ ระบบอุปกรณ์และโปรแกรมที่มีใช้งาน ต้องมีลิขสิทธิ์จากบริษัทผู้ผลิตและจำเป็นต้องต่อเนื่องทุกปีนั้น ควรสนับสนุนงบประมาณเป็นค่าลิขสิทธิ์ และจัดหาเทคโนโลยีที่ทันสมัยตามความจำเป็นใช้งานโดยเฉพาะเทคโนโลยีเชิงป้องปราม

3.2.5 จัดหาเทคโนโลยีที่จำเป็นมาใช้งาน และพัฒนายุทโธปกรณ์ทางไซเบอร์โดยเน้นที่การพัฒนา แลกเปลี่ยน หรือใช้งานทรัพยากรทางไซเบอร์ร่วมกับหน่วยงานด้านความมั่นคง

3.2.6 ระบบที่มีความจำเป็นทางด้านยุทธการเห็นควรให้จัดทำเป็นระบบปิดให้สามารถเชื่อมต่อได้เฉพาะผู้ใช้งานในระบบเท่านั้น โดยไม่สามารถเชื่อมต่อกับอินเทอร์เน็ตภายนอกหรือมีการเชื่อมต่อจากอุปกรณ์ที่ไม่เกี่ยวข้องกับระบบ หากมีการละเมิดต้องลงทัณฑ์ตามระเบียบที่กองทัพอากาศกำหนด

3.2.7 ปัจจัยสถานที่ เนื่องจากมีการติดตั้งอุปกรณ์เชิงรับไว้ 2 แห่ง หากมีการสร้างอาคารใหม่รองรับงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เห็นควรให้ติดตั้งระบบด้านไซเบอร์เชิงป้องกันไว้ภายในอาคารเดียวกันเพื่อสะดวกต่อการปฏิบัติงาน

3.2.8 จัดทำระบบการจัดการความรู้ (Knowledge Management System) ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพ และกำหนดให้ใช้งานได้ตามสิทธิ์ที่ได้รับ

ข้อเสนอแนะ

1. จากความแพร่หลายของเทคโนโลยีสารสนเทศ การเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ผ่านอินเทอร์เน็ตภายในกองทัพอากาศและหน่วยเกี่ยวข้อง ทำให้เกิดการติดต่อสื่อสารแลกเปลี่ยนข้อมูลได้อย่างรวดเร็ว โดยสามารถติดต่อกันได้ทุกสถานที่ทำให้ผู้ไม่ประสงค์ดีอาจเข้ามาโจมตีทำลายข้อมูลหรือการติดต่อเพื่อไม่ให้ระบบคอมพิวเตอร์ใช้งานได้ส่งผลกระทบให้ระบบควบคุมบังคับบัญชาและระบบที่จำเป็นในการปฏิบัติงานไม่สามารถใช้งานได้ ปัจจุบันโครงสร้างและอัตราด้านไซเบอร์ที่ได้รับการอนุมัติไว้อาจจะไม่สามารถรองรับการปฏิบัติงานด้านไซเบอร์ในอนาคต เห็นสมควรให้มีการศึกษาวิจัยเพิ่มเติมในส่วนของโครงสร้างและอัตราของหน่วยงานด้านไซเบอร์ให้สอดคล้องกับงานเชิงป้องกันและป้องปรามต่อไป

2. การพัฒนาบุคลากร ควรมีการจัดการฝึกศึกษา การอบรม ทบทวน และพิจารณาส่งบุคลากรไปศึกษานอกหน่วยให้กับบุคลากรทุกระดับ ได้แก่ ระดับผู้ปฏิบัติงาน ระดับผู้ตรวจสอบและผู้ที่เป็นวิทยากรให้การอบรม ระดับผู้รับผิดชอบดูแลระบบ ระดับเจ้าหน้าที่ทำงานด้านการรักษาความปลอดภัยระบบสารสนเทศ รวมถึงให้มีการจัดทำคู่มือการปฏิบัติงานเพื่อให้ผู้ที่มารับหน้าที่ใหม่ทราบถึงแนวทางการปฏิบัติงาน และต้องนำบุคลากรที่ได้จากการจัดการแข่งขัน Cyber Operations Contest

มาใช้งานให้เกิดประโยชน์สูงสุดโดยเฉพาะการตรวจสอบระบบเทคโนโลยีสารสนเทศที่กองทัพอากาศมีใช้งาน อีกทั้งควรบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติภารงานด้านไซเบอร์ทั้งเชิงป้องกันและเชิงป้องปราม และต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน พร้อมกับให้ผู้บังคับบัญชาและผู้รับผิดชอบผลักดันการดำเนินการขอเงินเพิ่มพิเศษให้กับผู้ปฏิบัติงานด้านไซเบอร์

3. ทบทวนและปรับปรุง ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ นโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกองทัพอากาศ โครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ แผนแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศให้ทันสมัยและครอบคลุมการปฏิบัติงาน พร้อมทั้งจัดทำแผนงานและคู่มือการปฏิบัติเมื่อมีเหตุการณ์ถูกโจมตีทางไซเบอร์แจกจ่ายให้หน่วยเกี่ยวข้อง และเร่งจัดทำแนวความคิดการปฏิบัติการไซเบอร์ของกองทัพอากาศเพื่อให้ผู้เกี่ยวข้องทราบและปฏิบัติเป็นแนวทางเดียวกัน รวมถึงควรจัดให้มีการซักซ้อมการปฏิบัติตามแผนงานด้านไซเบอร์ให้กับผู้เกี่ยวข้องอย่างต่อเนื่อง อีกทั้งควรจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพในปัจจุบันและที่จะจัดหามาใช้งานในอนาคต

4. สนับสนุนงบประมาณให้เพียงพอต่อการปฏิบัติงานด้านไซเบอร์ ทั้งด้านบุคลากร ด้านการจัดหาระบบเทคโนโลยีที่ทันสมัย เช่น เทคโนโลยีเชิงป้องกันควรจัดหาระบบตรวจสอบเฝ้าระวังระบบตรวจจับและป้องกันการบุกรุก ระบบป้องกันภัยคุกคาม ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูล และระบบอื่นที่เกี่ยวข้องที่มีประสิทธิภาพสูงเพื่อปิดช่องโหว่ที่อาจจะเกิดขึ้น ส่วนเทคโนโลยีเชิงป้องปรามควรจัดหา ระบบเข้ารหัสข้อมูล ระบบปฏิบัติการด้านการรักษาความปลอดภัยเชิงรุก ระบบตรวจสอบตรวจพิสูจน์หลักฐานทางไซเบอร์ และระบบจำลองยุทธทางไซเบอร์ที่มีประสิทธิภาพมาใช้งาน เป็นต้น รวมถึงสนับสนุนงบประมาณการจัดหาเทคโนโลยีที่ทันสมัยและค่าลิขสิทธิ์ของระบบเทคโนโลยีตามโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแผนแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศที่จัดทำไว้

5. หากมีการสร้างอาคารใหม่รองรับงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพอากาศอย่างเหมาะสม เห็นควรให้ติดตั้งระบบงานด้านไซเบอร์เชิงป้องกันไว้ภายในอาคารเดียวกันเพื่อสะดวกต่อการเฝ้าตรวจและเฝ้าระวังจากภัยคุกคามที่อาจจะเกิดขึ้น รวมถึงระบบที่มีความจำเป็นทางด้านยุทธการต้องจัดทำเป็นระบบปิดให้สามารถเชื่อมต่อได้เฉพาะผู้ใช้งานในระบบเท่านั้น หากพบบุคลากรกระทำผิดหรือฝ่าฝืนให้พิจารณาลงทัณฑ์ตามแนวทางที่กองทัพอากาศกำหนด

บรรณานุกรม

ภาษาไทย

หนังสือ

กรมกำลังพลทหารอากาศ. ระเบียบกองทัพอากาศว่าด้วยการแยกประเภทกำลังพลกองทัพอากาศ. กรุงเทพฯ : กองทัพอากาศ, 2552.

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพอากาศ. กรุงเทพฯ : กองทัพอากาศ, 2558.

เอกสารวิจัย

ประยูร ธรรมาธิวัฒน์, นาวาอากาศเอก. “แนวทางการพัฒนาขีดความสามารถการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศ”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557

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

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

สุทธิศักดิ์ สลักคำ, พลตรี. “ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557

อรัญ นำผล, พลเรือตรี. “การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2556

ฐานข้อมูลอิเล็กทรอนิกส์

“การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ : ความท้าทายของกองทัพบก”. (ออนไลน์). เข้าถึงได้จาก http://rittee1834.blogspot.com/2014/08/cyber-security-challenge-of-army.html, 2557.

“คู่มือ Cyber Security สำหรับประชาชน”. (ออนไลน์). เข้าถึงได้จาก http://www.nbtc.go.th/News/รวมบทความ-(1)/คู่มือ-Cyber-Security-สำหรับประชาชน.aspx.

“โครงสร้างกองทัพอากาศ”. (ออนไลน์). เข้าถึงได้จาก http://www.rtaf.mi.th/th/Pages/RTAFComponents.aspx, 2560.

“นโยบายผู้บัญชาการทหารอากาศ ประจำปีพุทธศักราช ๒๕๖๐ – ๒๕๖๑”. (ออนไลน์). เข้าถึงได้จาก http://www.rtaf.mi.th/th/Documents/Publication/RTAF_Policy_2560-2561.pdf, 2559.

“แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”. (ออนไลน์). เข้าถึงได้จาก http://www.rtna.ac.th/download/cyber/nationalcybersecurity.pdf.

“แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ”. (ออนไลน์). เข้าถึงได้จาก https://www.acisonline.net/?p=5040&lang=th, 2559.

“ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security”. (ออนไลน์). เข้าถึงได้จาก https://www.techtalkthai.com/cdic-2 0 1 6 -cyber-security-threats-and-trends/, 2559

“มาตรฐาน ISO/IEC 27001 : 2013”. (ออนไลน์). เข้าถึงได้จาก http://www.rtna.ac.th/download/27001-2013.pdf, 2556.

“ยุทธศาสตร์กองทัพอากาศ 20 ปี”. (ออนไลน์). เข้าถึงได้จาก http://www.rtaf.mi.th/th/Documents/Publication/RTAF_Strategy_20y_2560-2579.pdf, 2560.

“ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.2552”. (ออนไลน์). เข้าถึงได้จาก http://wwwrtaf.mi.th/th/Documents/Publication/RTAF_ICT_E_book_v4.0_E.pdf.

“ร่างแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564”. (ออนไลน์). เข้าถึงได้จาก http://www.komchadluek.net/news/politic/239278, 2559.

“ศัพท์น่ารู้ในโลกไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก https://krujayja.wordpress.com/blog-d-d/class-room/คำศัพท์น่ารู้ในโลกไซเบอร์.

“หลักการและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก http://www.dmsc.moph.go.th/itc/userfiles/files/law_lecture%20(2).pdf.

ภาคผนวก

รายชื่อผู้ให้สัมภาษณ์เชิงลึก

1. รายชื่อผู้ให้การสัมภาษณ์เชิงลึก และผู้ให้ข้อมูลหน่วยเกี่ยวข้อง

1.1 รายชื่อผู้ให้การสัมภาษณ์เชิงลึก

1.1.1 พล.อ.ต.จิโรจ บำรุงลาภ	รองเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.2 พล.อ.ต.ชวาลา ราชวงศ์	ผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.3 พล.อ.ต.อัศวิน รุจาคม	ผู้อำนวยการสำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.4 น.อ.ประยูร ธรรมาธิวัฒน์	รองผู้อำนวยการ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.5 น.อ.มาโนช สุตวัฒน์	รองผู้อำนวยการ สำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.6 น.อ.วิเชียร เรืองพระยา	รองผู้อำนวยการ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.7 น.อ.สิทธิศักดิ์ สายเงิน	ผู้อำนวยการ ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ
1.1.8 น.อ.วิสุทธิ์ สมภักดี	ผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.9 น.อ.ณัฐวุฒิ สามไพบูลย์	รองผู้อำนวยการ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.10 น.อ.อภิชาติ บุตรสาทร	รองผู้อำนวยการ กองสื่อสารอิเล็กทรอนิกส์ สำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
1.1.11 น.อ.สมเกียรติ สุนทรสุข	นายทหารสารสนเทศและสงครามอิเล็กทรอนิกส์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

1.1.12 น.อ.อนุชัฏ อรุณรัศมีโชติ นายทหารฝ่ายเสนาธิการประจำกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

1.1.13 น.อ.ณัฐพงษ์ จันทร์ก้อน นายทหารสารสนเทศและสงครามอิเล็กทรอนิกส์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

1.1.14 น.ท.กิตติศักดิ์ สุวรรณรักษ์ หัวหน้าแผนกสงครามไซเบอร์ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

1.2 รายชื่อผู้ให้ข้อมูลหน่วยงานที่เกี่ยวข้อง

1.2.1 พล.ร.ต.พงศักดิ์ จุลกาญจน์ ร.น. ผู้อำนวยการสำนักสนับสนุนกรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

1.2.2 น.อ.ปิยะพันธุ์ ขันถม ผู้อำนวยการกองแผนไซเบอร์ศูนย์ไซเบอร์กลาโหม กรมเทคโนโลยีสารสนเทศและอวกาศ กระทรวงกลาโหม

2. หัวข้อที่ใช้ในการสัมภาษณ์เชิงลึก มีรายละเอียดดังนี้

2.1 ท่านคิดว่าการดำเนินการด้านไซเบอร์ ตามวงรอบการป้องกันทางไซเบอร์ (Cyber Defense) วงรอบการป้องกันทางไซเบอร์ของกองทัพอากาศ ดำเนินการอย่างไร

2.1.1 การป้องกัน (Protect)

2.1.2 การตรวจจับ (Detect)

2.1.3 การตอบสนอง (React)

2.1.4 การฟื้นฟู (Recover)

2.2 ท่านคิดว่าการดำเนินการด้านไซเบอร์ตามวงรอบการโจมตีทางไซเบอร์ (Cyber Attack) ของกองทัพอากาศ ดำเนินการอย่างไร

2.2.1 การรวบรวมข้อมูลเป้าหมาย (Information Gathering)

2.2.2 การตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification)

2.2.3 การปฏิบัติการโจมตี (Attack)

2.2.4 การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access)

2.2.5 การลบร่องรอยการโจมตี (Covering Tracks)

2.3 โครงสร้างหน่วยงานด้านไซเบอร์

2.3.1 กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

2.3.2 กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ

2.3.3 หน่วยขึ้นตรงกองทัพอากาศ

2.4 บุคลากรทุกระดับ
    2.4.1 บุคลากรมีประสิทธิภาพในระดับใด
    2.4.2 บุคลากรมีจำนวนเหมาะสมต่อการปฏิบัติภารกิจหรือไม่
    2.4.3 บุคลากรมีความรู้ความสามารถเพียงพอหรือไม่
2.5 สถานที่ทำงานมีความเหมาะสมและเพียงพอต่อการปฏิบัติหน้าที่หรือไม่ อย่างไร

ประวัติย่อผู้วิจัย

ชื่อ	นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง
วัน เดือน ปีเกิด	3 มกราคม 2505
การศึกษา	โรงเรียนเตรียมทหาร รุ่นที่ 22 โรงเรียนนายเรืออากาศ รุ่นที่ 29 ศิษย์การบินโรงเรียนการการบิน รุ่นที่ 80 โรงเรียนนายทหารอากาศชั้นผู้บังคับฝูง รุ่นที่ 74 โรงเรียนเสนาธิการทหารอากาศ รุ่นที่ 40 วิทยาลัยการทัพอากาศ รุ่นที่ 42
ประวัติการทำงานโดยย่อ	1. นายทหารฝ่ายเสนาธิการ กองป้องกันทางอากาศ กรมควบคุมการปฏิบัติทางอากาศ 2. รองผู้อำนวยการกองยุทธการสื่อสารอิเล็กทรอนิกส์ กรมยุทธการทหารอากาศ 3. ผู้อำนวยการกองนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
ตำแหน่งปัจจุบัน	รองผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

สรุปย่อ

ลักษณะวิชา การทหาร
เรื่อง แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ
ผู้วิจัย นาวาอากาศเอก ณรงค์เวตย์ เรืองจวง **หลักสูตร** วปอ. **รุ่นที่** 59
ตำแหน่ง รองผู้อำนวยการสำนักนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ความเป็นมาและความสำคัญของปัญหา

กองทัพอากาศกำหนดให้มีการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร กระบวนการทำงานบุคลากรและหน่วยงานของกองทัพอากาศ ให้สามารถปฏิบัติภารกิจได้อย่างครบถ้วน ถูกต้อง ปลอดภัย และได้ปรับโครงสร้าง กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ โดยการจัดตั้งกองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เพื่อรับผิดชอบงานด้านสงครามไซเบอร์โดยตรง และได้รับการบรรจุบุคลากรจากหน่วยขึ้นตรงกองทัพอากาศตามความจำเป็นและเหมาะสม ซึ่งบุคลากรดังกล่าวมีพื้นฐานความรู้และความสามารถแตกต่างกัน ทำให้การปฏิบัติภารกิจในหน้าที่ด้านสงครามไซเบอร์มีข้อจำกัด การจัดหาระบบและอุปกรณ์ไม่สามารถดำเนินการได้ตามเวลาที่เหมาะสม อาจจะทำให้ไม่สามารถรับมือต่อการปฏิบัติของผู้ไม่หวังดีได้ ผู้วิจัยมีหน้าที่รับผิดชอบในการจัดทำแผนงานและโครงการด้านเทคโนโลยีสารสนเทศและสงครามสารสนเทศ การจัดการความรู้ การบริหารการฝึกและศึกษาบุคลากรด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ ซึ่งบุคลากรดังกล่าวปฏิบัติหน้าที่ในตำแหน่ง นายทหารเทคโนโลยีสารสนเทศและการสื่อสาร เจ้าหน้าที่เทคโนโลยีสารสนเทศและการสื่อสารภายในหน่วย ผู้วิจัยจึงมีความสนใจทำวิจัยเกี่ยวกับ ปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ การให้ความรู้ การฝึกศึกษา การอบรมของบุคลากรด้านไซเบอร์

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและข้อจำกัด การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
2. เพื่อศึกษาปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ
3. เพื่อเสนอแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

ขอบเขตของการวิจัย

การวิจัยครั้งนี้จะศึกษาและวิเคราะห์ถึงปัญหา ข้อจำกัด ปัจจัยที่เกี่ยวข้องในการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ โดยเฉพาะอย่างยิ่ง การพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องกับการปฏิบัติภารกิจด้านไซเบอร์ ซึ่งผู้วิจัยได้กำหนดขอบเขตของการวิจัย ดังนี้

1. ขอบเขตประชากร

ประชากรที่ใช้ในการวิจัยครั้งนี้ประกอบด้วยข้าราชการชั้นสัญญาบัตรของกองทัพอากาศที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยขึ้นตรงกองทัพอากาศที่ปฏิบัติงานในระหว่างปี 2559 ถึง 2560 โดยมีผู้ให้ข้อมูลสำคัญ ประกอบด้วย ผู้บังคับบัญชาชั้นสูงของกองทัพอากาศ และผู้บังคับบัญชาและผู้ปฏิบัติหน้าที่ของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ โดยเป็นการศึกษาในเรื่องการเตรียมบุคลากรในการปฏิบัติด้านไซเบอร์

2. ขอบเขตพื้นที่ กองทัพอากาศ

3. ขอบเขตระยะเวลาการวิจัย ตั้งแต่เดือน ธ.ค.59 ถึงเดือน มิ.ย.60

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาและวิเคราะห์จากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไปด้านสงครามไซเบอร์ นโยบายระดับชาติ นโยบายระดับกองทัพ นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของกองทัพอากาศ และการปฏิบัติงานด้านไซเบอร์ ดังนี้

1. รวบรวมเอกสารที่เกี่ยวข้อง เช่น ตำรา วารสาร บทความ เอกสารทางวิชาการ นโยบายที่เกี่ยวข้อง ตลอดจนค้นคว้าทางอินเทอร์เน็ต เป็นต้น

2. สัมภาษณ์ผู้บังคับบัญชา ผู้เชี่ยวชาญ และผู้ปฏิบัติงานด้านไซเบอร์ของกองทัพอากาศ

ผลการวิจัย

จากผลการศึกษาวิจัย จะเห็นได้ว่ากองทัพอากาศได้ตระหนักถึงความสำคัญการปฏิบัติงานด้านไซเบอร์เพื่อเตรียมรับมือกับภัยคุกคามที่อาจจะเกิดขึ้น โดยการจัดหาเทคโนโลยีสารสนเทศพร้อมอุปกรณ์และระบบป้องกันมาใช้ในการปฏิบัติภารกิจ จัดทำแผนงานที่เกี่ยวข้อง รวมถึงพัฒนาบุคลากรด้านไซเบอร์ พร้อมจัดให้มีการตรวจสอบระบบอย่างต่อเนื่อง ดังนี้

1. สภาพปัญหาและข้อจำกัด การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

1.1 ปัญหา

1.1.1 บุคลากรบางส่วนละเลยไม่ปฏิบัติตามนโยบายที่เกี่ยวข้อง รวมถึงบุคลากรด้านไซเบอร์มีจำนวนไม่เพียงพอและขาดทักษะในการปฏิบัติงาน

1.1.2 การศึกษาเฉพาะด้านยังไม่ครอบคลุม ไม่มีนักพัฒนาโปรแกรมประสงค์ร้าย รวมถึงระบบการจัดการความรู้ยังไม่ครอบคลุมเทคโนโลยีและคู่มือการใช้งานอุปกรณ์ อีกทั้งคู่มือการปฏิบัติเมื่อถูกโจมตีระบบสารสนเทศและการสื่อสารยังไม่มีการจัดทำแจกจ่ายให้หน่วย

1.1.3 ระเบียบกองทัพอากาศที่เกี่ยวข้องไม่ครอบคลุมการปฏิบัติ

1.2 ข้อจำกัด

1.2.1 ด้านสถานที่ ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งาน ติดตั้งใช้งาน 2 สถานที่ ทำให้ไม่สะดวกต่อการปฏิบัติงานของบุคคลากรในการเฝ้าตรวจ

1.2.2 ด้านลิขสิทธิ์ ระบบเทคโนโลยีที่จัดหามาใช้งานต้องมีลิขสิทธิ์จากบริษัทผู้ผลิต ทำให้ต้องใช้งบประมาณมากขึ้น

1.2.3 ด้านเทคโนโลยี เทคโนโลยีมีการพัฒนาจึงต้องมีการติดตามและจัดหามาใช้งานเพื่อป้องกันช่องโหว่ที่อาจจะเกิดขึ้น ทำให้ต้องใช้งบประมาณในการจัดหาตลอดเวลา

2. ปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

ปัจจัยการปฏิบัติการไซเบอร์ กองทัพอากาศมีการปฏิบัติตามองค์ประกอบ 3 องค์ประกอบ ดังนี้

2.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง กองทัพอากาศมีการดำเนินการในหลายด้าน เช่น จัดทำระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ จัดทำโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ การจัดการแข่งขัน Cyber Operations Contest จัดทำเอกสารคู่มือการปฏิบัติงานและการจัดองค์ความรู้ เป็นต้น ซึ่งการดำเนินการตามแผนและขั้นตอนดังกล่าว หากสามารถดำเนินการได้จะทำให้การปฏิบัติภารกิจด้านไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

2.2 ปัจจัยด้านเทคโนโลยี กองทัพอากาศได้ดำเนินการจัดหาระบบเทคโนโลยีทั้งเชิงป้องกัน และเชิงป้องปราม มาใช้งาน เช่น ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรอง ระบบเข้ารหัสข้อมูล และระบบจำลองยุทธทางไซเบอร์ เป็นต้น ซึ่งการจัดหาเทคโนโลยีมาใช้งานในกองทัพนั้น มีการจัดหาตามแผนงานที่กำหนดไว้ แต่จากการที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว จึงต้องมีการจัดเทคโนโลยีใหม่มาใช้งานอย่างต่อเนื่องซึ่งส่งผลกระทบต่อบุคลากรที่รับผิดชอบและงบประมาณของกองทัพอากาศ

2.3 ปัจจัยด้านบุคลากร กองทัพอากาศมีการดำเนินการด้านความรู้เพื่อรองรับบุคลากร โดยจัดทำหลักสูตรเพื่อพัฒนาบุคลากร เช่น หลักสูตรพื้นฐานรองรับผู้ปฏิบัติงาน หลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศ หลักสูตรอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งส่งบุคลากรเข้ารับการฝึกอบรมนอกกองทัพ รวมถึงมีการจัดการฝึกอบรมการในการเลื่อนระดับความชำนาญให้กับบุคลากรที่มีคุณสมบัติครบถ้วนเพื่อพิจารณาเลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น เป็นต้น อีกทั้งมีการสร้างจิตสำนึกและการแจ้งเตือนให้มีการเสริมสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ตามที่กองทัพอากาศได้ดำเนินการมาแล้วนั้น สามารถให้ความรู้และความสามารถบุคลากรได้ในระดับหนึ่ง แต่บุคลากรยังขาดทักษะและความชำนาญ รวมถึงมีจำนวนไม่เพียงพอต่อการปฏิบัติงาน

3. แนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ

3.1 แนวทางการพัฒนาบุคลากร ดังนี้

3.1.1 การพัฒนาบุคลากร ต้องจัดให้มี การฝึกอบรม ทบทวน และส่งไปศึกษานอกหน่วยให้กับ บุคลากรทุกระดับ ได้แก่ ระดับผู้ปฏิบัติงาน ระดับผู้ตรวจสอบและผู้ที่เป็นวิทยากรให้การอบรม ระดับผู้รับผิดชอบดูแลระบบ และระดับเจ้าหน้าที่ทำงานด้านการรักษาความปลอดภัยระบบสารสนเทศ รวมถึงให้มีการจัดทำคู่มือในการปฏิบัติงานด้วย อีกทั้งบรรจุบุคลากรให้เพียงพอต่อ การปฏิบัติภารกิจ และต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน

3.1.2 การดำเนินการด้านหลักสูตรและที่เกี่ยวข้อง

3.1.2.1 จัดเตรียมหลักสูตรและทบทวนหลักสูตรที่ใช้ในการฝึกศึกษาและอบรมด้านไซเบอร์อย่างต่อเนื่อง รวมถึงพิจารณาสถานศึกษาภายนอกเพื่อส่งบุคลากรไปฝึกศึกษาและอบรมตามความเหมาะสม

3.1.2.2 จัดทำและปรับปรุงการตรวจสอบระบบให้ทันสมัย รวมทั้งให้มีการสุ่มตรวจสอบระบบในภาพรวม หากพบข้อบกพร่องให้แจ้งหน่วยเกี่ยวข้องทราบ เมื่อพบบุคลากรกระทำผิดให้พิจารณาลงทัณฑ์ตามแนวทางที่กองทัพอากาศกำหนด

3.1.2.3 จัดให้มีการทบทวนความรู้ในการปฏิบัติงาน และการดำเนินการตามแผนงานให้กับผู้รับผิดชอบดูแลระบบที่อยู่ในความรับผิดชอบอย่างต่อเนื่อง

3.2 ปัจจัยที่เกี่ยวข้อง

3.2.1 โครงสร้างการจัดหน่วย ปัจจุบันหน่วยรับผิดชอบด้านไซเบอร์โดยตรงจัดตั้งเป็นระดับกอง เห็นควรพิจารณาให้ปรับขยายอัตราเพื่อรองรับการปฏิบัติภารกิจที่จะเกิดขึ้นในอนาคต

3.2.2 ทบทวน ปรับปรุง การจัดทำแผนงานและแนวทางการปฏิบัติที่เกี่ยวข้องให้ครอบคลุมการปฏิบัติงาน รวมถึงแนวทางการตรวจสอบระบบให้ทันสมัย พร้อมทั้งจัดทำคู่มือการปฏิบัติเมื่อมีเหตุการณ์แจกจ่ายให้หน่วยเกี่ยวข้อง อีกทั้งควรจัดทำคู่มือการใช้งานระบบอุปกรณ์และโปรแกรมที่มีใช้งานอยู่และที่จะจัดหามาใหม่เพิ่มเติมเมื่อได้รับระบบ และจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพ

3.2.3 การสร้างแรงจูงใจ การสร้างแรงจูงให้กับผู้ปฏิบัติภารกิจ เห็นควรให้ผู้บังคับบัญชาผลักดันในการดำเนินการขอเงินเพิ่มพิเศษเป็นค่าตอบแทนให้กับผู้ปฏิบัติงานด้านไซเบอร์

3.2.4 สนับสนุนงบประมาณเป็นค่าลิขสิทธิ์และการจัดหาเทคโนโลยีที่ทันสมัยตามความจำเป็นใช้งานโดยเฉพาะเทคโนโลยีเชิงป้องปราม

3.2.5 ระบบที่มีความจำเป็นทางด้านยุทธการ ต้องจัดทำเป็นระบบปิดให้สามารถเชื่อมต่อได้เฉพาะผู้ใช้งานในระบบเท่านั้น

3.2.6 หากมีการสร้างอาคารใหม่รองรับงานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ควรให้ติดตั้งระบบด้านไซเบอร์เชิงป้องกันไว้ภายในอาคารเดียวกัน

ข้อเสนอแนะ

1. ปัจจุบันโครงสร้างและอัตราที่ได้รับการอนุมัติไว้ อาจจะไม่สามารถรองรับการปฏิบัติงานด้านไซเบอร์ในอนาคตได้ เห็นสมควรให้มีการศึกษาวิจัยเพิ่มเติมในส่วนของโครงสร้างและอัตราของหน่วยงานด้านไซเบอร์ให้สอดคล้องกับงานเชิงป้องกันและป้องปราม

2. การพัฒนาบุคลากร ควรมีการจัดการฝึกศึกษา การอบรม การทบทวน และส่งไปศึกษานอกหน่วยให้กับบุคลากรทุกระดับ รวมถึงให้มีการจัดทำคู่มือในการปฏิบัติงาน อีกทั้งควรบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติภารกิจโดยต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน พร้อมกับให้ผู้รับผิดชอบผลักดันการดำเนินการขอเงินเพิ่มพิเศษให้กับผู้ปฏิบัติงานด้านไซเบอร์

3. ทบทวน ปรับปรุง การจัดทำแผนแม่บท แผนงาน แนวทางการปฏิบัติที่เกี่ยวข้องด้านไซเบอร์ให้ครอบคลุมการปฏิบัติ พร้อมทั้งจัดทำแผนและคู่มือการปฏิบัติเมื่อมีเหตุการณ์แจกจ่ายให้หน่วยเกี่ยวข้อง และควรจัดให้มีการซักซ้อมการดำเนินการตามแผนงานให้กับผู้เกี่ยวข้องอย่างต่อเนื่องรวมถึงควรจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพ

4. สนับสนุนงบประมาณให้เพียงพอต่อการปฏิบัติภารกิจด้านไซเบอร์และค่าลิขสิทธิ์ของระบบเทคโนโลยี ตามแผนงานที่กำหนดไว้

5. หากมีการสร้างอาคารใหม่รองรับงานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม เห็นควรให้ติดตั้งระบบงานด้านไซเบอร์เชิงป้องกันไว้ภายในอาคารเดียวกัน