การบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ

โดย

นาวาอากาศเอกเสกสัณน์ ไชยมาตย์
รองผู้อำนวยการสำนักนโยบายและแผน
กรมยุทธการทหารอากาศ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 62
ประจำปีการศึกษา พุทธศักราช 2562 - 2563

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “การบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ” ลักษณะวิชา การทหาร ของ นาวาอากาศเอก เสกสัณน์ ไชยมาตย์ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 62 ประจำปีการศึกษา พุทธศักราช 2562 - 2563

พลโท

(พิสัณห์ ปฐมเอม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง การบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ

ลักษณะวิชา การทหาร

ผู้วิจัย นาวาอากาศเอก เสกสัณน์ ไชยมาตย์ **หลักสูตร** วปอ. **รุ่นที่** 62

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาขีดความสามารถของมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ และนำเสนอแนวทางการเชื่อมโยงขีดความสามารถทางไซเบอร์กับสงครามอิเล็กทรอนิกส์เพื่อทวีความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ โดยศึกษาเนื้อหา วิเคราะห์ความสอดคล้องวิธีการและกระบวนการในการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ ศึกษาหลักการหรือแนวคิดที่เป็นไปได้จริงในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ในเชิงเปรียบเทียบขีดความสามารถ ประเด็นที่สอดคล้องและเกื้อกูลกันในการปฏิบัติจริง ในขอบเขตประชากรที่เป็นกำลังพลและเจ้าหน้าที่ผู้ปฏิบัติงานด้านไซเบอร์และสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ ดำเนินการวิจัยด้วยระเบียบวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับการวิจัยเชิงพรรณนา (Descriptive Research) โดยการรวบรวมข้อมูลทุติยภูมิ จากตำราและเอกสารและข้อมูลปฐมภูมิจากการสัมภาษณ์เชิงลึกกับผู้บังคับบัญชาที่รับผิดชอบ และผู้ปฏิบัติงานที่มีความเชี่ยวชาญในกองทัพอากาศ นำข้อมูลมาวิเคราะห์เนื้อหา (Content Analysis) วิเคราะห์เปรียบเทียบ สังเคราะห์ข้อมูลแล้วนำเสนอข้อมูลผลลัพธ์ที่เป็นแนวคิดใหม่จากการวิจัย ผลการวิจัยพบว่า ในขีดความสามารถการปฏิบัติการสงครามอิเล็กทรอนิกส์ สามารถสนับสนุนขีดความสามารถทางไซเบอร์ได้ ทั้งในปฏิบัติการไซเบอร์เชิงป้องกัน ปฏิบัติการเชิงป้องปราม และปฏิบัติการสนับสนุน ซึ่งจะเป็นการทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศให้มีประสิทธิภาพสูงขึ้นได้ จากข้อสรุปดังกล่าวนี้ นับเป็นข้อยืนยันในหลักการการเชื่อมโยงขีดความสามารถการปฏิบัติการที่เกื้อกูลกันเข้าด้วยกัน เพื่อการสนับสนุนหรือขยายขีดความสามารถในปฏิบัติการทางทหารด้านอื่น ๆ ให้ได้ผลดีมากยิ่งขึ้น มีข้อเสนอแนะ ดังนี้ 1) ข้อเสนอแนะระดับยุทธศาสตร์ 2) ข้อเสนอแนะระดับยุทธวิธี และ 3) ข้อเสนอแนะระดับปฏิบัติการ สำหรับข้อเสนอแนะในการทำวิจัยครั้งต่อไป ได้แก่ การศึกษา วิเคราะห์เชิงลึก ด้านความพร้อมและการเตรียมทรัพยากรทุกประเภทของกองทัพอากาศที่จำเป็นในการสนับสนุนด้านสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์ ศึกษา วิเคราะห์เชิงลึก การปฏิบัติการสงครามอิเล็กทรอนิกส์ ในแต่ละด้านเพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์ ตลอดจนวิเคราะห์ข้อได้เปรียบ และข้อด้อยที่อาจพบได้จากการปฏิบัติการ และ ศึกษา โครงการนำร่องการปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์

Abstract

Title The Integrating Cyber Capabilities with Electronic Warfare Operations for Increasing the Advantage in the RTAF's Cyber Security

Field Military

Name Group Captain Seksun Chaiyamart **Course** NDC **Class** 62

This Objectve of research are study the capabilities of the Cyber Domain with the Electronic Warfare to increase the Air Force's Cyber Security capabilities. By studying the content, analyzing the consistency in the process of the Air Force's Cyber Operation. To study possible concepts at the level of tactical, operational, and strategies, in comparison the capability issues that are consistent and complementary in practice, in the population boundary of the RTAF and the Air Force's Cyber and Electronic Warfare Operator. Conduct Qualitative Research with Descriptive Research, by collecting the secondary data from textbooks and documents, and the primary data from in-depth interviews with the responsible supervisors and operators in the RTAF, then doing the Content Analysis, comparative analysis, data synthesis, and presenting new conceptual results this research. This research results indicate that the capacity to conduct EW able to provide support the Cyber capabilities in the preventive Cyber Operations, Cyber Proactive Practices and Cyber Support Operations. Which will increase the advantage of the RTAF's Cyber security to be more efficient and expand the capability of the operations to be more effective. Suggestions are as follows. 1. Strategic Recommendations 2. Tactical Recommendations and 3. Operational Recommendations. Suggestions for further research are In-depth analysis study to evaluate readiness of RTAF in all resource preparing need to support EW due to provide support the Cyber capabilities in the preventive Cyber Operations. In-depth analysis study all type of EW operation to find strengths and weaknesses. Pilot study project about how electronic warfare operations to support cyber security.

คำนำ

กองทัพอากาศได้กำหนดกลยุทธ์การพัฒนาขีดความสามารถด้านสงครามไซเบอร์ตามคุณลักษณะที่เหมาะสมกับการใช้กำลังกองทัพอากาศ เพื่อตอบสนองประเด็นยุทธศาสตร์การเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศให้เต็มขีดความสามารถ โดยพัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ และใช้ประโยชน์จากการปฏิบัติการทางไซเบอร์ไปขยายขีดความสามารถปฏิบัติการทางทหารด้านอื่น ๆ รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุกและแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์

การปฏิบัติการสงครามอิเล็กทรอนิกส์ (Electronic Warfare) เป็นขีดความสามารถที่ถูกพัฒนาและนำมาใช้ในภารกิจด้านการทหารตั้งแต่ยุคโรมัน กองทัพอากาศได้เริ่มมีปฏิบัติการสงครามอิเล็กทรอนิกส์ในปี 2522 โดยใช้ขีดความสามารถด้านปฏิบัติการสงครามอิเล็กทรอนิกส์ในบริบทของการสนับสนุนการข่าวกรองเพื่อการตัดสินใจของผู้บังคับบัญชา ต่อมาโครงการจัดซื้อเครื่องบิน Gripen 39 C/D เข้าประจำการในกองทัพอากาศ ทำให้มีการถ่ายทอดเทคโนโลยีหลัก (Key Technologies) และการพัฒนาขีดความสามารถของกำลังทางอากาศในด้านสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) เมื่อพิจารณาศักยภาพของทั้งมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ ทำให้เกิดความสนใจผลลัพธ์จากปฏิบัติการสงครามอิเล็กทรอนิกส์ในหลายด้านที่จะนำมาบูรณาการทวีขีดความสามารถทางไซเบอร์ เพื่อสร้างความได้เปรียบในระดับปฏิบัติการทหารและในระดับความมั่นคงของชาติ ผู้วิจัยจึงมีความสนใจที่จะศึกษาแนวทางการพัฒนาขีดความสามารถทางไซเบอร์ด้วยการเชื่อมโยงกับขีดความสามารถการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ

นาวาอากาศเอก

(เสกสัณน์ ไชยมาตย์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 62
ผู้วิจัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในท่ามกลางกระแสโลกาภิวัฒน์และความก้าวหน้าทางเทคโนโลยี ทำให้บริบทความมั่นคงของโลกมีความสลับซับซ้อนมากขึ้น มีการแข่งขันสูงขึ้น จนนำไปสู่ความขัดแย้งในการแสวงหาผลประโยชน์และช่วงชิงการครอบครองทรัพยากรธรรมชาติ ก่อให้เกิดการเปลี่ยนแปลงสภาพแวดล้อมของโลกตามมา เห็นได้ชัดจากการเกิดภัยพิบัติทางธรรมชาติที่รุนแรงและส่งผลกระทบเชื่อมโยงทั่วโลก รวมถึงพฤติกรรมทางสังคมของมนุษย์ที่มีความแตกต่างทางอุดมการณ์ ความคิด ความศรัทธา มีความขัดแย้งที่เกิดขึ้นทั้งระหว่างรัฐต่อรัฐ รัฐกับประชาชน หรือประชาชนกับประชาชนในทั่วทุกภูมิภาคของโลก นอกจากนี้การมีบทบาทขององค์กรที่ไม่ใช่รัฐ ที่มีอิทธิพลในการชี้นำนโยบายภาครัฐมากขึ้นทั้งในระดับโลก ภูมิภาค หรือภายในรัฐ ทั้งหมดที่กล่าวมานี้ล้วนมีผลกระทบต่อสภาวะแวดล้อมด้านความมั่นคงทั้งสิ้น การวิเคราะห์สภาวะแวดล้อมอย่างรอบด้าน โดยเฉพาะการวิเคราะห์และพัฒนาศักยภาพและขีดความสามารถด้านต่าง ๆ ให้มีความพร้อมในการเผชิญกับภัยคุกคามจึงเป็นเรื่องที่มีความจำเป็นและสำคัญอย่างยิ่ง

การพัฒนาทางเทคโนโลยีสารสนเทศและการสื่อสารทั้งด้านเครือข่ายและอินเทอร์เน็ตนำมาซึ่งภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบการขัดขวาง สกัดกั้น การจารกรรมข้อมูล และการโจมตีทำลายล้าง ซึ่งล้วนก่อให้เกิดความเสียหายเป็นวงกว้าง ดังนั้น หลายประเทศจึงมีการจัดตั้งหน่วยงานรับผิดชอบมิติไซเบอร์โดยตรง รวมทั้งกำหนดเป็นมิติหนึ่งในการปฏิบัติการด้านความมั่นคงของชาติ สำหรับประเทศไทยได้ให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ โดยสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี ได้กำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564 ใช้เป็นนโยบายระดับชาติฉบับแรกของไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุด ตามสภาวะแวดล้อมที่ปรากฏ (สำนักนายกรัฐมนตรี, 2560)

ในยุทธศาสตร์ชาติ 20 ปี ในยุทธศาสตร์ด้านความมั่นคง ได้กำหนดประเด็นการพัฒนา ระบบ กลไก มาตรการ และความร่วมมือระหว่างประเทศในทุกระดับ เพื่อรักษาผลประโยชน์ของชาติสามารถป้องกันและแก้ไขปัญหาความมั่นคงรูปแบบใหม่ ภัยคุกคามข้ามชาติ ภัยก่อการร้าย และเสริมสร้างความมั่นคงเทคโนโลยีสารสนเทศและไซเบอร์ไว้ด้วยเช่นกัน (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561)

ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม 20 ปี (กระทรวงกลาโหม, 2560) มุ่งตอบสนองวัตถุประสงค์มูลฐานด้านความมั่นคงของประเทศ โดยกำหนดเป้าหมายการพัฒนาเสริมสร้างศักยภาพด้านการทหาร ที่รวมถึงการยกระดับศักยภาพด้วยเทคโนโลยีด้านการทหารระดับสูง หมายรวมถึงการพัฒนาและดำรงขีดความสามารถการปฏิบัติการด้านไซเบอร์ให้มีศักยภาพ

ทัดเทียมกับประเทศในภูมิภาคอย่างต่อเนื่อง ในยุทธศาสตร์ทหาร กองทัพไทย 20 ปี (กองบัญชาการกองทัพไทย, 2559) ในวัตถุประสงค์เฉพาะทางทหารได้กำหนดการปฏิบัติการในสงครามไซเบอร์ (Cyber Warfare) เพื่อให้กองทัพไทยมีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ (Cyber Domain) ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติ ตลอดจนสามารถบูรณาการและให้การสนับสนุนความมั่นคงไซเบอร์ (Cyber Security) ของประเทศในภาพรวมได้อย่างมีประสิทธิภาพ โดยกำหนดเป็นยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย เพื่อเป็นแนวทางในการปฏิบัติในมิติไซเบอร์กองทัพไทย ทั้งในขั้นการเตรียมกำลังและใช้กำลัง โดยแยกเป็น 3 ประเด็นยุทธศาสตร์ ได้แก่ 1) ยุทธศาสตร์การป้องกันเชิงรุกสำหรับปฏิบัติการในมิติไซเบอร์ เสริมสร้างพลังอำนาจทางไซเบอร์ของกองทัพไทย เพื่อการปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้าม โดยมุ่งหมายการลดทอน ขัดขวาง ระงับ ยับยั้ง หรือเชิงรุกในลักษณะจำกัด (Limited Offensive Action) และการตอบโต้ (Counter Attack) อย่างรวดเร็ว เพื่อความได้เปรียบต่อฝ่ายตรงข้ามตั้งแต่ในสภาวะปกติ และสร้างการตระหนักรู้ทางไซเบอร์ (Cyber Awareness) ที่จะนำไปสู่การตัดสินใจของผู้บังคับบัญชาทหารให้รู้เท่าทันต่อสถานการณ์ต่าง ๆ 2) ยุทธศาสตร์การผนึกกำลังป้องกันประเทศสำหรับปฏิบัติการในมิติไซเบอร์ โดยสร้างความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติไซเบอร์ของทุกภาคส่วนภายในประเทศอย่างเป็นระบบ และ 3) ยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับปฏิบัติการในมิติไซเบอร์ เป็นการเสริมสร้างความร่วมมือไซเบอร์กับประเทศเพื่อนบ้าน กลุ่มประเทศสมาชิกอาเซียนและมิตรประเทศ ทั้งในระดับภูมิภาคและระดับโลก ในส่วนกองทัพอากาศ ได้กำหนดกลยุทธ์การพัฒนาขีดความสามารถด้านสงครามไซเบอร์ ตามคุณลักษณะที่เหมาะสมกับการใช้กำลังกองทัพอากาศ เพื่อตอบสนองประเด็นยุทธศาสตร์การเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศ ให้เต็มขีดความสามารถ โดยพัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ และใช้ประโยชน์จากการปฏิบัติการทางไซเบอร์ในการขยายขีดความสามารถการปฏิบัติการทางทหาร รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์ (กองทัพอากาศ, 2562)

การปฏิบัติการสงครามอิเล็กทรอนิกส์ เป็นขีดความสามารถที่มีความสำคัญมากในการปฏิบัติการทางทหารในทุกยุคสมัย จนมีคำกล่าวว่า “ฝ่ายใดที่สามารถครองสมรภูมิสงครามอิเล็กทรอนิกส์ได้นั้น ก็แทบจะนับได้ว่าเป็นฝ่ายผู้ชนะ” เป็นขีดความสามารถที่ถูกพัฒนาและนำมาใช้ในภารกิจด้านการทหารตั้งแต่ยุคโรมัน ซึ่งต่อมาในยุคสงครามโลกครั้งที่ 2 มีการนำ RADAR : Radio Detection And Ranging มาใช้ในการรบโดยอังกฤษและเยอรมัน จากนั้นเทคโนโลยีสงครามอิเล็กทรอนิกส์ได้รับการพัฒนาอย่างรวดเร็ว ทั้งในด้านการตรวจจับ (Sensor) การติดตามเป้าหมาย (Tracking) การนำวิถี (Guidance) และการต่อต้านรูปแบบต่าง ๆ (Countermeasure) ในปัจจุบันระบบอิเล็กทรอนิกส์เป็นส่วนประกอบสำคัญของอาวุธยุทโธปกรณ์เกือบทุกชิ้นในสงคราม คำว่า “สงครามอิเล็กทรอนิกส์ หรือ Electronics Warfare” นั้น หมายถึงการปฏิบัติการทางทหารที่มีเป้าหมายอยู่ที่ระบบอิเล็กทรอนิกส์ของฝ่ายตรงข้าม โดยมุ่งโจมตีให้ระบบอิเล็กทรอนิกส์ของฝ่ายตรงข้ามไม่สามารถปฏิบัติการได้อย่างเต็มประสิทธิภาพ โดยการโจมตีนั้นแบ่งได้เป็นหลายรูปแบบ อาทิ การดักฟังสัญญาณ การก่อกวน รวมไปถึงการทำลายเป้าหมาย เช่น การก่อกวนทำลายเรดาร์

และระบบตรวจจับต่าง ๆ เพื่อให้ฝ่ายตรงข้ามไม่สามารถตรวจจับฝ่ายเราได้ การดักฟังและรวบรวมข่าวกรอง รวมทั้งการโจรกรรมข้อมูล (Hack) เป็นต้น

การปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ ได้เริ่มมีปฏิบัติการ ในปี 2522 โดยใช้ขีดความสามารถด้านการสงครามอิเล็กทรอนิกส์ในบริบทของการสนับสนุนการข่าวกรองเพื่อการตัดสินใจของผู้บังคับบัญชา โดยใช้เครื่องบินตรวจการณ์บินลาดตระเวนทางอากาศด้วยอุปกรณ์การหาข่าวทางสัญญาณ (SIGINT: Signal Intelligent) และอุปกรณ์การหาข่าวทางการสื่อสาร (COMINT : Communication Intelligent) และจากโครงการจัดซื้อเครื่องบิน Gripen 39 C/D เข้าประจำการในกองทัพอากาศ นอกจากการได้รับเครื่องบินที่มีสมรรถนะสูง และระบบบัญชาการและควบคุมที่ทันสมัยแล้ว เรายังได้รับการถ่ายทอดเทคโนโลยีหลัก (Key Technologies) และการพัฒนาขีดความสามารถของกำลังทางอากาศในด้านสงครามอิเล็กทรอนิกส์ (Electronic Warfare : EW) การจัดทำฐานข้อมูลทางภูมิศาสตร์ (Geographical Databases : Geo Data) และระบบเชื่อมโยงข้อมูล (Data Link : DL) ในขณะที่เครื่องบิน Gripen 39 C/D เป็นเครื่องบินขับไล่ที่มีความทันสมัย มีระบบการตรวจจับที่ดี (Active Electronically Scanned Array : AESA) มีระบบเชื่อมโยงข้อมูลความเร็วสูง (High Speed Data Links) และสามารถใช้อาวุธสมัยใหม่ที่มีความแม่นยำสูง (Latest Precision Weapons) จึงนับว่าเป็นจุดแข็งของกำลังทางอากาศในยุคปัจจุบัน ที่สามารถสร้างความได้เปรียบทั้งระดับยุทธวิธีถึงระดับยุทธศาสตร์ มีขีดความสามารถในการปฏิบัติภารกิจการสงครามอิเล็กทรอนิกส์ใน 3 รูปแบบ คือ 1) ภารกิจหลัก ได้แก่ การทำลายหรือตัดรอนขีดความสามารถของระบบตรวจจับของข้าศึกด้วยการรบกวน (Jamming) หรือการทำลายด้วยจรวดต่อต้านเรดาห์ (Anti Radiation Missile) การลาดตระเวนทางอิเล็กทรอนิกส์ เพื่อการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ (Electronic Support Measure : ESM) 2) ภารกิจสนับสนุนหน่วยอื่นเพื่อให้เกิดความปลอดภัยจากอาวุธของฝ่ายตรงข้าม เช่น การบินคุ้มกันทางอิเล็กทรอนิกส์ (Escort Jamming) 3) การปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อป้องกันตัวเอง (Self-Protection Jamming) ในส่วนของอุปกรณ์ (Equipment) แบ่งเป็น 2 กลุ่มใหญ่คือ กลุ่มรับข้อมูล ได้แก่อุปกรณ์ตรวจจับทาง EW (EW Picture) อุปกรณ์ตรวจจับอื่น ๆ และระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link) อีกกลุ่มหนึ่งคือ อุปกรณ์ที่วิเคราะห์และใช้ต่อต้านภัยคุกคามต่าง ๆ (Countermeasure Technique) เช่น ชุดประมวลผลกลาง (Mission Central Processor Unit) ชุดควบคุมการปล่อย Chaff/Fair เป็นต้น

เมื่อพิจารณาจากขีดความสามารถทั้งมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ ซึ่งเป็นขีดความสามารถที่มีการดำเนินการอยู่แล้ว ประกอบกับมีแนวทางปฏิบัติในการดำเนินงานที่คล้ายกัน คือมีลักษณะปฏิบัติการเชิงรุก ปฏิบัติการเชิงรับ และปฏิบัติการสนับสนุน โดยผู้วิจัยมีข้อสันนิษฐานว่าผลลัพธ์จากปฏิบัติการสงครามอิเล็กทรอนิกส์ในบางเรื่องจะสามารถนำมาเสริมสร้างขีดความสามารถทางไซเบอร์ได้อีกด้วย โดยการเชื่อมโยงจุดเด่นของทั้งสองขีดความสามารถ ซึ่งจะเป็นประโยชน์และสร้างความได้เปรียบด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งในระดับการปฏิบัติการทางทหารและในระดับความมั่นคงของชาติโดยรวม ผู้วิจัยจึงสนใจที่จะศึกษาแนวทางการพัฒนาขีดความสามารถทางไซเบอร์ด้วยการเชื่อมโยงกับขีดความสามารถการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ

จึงกำหนดเป็นหัวข้อในการจัดทำเอกสารวิจัยส่วนบุคคลของหลักสูตรการป้องกันราชอาณาจักร ปีการศึกษา 2562 - 2563 (วปอ.62) ฉบับนี้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการดำเนินงาน ขีดความสามารถ และขอบขีดจำกัดของมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ทั้งในอดีตและปัจจุบัน

2. เพื่อศึกษาการเชื่อมโยงการดำเนินภารกิจ ขีดความสามารถและขอบขีดจำกัดของมิติไซเบอร์กับการปฏิบัติการสงครามอิเล็กทรอนิกส์

3. เพื่อเสนอแนวทางการบูรณาการเชื่อมโยงขีดความสามารถในมิติไซเบอร์กับสงครามอิเล็กทรอนิกส์ ในการทวีขีดความสามารถเพื่อความได้เปรียบในความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศและความมั่นคงของชาติ

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา

1.1 การวิจัยนี้เน้นการศึกษา วิเคราะห์ เนื้อหา ความสอดคล้องในรูปแบบและกระบวนการในการดำเนินภารกิจด้านไซเบอร์ของกองทัพอากาศ เท่านั้น

1.2 การวิจัยนี้จะศึกษาหลักการหรือแนวคิดที่เป็นไปได้จริงทั้งในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ ในเชิงเปรียบเทียบขีดความสามารถที่มีความสอดคล้องสัมพันธ์และเกื้อกูลกันได้ในเชิงปฏิบัติ

1.3 การวิจัยนี้จะเน้นเฉพาะหลักการหรือเนื้อหาในแต่ละขีดความสามารถที่สามารถเปิดเผยได้เท่านั้น เนื่องจากในขีดความสามารถทั้งสองด้านเป็นหัวข้อที่ดำเนินการเกี่ยวกับภารกิจที่มีความเกี่ยวข้องกับเนื้อหาที่มีชั้นความลับ จึงจำเป็นต้องมีการกลั่นกรองเนื้อหาอย่างรอบคอบและใช้ความระมัดระวังสูง

2. ขอบเขตด้านประชากร

ประชากรที่เกี่ยวข้องในการศึกษาครั้งนี้ ได้แก่ กำลังพลและเจ้าหน้าที่ผู้ปฏิบัติงานด้านไซเบอร์และสงครามอิเล็กทรอนิกส์กองทัพอากาศ ทั้งระดับผู้บังคับบัญชาหน่วย (ผู้บริหาร) และผู้ปฏิบัติงานจริง

วิธีดำเนินการวิจัย

ดำเนินการด้วยระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับการวิจัยเชิงพรรณนา (Descriptive Research) ดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ ดำเนินการโดยการศึกษาจากตำรา คู่มือและเอกสารต่าง ๆ เรื่องมิติไซเบอร์ และภารกิจสงครามอิเล็กทรอนิกส์ ทั้งข้อมูลภายในประเทศและกองทัพมิตรประเทศ

1.2 ข้อมูลปฐมภูมิ ดำเนินการโดยการสัมภาษณ์เชิงลึกผู้บังคับบัญชาหน่วยงานที่เกี่ยวข้องในกองทัพอากาศ ผู้รับผิดชอบงานและผู้ปฏิบัติงานจริง ตลอดจนผู้ชำนาญที่มีความเชี่ยวชาญ

2. การวิเคราะห์ข้อมูล

ดำเนินการวิเคราะห์เนื้อหา (Content Analysis) การวิเคราะห์เปรียบเทียบ (Comparison Analysis) และสังเคราะห์ข้อมูล (Synthesis) จากทฤษฎี หลักการที่เกี่ยวข้อง ทั้งในและต่างประเทศ

3. การนำเสนอข้อมูล

นำเสนอข้อมูลแบบรายงานวิจัยเชิงพรรณนาและวิเคราะห์ ได้ผลงานที่เป็นแนวคิดใหม่ ๆ จากการวิจัย

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบการดำเนินการ ขีดความสามารถและขอบขีดจำกัดมิติไซเบอร์และ ภารกิจสงครามอิเล็กทรอนิกส์ทั้งในอดีตและยุคปัจจุบัน

2. ทำให้ทราบประโยชน์ที่จะได้รับจากการปฏิบัติการไซเบอร์ของหน่วยในระดับต่าง ๆ เมื่อมีการเชื่อมโยง (หรือบูรณาการ) กับขีดความสามารถของสงครามอิเล็กทรอนิกส์

3. ได้แนวทางในการบูรณาการความเชื่อมโยงความสามารถในมิติไซเบอร์ กับสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบในความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศและความมั่นคงของชาติ

คำจำกัดความ

ยุทธศาสตร์จำกัด	หมายถึง	วิธีการ (WAYS) ที่จะนำเครื่องมือ (MEANS) ที่มีอยู่อย่างมาใช้อย่างดีที่สุดให้บรรลุจุดมุ่งหมาย (ENDS) ที่ตั้งไว้
ยุทธศาสตร์ชาติ	หมายถึง	ศิลป์และศาสตร์ในการพัฒนา และการใช้การเมือง เศรษฐกิจ สังคมจิตวิทยา การทหารของชาติ วิทยาศาสตร์เทคโนโลยีและนวัตกรรม ทั้งในยามปกติและยามสงคราม เพื่อส่งเสริมผลประโยชน์ของชาติ และเพื่อให้บรรลุวัตถุประสงค์ของชาติ และอีกความหมายหนึ่งคือศิลป์และศาสตร์ในการพัฒนาและการใช้กำลังอำนาจแห่งชาติ ทั้งในยามสงบและยามสงคราม ทำการสนับสนุนนโยบายของชาติให้ได้ผลดีที่สุด เพื่อเพิ่มพูนโอกาสและความได้เปรียบที่ได้มา ซึ่งชัยชนะและลดโอกาสที่ประสบความพ่ายแพ้ให้น้อยลง
ยุทธศาสตร์ความมั่นคงแห่งชาติ	หมายถึง	ศิลป์และศาสตร์ในการพัฒนา ประยุกต์ และประสานงานในการใช้ กำลังอำนาจแห่งชาติ ได้แก่ การเมือง/การทูต

การเศรษฐกิจ การทหาร สังคมจิตวิทยา วิทยาศาสตร์ เทคโนโลยีและนวัตกรรมและข้อมูล ข่าวสาร ฯลฯ เพื่อบรรลุวัตถุประสงค์ ที่เกื้อกูลต่อความมั่นคงแห่งชาติสามารถเรียกได้ว่า ยุทธศาสตร์ชาติหรือมหายุทธศาสตร์

ยุทธศาสตร์ทหาร หมายถึง ศิลป์และศาสตร์ในการใช้กำลังกองทัพเพื่อให้บรรลุวัตถุประสงค์แห่งชาติ โดยการใช้กำลังหรือคุกคามด้วยกำลังเป็นการใช้กำลังทหารในยามสงบและยามสงคราม

ยุทธศาสตร์กองทัพอากาศ หมายถึง การใช้วิธีการ (WAYS) ที่จะนำเครื่องมือ (MEANS) ที่มีอยู่อย่างจำกัดมาใช้อย่างดีที่สุดให้บรรลุจุดมุ่งหมาย (ENDS) ที่ตั้งไว้ ได้แก่ 1) การพัฒนากองทัพอากาศให้สอดคล้องกับสภาวะแวดล้อม ด้านความมั่นคงที่เปลี่ยนแปลงไปอย่างมีความสอดคล้องกับยุทธศาสตร์ชาติ ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม และยุทธศาสตร์ทหาร กองทัพไทย 2) แปลงนโยบายและทิศทางการพัฒนาไปสู่การปฏิบัติเพื่อพัฒนาขีดความสามารถในแต่ละองค์ประกอบของกองทัพอากาศอย่างเป็นรูปธรรม โดยใช้เป็นแนวทางจัดทำความต้องการยุทโธปกรณ์หลักของกองทัพอากาศ 3) เป็นเครื่องมือในการติดตามความก้าวหน้าและประเมินผลการพัฒนากองทัพอากาศ โดยมีเป้าหมาย วัตถุประสงค์ กลยุทธ์ และกรอบระยะเวลาในการพัฒนาอย่างชัดเจน

มิติไซเบอร์ หมายถึง มิติหนึ่งในการปฏิบัติการด้านความมั่นคงชาติ มีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารด้านเครือข่ายในปัจจุบันที่ก่อให้เกิดความเสี่ยงในการเกิดภัยคุกคามในมิติไซเบอร์ ทั้งในรูปแบบการจารกรรมข้อมูลและการโจมตีเพื่อทำลายล้าง

ขีดความสามารถทางไซเบอร์ หมายถึง ขีดความสามารถทางไซเบอร์ของกองทัพอากาศ ที่กำหนดโดยยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ ยุทธศาสตร์ด้านสงครามไซเบอร์กองทัพไทย ดังนี้ 1) การป้องกันภัยคุกคามทางไซเบอร์ 2) การพัฒนาและใช้ประโยชน์จากขีดความสามารถทางไซเบอร์ในการปฏิบัติการทางทหาร และ 3) ความร่วมมือกับหน่วยงานภายในเพื่อการผนึกกำลังป้องกันประเทศ

สงครามอิเล็กทรอนิกส์ หมายถึง การปฏิบัติการทางทหารที่มีเป้าหมายอยู่ที่ระบบอิเล็กทรอนิกส์ของฝ่ายตรงข้าม ด้วยการโจมตีเพื่อให้ระบบอิเล็กทรอนิกส์ของฝ่ายตรงข้ามไม่สามารถใช้การได้เต็มประสิทธิภาพ แบ่งออกได้หลายรูปแบบ อาทิ การดักฟังสัญญาณ การก่อกวน การทำลายเป้าหมาย เช่น การก่อกวน/ทำลายเรดาร์และระบบตรวจจับต่าง ๆ เพื่อให้ข้าศึกไม่สามารถตรวจจับฝ่ายเราได้ การดักฟังและรวบรวมข่าวกรอง หรือ การโจรกรรมข้อมูล

ขีดความสามารถสงครามอิเล็กทรอนิกส์ หมายถึง ผลของการใช้ประโยชน์จากคลื่นแม่เหล็กไฟฟ้า ในการโจมตี ได้แก่ การรบกวน การลวง การทำลายระบบการสื่อสาร การค้นหา การวางกำลังอิเล็กทรอนิกส์ของฝ่ายตรงข้าม เพื่อวางแผนการป้องกัน หรือทำลายอาวุธอิเล็กทรอนิกส์ของฝ่ายตรงข้าม จนไม่สามารถใช้การได้

การทวีกำลัง หมายถึง การมีกำลังเพิ่มมากขึ้น หรือมากขึ้นเป็นสองเท่า ในที่นี้หมายถึง การเพิ่มขีดความสามารถเป็นสองเท่าจากเดิม

บทที่ 2
แนวคิด ทฤษฎี และยุทธศาสตร์ของไซเบอร์ และสงครามอิเล็กทรอนิกส์

ไซเบอร์ (Cyber) และสงครามอิเล็กทรอนิกส์ (Electronic Warfare) เป็นพัฒนาการหรือความก้าวหน้าทางเทคโนโลยีสารสนเทศและการสื่อสารที่ถูกนำมาใช้ประโยชน์ในการดำเนินกิจกรรมของมนุษย์ในปัจจุบันอย่างกว้างขวาง ทั้งในการช่วยปฏิบัติงาน ช่วยสนับสนุนข้อมูล ช่วยการตัดสินใจให้เกิดความง่าย สะดวก รวดเร็ว แม่นยำ และบรรลุเป้าหมายขององค์การ ขณะเดียวกันจะมีสภาวะความเสี่ยงมาคู่กับความมั่นคงปลอดภัยในโลกไซเบอร์อยู่เสมอ ซึ่งในด้านการดำเนินงานนั้นถือได้ว่าความมั่นคงปลอดภัยของไซบอร์นั้น เป็นสิ่งประกันความสำเร็จในการบรรลุเป้าหมายขององค์การ ในบทนี้จะรวบรวมเนื้อหาที่เป็นแนวคิด ทฤษฎีและยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ขีดความสามารถด้านไซเบอร์ และสงครามอิเล็กทรอนิกส์

แนวคิด ทฤษฎี ขีดความสามารถด้านไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562 ได้ให้คำจำกัดความของไซเบอร์ ว่าหมายถึงข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ (Computer Networks) ระบบสารสนเทศ (Information Systems) ระบบอินเทอร์เน็ต (Internet Systems) ระบบโทรคมนาคม (Telecommunication Systems) ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition : SCADA) และระบบควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Embedded Systems) รวมทั้งการให้บริการโดยปกติของดาวเทียม (Satellite) และระบบเครือข่าย (Networks) ที่คล้ายคลึงกันที่มีการเชื่อมต่อกัน มีคุณลักษณะเฉพาะ (สำนักนายกรัฐมนตรี, 2560) ดังนี้

1. ไซเบอร์ถูกสร้างขึ้น ดำเนินการบำรุงรักษา และครอบครองเป็นเจ้าของ ตลอดจนดำเนินการทั้งในลักษณะที่เป็นสาธารณะ เป็นของเอกชน และดำเนินการโดยรัฐบาล ซึ่งเกิดขึ้นทั่วไปในโลก เปลี่ยนแปลงอย่างรวดเร็วเมื่อเทคโนโลยี สถาปัตยกรรม กระบวนการและความรู้ความชำนาญมีการพัฒนาร่วมกัน เพื่อสร้างขีดความสามารถให้มีประสิทธิภาพเพิ่มขึ้น

2. การปฏิบัติการทางไซเบอร์มีอัตราสูงขึ้น ซึ่งได้ประโยชน์จากข้อมูลที่มีคุณภาพต่อการตกลงใจที่มีการเคลื่อนที่ด้วยความเร็วใกล้กับความเร็วของแสง โดยสามารถปฏิบัติการข้ามมิติได้ทั้งมิติทางบก มิติทางน้ำ มิติทางอากาศ และมิติอวกาศ

3. การปฏิบัติการไซเบอร์เป็นการปฏิบัติการไร้พรมแดน อยู่เหนือจากเขตแดนทางภูมิรัฐศาสตร์และองค์การที่กำหนดไว้โดยทั่วไป ซึ่งปฏิบัติการทางไซเบอร์จะเข้ามามีบทบาทในทุกมิติและทุกระดับของสงคราม

4. สงครามไซเบอร์เป็นสงครามอสมมาตร (Asymmetric Warfare) ที่อาศัยความได้เปรียบด้านความเร็ว ซึ่งเกิดจากบุคลากรที่เหนือกว่า เทียบกับความได้เปรียบด้านขนาด ซึ่งเกิดจากยุทโธปกรณ์ในสงครามตามรูปแบบและสมมาตร

5. บุคลากรที่เชี่ยวชาญด้านปฏิบัติการไซเบอร์ มีอยู่โดยทั่วไปในองค์กรทั่วประเทศ

6. ความร่วมมือระหว่างหน่วยงานภาครัฐ เอกชน และชาติพันธมิตรเป็นสิ่งจำเป็นอย่างยิ่งในการดำเนินงานด้านปฏิบัติการไซเบอร์ให้เป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ

7. ทุกคนมีส่วนร่วมในปฏิบัติการไซเบอร์ทันทีที่ต่อเชื่อมเข้าสู่ระบบอินเทอร์เน็ตหรือเข้าสู่ระบบเครือข่ายสาธารณะ

แนวคิด ทฤษฎี และยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

ความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร ก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็ว และปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลจนถึงระดับประเทศชาติ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงทางไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อการป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ความมั่นคงปลอดภัยไซเบอร์ มีวิวัฒนาการมาจากการเติบโตของระบบคอมพิวเตอร์สู่การพัฒนาเป็นเครือข่ายคอมพิวเตอร์ และการใช้ประโยชน์ผ่านการติดต่อสื่อสาร นั่นคือเกี่ยวกับความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศเป็นหลักนั่นเอง

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (สำนักนายกรัฐมนตรี, 2560)

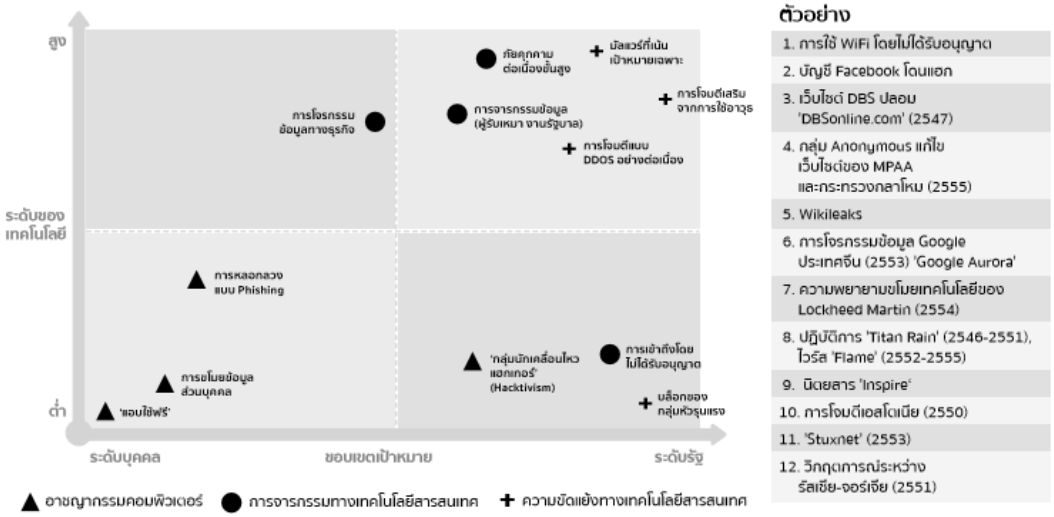
“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ภัยคุกคามทางไซเบอร์ที่พบในระบบเครือข่าย (ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ, ออนไลน์, 2558) มีดังนี้

1. Distributed Denial of Service: DDoS คือ การโจมตีเครื่องคอมพิวเตอร์เป้าหมายหรือระบบเป้าหมายบนอินเทอร์เน็ตของแฮกเกอร์ เพื่อทำให้ระบบเป้าหมายไม่มีการตอบสนองต่อการร้องขอหรือหยุดให้บริการ (Danial of Service) โดยลักษณะการโจมตีจะมีหลากหลายรูปแบบ ได้แก่ การโจมตีแบบ Ping of Death, UDO Flood, Tear Drop

2. Ransomware หรือ มัลแวร์ (Malware) เรียกค่าไถ่ ที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น คือ ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้อื่นแต่อย่างใด แต่จะเข้ารหัสหรือล็อคไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดหรือเข้าถึงไฟล์เหล่านั้นได้ ดังนั้น ผู้ใช้ต้องทำการจ่ายเงินตามการเรียกเก็บ เพื่อให้ได้ข้อมูลคืนมา

ท่ามกลางการขยายตัวของภัยคุกคามจากการโจมตี แอปพลิเคชั่น (Application) ที่มากมายในตลาดโลก และเทคโนโลยีอัจฉริยะมีความก้าวหน้ามาก การถือกำเนิดของ อินเทอร์เน็ตของสรรพสิ่ง หรือ Internet of Things (IoT) ทำให้อุปกรณ์อัจฉริยะเป็นจุดอ่อน และจุดแข็งในคราวเดียวกัน เนื่องจากอาจเป็นเป้าหมายการโจมตีเพื่อควบคุมระบบประมวลผลของข้าศึกปัจจุบัน ระบบที่น่าเป็นห่วงอย่างยิ่งในการถูกโจมตี คือ ระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งรัฐนิยมใช้ควบคุมอุปกรณ์ของโรงงาน สาธารณูปโภคและโครงสร้างพื้นฐาน

แผนภาพที่ 2-1 ภัยคุกคามต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการจารกรรมต่อบุคคลหรือรัฐ



ที่มา : ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ, ออนไลน์, 2558

การก่อการร้ายและทฤษฎีการก่อการร้าย

แนวคิดเกี่ยวกับการก่อการร้ายและทฤษฎีการก่อการร้าย โดยทั่วไปมีการให้คำนิยามและความหมายที่แตกต่างกันออกไป ขึ้นอยู่กับมุมมองของแต่ละประเทศว่ามีการเผชิญสถานการณ์และความสัมพันธ์กับระดับหรือรูปแบบการก่อการร้ายอย่างไร โดยหน่วยงาน Central Intelligence Agency (CIA) ให้นิยามว่า “การก่อการร้าย หมายถึง ปฏิบัติการรุนแรงที่มีการคิดและการเตรียมการไว้ล่วงหน้า โดยมีเหตุจูงใจทางการเมือง กระทำต่อเป้าหมายซึ่งไม่ได้มีส่วนเกี่ยวข้องกับสงครามและไม่มีศักยภาพในการทำการรบ โดยกลุ่มหรือขบวนการที่มิได้เป็นตัวแทนของรัฐในทางการเมืองระหว่างประเทศ หรือโดยกลุ่มสายลับของรัฐที่กระทำการในทางลับ” (ธันยวัต ชูส่งแสง, 2547)

กระทรวงกลาโหมสหรัฐฯ ให้ความหมายว่า “การก่อการร้าย คือการใช้ความรุนแรงหรือการข่มขู่ว่าจะใช้ความรุนแรงที่ได้คิดการไว้ จนทำให้ฝ่ายตรงข้ามเกิดความรู้สึกหวาดกลัว โดยมีเจตนาที่จะบีบบังคับหรือคุกคามรัฐบาลหรือสังคมกลุ่มใด เพื่อให้บรรลุจุดมุ่งหมาย ซึ่งโดยทั่วไปเป็นทางการเมือง ศาสนา และลัทธิ” (พงศธร สัตย์เจริญ, 2549) อีกความหมายหนึ่ง คือ ยุทธศาสตร์ของความรุนแรงซึ่งมุ่งผลด้านจิตใจ โดยเฉพาะอย่างยิ่งความหวาดกลัวต่อกลุ่มเป้าหมาย เพื่อบรรลุวัตถุประสงค์ทางการเมืองอย่างใดอย่างหนึ่งหรือหลายอย่าง หรือเป็นแนวทางปฏิบัติหรือทฤษฎีที่อยู่เบื้องหลังแนวทางปฏิบัติ ซึ่งกลุ่มใดหรือพรรคใด ๆ นำไปใช้ปฏิบัติเพื่อบรรลุเป้าหมายที่ตั้งใจไว้โดยการใช้ความรุนแรงอย่างเป็นระบบ (ศูนย์การศึกษาการก่อการร้าย, 2563) การกระทำที่เป็นลักษณะที่เรียกว่าการก่อการร้ายตามทฤษฎีสงคราม การก่อการร้ายถือเป็นการทำสงครามในลักษณะหนึ่ง หรือเป็นสงครามที่มีต้นทุนต่ำที่สุด เปิดศึกได้ง่าย ความเสี่ยงต่ำ ความอยู่รอดสูง การสูญเสียชีวิตและทรัพย์สินในการก่อสงครามต่ำ (Geocities, 2004) ในขณะเดียวกันคู่กรณีมีความเสียหายสูง ในลักษณะเชิงเปรียบเทียบ ตามประวัติศาสตร์ทางสงครามพบว่า สงครามก่อการร้าย สงครามกบฏศึก หรือสงครามกองโจร และสงครามกลางเมืองมีความสัมพันธ์กัน เนื่องจากเห็นว่าเป็นการสร้างความศรัทธา หรือการสร้างความหวาดกลัวให้กับผู้ที่ไม่เกี่ยวข้องกับสงคราม ทำให้ต้องเลือกฝ่ายเข้าเป็นแนวร่วม เพื่อให้การสนับสนุนทั้งรูปธรรม เช่น การสนับสนุนเสบียง เสื้อผ้า อาวุธ ยุทโธปกรณ์ และรูปธรรม เช่น การหาข่าว เป็นฐานเสียงแสดงพลังฐานความนิยม ซึ่งเป็นองค์ประกอบสำคัญในการสถาปนาอำนาจรัฐเมื่อบรรลุเป้าหมายสงครามเรียบร้อยบริบูรณ์ ดังนั้น ผู้ที่ได้รับผลกระทบคือประชาชนโดยตรง นอกจากนี้ ยังมีการนำประชาชนมาเป็นเครื่องต่อรองเพื่อความสำเร็จในการใช้เป็นเครื่องเรียกร้องความสนใจจากมวลชน จนมีคำกล่าวว่า การก่อการร้ายเป็นส่วนหนึ่งของกลยุทธ์หรือยุทธวิธีในสงครามกองโจร (Guerrilla Warfare) (โกวิท วงศ์สุรวัฒน์, 2550)

การก่อการร้าย (Terrorism) มีต้นกำเนิดมาจากเหตุการณ์ความรุนแรงทางการเมืองในประเทศฝรั่งเศสหลังการปฏิวัติเปลี่ยนแปลงการปกครองจากระบอบสมบูรณาญาสิทธิราชย์มาเป็นสาธารณรัฐ ในปี ค.ศ.1789 ตั้งแต่นั้นมาคำว่า การก่อการร้ายได้ถูกใช้อย่างกว้างขวางในการอธิบายถึงพฤติกรรมที่รุนแรง เท็ด โรเบิร์ต กูร์ (Gurr, 1988) สรุปว่า การก่อการร้ายประกอบด้วยองค์ประกอบ 3 ส่วน ได้แก่ 1) มียุทธศาสตร์ รูปแบบ และวิธีการที่เด่นชัดเพื่อบรรลุเป้าหมายที่ต้องการ เช่น การลอบวางระเบิด การลอบวางเพลิง 2) มีการพุ่งเป้าประสงค์ไปที่สาธารณะชนหรือเป้าหมายทางการเมือง รวมถึงตึกอาคาร สัญลักษณ์ทางการเมือง กองกำลังทหารและตำรวจ อีกทั้งเป้าหมายเอกชนที่อาจเป็นตัวเลือก อันเนื่องมาจากมีความเกี่ยวพันกับกลุ่มการเมืองหรือเนื่องจากเหตุผลส่วนบุคคล 3) ลักษณะของการกระทำการก่อการร้ายจะมีการแสดงออกถึงการใช้ความรุนแรง (Violence) โดยกลุ่มหรือบุคคลหรือกลุ่มบุคคลอย่างลับ เป็นแนวทางเดียวกับ ธอมัส พี. ทอร์นตัน (Thornton, 2005) ได้นำเสนอคำนิยามของการก่อการร้ายว่าเป็นการกระทำเชิงสัญลักษณ์ มีจุดมุ่งหมายเพื่อสร้างอิทธิพลเหนือพฤติกรรมทางการเมืองของประเทศ โดยวิถีทางที่ไม่ปกติ อย่างเช่นการใช้ความรุนแรงเป็นเครื่องมือบรรลุเป้าหมาย ในมุมมองของทอร์นตัน การก่อการร้ายจึงเป็นเสมือนสัญลักษณ์การตอบโต้ทางการเมืองและเป็นอาวุธของผู้ที่อ่อนแอกว่าในการใช้ต่อต้านผู้ที่มีอำนาจเหนือกว่าทางการเมือง นอกจากนี้ ทอร์นตันเชื่อว่า การกระทำที่สร้างความหวาดกลัวคล้ายกับการจงใจเพื่อการโฆษณาการกระทำของตน

โดยการส่งผ่านข้อความ สัญลักษณ์ หรือการเตือนไปถึงฝ่ายตรงข้าม กลุ่มประชาชนที่เป็นกลาง และประชาชนที่เป็นพวกเดียวกันกับพวกเขาหรือเข้าข้างหรือเห็นอกเห็นใจกับขบวนการก่อการร้าย เห็นได้ชัดว่าการให้ความหมายของคำว่า การก่อการร้ายของแต่ละประเทศมีความแตกต่างกัน มีลักษณะไม่ชัดเจน จึงสรุปได้ว่า การก่อการร้าย หมายถึงการกระทำความผิดโดยใช้กำลังประทุษร้าย หรือการกระทำการอันใดอันก่อให้เกิดอันตรายต่อชีวิต ร่างกายหรือเสรีภาพของผู้อื่น ทำให้เกิดความเสียหายอย่างร้ายแรงต่อโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ทำให้เกิดการเสียหายต่อทรัพย์สินไม่ว่าของรัฐใด บุคคลใด หรือแก่สิ่งแวดล้อมโดยเป็นการกระทำเพื่อขู่เข็ญหรือบังคับรัฐบาลในระดับประเทศ ระดับองค์กร หรือระหว่างประเทศหรือสร้างความหวาดกลัวในหมู่ประชาชน

ประเภทของการก่อการร้าย มีการแบ่งประเภทหลายรูปแบบแตกต่างกันออกไป อาทิ ดลยา เทียนทอง (2549) แบ่งประเภทการก่อการร้ายตามขอบเขตของการปฏิบัติการ (Rage of Operations) ได้ 8 ประเภท ดังนี้ การก่อการร้ายโดยรัฐ (State Terrorism) การก่อการร้ายที่เกิดจากความคิดเห็นที่ไม่ลงรอย (Dissident Terrorism) การก่อการร้ายโดยกลุ่มฝ่ายซ้าย (Leftist Terrorism) การก่อการร้ายโดยกลุ่มฝ่ายขวา (Rightist Terrorism or Neo – fascism) การก่อการร้ายในทางอาชญากรรม (Criminal Dissident Terrorism) การก่อการร้ายโดยกลุ่มเคร่งศาสนา (Religious Terrorism) การก่อการร้ายโดยกลุ่มอนาธิปไตย (Anarchist Terrorism) และการก่อการร้ายสากลหรือระหว่างประเทศ (International Terrorism) ด้านแนวทาง มีการแบ่งประเภทลัทธิของการก่อการร้ายตามวัตถุประสงค์ของการก่อการร้าย เป็น 4 ประเภท คือ 1) กระทำความผิดกฎหมาย (Criminal) เป็นปฏิบัติใช้ความสยดสยอง หวาดกลัว เพื่อผลประโยชน์ตามต้องการ 2) ทางจิตวิญญาณ (Psychic) จะเกี่ยวข้องกับความเชื่อเรื่องเวทย์มนต์คาถา เทพนิยายและลัทธิไสยศาสตร์ ซึ่งถูกโน้มน้าวจากการคลั่งศาสนา 3) ด้านการสงคราม (War) เป็นการทำลายล้างศัตรูในทุกวิถีทางที่จะทำได้ 4) ด้านการเมือง (Political) เป็นการใช้ความรุนแรงและความกลัวอย่างเป็นระบบเพื่อให้บรรลุวัตถุประสงค์ทางการเมือง สรุปได้ว่า การแบ่งประเภทของการก่อการร้ายในปัจจุบันยังมีความหลากหลาย ขึ้นอยู่กันแนวคิดหรือปรัชญาพื้นฐานในการนำมาแบ่งกลุ่มหรือจัดประเภท ซึ่งผู้วิจัยมุ่งเน้นศึกษาการก่อการร้ายทางไซเบอร์ตามวัตถุประสงค์หลักของการวิจัย

การก่อการร้ายทางไซเบอร์ (Cyber Terrorism) เป็นการก่อการร้ายที่มีความเกี่ยวพันกับความทันสมัยของเทคโนโลยีที่ช่วยให้กลุ่มก่อการร้ายดำเนินกิจกรรมต่าง ๆ ได้อย่างมีประสิทธิภาพ โดยใช้พลังอำนาจของเทคโนโลยีสารสนเทศเป็นแนวทางปฏิบัติหรือปรับองค์กรไปสู่รูปแบบใหม่ มีการคาดการณ์ว่าการก่อการร้ายทางไซเบอร์จะเป็นรูปแบบการก่อการร้ายที่เป็นอีกหนึ่งยุทธวิธีในการต่อสู้มากขึ้น โดยสามารถสร้างความเสียหายให้เกิดผลกระทบทั้งทางด้านจิตวิทยาและดึงดูดความสนใจจากสื่อมวลชนหรือบุคคล การก่อการร้ายรูปแบบนี้จะอาศัยช่องว่างจากการขยายตัวของระบบที่มีลักษณะของการเชื่อมโยงข้อมูลผ่านคอมพิวเตอร์ในระบบเครือข่ายสมัยใหม่ จึงตกเป็นเป้าหมายของการโจมตีทางไซเบอร์เพื่อทำลายหรือขัดขวางการทำงานของระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายคอมพิวเตอร์ที่ควบคุมการทำงานระบบสาธารณูปโภค โครงสร้างพื้นฐาน ระบบทางด้านความมั่นคงทางทหาร หรือการล้วงข้อมูลสำคัญต่าง ๆ เป็นต้น

ยุทธศาสตร์ด้านความมั่นคง และยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การพัฒนาด้านเทคโนโลยี ระบบสารสนเทศ ระบบสื่อสารโทรคมนาคม และระบบดิจิทัลของประเทศไทยต้องดำเนินการควบคู่กัน มีความสอดคล้องกันตามยุทธศาสตร์ชาติ 20 ปี ในส่วนยุทธศาสตร์ความมั่นคงและยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 - 2564 ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องอาศัยความร่วมมือจากทุกภาคส่วนตามบทบาทและหน้าที่ที่รับผิดชอบของทั้งภาครัฐ ภาคเอกชน ประชาชน รวมทั้งจัดหาเครื่องมือและขั้นตอนที่มีประสิทธิภาพในการลดความเสี่ยง การควบคุมดูแลภัยคุกคามต่าง ๆ ให้อยู่ในระดับที่ปลอดภัย การดำเนินการภาคประชาขน เช่น การรับมือกับสถานการณ์การคุกคามทางไซเบอร์ ต้องสร้างความตระหนักรู้ให้กับประชาชน โดยแนวคิดนี้ได้ถูกกำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งนับเป็นการดำเนินการอย่างจริงจังเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่บูรณาการจากทุกภาคส่วน

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580)

เป็นยุทธศาสตร์ชาติฉบับแรกของประเทศไทย ใช้เป็นกรอบในการจัดทำแผนด้านต่าง ๆ ให้สอดคล้องและบูรณาการร่วมกัน เพื่อให้เกิดเป็นพลังผลักดันไปสู่การบรรลุเป้าหมายตามวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” มีการกำหนดเป้าหมายและประเด็นการพัฒนาประเทศตามแนวทางยุทธศาสตร์ชาติ ที่มุ่งเน้นการสร้างสมดุลระหว่างการพัฒนาความมั่นคง เศรษฐกิจ สังคม และสิ่งแวดล้อม โดยการมีส่วนร่วมของทุกภาคส่วนในรูปแบบ “ประชารัฐ” ประกอบด้วย 6 ยุทธศาสตร์ โดยมีเป้าหมายและประเด็นการพัฒนา (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561) ดังนี้

1. **ยุทธศาสตร์ชาติด้านความมั่นคง** มีเป้าหมายการพัฒนาที่สำคัญ คือ ประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัย เอกราช อธิปไตย และมีความสงบเรียบร้อยในทุกระดับ ตั้งแต่ระดับชาติ สังคม ชุมชน มุ่งเน้นการพัฒนาคน เครื่องมือ เทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ให้มีความพร้อม สามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบและทุกระดับความรุนแรง ควบคู่ไปกับการป้องกันและแก้ไขปัญหาด้านความมั่นคงที่มีอยู่ในปัจจุบันและที่อาจจะเกิดขึ้นในอนาคต ใช้กลไกการแก้ไขปัญหาแบบบูรณาการทั้งกับส่วนราชการ ภาคเอกชน ประชาสังคม และองค์กรที่ไม่ใช่รัฐ รวมถึงประเทศเพื่อนบ้าน และมิตรประเทศทั่วโลกบนพื้นฐานของหลักธรรมาภิบาล เพื่อเอื้ออำนวยประโยชน์ต่อการดำเนินการของยุทธศาสตร์ชาติด้านอื่น ๆ ให้สามารถขับเคลื่อนไปได้ตามทิศทางและเป้าหมายที่กำหนด

2. **ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน** มีเป้าหมายการพัฒนาที่มุ่งเน้นการยกระดับศักยภาพของประเทศในหลากหลายมิติ บนพื้นฐานแนวคิด 3 ประการ ได้แก่ (1) “ต่อยอดอดีต” โดยมองกลับไปที่รากเหง้าทางเศรษฐกิจ อัตลักษณ์ วัฒนธรรม ประเพณี วิถีชีวิต และจุดเด่นทางทรัพยากรธรรมชาติที่หลากหลาย รวมทั้งความได้เปรียบเชิงเปรียบเทียบของประเทศ

ในด้านอื่น ๆ นำมาประยุกต์ผสมผสานกับเทคโนโลยีและนวัตกรรม เพื่อให้สอดรับกับบริบทของเศรษฐกิจและสังคมโลกสมัยใหม่ (2) “ปรับปัจจุบัน” เพื่อปูทางสู่อนาคต ผ่านการพัฒนาโครงสร้าง พื้นฐานของประเทศในมิติต่าง ๆ ทั้งโครงข่ายระบบคมนาคมและขนส่ง โครงสร้างพื้นฐานวิทยาศาสตร์ เทคโนโลยีและดิจิทัล และการปรับสภาพแวดล้อมให้เอื้อต่อการพัฒนาอุตสาหกรรมและบริการอนาคต และ (3) “สร้างคุณค่าใหม่ในอนาคต” ด้วยการเพิ่มศักยภาพของผู้ประกอบการพัฒนาคนรุ่นใหม่ รวมถึงปรับรูปแบบธุรกิจเพื่อตอบสนองต่อความต้องการของตลาด ผสมผสานกับยุทธศาสตร์ที่รองรับอนาคต บนพื้นฐานของการต่อยอดอดีตและปรับปัจจุบัน พร้อมทั้งการส่งเสริมและสนับสนุนจากภาครัฐ ให้ประเทศไทยสามารถสร้างฐานรายได้และการจ้างงานใหม่ ขยายโอกาสทางการค้าและการลงทุนในเวทีโลก ควบคู่ไปกับการยกระดับรายได้และการกินดีอยู่ดี รวมถึงการเพิ่มขึ้นของคนชั้นกลาง และลดความเหลื่อมล้ำของคนในประเทศได้ในคราวเดียวกัน

3. ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ มีเป้าหมายการพัฒนาที่สำคัญเพื่อพัฒนาคนในทุกมิติและในทุกช่วงวัยให้เป็นคนดี เก่ง และมีคุณภาพ โดยคนไทย มีความพร้อมทั้งกาย ใจ สติปัญญา มีพัฒนาการที่ดีรอบด้านและมีสุขภาวะที่ดีในทุกช่วงวัย มีจิตสาธารณะ รับผิดชอบต่อสังคมและผู้อื่น มัธยัสถ์ อดออม โอบอ้อมอารี มีวินัย รักษาศีลธรรม และเป็นพลเมืองดีของชาติ มีหลักคิดที่ถูกต้อง มีทักษะที่จำเป็นในศตวรรษที่ 21 มีทักษะสื่อสารภาษาอังกฤษและภาษาที่สามและอนุรักษ์ภาษาท้องถิ่น มีนิสัยรักการเรียนรู้และการพัฒนาตนเองอย่างต่อเนื่องตลอดชีวิต สู่การเป็นคนไทยที่มีทักษะสูง เป็นนวัตกร นักคิด ผู้ประกอบการ เกษตรกรยุคใหม่ และอื่น ๆ โดยมีสัมมาชีพตามความถนัดของตนเอง

4. ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม มีเป้าหมายการพัฒนาที่ให้ความสำคัญกับการดึงเอาพลังของภาคส่วนต่าง ๆ ทั้งภาคเอกชน ประชาสังคม ชุมชนท้องถิ่น มาร่วมขับเคลื่อน โดยการสนับสนุนการรวมตัวของประชาชน ในการร่วมคิดร่วมทำเพื่อส่วนรวม การกระจายอำนาจและความรับผิดชอบไปสู่กลไกบริหารราชการแผ่นดินในระดับท้องถิ่น การเสริมสร้างความเข้มแข็งของชุมชนในการจัดการตนเอง และการเตรียมความพร้อมของประชากรไทย ทั้งในมิติสุขภาพ เศรษฐกิจ สังคม และสภาพแวดล้อม ให้เป็นประชากรที่มีคุณภาพ สามารถพึ่งตนเองและทำประโยชน์แก่ครอบครัว ชุมชนและสังคมให้นานที่สุด โดยรัฐให้หลักประกันการเข้าถึงบริการและสวัสดิการที่มีคุณภาพอย่างเป็นธรรมและทั่วถึง

5. ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม มีเป้าหมายการพัฒนาที่สำคัญเพื่อการบรรลุเป้าหมายการพัฒนาที่ยั่งยืนในทุกมิติ ทั้งด้านสังคม เศรษฐกิจ สิ่งแวดล้อม ธรรมาภิบาล และความเป็นหุ้นส่วนความร่วมมือระหว่างกัน ทั้งภายในและภายนอกประเทศอย่างบูรณาการ ใช้พื้นที่เป็นตัวตั้งในการกำหนดกลยุทธ์และแผนงาน และการให้ทุกฝ่ายที่เกี่ยวข้องได้เข้ามามีส่วนร่วมในแบบทางตรงให้มากที่สุดเท่าที่จะเป็นไปได้ โดยเป็นการดำเนินการบนพื้นฐานการเติบโตร่วมกัน ไม่ว่าจะเป็นทางเศรษฐกิจ สิ่งแวดล้อม และคุณภาพชีวิต โดยให้ความสำคัญกับการสร้างสมดุลทั้ง 3 ด้าน อันจะนำไปสู่ความยั่งยืนเพื่อคนรุ่นต่อไปอย่างแท้จริง

6. ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ
มีเป้าหมายการพัฒนาที่สำคัญเพื่อปรับเปลี่ยนภาครัฐที่ยึดหลัก “ภาครัฐของประชาชน เพื่อประชาชน และประโยชน์ส่วนรวม” โดยภาครัฐต้องมีขนาดที่เหมาะสมกับบทบาทภารกิจ แยกแยะบทบาทหน่วยงานของรัฐที่ทำหน้าที่ในการกำกับหรือในการให้บริการในระบบเศรษฐกิจที่มีการแข่งขัน มีสมรรถนะสูง ยึดหลักธรรมาภิบาล ปรับวัฒนธรรมการทำงานให้มุ่งผลสัมฤทธิ์และผลประโยชน์ส่วนรวม มีความทันสมัย และพร้อมที่จะปรับตัวให้ทันต่อการเปลี่ยนแปลงของโลกอยู่ตลอดเวลา โดยเฉพาะอย่างยิ่งการนำนวัตกรรม เทคโนโลยีข้อมูลขนาดใหญ่ระบบการทำงานที่เป็นดิจิทัลเข้ามาประยุกต์ใช้อย่างคุ้มค่า และปฏิบัติงานเทียบได้กับมาตรฐานสากล รวมทั้งมีลักษณะเปิดกว้างเชื่อมโยงถึงกัน และเปิดโอกาสให้ทุกภาคส่วนเข้ามามีส่วนร่วมเพื่อตอบสนองความต้องการของประชาชนได้อย่างสะดวก รวดเร็ว และโปร่งใส โดยทุกภาคส่วนในสังคมต้องร่วมกันปลูกฝังค่านิยมความซื่อสัตย์สุจริต ความมัธยัสถ์ และสร้างจิตสำนึกในการปฏิเสธไม่ยอมรับการทุจริตประพฤติมิชอบ อย่างสิ้นเชิง นอกจากนั้น กฎหมายต้องมีความชัดเจน มีเพียงเท่าที่จำเป็น มีความทันสมัย มีความเป็นสากล มีประสิทธิภาพ และนำไปสู่การลดความเหลื่อมล้ำและเอื้อต่อการพัฒนา โดยกระบวนการยุติธรรมมีการบริหารที่มีประสิทธิภาพ เป็นธรรม ไม่เลือกปฏิบัติ และการอำนวยความยุติธรรมตามหลักนิติธรรม

ยุทธศาสตร์การรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564

จากกรอบยุทธศาสตร์ชาติ 20 ปี นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2560 - 2564) แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ตลอดจนแนวคิดของนายกรัฐมนตรี ที่นำเสนอในการประชุมสุดยอดอาเซียน ประมวลเป็นยุทธศาสตร์การรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564 โดยกำหนดวิสัยทัศน์ “ไซเบอร์สเปซของไทยมีความมั่นคงปลอดภัย ทุกภาคส่วนมั่นใจ มีความพร้อมรับมือกับภัยคุกคามทางไซเบอร์และร่วมมือกันใช้ไซเบอร์อย่างสร้างสรรค์ เพื่อส่งเสริมความมั่นคงทางเศรษฐกิจและคุณภาพชีวิตที่ดี” ซึ่งแผนยุทธศาสตร์ฉบับนี้มุ่งหมายให้ภาครัฐ ภาคธุรกิจ และภาคประชาชนใช้เป็นกรอบการดำเนินงานให้เกิดสมดุลระหว่างสิทธิเสรีภาพของประชาชนและการใช้อำนาจรัฐเชิงนโยบาย ในการควบคุมและรักษาความสงบเรียบร้อยของสังคม (สำนักนายกรัฐมนตรี, 2560) ประกอบด้วย

ประเด็นยุทธศาสตร์ที่ 1 เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ 3 ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ 4 เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ 5 สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ 6 ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซไปในทางที่เหมาะสมและเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์

ประเด็นยุทธศาสตร์ที่ 7 ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ 8 ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

สภาพแวดล้อมขีดความสามารถด้านไซเบอร์ของประเทศไทยและต่างประเทศ

ในสภาวการณ์ปัจจุบันที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็วที่เรียกว่า Disruptive เป็นภาวะการเปลี่ยนแปลงฉับพลันสู่ยุคดิจิทัล ที่ความปลอดภัยทางไซเบอร์นับเป็นเรื่องที่มีความสำคัญและจำเป็น แต่ปัจจัยที่ต้องไตร่ตรองให้รอบคอบคือความสมดุลระหว่างความปลอดภัยและความเจริญเติบโตของยุคดิจิทัล ซึ่งถ้าให้น้ำหนักที่ระดับความปลอดภัยมากเกินไป อาจทำให้เป็นอุปสรรคต่อการเจริญเติบโตของอุตสาหกรรมหรือธุรกิจในอนาคตได้ การให้ความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลเพิ่มสูงขึ้น ดังในรายงาน Global Risks Report 2019 ของ Economic Forum ชี้ให้เห็นว่า การโจมตีทางไซเบอร์และการจารกรรมข้อมูล ถูกจัดอยู่ 1 ใน 5 อันดับแรกของความเสี่ยงทั่วโลก ซึ่งถือเป็นความท้าทายทางเศรษฐกิจ ความมั่นคงของประเทศ เสถียรภาพการจ้างงาน และสำหรับประเทศไทย ตามการจัดอันดับ Global Cyber Security Index 2018 (CGI) หรือดัชนีความมั่นคงปลอดภัยไซเบอร์โลกพบว่า ประเทศไทยมีความพร้อมอยู่ในอันดับที่ 35 ซึ่งลดลงจาก 2 ปีที่ผ่านมา (อยู่ในอันดับที่ 20) แสดงให้เห็นว่าการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ยังเป็นสิ่งที่ภาครัฐและเอกชนควรให้ความสำคัญอย่างเร่งด่วน ทั้งนี้ องค์การการค้าโลก (WTO) ได้ระบุว่า แม้มาตรการเพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ ถือเป็นสิ่งสำคัญและจำเป็นสำหรับรัฐในการสร้างความมั่นคงของรัฐ (National Security Exception) และสร้างความเชื่อมั่นของผู้บริโภคในการใช้บริการดิจิทัล แต่หากมาตรการดังกล่าวมีลักษณะกีดกันทางการค้า แอบแฝงการสนับสนุนผู้ประกอบการภายในประเทศเป็นการเฉพาะ ย่อมเป็นการขัดต่อหลักการของความตกลงทั่วไปว่าด้วยการค้าบริการ (GATS) จากการสำรวจกฎหมายและมาตรการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป ซึ่งเป็นต้นแบบของกฎหมายและมาตรการของประเทศไทย เวียดนาม และสิงคโปร์ พบว่ามาตรการของสหภาพยุโรปส่วนใหญ่นั้น ต้องการสร้างความมั่นคงปลอดภัยทางไซเบอร์บนพื้นฐานของการก่อให้เกิดอุปสรรคทางการน้อยที่สุด เนื่องจากสหภาพยุโรปมีแนวคิดเรื่องการเป็นตลาดเดียวและมีแผนปฏิบัติการอย่างชัดเจน

นงรัตน์ สายเพชร (2556) การพัฒนาด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศเริ่มต้นนับตั้งแต่ประมาณ ปี ค.ศ.1969 สหรัฐอเมริกาและสหภาพโซเวียต ได้แข่งขันกันพัฒนาเทคโนโลยีทางทหารจนเกิดเทคโนโลยีใหม่ในกองทัพเพื่อสร้างความได้เปรียบในเชิงยุทธศาสตร์และการสงคราม โดยเริ่มจากอาร์พาเน็ต (ARPAnet) ซึ่งเป็นเครือข่ายคอมพิวเตอร์ภายใต้ความรับผิดชอบของหน่วยงานวิจัยด้านการทหารเป็นครั้งแรก และพัฒนาอย่างต่อเนื่อง จนกระทั่งในปี ค.ศ.2000 สหรัฐฯ ได้รับการยอมรับว่ามีสัดส่วนการใช้งานอินเตอร์เน็ตต่อประชากรสูงที่สุดในโลก จุดเริ่มต้นสงครามคอมพิวเตอร์ เริ่มขึ้นในช่วงกลางยุค 1990 สหรัฐฯ ออกคำเตือนเรื่องการโจมตีระบบสื่อสารและระบบโครงสร้างพื้นฐานที่สำคัญ โดยผู้ก่อการร้ายที่อยู่ทั้งภายในรัฐและนอกรัฐ ภัยก่อการร้ายไซเบอร์ที่เกิดขึ้นกับความมั่นคงแห่งชาติของสหรัฐฯ ไม่ได้จำกัดอยู่เพียงเป้าหมายทางทหาร แฮคเกอร์และรัฐบาลประเทศต่าง ๆ ได้เพิ่มความสามารถในการบุกรุกเข้าสู่เครือข่ายโครงสร้างสาธารณูปโภคของพลเรือนที่มีการพึ่งพาเทคโนโลยีเครือข่าย นอกจาก

การโจมตีทางไซเบอร์แล้ว สหรัฐฯ ได้ใช้ศักยภาพการทำสงครามไซเบอร์ร่วมกับการนำระบบสารสนเทศมาใช้ในการจัดการกับสมรภูมิรบ ไม่ว่าจะเป็นภาคพื้นดิน ทะเล อากาศ และอวกาศ มีการพัฒนาเครื่องบินสอดแนมที่ทันสมัยมาใช้มากขึ้น และดำเนินภารกิจต่อสู้และโจมตีกลุ่มก่อการร้ายในหลายประเทศ พร้อมปรับยุทธวิธีด้วยการนำอากาศยานไร้คนขับ (Unmanned Arial Vehicle: UAV) หรือโดรน (Drone) มาใช้ในการปฏิบัติการ ในปี ค.ศ.2012 รัฐบาลสหรัฐฯ มีแผนปรับลดกำลังทางทหารลงร้อยละ 14 เพื่อนำงบประมาณไปลงทุนในการพัฒนาเทคโนโลยีในห้วงอวกาศและโลกไซเบอร์ ที่สามารถรับมือจากการโจมตีได้ทุกสมรภูมิ และสามารถใช้ความก้าวหน้านี้ตอบโต้กับการท้าทายอำนาจของสหรัฐฯ แสดงให้เห็นว่า ทั้งนโยบายและยุทธศาสตร์ด้านความมั่นคงทางไซเบอร์ ไม่ได้เป็นเพียงนโยบายเพื่อการรักษาความมั่นคงเท่านั้น แต่ยังเป็นยุทธศาสตร์เพื่อการสู้รบในอนาคตที่สหรัฐฯ จะดำรงความเป็นมหาอำนาจของโลกอีกด้วย

ในกลุ่มประเทศอาเซียน จากการประเมินความจำเป็นของมาตรการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย เวียดนาม และสิงคโปร์ พบว่า ทั้ง 3 ประเทศ ได้รับเอาต้นแบบในการสร้างความมั่นคงปลอดภัยทางไซเบอร์จากสหภาพยุโรปมากำหนดเป็นกฎหมายภายใน แต่ได้ขยายขอบเขตของประเด็นผลกระทบต่อความมั่นคงของรัฐ การกำหนดมาตรการสร้างความมั่นคงปลอดภัยทางไซเบอร์ดังกล่าว ส่งผลกระทบต่อความเชื่อมั่นในความมั่นคงของกฎหมายของผู้ประกอบการ และเป็นอุปสรรคทางการค้ากับผู้ประกอบการดิจิทัลที่ให้บริการข้ามพรมแดน นโยบายความมั่นคงไซเบอร์ของสหรัฐฯ มุ่งเน้นให้ประเทศเป็นมหาอำนาจในสมรภูมิใหม่ที่เรียกว่าโลกไซเบอร์ โดยสร้างความเข้มแข็งในระบบความปลอดภัยของเครือข่ายคอมพิวเตอร์แห่งชาติ ครอบคลุมภาคเอกชน สถาบันการเงิน กลุ่มอุตสาหกรรม โทรคมนาคม และกลุ่มพลังงาน

หลักนิยมปฏิบัติการไซเบอร์ของกองทัพอากาศ

กองทัพอากาศได้มุ่งมั่นพัฒนาเสริมสร้างนภานุภาพ (Air Power) ในทั้ง 3 มิติ ได้แก่ มิติทางอากาศ (Air Domain) มิติไซเบอร์ (Cyber Domain) และมิติอวกาศ (Space Domain) อย่างต่อเนื่อง โดยคำนึงถึงความสอดคล้องของการพัฒนาอย่างเป็นระบบและการปฏิบัติที่ประสานสอดคล้องกัน ดังนั้น การปฏิบัติการไซเบอร์จึงเป็นมิติการปฏิบัติการที่มิอาจละเลยได้ โดยเฉพาะอย่างยิ่งการเตรียมความพร้อมในการป้องกันภัยคุกคามทางไซเบอร์ทุกรูปแบบทั้งในปัจจุบันและอนาคตบนพื้นฐานการพึ่งพาตนเอง การเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศภายใต้แนวความคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ประกอบด้วย 6 องค์ประกอบ ได้แก่ ระบบบัญชาการและควบคุม (Command and Control) ระบบการตรวจจับ (Sensor) ผู้ปฏิบัติและหน่วยปฏิบัติ (Shooter) เครือข่าย (Network) ทรัพยากรบุคคลและองค์การ (Human & Organization) และการสนับสนุนและบริการ (Support and Service) โดยมีเครือข่าย (Network) เป็นศูนย์กลางการเชื่อมต่อที่สำคัญของทุกองค์ประกอบ ทั้งนี้ องค์ประกอบสำคัญในการดำรงขีดความสามารถในการติดต่อสื่อสารอย่างเสรี คือระบบเครือข่ายซึ่งต้องมีการรักษาความปลอดภัยจากภัยคุกคามไซเบอร์อย่างเข้มงวดและจริงจัง โดยเฉพาะภัยคุกคามในรูปของสงครามไซเบอร์ (Cyber Warfare) ที่ทวีจำนวนและมีระดับความรุนแรงเพิ่มมากขึ้นทุกขณะ โดยอาศัยความร่วมมือจากบุคลากรทุกระดับ หากระบบเครือข่ายสารสนเทศไม่สามารถตอบสนองต่อความต้องการใช้งานในเวลาที่ต้องการ ระบบบัญชาการและควบคุมก็จะลดประสิทธิภาพลงก่อให้เกิดความไม่สัมฤทธิ์ผล

ในการปฏิบัติในองค์รวม ดังนั้น จึงจำเป็นที่จะต้องหาแนวทางปฏิบัติเพื่อป้องกันภัยอันเกิดจากการกระทำทางไซเบอร์ (หลักนิยมกองทัพอากาศ, 2562)

การปฏิบัติการไซเบอร์ดำเนินการได้ทั้งในยามปกติและยามเกิดเหตุภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนภารกิจของกองทัพอากาศ นับเป็นปัจจัยหลักของความสำเร็จในการปฏิบัติภารกิจภายใต้แนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง เนื่องจากเทคโนโลยีด้านไซเบอร์เปลี่ยนแปลงอยู่เสมออย่างรวดเร็ว จำเป็นที่ผู้เกี่ยวข้องทุกฝ่ายและทุกระดับต้องติดตามและก้าวทันเทคโนโลยี พร้อมทั้งมีจิตสำนึกในเรื่องความมั่นคงปลอดภัยด้านไซเบอร์อย่างจริงจังและต่อเนื่อง จึงจะทำให้การดำเนินการด้านไซเบอร์ของกองทัพอากาศประสบความสำเร็จ

วัตถุประสงค์และขอบเขตการปฏิบัติการไซเบอร์

การปฏิบัติการไซเบอร์เป็นการดำเนินการ (Ways) ที่ใช้ขีดความสามารถทางไซเบอร์ทั้งปวง (Means) ของกองทัพอากาศ เพื่อสนับสนุนหรือเกื้อกูลการปฏิบัติการทางทหารในมิติอื่น ๆ ให้บรรลุวัตถุประสงค์ (Ends) ได้แก่ การได้มาซึ่งความได้เปรียบในมิติไซเบอร์ (Cyberspace Superiority) หรือการครองมิติไซเบอร์ (Cyberspace Control) โดยการขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมถึงการทำลาย การเปลี่ยนแปลง หรือจารกรรมข้อมูลสำคัญ โดยหวังผลให้เกิดความเสียหายทางกายภาพ กระบวนการทำงานหรือทางจิตใจของผู้ปฏิบัติงาน และดำรงอิสระในการใช้งานมิติไซเบอร์ของฝ่ายเรา ซึ่งหมายถึงสภาวะที่ฝ่ายเรามีความได้เปรียบหรือมีอิสระในการปฏิบัติการทางไซเบอร์ได้อย่างปลอดภัย (Secure) เชื่อถือได้ (Reliable) ในห้วงเวลาและสถานที่ที่ต้องการ (Available) โดยปราศจากการกีดขวางหรือรบกวน โดยวัตถุประสงค์ของการปฏิบัติการไซเบอร์ของกองทัพอากาศแบ่งออกเป็น 4 ด้าน (หลักนิยมกองทัพอากาศ, 2562) ดังนี้

1. การป้องกันในมิติไซเบอร์ (Cyberspace Defense) เป็นการปฏิบัติการไซเบอร์เพื่อดำรงการใช้งานระบบเครือข่ายสารสนเทศของกองทัพอากาศ ทั้งระบบสารสนเทศเพื่อการยุทธ์ (Combat Information System: CIS) และระบบสารสนเทศเพื่อการสนับสนุน (Support Information System: SIS) ด้วยการใช้ขีดความสามารถทางไซเบอร์เชิงป้องกัน โดยหน่วยงานไซเบอร์จะรับผิดชอบกำกับดูแลเรื่องการป้องกันระบบเครือข่ายสารสนเทศในภาพรวม ร่วมกับผู้รับผิดชอบของแต่ละระบบสารสนเทศ ซึ่งจะเป็นผู้ดำเนินการป้องกันตามมาตรการที่กำหนด

2. การข่าวกรอง การลาดตระเวนและการเฝ้าตรวจในมิติไซเบอร์ (Cyberspace Intelligence, Surveillance and Reconnaissance : Cyberspace ISR) เป็นการปฏิบัติการไซเบอร์เพื่อรวบรวมข้อมูลข่าวกรองที่มีความสำคัญหรือจำเป็นต่อการปฏิบัติการไซเบอร์ทั้งเชิงป้องกันและเชิงป้องปราม รวมทั้งการปฏิบัติการทางทหารของกองทัพอากาศในมิติอื่น ๆ โดยปฏิบัติการเหล่านี้ ต้องมีความสอดประสาน (Synchronization) กับระบบการวางแผนและการปฏิบัติการทางทหาร สามารถสนับสนุนได้ทั้งการปฏิบัติการในปัจจุบันและในอนาคต ทั้งนี้ ปฏิบัติการ Cyber ISR จะมุ่งเป้าไปที่ข้อมูลข่าวกรองในระดับยุทธการและระดับยุทธวิธี เพื่อเชื่อมโยงข้อมูลของฝ่ายตรงข้ามที่ได้จากปฏิบัติการในมิติไซเบอร์ไปสู่การวางแผนทางทหาร ปฏิบัติการ Cyber ISR จะปฏิบัติโดยหน่วยงานไซเบอร์ของกองทัพอากาศ ภายใต้ความร่วมมือกับหน่วยข้อมูลข่าวกรองอื่นที่เกี่ยวข้องเพื่อการกระจายและแลกเปลี่ยนข้อมูลข่าวกรองร่วม

3. การเตรียมสภาวะแวดล้อมในการปฏิบัติการในมิติไซเบอร์ (Cyberspace Operational Preparation of the Environment : Cyberspace OPE) เป็นการปฏิบัติการไซเบอร์เพื่อสร้างสภาวะความพร้อมการปฏิบัติการทางทหารในมิติไซเบอร์และมิติอื่น ๆ ด้วยปฏิบัติการไซเบอร์เชิงป้องกันเพื่อดำรงขีดความสามารถการปฏิบัติการในมิติไซเบอร์ของฝ่ายเรา รวมทั้งปฏิบัติการไซเบอร์เชิงป้องปราม เพื่อการขัดขวาง ทำลาย หรือควบคุมการใช้งานในมิติไซเบอร์ของฝ่ายตรงข้าม ภายใต้การสร้างสภาวะการปฏิบัติการที่ปลอดภัยด้วยการลบร่องรอยหรือกลบเกลื่อนบิดเบือนร่องรอยของการปฏิบัติการให้ยากแก่การสืบย้อนกลับมาถึงแหล่งปฏิบัติการหรือผู้ปฏิบัติการ เพื่อให้เกิดสภาวะแวดล้อมที่เกื้อกูลต่อการปฏิบัติการทางทหารในทุกมิติ ในห้วงเวลาและสถานที่ที่ต้องการ

4. การป้องปรามในมิติไซเบอร์ (Cyberspace Offense) เป็นปฏิบัติการไซเบอร์ที่แสวงประโยชน์จากช่องโหว่ทางไซเบอร์เพื่อเจาะระบบ (Exploitation) และสร้างผลกระทบในเชิงความเสียหายหรือเข้าควบคุมต่อระบบเป้าหมายทั้งในระดับเครือข่ายเชิงกายภาพ (Physical Network Layer) ระดับเครือข่ายเชิงตรรกะ (Logical Network Layer) และระดับเครือข่ายเชิงบุคคลหรือหน่วยงาน (Cyber-Persona Layer) ดังนี้

4.1 การปฏิเสธการใช้งาน (Deny) มีวัตถุประสงค์เพื่อสร้างผลกระทบให้เกิดขึ้นต่อความพร้อมใช้งานระบบเป้าหมายของฝ่ายตรงข้ามในระดับที่ต้องการในห้วงเวลาที่ต้องการ เป็นการลด/ขัดขวาง/ทำลาย ขีดความสามารถในการใช้ทรัพยากรทางไซเบอร์ด้านการทหารของฝ่ายตรงข้าม แบ่งออกเป็น 3 ระดับ ดังนี้

4.1.1) ระดับลดขีดความสามารถ (Degrade) เป็นลักษณะของการพยายามลดขีดความสามารถในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายให้ไปอยู่ในระดับที่ต้องการโดยระบุเป็นค่าเปอร์เซ็นต์เป้าหมายของขีดความสามารถ (Percentage of Capacity) โดยระดับของการลดขีดความสามารถจะต้องกำหนดให้ชัดเจน และหากมีความต้องการระบุห้วงเวลา ให้กำหนดห้วงเวลาด้วย

4.1.2) ระดับขัดขวางขีดความสามารถ (Disrupt) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมาย แบบชั่วคราวเฉพาะระหว่างห้วงเวลาที่ต้องการ โดยระบุเวลาเริ่มและเวลาสิ้นสุด ทั้งนี้ การขัดขวางขีดความสามารถอาจพิจารณาเป็นรูปแบบของการลดขีดความสามารถ (Degrade) ที่กำหนดระดับของการลดขีดความสามารถเท่ากับ 100 เปอร์เซ็นต์ได้

4.1.3) ระดับทำลายขีดความสามารถ (Destroy) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายแบบถาวร (กำหนดให้ค่าเปอร์เซ็นต์เป้าหมายของขีดความสามารถและห้วงเวลาที่ต้องการมีค่าสูงสุด)

4.2 การเข้าควบคุม (Manipulate) เป็นการเข้าควบคุมหรือเปลี่ยนแปลงแก้ไขข้อมูล/สารสนเทศ ตลอดจนระบบเครือข่าย/ระบบสารสนเทศของเป้าหมาย ให้เป็นไปตามเจตนารมณ์/วัตถุประสงค์/การสั่งการ ของผู้บังคับบัญชาฝ่ายเรา

4.3 การเตรียมความพร้อม

4.3.1 ความพร้อมของกำลังรบในภาวะปกติ ได้แก่ ผู้ทดสอบการเจาะระบบ (Pen-Tester) ทำหน้าที่ในการทดสอบเจาะระบบสารสนเทศของกองทัพอากาศ พร้อมทั้งให้คำแนะนำหรือทำการแก้ไขปรับปรุงช่องโหว่ทางไซเบอร์ที่ตรวจพบให้มีความปลอดภัยจากการถูกโจมตีทางไซเบอร์

4.3.2 ความพร้อมของกำลังรบในภาวะไม่ปกติ ได้แก่ ชุดป้องปรามทางไซเบอร์ (Cyber Warriors) ทำหน้าที่ปฏิบัติการไซเบอร์เพื่อโจมตีต่อเป้าหมายทางไซเบอร์ทันทีที่ได้รับการสั่งการจากผู้บัญชาการศูนย์ปฏิบัติการกองทัพอากาศ รวมทั้งให้การสนับสนุนการปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวกรองและการปฏิบัติการข่าวสารของกองทัพอากาศ

5. การปฏิบัติการไซเบอร์ (Cyber Operations) ของกองทัพอากาศ เป็นการปฏิบัติภายใต้การบัญชาการและการควบคุมของกองทัพอากาศ ซึ่งต้องมีการปฏิบัติที่สอดคล้องกับมิติทางอากาศ (Air Domain) และมิติอวกาศ (Space Domain) เพื่อให้เกิดการทวีกำลังกองทัพอากาศ (Force Multiplier) อย่างเป็นรูปธรรม นอกจากนี้ยังเป็นการปฏิบัติการเพื่อการรักษาความลับของข้อมูล (Confidentiality) ซึ่งหมายถึงการรับประกันถึงความปลอดภัยของข้อมูลในระบบว่าผู้ที่ไม่มีส่วนเกี่ยวข้องหรือไม่มีสิทธิ์จะไม่สามารถเข้าถึงเนื้อหาของข้อมูลได้ ควบคู่ไปกับการรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) ซึ่งหมายถึงการยืนยันถึงความถูกต้องครบถ้วนของข้อมูลที่มีการรับส่งในระบบ ว่าจะไม่ถูกเปลี่ยนแปลงหรือแก้ไข ตลอดจนการดำรงความพร้อมใช้งานของระบบและข้อมูล/สารสนเทศ (Availability) ซึ่งหมายถึงการรับประกันความพร้อมในการใช้งานอุปกรณ์เครือข่ายสารสนเทศและการสื่อสารรวมทั้งความพร้อมในใช้งานข้อมูลและบริการประเภทต่าง ๆ ในระบบทุกครั้งที่มีความต้องการใช้งาน โดยการปฏิบัติการไซเบอร์ของกองทัพอากาศประกอบด้วยการปฏิบัติการหลักทางไซเบอร์และปฏิบัติการสนับสนุนทางไซเบอร์ ดังนี้

5.1 การปฏิบัติการหลักทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถทางไซเบอร์ทั้งมวล เพื่อให้บรรลุวัตถุประสงค์ในมิติ/ผ่านมิติไซเบอร์ กำหนดกิจเฉพาะสำคัญ ดังนี้

5.1.1 การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) เป็นปฏิบัติการเพื่อการป้องกันทางไซเบอร์ มีขั้นตอนการปฏิบัติตามวงรอบการป้องกันทางไซเบอร์ (Defense Cycle) ใน 4 ขั้นตอน ดังนี้

5.1.1.1 การป้องกัน (Protect) หมายถึง การสำรวจสินทรัพย์ทางสารสนเทศ (Information Asset Identification) การตรวจสอบและแก้ไขจุดอ่อน/ช่องโหว่ทางสารสนเทศ (Vulnerability Identification) ในระบบเครือข่ายสารสนเทศของกองทัพอากาศ พร้อมทั้งการเฝ้าระวังและป้องกันไม่ให้เกิดความเสียหายขึ้นกับระบบสารสนเทศที่ใช้งานในส่วนที่รับผิดชอบ โดยจัดทำแผนบริหารความเสี่ยงด้านไซเบอร์ และถือปฏิบัติตามแนวทางหรือมาตรการต่าง ๆ ในการป้องกันระบบสารสนเทศ หรือปฏิบัติตาม กฎ ระเบียบ รวมทั้งข้อปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ ตามที่กองทัพอากาศกำหนด

5.1.1.2 การตรวจจับ (Detect) หมายถึง การเฝ้าระวังการถูกโจมตีหรือการถูกคุกคามทางไซเบอร์ ด้วยการสังเกตสิ่งผิดปกติใด ๆ ที่เกิดขึ้นในการใช้งานระบบสารสนเทศหรือการใช้ซอฟต์แวร์ตลอดจนระบบตรวจจับอื่น ๆ ที่ช่วยในการตรวจจับสิ่งผิดปกติขณะที่ใช้งานและไม่ได้ใช้งานระบบพร้อมทั้งรายงานเหตุการณ์ความผิดปกติที่ตรวจพบให้กับผู้รับผิดชอบที่เกี่ยวข้อง เพื่อให้สามารถตอบสนองและแก้ไขได้ทันท่วงที

5.1.1.3 การตอบสนอง (React) หมายถึง การปฏิบัติเพื่อแก้ไขปัญหาและระงับเหตุการณ์การล่วงละเมิดการรักษาความปลอดภัยทางไซเบอร์ที่เกิดขึ้นโดยทันทีตามมาตรการปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ขยายผลกระทบต่อไปยังระบบสารสนเทศอื่นที่เกี่ยวข้อง

5.1.1.4 การฟื้นฟู (Recover) หมายถึง การปฏิบัติเพื่อฟื้นฟูระบบสารสนเทศที่ได้รับผลกระทบทั้งหมด ให้กลับคืนสู่สภาพปกติที่พร้อมใช้งานโดยเร็วที่สุดพร้อมทำการปรับปรุงกระบวนการป้องกันให้มีประสิทธิภาพในการรักษาความปลอดภัยมากยิ่งขึ้น

5.1.2 การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations : OCO) เป็นปฏิบัติการเพื่อการโจมตีทางไซเบอร์มีขั้นตอนการปฏิบัติตามวงรอบการโจมตีทางไซเบอร์ (Attack Cycle) จำนวน 5 ขั้นตอน ดังนี้

5.1.2.1 การรวบรวมข้อมูลเป้าหมาย (Information Gathering) หมายถึงการรวบรวมข้อมูลโครงสร้างสถาปัตยกรรมระบบลักษณะอุปกรณ์และเครื่องมือที่ใช้วิธีการใช้งานและข้อมูลของบุคลากรที่เป็นประโยชน์ในการโจมตีโดยการสืบค้นข้อมูลจากกระบวนการทางเทคนิคทุกวิธีที่สามารถปฏิบัติได้รวมถึงการใช้วิธีวิศวกรรมสังคม (Social Engineering) ด้วย

5.1.2.2 การตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification) หมายถึง การตรวจสอบหาช่องโหว่หรือการวิเคราะห์ช่องโหว่ของระบบเครือข่ายสารสนเทศของฝ่ายตรงข้ามเพื่อการโจมตีจากข้อมูลเป้าหมายที่รวบรวมได้

5.1.2.3 การปฏิบัติการโจมตี (Attack) หมายถึง การใช้อาวุธทางไซเบอร์ (Cyber Weapons) ทุกรูปแบบในการเข้าโจมตีระบบเป้าหมาย โดยแสวงประโยชน์จากช่องโหว่ทางไซเบอร์เพื่อเจาะระบบ (Exploitation/Attack) ให้เกิดผลตามที่คาดหวัง ทั้งนี้ปฏิบัติการโจมตี ยังสามารถปฏิบัติเพื่อให้ได้มาซึ่งข้อมูลข่าวกรองที่ต้องการจากระบบเป้าหมายด้วย

5.1.2.4 การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) หมายถึง การเปิดช่องโหว่ทิ้งไว้ในระบบเป้าหมาย เพื่อใช้เป็นช่องทางสำหรับการเข้าปฏิบัติการครั้งต่อไป ด้วยวิธีการฝังทางลับ (Backdoor) ไว้ในระบบที่เป็นเป้าหมาย

5.1.2.5 การลบร่องรอยการโจมตี (Covering Tracks) หมายถึง การลบร่องรอยหรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบ เพื่อไม่ให้ฝ่ายตรงข้ามสามารถสืบย้อนกลับมาถึงผู้โจมตีได้

5.1.3. การปฏิบัติการข่าวกรองทางไซเบอร์ (Cyber Intelligence : CI) และการปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ (Cyber Counterintelligence : CCI) ดังนี้

5.1.3.1 การปฏิบัติการข่าวกรองทางไซเบอร์ (CI) หมายถึง การปฏิบัติการเพื่อรวบรวมข้อมูลข่าวกรองทางไซเบอร์ด้วยวิธีต่าง ๆ เช่น การรวบรวมข้อมูลข่าวกรองจากแหล่งเปิด (Open-Source Intelligence : OSINT) จากข่าวกรองทางบุคคล (Human

Intelligence : HUMINT) จากข่าวกรองทางสัญญาณ (Signal Intelligence : SIGINT) จากข่าวกรองทางภาพ (Image Intelligence : IMINT) และจากข่าวกรองทางภูมิสารสนเทศเชิงพื้นที่ (Geospatial Intelligence : GEOINT) เป็นต้น โดยมีวัตถุประสงค์เพื่อรวบรวมและวิเคราะห์แนวโน้มเกี่ยวกับภัยคุกคามทางไซเบอร์ในทุกรูปแบบ

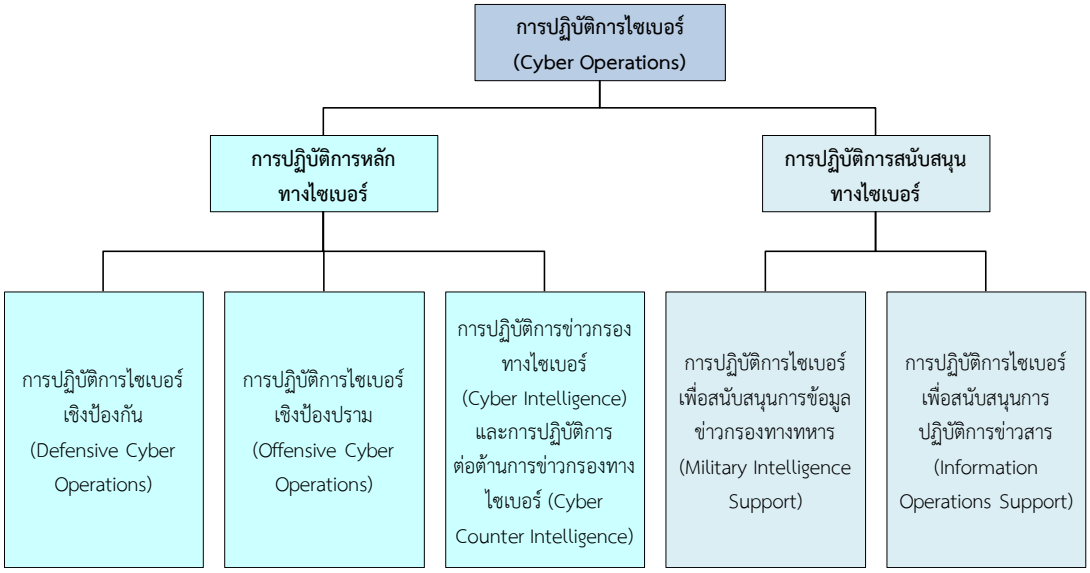
5.1.3.2 การปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ (CCI) หมายถึง การปฏิบัติการเพื่อป้องกันระงับยับยั้งและลดทอนประสิทธิภาพการปฏิบัติการข่าวกรองทางไซเบอร์ (CI) ของฝ่ายตรงข้ามที่กระทำต่อฝ่ายเรา

5.2 การปฏิบัติการสนับสนุนทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถด้านไซเบอร์ในการสนับสนุนภารกิจอื่น ๆ เพื่อเอื้ออำนวยให้ภารกิจนั้นสามารถดำเนินการได้อย่างมีประสิทธิภาพกำหนดกิจเฉพาะสำคัญ ดังนี้

5.2.1 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support : MIS) เป็นการปฏิบัติการข่าวกรองทางไซเบอร์ (CI) และการปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ (CCI) ด้วยอุปกรณ์/วิธีทางไซเบอร์ วิธีวิศวกรรมสังคม (Social Engineering) และวิธีอื่น ๆ เพื่อให้ได้มาซึ่งข้อมูลข่าวสารที่จำเป็นสำหรับการสนับสนุนการปฏิบัติการทางทหารในมิติอื่น ๆ พร้อมทั้งป้องกันระงับยับยั้ง และลดทอนประสิทธิภาพ การปฏิบัติการข่าวกรองทางไซเบอร์ (CI) ของฝ่ายตรงข้ามที่กระทำต่อฝ่ายเรา โดยต้องมีความสอดประสาน (Synchronization) ระหว่างการปฏิบัติการทางทหารในมิติไซเบอร์และการปฏิบัติการทางทหารในมิติอื่น ๆ ภายใต้แผนการรบ เพื่อให้บรรลุวัตถุประสงค์ทางทหารตามที่ต้องการ ดังนั้น การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร จะต้องมีความสัมพันธ์เชิงร่วมมือกับการปฏิบัติการข่าวกรองของกรมข่าวทหารอากาศ ในลักษณะให้การสนับสนุนซึ่งกันและกันทั้งในยามปกติและยามเกิดความขัดแย้ง

5.2.2 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support : IO Support) เป็นการปฏิบัติการไซเบอร์เชิงป้องกัน (DCO) การปฏิบัติการไซเบอร์เชิงป้องปราม (OCO) และการปฏิบัติการข่าวกรองทางไซเบอร์ (CI)/การปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ (CCI) เพื่อสนับสนุนการดำรงขีดความสามารถในการปฏิบัติการข่าวสาร (Information Operations : IO) ในการสร้างสภาวะที่ได้เปรียบเชิงข่าวสารต่อฝ่ายตรงข้าม เช่น การสนับสนุนการปฏิบัติการลวงทางทหาร (Military Deception : MILDEC) การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security : OPSEC) การประกันข่าวสาร (Information Assurance : IA) และการต่อต้านข่าวกรอง (Counter Intelligence) เป็นต้น

แผนภาพที่ 2-2 การปฏิบัติการไซเบอร์ของกองทัพอากาศ



ที่มา : หลักนิยมกองทัพอากาศ, 2562 : 78

5.3 การจัดโครงสร้างการปฏิบัติการไซเบอร์

5.3.1 การจัดโครงสร้างการปฏิบัติการไซเบอร์เพื่อเตรียมกำลังรบ (Cyber Force Preparation Planning) เพื่อให้กองทัพอากาศมีความพร้อมในการปฏิบัติการหลักทางไซเบอร์และปฏิบัติการสนับสนุนทางไซเบอร์ควรมีองค์ประกอบผู้ปฏิบัติที่สำคัญ ดังนี้ 1) ผู้ดูแลเครือข่ายสารสนเทศและการสื่อสารของกองทัพอากาศทำหน้าที่กำกับดูแลให้เครือข่ายมีความพร้อมใช้งานอยู่เสมอ 2) ผู้ตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศทำหน้าที่ตรวจประเมินความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยขึ้นตรงกองทัพอากาศ 3) ผู้ดูแลระบบสารสนเทศภายในหน่วยงานทำหน้าที่ดูแลระบบสารสนเทศของหน่วยงาน และเป็นผู้ติดต่อประสานด้านเทคโนโลยีสารสนเทศและการสื่อสารกับกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ 4) ผู้สนับสนุนทางไซเบอร์ดำเนินการโดยกำลังพลพร้อมเรียกด้านไซเบอร์ (Cyber On Call List) ซึ่งเป็นกำลังพลที่มีขีดความสามารถด้านไซเบอร์และได้รับการขึ้นทะเบียนเป็นกำลังพลพร้อมเรียกด้านไซเบอร์ของกองทัพอากาศ 5) ผู้ปฏิบัติการข่าวกรองทางไซเบอร์ ทำหน้าที่ปฏิบัติการข่าวกรองทางไซเบอร์และการปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ รวมทั้งให้การสนับสนุนด้านการข่าวกรองในภาพรวมของการรบ

5.3.2 การจัดโครงสร้างการปฏิบัติการไซเบอร์เพื่อเตรียมกำลังรบเชิงป้องกัน (Cyber Force Prevention Planning) เพื่อให้กองทัพอากาศสามารถปฏิบัติการไซเบอร์เชิงป้องกันให้เกิดประสิทธิภาพสูงสุด ควรมีองค์ประกอบชุดปฏิบัติที่สำคัญ ดังนี้

5.3.2.1 ชุดปฏิบัติการเครือข่าย ทำหน้าที่ดูแลระบบเครือข่ายสารสนเทศและการสื่อสาร ให้มีความพร้อมใช้งาน ตลอด 24 ชั่วโมงทุกวัน

5.3.2.2 ชุดเฝ้าระวังและตรวจจับทางไซเบอร์ทำหน้าที่เฝ้าระวังตรวจจับการบุกรุก/โจมตี และรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ ตลอด 24 ชั่วโมง

5.3.2.3 ชุดเผชิญเหตุทางไซเบอร์ (Cyber Security Incident Response Team: CSIRT) ทำหน้าที่ตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ทันทีที่ได้รับการสั่งการจากผู้บัญชาการศูนย์ปฏิบัติการกองทัพอากาศพร้อมทั้งตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics)

5.3.2.4 ชุดวางแผนและปฏิบัติการข่าวกรองไซเบอร์ ทำหน้าที่ด้านการข่าวกรองไซเบอร์และวางแผนร่วมกับส่วนวางแผนการยุทธ์ศูนย์ยุทธการทางอากาศ ศูนย์ปฏิบัติการกองทัพอากาศ

5.3.2.5 ชุดสนับสนุนทางไซเบอร์ทำหน้าที่สนับสนุนส่วนปฏิบัติการไซเบอร์ของศูนย์ปฏิบัติการไซเบอร์ กรณีเกิดเหตุภัยคุกคามทางไซเบอร์จะสนับสนุนทันทีที่ได้รับการประสานจากส่วนปฏิบัติการไซเบอร์ ศูนย์ปฏิบัติการไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ

แนวคิด ทฤษฎี และยุทธศาสตร์ของสงครามอิเล็กทรอนิกส์

ระบบความปลอดภัยมีความสำคัญต่อการทำงานในทุกด้านเป็นอย่างมาก โดยเฉพาะความมั่นคงความปลอดภัยด้านเทคโนโลยี ข้อมูลในระบบเป็นสิ่งสำคัญที่ต้องรักษาไว้ ปัจจุบันมีการคุกคามต่อข้อมูลอย่างมากมาย ทำให้เกิดความเสียหายต่อองค์กรต่าง ๆ เป็นอย่างมาก กระบวนการโจรกรรมข้อมูลมีอยู่หลายรูปแบบ ปฏิบัติการสงครามทางอิเล็กทรอนิกส์ (Electronic Warfare : EW) ก็นับเป็นกระบวนการหนึ่งในปฏิบัติการคุกคามต่อข้อมูลข่าวสารที่มีทั้งเชิงรุกและรับ

การทำสงครามทางอิเล็กทรอนิกส์ (Electronic Warfare หรือ EW) เป็นปฏิบัติการที่มุ่งทำลายระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เพื่อสร้างความเสียหายกับข้อมูลในระบบหรือคอมพิวเตอร์ทำให้ระบบหยุดทำงานเองและลบข้อมูลในระบบหน่วยความจำโดยที่เจ้าของไม่รู้ตัว เป็นการสร้างความเสียหายแก่ผู้โดนกระทำนอกจากการโจมตีต่อระบบคอมพิวเตอร์แล้วการโจมตีทางอิเล็กทรอนิกส์ ก็นับเป็นการคุกคามต่อระบบข้อมูลข่าวสาร ซึ่งมีหลายรูปแบบ เช่น การดักฟังสัญญาณการก่อกวนและโจมตีทำลายเป้าหมายทำให้ระบบทางอิเล็กทรอนิกส์มีความเสี่ยงมาก จึงต้องมีการรักษาความปลอดภัยสูงเพื่อป้องกันการถูกโจมตีหรือให้มีความเสี่ยงน้อยที่สุด

แนวคิด ทฤษฎี และคุณลักษณะของสงครามอิเล็กทรอนิกส์

สงครามอิเล็กทรอนิกส์ หรือ Electronics Warfare นั้น หมายถึง ปฏิบัติการทางทหารที่มีเป้าหมายอยู่ที่ระบบอิเล็กทรอนิกส์ของข้าศึกด้วยการโจมตีเพื่อให้ระบบอิเล็กทรอนิกส์ของข้าศึกไม่สามารถใช้การได้เต็มประสิทธิภาพโดยการโจมตีนั้นแบ่งออกได้หลายรูปแบบ อาทิ การดักฟังสัญญาณการก่อกวน รวมไปถึงการทำลายเป้าหมาย ซึ่งรูปแบบการทำสงครามอิเล็กทรอนิกส์ที่คุ้นเคยก็เช่น การก่อกวน/ทำลายเรดาร์และระบบตรวจจับต่าง ๆ เพื่อให้ข้าศึกไม่สามารถตรวจจับฝ่ายเราได้

การดักฟังและรวบรวมข่าวกรอง หรือแม้กระทั่งการโจรกรรมข้อมูล (Hack) นั้นก็นับว่าเป็นสงครามอิเล็กทรอนิกส์รูปแบบหนึ่ง ปัจจุบันสงครามอิเล็กทรอนิกส์ นับเป็นปฏิบัติการที่มีความสำคัญมาก ในการรบหากฝ่ายใดสามารถครองสมรภูมิสงครามอิเล็กทรอนิกส์ได้แทบจะนับได้ว่าเป็นฝ่ายผู้ชนะ เช่นในสมรภูมิสงครามอ่าวเปอร์เซียเพียงในวันแรกของสงครามกองทัพอากาศสหรัฐฯ และพันธมิตร สามารถโจมตีทำลายฐานเรดาร์และระบบสื่อสารของอิรักได้ทั้งหมด ทำให้กองทัพอิรักไม่สามารถป้องกันตัวเองได้ (What is an Electronic Warfare, ออนไลน์, 2563)

คุณลักษณะสงครามอิเล็กทรอนิกส์

การปฏิบัติการสงครามอิเล็กทรอนิกส์ (Electronic Warfare Operations : EWO) เป็นการปฏิบัติทางทหารเกี่ยวกับการใช้พลังงานแม่เหล็กไฟฟ้า (Electromagnetic) และพลังงานแบบอื่น เพื่อควบคุมแถบความถี่แม่เหล็กไฟฟ้า (Electromagnetic Spectrum) หรือเพื่อโจมตีข้าศึก โดยการครอบคลุมยุทธบริเวณของแถบคลื่นแม่เหล็กไฟฟ้า การควบคุมแถบความถี่แม่เหล็กไฟฟ้าได้รับการขยายเครือข่ายจากระบบป้องกันฝ่ายเราและจากระบบการต่อต้านของฝ่ายตรงข้ามไม่จำกัดเพียงแค่คลื่นวิทยุ แต่รวมถึงในย่านที่ใช้ใยแก้วนำแสง (Optical) และอินฟราเรดการสงครามอิเล็กทรอนิกส์ (EW) กำหนดกิจเฉพาะสำคัญ (กองทัพบก, ม.ป.ป.) ได้แก่

1. การสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Support : ES) เป็นการใช้สงครามอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการค้นหา ดักจับ ระบุตัวตน และชี้ตำบลที่ตั้งของแหล่งกำเนิดพลังงานแม่เหล็กไฟฟ้าที่ปล่อยออกมาโดยตั้งใจและไม่ตั้งใจ เพื่อตรวจสอบภัยคุกคามที่เกิดขึ้น

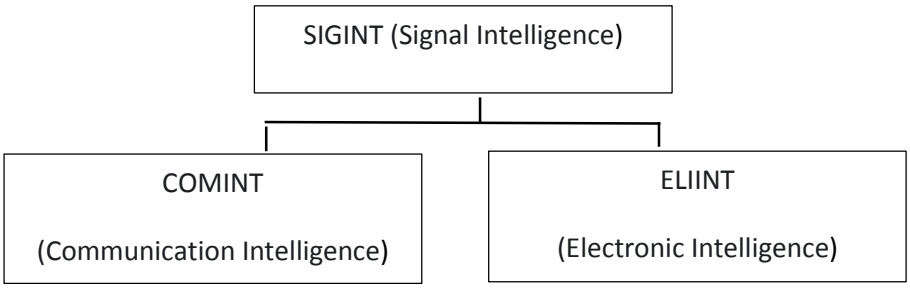
2. การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection : EP) เป็นการใช้สงครามอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการป้องกันบุคคลยุทโธปกรณ์และระบบอิเล็กทรอนิกส์ต่าง ๆ จากการโจมตีทางอิเล็กทรอนิกส์ของฝ่ายข้าศึก เพื่อให้มีความอยู่รอดสูงในพื้นปฏิบัติการ

3. การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack : EA) เป็นการใช้สงครามอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการใช้คลื่นแม่เหล็กไฟฟ้าหรือการควบคุมพลังงานในการโจมตีบุคคลยุทโธปกรณ์ และระบบอิเล็กทรอนิกส์ต่าง ๆ เพื่อทำให้ลดประสิทธิภาพไม่สามารถใช้งานอุปกรณ์ได้

รูปแบบของสงครามอิเล็กทรอนิกส์ (กองทัพเรือ, 2554)

1. Electronic Support (ES) หรือ ESM หรือ SIGINT เพื่อดักรับระบุประเภท/ชนิด และหาตำแหน่ง แหล่งของการแพร่คลื่นของฝ่ายตรงข้ามดังนั้น ในการทำสงครามอิเล็กทรอนิกส์ทุกครั้ง ย่อมจะต้องมีการเตรียมการไว้ตั้งแต่ในยามสงบนั่นคือการหาข้อมูลเกี่ยวกับการใช้ประโยชน์จากคลื่นแม่เหล็กไฟฟ้าของฝ่ายตรงข้ามไว้ล่วงหน้าข้อมูลที่ได้จากการกระทำดังกล่าวเรียกว่าข่าวกรองสัญญาณ (Signal Intelligence: SIGINT) ซึ่งมีองค์ประกอบ ดังแผนภาพที่ 2 - 3

แผนภาพที่ 2-3 องค์ประกอบของข่าวกรองสัญญาณ



ที่มา : ประมวลโดยผู้วิจัย

ความหมายของ ข่าวกรองสัญญาณ (Signal Intelligence: SIGINT) คือ การหาข่าวเกี่ยวกับการปฏิบัติการและการเคลื่อนไหวของฝ่ายตรงข้ามหรือของประเทศ ที่อาจเป็นปฏิปักษ์ต่อฝ่ายเรามีความหมายเฉพาะถึงการค้นหาตรวจจับกำหนดที่ตั้งและบันทึกข้อมูลเกี่ยวกับคลื่นแม่เหล็กไฟฟ้าของฝ่ายตรงข้ามเพื่อนำมารวบรวมวิจัยจัดหมวดหมู่ตีความและประเมินค่าของข่าวนั้น ๆ เพื่อประโยชน์ของฝ่ายตนที่จะลดประสิทธิภาพในการใช้คลื่นแม่เหล็กไฟฟ้าของฝ่ายตรงข้าม SIGINT เป็นคำที่เกิดขึ้นมาก่อนคำว่า EW กิจกรรม EW นั้น จะต้อเริ่มต้นจากการปฏิบัติการข่าวกรองสัญญาณ (SIGINT) ก่อนเป็นเบื้องต้น แม้ว่าจะอยู่ในภาวะปกติก็ตามเพราะสิ่งนี้เป็นพื้นฐานที่จำเป็นต่อการใช้มาตรการสนับสนุนและการต่อต้านทางอิเล็กทรอนิกส์ SIGINT นั้น จะมีพันธกิจที่เกี่ยวข้องกับการดักรับการแพร่คลื่นแม่เหล็กไฟฟ้าของข้าศึกซึ่งรวมทั้งการสื่อสารและมิใช่การสื่อสารแล้วจึงนำมาวิเคราะห์พิสูจน์ทราบประเมินค่าสัญญาณที่ดักรับได้นั้นเพื่อที่จะขยายผลที่เกี่ยวข้องกับเทคนิคกลยุทธ์ข้าศึกและเป็นฐานข้อมูลต่อการนำไปใช้เพื่อการต่อต้านและตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ต่อไปในการทำสงครามอิเล็กทรอนิกส์ข่าวกรองทางการสัญญาณ แบ่งออกเป็น 2 ส่วน ได้แก่

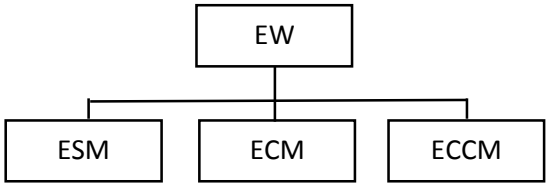
1.1 ข่าวกรองทางการสื่อสาร (Communication Intelligence: COMINT) เป็นเทคนิคและข่าวกรองที่ได้มาจากการดักรับเฝ้าฟังการติดต่อสื่อสารของฝ่ายอื่นและโดยทางอื่น ๆ ที่นอกเหนือจากการรับฟังแต่ต้องระมัดระวังกลการส่งข่าวลวงของฝ่ายตรงข้ามด้วยเช่นกัน COMINT เน้นที่ตรวจค้นบันทึกข่าวถอดรหัสข้อความการสื่อสารของข้าศึกด้วยการดักรับเฝ้าฟัง เก็บรวบรวมข้อมูลและข่าวสารจากระบบสื่อสารทางอิเล็กทรอนิกส์ของข้าศึกและเอามาดำเนินกรรมวิธีทางการข่าวกรองและการแปรรหัสลับทำเนียบกำลังรบ

1.2 ข่าวกรองทางอิเล็กทรอนิกส์ (Electronic Intelligence: ELINT) คือการปฏิบัติการเก็บรวบรวม (สังเกต และบันทึก) และดำเนินกรรมวิธีต่าง ๆ เพื่อให้ได้มาซึ่งข้อมูลข่าวกรองจากการแพร่กระจายคลื่นแม่เหล็กไฟฟ้าที่มิได้เกิดจากการติดต่อสื่อสารของต่างชาติข้อมูลเหล่านี้จะนำมาจัดทำ “ทำเนียบสถานีอิเล็กทรอนิกส์” สำหรับดำเนินมาตรการต่อต้านทางอิเล็กทรอนิกส์ (ECM) ต่อไป ELINT มี 3 รูปแบบ คือ 1) Navigation Aids (เครื่องช่วยในการเดินอากาศ) 2) Identification Friend or Foe (IFF) ระบบพิสูจน์ฝ่าย และ 3) Radar โดยเมื่อเกิดวิกฤติการณ์

ทางทหารขึ้นหน่วยบัญชาการทหารจะนำเอาข้อมูลจากข่าวกรองสัญญาณ (SIGINT) มาพิจารณาวางแผนเพื่อกำหนดมาตรการในการทำสงครามอิเล็กทรอนิกส์ต่อฝ่ายตรงข้าม

2. มาตรการสงครามอิเล็กทรอนิกส์ มี 3 มาตรการ ได้แก่ มาตรการสนับสนุนทางอิเล็กทรอนิกส์ (ESM) มาตรการต่อต้านทางอิเล็กทรอนิกส์ (ECM) และมาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (ECCM) ดังแผนภาพที่ 2-4

แผนภาพที่ 2-4 มาตรการสงครามอิเล็กทรอนิกส์



ที่มา : ประมวลโดยผู้วิจัย

2.1 มาตรการสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Warfare Support Measures : ESM) คือ การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึก และวิเคราะห์เพื่อรวบรวมเป็นข้อมูลนำมาสนับสนุน ECM , ECCM และการใช้กำลังทางยุทธวิธีอื่น ๆ

2.1.1 การค้นหา กระทำเพื่อ 1) ค้นหาระดับความรุนแรงของพลังงานแม่เหล็กไฟฟ้าของข้าศึกและสัญญาณต่าง ๆ ที่น่าจะส่งออกมา 2) ระบุตำแหน่งที่ตั้งของเครื่องส่งวิทยุและที่ตั้งศูนย์บัญชาการของข้าศึก และ 3) ระบุทิศทางการเคลื่อนที่ของกำลังของข้าศึกเพื่อค้นหาเป้าหมายเพื่อทำการโจมตี

2.1.2 การวิเคราะห์ เป็นการดำเนินกรรมวิธีต่อข่าวสารที่ส่งออกมาของข้าศึกเพื่อได้มาซึ่งความรู้เกี่ยวกับยุทธวิธีและการจัดหน่วย เป็นต้น กระทำเพื่อเปลี่ยนข่าวสารที่อุปกรณ์ระบบหาทิศทางได้รับมาให้เป็นข่าวกรองนอกจากนี้การดำเนินงานวิเคราะห์จะต้องใช้เจ้าหน้าที่ข่าวกรองที่ได้รับการฝึกมาเป็นอย่างดี

2.1.3 การบันทึก จะกระทำหลังการวิเคราะห์ข้อมูลที่ได้รับ เพื่อนำไปใช้ประโยชน์ได้ต่อไป โดยการใช้ประโยชน์นั้นอาจนำไปใช้ตามกิจเฉพาะ หรือสำหรับอุปกรณ์ก่อกวนการสกัดกั้น ซึ่งต้องมีอุปกรณ์พร้อมมูล และอาศัยเจ้าหน้าที่ที่มีความชำนาญทางด้านนี้เป็นอย่างมาก

2.1.4 การดักรับทำให้ทราบถึง 1) ข่าวสารเกี่ยวกับระบบอิเล็กทรอนิกส์ของข้าศึก ทำให้ฝ่ายเราสามารถสั่งการปฏิบัติเพื่อลดผลการรบกวนระบบโดยข้าศึก 2) ข่าวที่ตั้งหน่วยและการปฏิบัติของข้าศึก แล้วกระจายข่าวสารข่าวกรองที่ได้แก่หน่วยฝ่ายเรา 3) นำข่าวสารที่ได้มาใช้ป้องกันเครื่องมือของฝ่ายเรา 4) ทำให้ทราบขีดความสามารถของข้าศึกที่จะรบกวนระบบของฝ่ายเราว่ามีมากน้อยเพียงใด ณ ที่ข้าศึกตั้งอยู่ นอกจากนี้ เครื่องมือทางสงครามอิเล็กทรอนิกส์ของข้าศึกยังเป็นเป้าหมายสำหรับการทำลายอีกด้วย 5) ทำให้ทราบว่าข้าศึกได้นำเอาวิทยุซึ่งมีคุณลักษณะทางเทคนิคบางประการเข้ามาในพื้นที่การรบ ดังนั้นการดำเนินการด้าน ESM

จึงจำเป็นจะต้องมีเครื่องมือ COMINT และ ELINT ที่มีการค้นคว้าวิจัยเป็นอย่างดี ประดิษฐ์และพัฒนาผลิตขึ้นมาให้สามารถทำการค้นหาดักรับ จับตำแหน่งที่มาของสัญญาณและพร้อมที่จะพิสูจน์ชนิดหรือระบบการสื่อสารและระบบทางอิเล็กทรอนิกส์ของฝ่ายตรงข้ามให้ได้ เพื่อนำมารวบรวมเป็นข่าวกรองทางการสื่อสารและข่าวกรองทางอิเล็กทรอนิกส์ต่อไปซึ่งจะสนับสนุนเพิ่มเติมให้ข่าวกรองสัญญาณมีประสิทธิภาพมากยิ่งขึ้นอันจะทำให้ฝ่ายอำนวยการสามารถพิจารณาประมาณการขีดความสามารถของระบบการสั่งการบังคับบัญชาและระบบอาวุธของฝ่ายตรงข้ามเพื่อให้ผู้บังคับบัญชาสามารถตกลงใจได้ถูกต้อง

2.1.5 วัตถุประสงค์ของมาตรการ ESM เพื่อให้ได้ข้อมูล ด้านคุณลักษณะทางเทคนิคของอุปกรณ์นั้น ๆ เช่น กำลังออกอากาศ ชนิดของสายอากาศ ย่านความถี่คลื่นที่ส่งการปรุงคลื่น (Modulation: MOD) และคุณลักษณะพิเศษอื่น ๆ ของอุปกรณ์สื่อสารของข้าศึกข้อมูลด้านที่ตั้งของเครื่องส่ง ข้อมูลของระบบการทำงานทางยุทธการที่ใช้อุปกรณ์นั้น ๆ อยู่ ข้อมูลชนิดอุปกรณ์/ขีดความสามารถ และข้อมูลข่าวสารที่ส่ง

2.1.6 ประโยชน์ของมาตรการ ESM

2.1.6.1 ฝ่ายเราสามารถก่อกวน (Jamming) ระบบการสื่อสารของข้าศึกอย่างได้ผล ดังนี้ 1) สามารถวางแผน/ออกคำสั่งได้ละเอียดมากขึ้น การระบุเป้าหมายทาง ภูมิศาสตร์และความถี่แน่นอนได้ 2) สามารถคาดการณ์เวลาปฏิบัติการของเครื่องมือข้าศึกล่วงหน้าได้ 3) สามารถทำการรักษาความปลอดภัยได้อย่างถูกต้องมีเหตุผล

2.1.6.2 สามารถวางแผนยุทธศาสตร์การลวงทางอิเล็กทรอนิกส์ถ้าเราทราบการวางกำลังของข้าศึก ดังนี้ 1) แผนสามารถวางได้ตรงตามเป้าหมาย 2) สามารถคาดการณ์ได้ล่วงหน้าถึงการตอบโต้ของข้าศึกได้อย่างถูกต้อง 3) ความรู้เรื่องระบบการสื่อสารของข้าศึกจะทำให้เราลวงข้าศึกได้เชื่อถือมากขึ้น

2.1.6.3 การวางแผนอิเล็กทรอนิกส์เชิงรับ หรือเชิงป้องกันมีผลมากขึ้นเนื่องจาก 1) รู้ขีดความสามารถด้าน EW ของข้าศึกจะทำให้เราพร้อมที่จะป้องกันต่อขีดความสามารถนั้น ๆ 2) รักษาความปลอดภัยได้อย่างถูกต้อง 3) เทคนิคการป้องกันสามารถพัฒนาขึ้น เพื่อตอบโต้ขีดความสามารถในการก่อกวนของข้าศึก

2.1.6.4 งานข่าวกรองในการจัดทำทำเนียบกำลังรบ เก็บข้อมูลจากการส่งข่าวของข้าศึกผ่านข่ายสื่อสารอิเล็กทรอนิกส์

2.1.6.5 จัดทำทำเนียบสถานีอิเล็กทรอนิกส์ ซึ่งเป็นพื้นฐานของการดำเนินงาน มาตรการต่อต้านทางอิเล็กทรอนิกส์ (ECM) และ มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (ECCM) ต่อไป

2.1.7 ความสัมพันธ์ระหว่าง SIGINT – ESM การรวบรวมข่าวสารข่าวกรองโดย SIGINT จะต้องกระทำอย่างต่อเนื่อง โดยใช้เครื่องมือแบบเดียวกับ ESM แต่จะดำเนินการโดยหน่วยเหนือ การดำเนินการด้าน ESM จะกระทำให้หน่วยทางยุทธวิธี สามารถนำข้อมูลจากข่าวกรองสัญญาณ (SIGINT) ที่ได้รับมาใช้ประโยชน์ โดยการนำข่าวกรองทางการสื่อสาร (COMINT) และข่าวกรองทางอิเล็กทรอนิกส์ (ELINT) เกี่ยวกับฝ่ายตรงข้ามที่ได้รับเพิ่มเติมในการดำเนินมาตรการ ESM ในขณะนั้น นำมาเป็นประโยชน์ในการประมาณสถานการณ์และการตกลงใจของผู้บังคับบัญชา

ที่จะตอบโต้ต่อฝ่ายตรงข้ามที่เผชิญหน้ากับฝ่ายเรา เพื่อการรบกวนหรือการลวง หรือการทำลายให้ระบบ การสื่อสารและระบบอาวุธอิเล็กทรอนิกส์ของฝ่ายตรงข้ามหมดสมรรถนะลงไป กล่าวโดยสรุปมาตรการ ESM เป็นสิ่งจำเป็นอย่างยิ่ง ในฐานะเป็นขั้นแรกไปสู่การปฏิบัติการ EW ด้านการทำลายและด้านการป้องกันที่เป็นผล (การรุกและการรับ)

2.2 มาตรการต่อต้านทางอิเล็กทรอนิกส์ (Electronic Counter Measures: ECM) เป็นการปฏิบัติที่กระทำเพื่อขัดขวางหรือลดประสิทธิผลการใช้คลื่นแม่เหล็กไฟฟ้าของข้าศึก ถือว่า ECM เป็นอาวุธหลักของ EW และเป็นองค์ประกอบของอำนาจกำลังรบ ประกอบด้วยอาวุธ คือเครื่องก่อกวนและเครื่องค้นหาเป้าหมายสั่งการ และการบังคับบัญชาควบคุมที่จะใช้อาวุธตามลำดับความ สำคัญของผู้บังคับบัญชา ในสงครามสมัยใหม่ถือว่า ECM มีความสำคัญอย่างยิ่ง เนื่องจากมีการใช้เครื่องมือทางอิเล็กทรอนิกส์อย่างกว้างขวางสำหรับการปฏิบัติการทางทหารในทุกรูปแบบ ในเรื่องการใช้เทคนิค ECM แบ่งการดำเนินการออกเป็น 2 ประเภท คือ

2.2.1 การแพร่กระจายคลื่น (Active) ประกอบด้วย

2.2.1.1 การก่อกวน (Jamming) คือ การแผ่รังสีย้อนกลับด้วยพลังงานแม่เหล็กไฟฟ้า โดยมุ่งหมายที่จะทำให้การใช้เครื่องอิเล็กทรอนิกส์ของข้าศึกไม่บังเกิดผลเต็มที่

2.2.1.2 การลวง (Deception) คือ การจงใจแพร่คลื่น แพร่คลื่นใหม่ การดูดซับ หรือการสะท้อนพลังงานแม่เหล็กไฟฟ้า ซึ่งจะทำให้ข้าศึกแปรความหมายผิด

โดยที่การลวงดังกล่าว แบ่งเป็น

1. การลวงในระบบการสื่อสาร เช่น การส่งข่าวลวงในการติดต่อการสื่อสารของฝ่ายเราและคาดว่าสัญญาณนี้ข้าศึกจะดักรับได้เมื่อดักรับได้แล้วจะทำให้ข้าศึกหลงผิดในข่าวสารนั้น แบ่งออกเป็น 2 แบบ คือ การลวงเล่ห์ (Manipulative Deception) เป็นการแพร่คลื่นแม่เหล็กไฟฟ้าของฝ่ายเราโดยเจตนาปล่อยข่าวสารผิด ๆ เพื่อให้ข้าศึกวิเคราะห์และยอมรับข่าวสารอย่างมีเหตุมีผล และ การลวงเลียน เป็นการนำเอาการแพร่คลื่นเข้าไปสู่ช่องการสื่อสารของข้าศึกซึ่งเลียนแบบการปล่อยคลื่นของข้าศึกเองแล้วส่งข่าวลวงเข้าไปในข่ายของข้าศึกเพื่อให้เกิดการสับสนและเข้าใจผิด

2. การลวงที่มิใช่ระบบการสื่อสารได้แก่ การลวงในระบบเรดาร์ของข้าศึกซึ่งจะกระทำโดยการส่งคลื่นปลอมเข้าไปให้ปรากฏบนจอภาพเรดาร์ของข้าศึก เพื่อให้ข้าศึกเข้าใจผิดทั้งทางระยะทางและทิศทางของเป้าหมาย การลวงจะกระทำได้ 2 แบบ ได้แก่ การลวงทางระยะ และการลวงทางทิศการลวงทางระยะ (Range Deception) กระทำโดยใช้เครื่องรบกวนดักรับสัญญาณ ของเรดาร์ข้าศึก แล้วทำการขยายและส่งสัญญาณพัลส์ (Pulse) แทรกเข้าไปในความถี่ของเรดาร์ข้าศึก จะทำให้ปรากฏเป้าบนจอภาพแต่เป็นภาพลวงมีระยะทางไม่ตรงกับเป้าจริง การลวงทางทิศ (Azimuth Deception) กระทำโดยใช้เครื่องรบกวนดักรับสัญญาณของเรดาร์ข้าศึกขยายและส่งสัญญาณพัลส์เข้าไปในทิศทางทางด้านข้างของรูปทรงการแพร่คลื่นของสายอากาศด้วยวิธีนี้จะทำให้จอเรดาร์ฝ่ายตรงข้ามเห็นเป้าหมายปลอมคนละทิศกับเป้าจริง

2.2.2 การทำ ECM แบบไม่แพร่กระจายคลื่น (Passive ECM) หมายถึงการใช้เทคนิคทั้งหลายที่ไม่มีการแพร่กระจายคลื่นแม่เหล็กไฟฟ้าเพื่อใช้กับเรดาร์ ประกอบด้วย 1) ชาฟฟ์ (Chaff) เป็นวัสดุที่สามารถสะท้อนคลื่นแม่เหล็กไฟฟ้าเพื่อใช้ลวงระบบกำหนดเป้าหมาย

ของข้าศึก 2) แฟลร์ (Flares) สร้างมาเพื่อใช้ในการต่อต้านอาวุธนำวิถีด้วยความร้อนหรือรังสีอินฟราเรด โดยทำให้เกิดเป็นพลังงานย่านความถี่รังสีอินฟราเรด คล้ายกับพลังงานความร้อนของเครื่องยนต์เครื่องบินที่ตกเป็นเป้าหมาย 3) อากาศยานเป้าลวงหรือโดรน (Decoy or Drones) ใช้ลวงระบบเรดาร์ของฝ่ายตรงข้ามให้หลงเป้าหมาย โดยไม่สามารถแยกออกได้ว่าเป็นเป้าหมายจริงหรือเป้าหมายปลอมในจอเรดาร์

2.3 มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (Electronic Counter Counter Measures: ECCM) เป็นยุทธวิธีทางอิเล็กทรอนิกส์ที่ป้องกันเครื่องส่งของเรามิให้ข้าศึกรบกวน และป้องกันการค้นหาเป้าหมายของข้าศึก เป็นส่วนช่วยให้ย่านความถี่คลื่นแม่เหล็กไฟฟ้าของฝ่ายเรายังคงอยู่ได้ พนักงานเครื่องสื่อสารเป็นผู้ใช้เทคนิค ECCM ในสถานการณ์แวดล้อมทางยุทธวิธีและเป็นความรับผิดชอบทางการบังคับบัญชาในการฝึกพนักงานให้ใช้เทคนิคเหล่านี้ให้ได้ผล ECCM มีความต้องการในการฝึกทางการสื่อสารอิเล็กทรอนิกส์และเป็นเรื่องที่ดำเนินการร่วมกันอย่างใกล้ชิดกับการรักษาความปลอดภัยทางการสื่อสาร

2.3.1 กิจกรรม ECCM ได้แก่ กิจกรรมมาตรการป้องกันและมาตรการแก้ไขเยียวยา ดังนี้ 1) มาตรการป้องกันกระทำเพื่อป้องกันข้าศึกมิให้สามารถใช้คลื่นแม่เหล็กไฟฟ้าต่อระบบของเราได้แก่การให้มีการสื่อสารให้น้อยที่สุดเท่าที่จำเป็นป้องกันการสื่อสารของฝ่ายเราจากการดักรับของข้าศึก การฝึกพนักงานในเรื่องการหลีกเลี่ยงงานวงรอบ การใช้ระบบรับรองฝ่าย การเข้ารหัสและการซ้ำคำพูดตามระเบียบการ 2) มาตรการแก้ไขเยียวยาเป็นการกระทำในเมื่อข้าศึกได้ใช้กิจกรรม EW ต่อระบบการสื่อสารของฝ่ายเราแล้ว ได้แก่การจดจำลักษณะการก่อกวนและการรบกวน การปฏิบัติเมื่อเผชิญการก่อกวนและการรบกวน การปฏิบัติเมื่อเผชิญกับการลวงด้วยการใช้ระบบการรับรองฝ่าย

2.3.2 การวางแผนป้องกัน ภารกิจ ESM และ ECM ส่วนใหญ่จะเกี่ยวข้องกับเรื่องทางด้านเทคนิค ส่วนภารกิจ ECCM จะต้องดำเนินการโดยเจ้าหน้าที่ทุกนายภายในหน่วยที่จะต้องวางแผนการใช้หรือเป็นผู้ใช้อุปกรณ์ต่าง ๆ อาทิ วิทยุ เรดาร์รวมทั้งเครื่องมือตรวจการณ์และค้นหาเป้าหมาย ดังนั้นจะต้องดำเนินการฝึกเจ้าหน้าที่ให้สามารถแก้ไขปัญหาเฉพาะหน้าในกรณีที่ถูก ก่อกวน จะเห็นได้ว่าการก่อกวนมิได้เป็นอาวุธน่ากลัวในแง่ของ EW และในความเป็นจริงแล้ว ESM ของฝ่ายข้าศึกเป็นเพียงสิ่งบ่งชี้ว่าข้าศึกจะประสบความสำเร็จในการปฏิบัติ EW หรือไม่ ซึ่งถ้าหากฝ่ายเราสามารถใช้มาตรการต่าง ๆ อาทิการพราง และการรักษาความปลอดภัยทางการสื่อสาร ป้องกันกำลังและอุปกรณ์อิเล็กทรอนิกส์ให้พ้นจากฝ่ายข้าศึกซึ่งเท่ากับฝ่ายเราได้ดำเนินมาตรการ ECCM อันจะส่งผลให้ฝ่ายข้าศึกไม่ได้รับทราบข้อมูลข่าวสารที่เป็นประโยชน์จากฝ่ายเราได้

2.3.3 ความรับผิดชอบของผู้บังคับบัญชา มาตรการ ECCM นั้นถือเป็นความรับผิดชอบโดยตรงของผู้บังคับบัญชาทุกระดับ โดยหลักการพื้นฐานแล้วผู้บังคับบัญชาหน่วยจะต้องดำเนินการให้หน่วยของตนได้รับการฝึกฝนจนสามารถปฏิบัติงานได้ภายใต้สภาพแวดล้อมที่เต็มไปด้วยปฏิบัติการ EW ของข้าศึก แนวทางที่จะใช้ในการตรวจสอบขีดความสามารถในด้าน ECCM ของหน่วยในการบังคับบัญชา มีดังนี้ 1) ตรวจสอบรายงานหลังการปฏิบัติ (After-Action Report) กรณีที่เกิดการก่อกวนและการลวง รวมทั้งตรวจสอบประสิทธิภาพมาตรการตอบโต้ของฝ่ายเรา 2) ต้องแน่ใจ

ว่าจะต้องรายงานทุกขั้นตอนการปฏิบัติที่เกิดการก่อกวนและส่งรายงานนั้นไปวิเคราะห์อย่างเหมาะสม โดยนายทหารฝ่ายการสื่อสารและนายทหารของหน่วยงานรักษาความปลอดภัย 3) วิเคราะห์ความเป็นไปได้ของมาตรการสงครามอิเล็กทรอนิกส์ที่ฝ่ายข้าศึกจะใช้ตอบโต้แผนการปฏิบัติฝ่ายเรา 4) ต้องแน่ใจว่ามีการฝึกปฏิบัติเทคนิคการรักษาความปลอดภัยอย่างต่อเนื่องทุกวัน ซึ่งรวมทั้งเปลี่ยนนามเรียกขาน การใช้ระบบรับรองฝ่าย และที่สำคัญที่สุดก็คือการควบคุมการแพร่กระจายคลื่นวิทยุ 5) ดำเนินการให้เจ้าหน้าที่สามารถใช้อุปกรณ์ ECCM ได้อย่างรวดเร็วและมีประสิทธิภาพ

2.3.4 การรักษาความปลอดภัยทางการสื่อสาร/SIGSEC (Signal Security) ตามปกติแล้ว ECCM และการรักษาความปลอดภัยทางการสื่อสาร (SIGSEC) จะมีความสัมพันธ์อย่างใกล้ชิด โดยมาตรการทั้งสองต่างก็เป็นมาตรการเชิงรับและตั้งอยู่บนหลักการพื้นฐานเดียวกัน หลักการสำคัญของ SIGSEC ก็คือดำเนินการให้แน่ใจว่าการใช้คลื่นแม่เหล็กไฟฟ้าของฝ่ายเดียวกันจะไม่ทำให้ฝ่ายข้าศึกนำไปใช้ประโยชน์ได้ส่วน ECCM ก็คือการปฏิบัติทั้งหลายเพื่อให้แน่ใจว่าฝ่ายเราจะสามารถใช้อุปกรณ์ติดต่อสื่อสารอุปกรณ์ตรวจการณ์และอุปกรณ์ค้นหาเป้าหมายได้อย่างต่อเนื่อง แม้ว่าฝ่ายข้าศึกจะพยายามก่อกวนก็ตาม โดยหลักการพื้นฐานแล้วเทคนิคของ SIGSEC มีจุดมุ่งหมายเพื่อให้ผู้บังคับบัญชาเกิดความมั่นใจในด้านการรักษาความปลอดภัยในการสื่อสาร ส่วนเทคนิค ECCM จะทำให้ผู้บังคับบัญชามั่นใจว่าจะสามารถดำรงการติดต่อสื่อสารได้อย่างต่อเนื่อง ถ้าหากเรานำเทคนิคของการรักษาความปลอดภัยในการสื่อสาร (SIGSEC) มาใช้มากเท่าใดก็จะลดความต้องการในการใช้ ECCM ลงเท่านั้น จุดประสงค์ของฝ่ายเราจะต้องทำให้แน่ใจว่าบรรดาการติดต่อสื่อสาร การตรวจการณ์และอุปกรณ์ค้นหาเป้าหมายของฝ่ายเราสามารถดำเนินไปได้อย่างมีประสิทธิภาพท่ามกลางความพยายามของฝ่ายข้าศึกที่จะลดประสิทธิภาพของการทำงานของฝ่ายเรา การดัดแปลงเครื่องมือเพื่อให้หลุดพ้นจากการปฏิบัติการด้าน EW ของฝ่ายข้าศึกดูเหมือนจะเป็นการลงทุนที่สูงเกินไป นอกจากนั้นวิทยาศาสตร์และเทคโนโลยีไม่สามารถทำให้เราแก้ไขปัญหาด้าน ECCM ได้ในเวลาใกล้ ๆ นี้ การแก้ปัญหา ECCM จะต้องดำเนินการโดยเร่งด่วนและเป็นสัญชาติญาณ แม้แต่เจ้าหน้าที่ซ่อมบำรุงจะต้องระมัดระวังเกี่ยวกับอันตรายที่ก่อให้เกิดขึ้นระหว่างทำการซ่อมบำรุง ซึ่งถ้าหากเจ้าหน้าที่ใช้เครื่องมือที่ไม่เหมาะสมแล้วอาจจะทำให้ฝ่ายข้าศึกรับทราบข้อมูลทางอิเล็กทรอนิกส์ของฝ่ายเราได้ ถ้าหากระหว่างซ่อมบำรุงมีการใช้ความถี่ปฏิบัติงาน หรือทดสอบเครื่องมือด้วยกำลังออกอากาศสูง ข้อมูลข่าวสารอันทรงคุณค่าก็จะตกไปอยู่ในมือของข้าศึกได้โดยง่ายเช่นกัน เทคนิค ECCM อาจแบ่งออกเป็น 2 ประเภทใหญ่ ๆ ก็คือด้านการปฏิบัติการและด้านเทคนิค ด้านการปฏิบัติการเป็นวิธีการต่าง ๆ ที่เจ้าหน้าที่ควรปฏิบัติ ส่วนงานด้านเทคนิคได้แก่การหาวิธีการต่าง ๆ ที่จะเพิ่มหรือดัดแปลงเครื่องมือก่อนที่จะไปติดตั้งใช้งาน การแก้ปัญหา ECCM จะต้องผสมผสานทั้งในด้านเทคนิคและการปฏิบัติ ECCM สามารถดำเนินการได้ทั้งเชิงรุกและเชิงรับ การใช้อุปกรณ์เข้ารหัสระบบรับรองฝ่ายและที่ตั้งลวงถือว่าเป็นเทคนิค ECCM เชิงรับ การเพิ่มกำลังออกอากาศเพื่อเอาชนะการก่อกวนของฝ่ายข้าศึกหรือการใช้เสาอากาศบังคับทิศทางถือว่าเป็นเทคนิค ECCM เชิงรุกขนาดและลักษณะทางเทคนิคของเครื่องมือจะเป็นตัวกำหนดว่าสมควรใช้มาตรการเชิงรุกหรือเชิงรับ

2.3.5 การควบคุมการแพร่กระจายคลื่น: EMCON (Emission Control) เป็นกุญแจสำคัญที่จะทำให้ประสบความสำเร็จในการป้องกันปฏิบัติการจากฝ่ายข้าศึก โดยการส่งคลื่นแม่เหล็กไฟฟ้า จะกระทำต่อเมื่อมีผลต่อความสำเร็จของภารกิจเท่านั้น เจ้าหน้าที่วิเคราะห์ของข้าศึกสามารถตรวจสอบรูปแบบการแพร่กระจายคลื่น จากนั้นเก็บข้อมูลที่เป็นประโยชน์ไปรายงานผู้บังคับบัญชาฝ่ายข้าศึกได้รับการส่งข่าวด้วยระยะเวลาอันสั้น การเปลี่ยนความถี่และนามเรียกขานบ่อย ๆ และการย้ายที่ตั้งก็เป็นวิธีการที่จะช่วยให้เจ้าหน้าที่ ผู้บังคับบัญชาประสบความสำเร็จในการต่อต้านและตอบโต้ความพยายามดำเนินการสงครามอิเล็กทรอนิกส์ของฝ่ายข้าศึก EMCON สามารถทำได้โดยรวมและเฉพาะข่าย การกระทำโดยรวม ตัวอย่างเช่น ให้ทุกหน่วยเงียบฟังขณะที่หน่วยเคลื่อนย้ายทางยุทธวิธี หรืออาจจะกระทำเฉพาะข่าย ผู้บังคับบัญชาจะเป็นผู้ออกแบบว่าข่ายใดควรจะเป็นข่ายบังคับและข่ายใดควรจะเป็นข่ายอิสระ การควบคุมการแพร่กระจายคลื่นควรจะเป็นสิ่งที่ทำอยู่ตลอดเวลา การติดต่อสื่อสารควรกระทำเมื่อต้องการให้บรรลุภารกิจเท่านั้น การมีวินัยและระเบียบปฏิบัติที่ดีจะช่วยทำให้การตรวจการณ์ทางอิเล็กทรอนิกส์และการติดต่อสื่อสารโดยปราศจากรูปแบบที่ฝ่ายตรงข้ามจะรับทราบได้ การประยุกต์ใช้เทคนิคการรักษาความปลอดภัยทางการสื่อสาร (SIGSEC) ที่ดีจะช่วยให้การวางแผน ECCM ง่ายขึ้น ทั้งนี้เนื่องจากการวางแผน EW ของข้าศึกจะต้องอยู่บนพื้นฐานของข้อมูลที่ทราบล่วงหน้าเกี่ยวกับรูปแบบรัศมีทำการ และความถี่ของเครื่องมือการรักษาความปลอดภัยทางการสื่อสารสามารถหลีกเลี่ยง ESM ของฝ่ายข้าศึก ซึ่งเป็นสิ่งที่ทำให้ข้าศึกทราบล่วงหน้าแผนการลวงเลียนนับเป็นสิ่งหนึ่งที่ช่วยให้ข้าศึกสับสนในการสั่งการไปยังอุปกรณ์รวบรวมข้อมูลและปฏิบัติการก่อกวนผู้บังคับบัญชาต้องติดตั้งอุปกรณ์ทุกอย่างเท่าที่มีให้พร้อมใช้งาน ก่อนหน้าจะเผชิญหน้ากับข้าศึกทางสงครามอิเล็กทรอนิกส์ Electronic Attack (EA) หรือ ECM โดยการใช้คลื่นแม่เหล็กไฟฟ้าหรืออาวุธต่อต้านการแพร่คลื่นเพื่อโจมตีคน อุปกรณ์หรือสิ่งอำนวยความสะดวกในการรบต่าง ๆ เพื่อลดหรือหยุดยั้งหรือทำลายขีดความสามารถในการรบของฝ่ายตรงข้าม สำหรับ Radar ECM ทำได้ 3 วิธี คือ 1) การรบกวนการทำงานของเรดาร์ (Jamming) 2) การใช้เป้าลวงแบบต่าง ๆ 3) การทำลายเรดาร์หรืออุปกรณ์ที่เกี่ยวข้อง นอกจากนี้ EA ยังรวมถึง Communication ECM, laser ECM, IR ECM ด้วย

3. Electronic Protection (EP) หรือ ECCM เพื่อป้องกันคน อุปกรณ์ หรือสิ่งอำนวยความสะดวกในการรบต่าง ๆ ของฝ่ายเราจาก ECM ของฝ่ายตรงข้าม เพื่อลดหรือหยุดยั้งหรือทำลายขีดความสามารถในการรบของฝ่ายตรงข้ามสำหรับ Radar ECCM มีหลายวิธี เช่น การลดการถูกจับได้ด้วย Stealth, RAM Coating หรือ EMCON ของอากาศยานการใช้เทคนิค Pulse Compression หรือ Frequency Hopping กับเรดาร์ของเราการใช้เทคนิค Home-on-Jam ในอาวุธปล่อยนำวิถีปฏิบัติการ Radar Jamming จากอากาศยานแบ่งเป็น 4 แบบขึ้นกับระยะห่างระหว่างอุปกรณ์ฝ่ายเรากับเป้าหมาย คือ

3.1 Stand-off Jamming คือ อากาศยานฝ่ายเราที่ติดตั้งอุปกรณ์ ECM อยู่นอกระยะยิงอาวุธปล่อยฝ่ายตรงข้าม

3.2 Escort Jamming คือ อากาศยานฝ่ายเราที่ติดตั้งอุปกรณ์ ECM ทำหน้าที่ปกป้อง เครื่องบินโจมตี ที่บินเข้าหาเป้าหมาย

3.3 Self-Protection Jamming คือการใช้อุปกรณ์ ECM บน บ.โจมตีเอง เช่น ECM Pod

3.4 Stand-in Jamming คือ การใช้ UAV ที่ติดตั้งอุปกรณ์ ECM หรือใช้เป้าลวง เช่น TALD/I-TALD หรือ MALD บินอยู่เหนือเป้าหมายโดยตรง การทำ Radar Jamming มีเทคนิค 2 แบบ คือ 1) Noise jamming คือ ใช้สัญญาณจากอุปกรณ์ ECM ที่แรงกว่าจากเรดาร์ เพื่อปิดบังทิศทาง/ระยะที่แท้จริงของเครื่องบินฝ่ายเรา 2) Deception Jamming คือ ใช้สัญญาณจากอุปกรณ์ ECM เพื่อลวงเรดาร์ ซึ่งมี 2 วิธี คือ Range Deception คือ ลวงระยะห่างที่แท้จริงจากเครื่องบินฝ่ายเราถึงตัวเรดาร์ และ Bearing Deception คือ ลวงทิศทางที่แท้จริงระหว่างเครื่องบินฝ่ายเรากับตัวเรดาร์

สภาพแวดล้อมด้านสงครามอิเล็กทรอนิกส์

สงครามอิเล็กทรอนิกส์ เป็นมิติการปฏิบัติที่ถูกใช้ในการช่วงชิงความได้เปรียบในการต่อสู้หรือการได้มาซึ่งชัยชนะ ถือว่าเป็นรูปแบบหนึ่งของสงครามนับแต่เริ่มใช้เครื่องรับส่งวิทยุในการสื่อสารทางการทหารในระหว่างสงครามโลกครั้งที่ 2 ซึ่งได้มีการทำสงครามอิเล็กทรอนิกส์กันอย่างกว้างขวาง ในขณะนั้น ปัจจุบัน นานาประเทศทั่วโลกล้วนให้ความสำคัญกับการพัฒนาขีดความสามารถของสงครามอิเล็กทรอนิกส์ เช่น กองทัพอากาศสหรัฐฯ (USAF) มีการพัฒนาและความคืบหน้าในการทดสอบระบบ EW แบบ EPAWSS (Eagle Passive/ Active Warning and Survivability System) สำหรับปรับปรุงระบบแจ้งเตือนความอยู่รอดเชิงรับ/เชิงรุก กับเครื่องบินขับไล่ Boeing F–15 Eagle โดยระบบ EPAWSS นี้ถูกออกแบบเพื่อหาตัวอย่างคลื่นวิทยุ RF (Radio Frequency) การระบุภัยคุกคาม การจัดลำดับความสำคัญ และจัดสรรทรัพยากรก่อกวนเพื่อต่อต้านภัยคุกคาม และมีเป้าหมายที่จะนำมาทดแทนระบบเดิม TEWS (Tactical Electronic Warfare Suite) ที่ปัจจุบันใช้ติดตั้งกับ F-15C และ F-15E มากกว่า 400 เครื่อง ในกองทัพอากาศสหรัฐฯ ในขณะที่รัสเซียมีการพัฒนาและทดสอบ “ปืนพลังงานไมโครเวฟ” สำหรับติดตั้งเป็นอาวุธหลักกับเครื่องบินขับไล่ในยุคที่ 6 โดยมีวัตถุประสงค์ในการออกแบบมาเพื่อยิงเผาไหม้ระบบนำวิถีของจรวดและขีปนาวุธด้วยพลังงานคลื่นแม่เหล็กไฟฟ้าที่ทรงพลัง สามารถทำให้วงจรอิเล็กทรอนิกส์ลุกไหม้ จนทำให้ระบบนำวิถีของจรวดหรือขีปนาวุธที่โจมตีเข้ามาหมดความสามารถทางด้านจีนหลังจากประสบความสำเร็จในการผลิตเครื่องบินที่เป็นเทคโนโลยีล่องหน (Stealth) จนทำให้เครื่องบิน “เฉิงตู J-20” เป็นเครื่องบินขับไล่ล่องหนรุ่นที่ 5 ของโลกแล้ว ยังได้มีแผนการพัฒนาศักยภาพเครื่องบินรุ่นนี้อย่างต่อเนื่อง ด้วยการพัฒนาด้วยเทคโนโลยีที่ล้ำยุคและสมบูรณ์แบบยิ่ง ๆ ขึ้นโดยมีเป้าหมายการพัฒนาเพื่อใช้ในสงครามอิเล็กทรอนิกส์และเพิ่มบทบาทการเป็นเครื่องบินโจมตีทางอากาศที่ทรงพลัง

ความเป็นมาของสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ

กองทัพอากาศเริ่มมีปฏิบัติการสงครามอิเล็กทรอนิกส์ ตั้งแต่ปี 2522 โดยการใช้ขีดความสามารถในบริบทของการสนับสนุนการข่าวกรองเพื่อการตัดสินใจของผู้บังคับบัญชาหรือการบังคับบัญชาและควบคุม (Command and Control) ด้วยการจัดหาเครื่องบินตรวจการณ์จากประเทศอิสราเอลชื่อ อาราวา (IAI Arava 201) หรือ บ.ตล.7 จำนวน 3 เครื่อง นำมาใช้ในภารกิจลาดตระเวนทางอากาศ การปฏิบัติการสงครามอิเล็กทรอนิกส์ ซึ่งเป็นหลักในการลาดตระเวนทางอิเล็กทรอนิกส์ในพื้นที่บริเวณชายแดนและในกรณีเหตุพิพาทต่าง ๆ โดยมีอุปกรณ์การหาข่าว

ทางสัญญาณ (SIGINT: Signal Intelligent) และอุปกรณ์การหาข่าวทางการสื่อสาร (COMINT: Communication Intelligent) จึงนับเป็นก้าวที่สำคัญของกองทัพอากาศ ในการจัดหาอากาศยานที่ปฏิบัติการทางสงครามอิเล็กทรอนิกส์โดยเฉพาะที่รวมถึงการจัดหาระบบเรดาห์และระบบอาวุธนำวิถีแบบต่าง ๆ ที่ตามมา

แผนภาพที่ 2-5 บ.ตล.7 กับอุปกรณ์ด้าน ESM ปฏิบัติภารกิจลาดตระเวน
และหาข่าวทางอิเล็กทรอนิกส์

ที่มา : ความเป็นมาของสงครามอิเล็กทรอนิกส์ ทอ., ออนไลน์, 2563

แผนภาพที่ 2-6 AIM-9B เป็นจรวดนำวิถีด้วยความร้อนอากาศ-อากาศแบบแรกของกองทัพอากาศ

ที่มา : ความเป็นมาของสงครามอิเล็กทรอนิกส์ ทอ., ออนไลน์, 2563

แผนภาพที่ 2-7 เรดาร์ยุคแรกที่กองทัพอากาศใช้งาน

ที่มา : ความเป็นมาของสงครามอิเล็กทรอนิกส์ ทอ., ออนไลน์, 2563

ในปี 2552 กองทัพอากาศได้มีการจัดตั้งหน่วยงานที่มีความเกี่ยวข้องกับการสงครามอิเล็กทรอนิกส์ คือ กองสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) มีหน้าที่พิจารณาเสนอนโยบายวางแผนอำนวยการประสานงานควบคุม กำกับการ พัฒนาและดำเนินงานเกี่ยวกับการสงครามอิเล็กทรอนิกส์และสงครามสารสนเทศของกองทัพอากาศ ส่วนกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ มีขอบเขตความรับผิดชอบและหน้าที่ให้สนับสนุนการปฏิบัติการสงครามอิเล็กทรอนิกส์ นอกจากนี้ยังมีหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เช่น กรมยุทธการทหารอากาศกรมข่าวทหารอากาศ กรมควบคุมการปฏิบัติทางอากาศ กรมสรรพาวุธทหารอากาศ (กองโรงงานสรรพาวุธ 5) และ กองบิน 4 เป็นต้น

ศักยภาพของกองทัพอากาศด้านการปฏิบัติการสงครามอิเล็กทรอนิกส์ได้รับการพัฒนามากยิ่งขึ้นในโครงการจัดซื้อเครื่องบิน Gripen JAS 39 C/D ของกองทัพอากาศ สิ่งที่ได้รับจากโครงการนี้ นอกจากเครื่องบินที่มีสมรรถนะสูงและระบบบัญชาการและควบคุมที่ทันสมัยแล้ว ยังได้รับการถ่ายทอดเทคโนโลยีหลัก (Key Technologies) และการพัฒนาขีดความสามารถด้านการสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) การจัดทำฐานข้อมูลทางภูมิศาสตร์ (Geographical Databases: Geo Data) และระบบเชื่อมโยงข้อมูล (Data Link: DL) รวมทั้งทุนการศึกษาในระดับสูงกว่าปริญญาตรีที่เกี่ยวข้องในการพัฒนาศักยภาพของประเทศอีกหลายทุน ทั้งนี้ กองทัพอากาศได้กำหนดวัตถุประสงค์หลักในการรับการถ่ายทอดเทคโนโลยีด้าน EW ไว้ 3 ประการ ดังนี้ 1) กำหนดแนวทางการพัฒนาขีดความสามารถด้านสงครามอิเล็กทรอนิกส์ โดยรวมของกองทัพอากาศในระยะยาว 2) การเตรียมบุคลากรทั้ง นักบินและเจ้าหน้าที่เทคนิค เพื่อสนับสนุนทางยุทธการด้านการสงครามอิเล็กทรอนิกส์ (EW Operation Support) ให้กับฝูงบิน Gripen 39 C/D 3) การจัดทำฐานข้อมูลทางสงครามอิเล็กทรอนิกส์ (EW Database) ข้อมูลอิเล็กทรอนิกส์ในพื้นที่การรบ (Electronic Order of Battle: EOB) และห้องสมุด

อิเล็กทรอนิกส์ (EW Library) เพื่อสนับสนุนให้ฝูงบิน Gripen 39 C/D รวมทั้งอากาศยาน ระบบอาวุธ และระบบ C4ISR อื่น ๆ ของกองทัพอากาศ

แนวทางการปฏิบัติการ EW ขีดความสามารถในปัจจุบัน และเป้าหมายของการพัฒนา EW ของกองทัพอากาศ

การปฏิบัติการสงครามอิเล็กทรอนิกส์นั้นมีความเกี่ยวข้องในหลายระดับ ในระดับสูงสุดของการปฏิบัติของกองกำลัง (Force) จะมีภารกิจด้านการสงครามอิเล็กทรอนิกส์ ภารกิจของการปฏิบัติการสงครามอิเล็กทรอนิกส์อาจแบ่งออกเป็น 3 รูปแบบ ดังนี้

1. ภารกิจหลักที่ให้ปฏิบัติการสงครามอิเล็กทรอนิกส์ เช่น การทำลายหรือตัดรอนขีดความสามารถของระบบตรวจจับของข้าศึกด้วยการรบกวน (Jamming) หรือการทำลายด้วยจรวดต่อต้านเรดาห์ (Anti Radiation Missile) การลาดตระเวนทางอิเล็กทรอนิกส์ เพื่อการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ (Electronic Support Measure: ESM)

2. ภารกิจที่สนับสนุนหน่วยอื่นเพื่อให้เกิดความปลอดภัยจากอาวุธของฝ่ายตรงข้าม เช่น การบินคุ้มกันทางอิเล็กทรอนิกส์ (Escort Jamming)

3. การปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อป้องกันตัวเอง (Self-Protection Jamming)

ผลที่ได้ส่วนหนึ่งจากการปฏิบัติภารกิจที่เกี่ยวกับการปฏิบัติการสงครามอิเล็กทรอนิกส์ คือ ภาพรวมของสถานการณ์ที่เกิดขึ้นในพื้นที่การรบ (Intelligence, Surveillance, Target Acquisition, and Reconnaissance : ISTAR) ซึ่งจะถูกส่งกลับไปยังหน่วยที่เก็บข้อมูลและใช้งานข้อมูลที่เกี่ยวข้อง ระดับรองจากกองกำลังคืออากาศยาน (Platform) ที่ใช้ในการปฏิบัติภารกิจ ในระดับนี้จะต้องคำนึงถึงการใช้ EW ในการป้องกันอากาศยาน (Platform Protection) ซึ่งจะต้องมีปัจจัยต่าง ๆ ที่มีผลกระทบต่อการป้องกัน ได้แก่ การฝึก ขั้นตอนการปฏิบัติ และคุณลักษณะของอากาศยาน เป็นต้น โดยผลการอยู่รอดของอากาศยานจะส่งผลถึงการปฏิบัติภารกิจในระดับที่สูงขึ้นไป สิ่งที่จะส่งผลถึงความอยู่รอดของอากาศยานมีสองส่วน คือ การระมัดระวังสถานการณ์ (Situation Awareness) ของนักบิน (Operator) กับเทคนิคการต่อต้านทางสงครามอิเล็กทรอนิกส์ที่กำหนดไว้ในอุปกรณ์ประจำอากาศยานนั้น ๆ (Countermeasure Technique)

ในระดับของผู้ปฏิบัติ (Operator) จะต้องได้รับการฝึกฝนที่เพียงพอในการประมวลภาพเหตุการณ์รอบตัว และมีข้อมูลข่าวสารที่ครบถ้วนรวมทั้งมีความแข็งแรงทั้งร่างกายและจิตใจเพื่อสร้างการระมัดระวังในสถานการณ์หรือการหยั่งรู้ในสถานการณ์ปัจจุบัน (Situation Awareness) สำหรับผู้ปฏิบัตินั้นจะได้รับข้อมูลสถานการณ์ทางยุทธวิธี (Tactical Picture) จากในห้องนักบิน (Cabin) ซึ่งมีการประมวลผลจากข้อมูลต่าง ๆ ที่ได้รับจากอุปกรณ์ EW ที่ติดตั้งบนอากาศยานในระดับของอุปกรณ์ (Equipment) นั้น ๆ จะแบ่งเป็นสองกลุ่มใหญ่ คือ กลุ่มรับข้อมูล ได้แก่ อุปกรณ์ตรวจจับทาง EW อุปกรณ์ตรวจจับอื่น ๆ และระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link) อีกกลุ่มหนึ่งคือ อุปกรณ์ที่วิเคราะห์และใช้ต่อต้านภัยคุกคามต่าง ๆ (Countermeasure Technique) เช่น ชุดประมวลผลกลาง (Mission Central Processor Unit)

ชุดควบคุมการปล่อย Chaff/Fair เป็นต้น สิ่งที่จำเป็นอย่างยิ่งในการทำงานของอุปกรณ์ EW ต่าง ๆ คือการขุดข้อมูลด้านสงครามอิเล็กทรอนิกส์เฉพาะที่ใช้ในภารกิจ (Electronic War-fare Mission Data Set: EWMDS) ที่มาจากระดับ Mission Data, Functional Specification, Models และ Source Data ตามลำดับ

ในกระบวนการที่จะได้มาซึ่ง EWMDS ซึ่งเป็นส่วนสำคัญของการสงครามอิเล็กทรอนิกส์นั้น จะเริ่มจากการรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น ISTAR Picture ในระดับข้อมูลดิบ นำมาจำลองในการจำลองและทดสอบแบบ (Modeling and Simulator) เมื่อได้แบบจำลองของข้อมูลที่น่าเชื่อถือแล้วข้อมูลจะถูกเลือกเพื่อนำไปวิเคราะห์ในการต่อต้านภัยคุกคามที่จะเผชิญในพื้นที่การรบ ซึ่งจะแบ่งเป็นส่วนการตรวจจับทางอิเล็กทรอนิกส์ (EW Sensor Functional Specification) และส่วนที่มีผลกระทบทางสงครามอิเล็กทรอนิกส์ (EW Effecter Functional Specification) ในระดับของข้อมูลจำเพาะของการทำงาน (Functional Specification) ผลที่ได้จากการวิเคราะห์ข้อมูลจำเพาะการทำงานของอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับการสงครามอิเล็กทรอนิกส์ในพื้นที่การรบจะถูกนำมาสังเคราะห์เป็นชุดข้อมูลด้านสงครามอิเล็กทรอนิกส์เฉพาะที่ใช้ในภารกิจ (EWMDS) ซึ่งจะถูกนำไปใช้งานในอุปกรณ์ต่าง ๆ ที่ติดตั้งบนอากาศยานต่อไป

ปัจจุบันกองทัพอากาศมีขีดความสามารถในการปฏิบัติการ EW ในระดับผู้ใช้งาน นั่นคือมีการใช้งาน EW ตั้งแต่ระดับอุปกรณ์ (Equipment) ขึ้นไป โดยมีข้อจำกัดในด้านการพัฒนาการต่อต้านทางสงครามอิเล็กทรอนิกส์ (Countermeasure Development) ด้วยตนเอง เนื่องจากขาดบุคลากรและหน่วยงานที่รับผิดชอบรวมทั้งปัญหาในการถ่ายทอดเทคโนโลยีของผู้จำหน่ายอุปกรณ์หรืออากาศยาน จากวัตถุประสงค์หลักในการรับการถ่ายทอดเทคโนโลยี EW ของโครงการจัดซื้อเครื่องบิน Gripen 39 C/D ในการพัฒนาขีดความสามารถด้านสงครามอิเล็กทรอนิกส์โดยรวมของกองทัพอากาศระยะยาว และการจัดทำฐานข้อมูลทางสงครามอิเล็กทรอนิกส์ (EW Database) ข้อมูลอิเล็กทรอนิกส์ในพื้นที่การรบ (Electronic Order of Battle: EOB) และห้องสมุดอิเล็กทรอนิกส์ (EW Library) ตลอดจนสามารถพัฒนาการต่อต้านทางสงครามอิเล็กทรอนิกส์ (EW Countermeasure Development) ด้วยตัวเองได้กองทัพอากาศจำเป็นต้องมีหน่วยงานที่รับผิดชอบในเรื่องนี้โดยตรงและมีบุคลากรที่มีความรู้ความสามารถในการจัดการ รวมทั้งวิเคราะห์ข้อมูลต่าง ๆ ที่เกี่ยวข้อง

ประโยชน์ที่กองทัพอากาศจะได้รับจากการพัฒนา EW

ในการพัฒนาสิ่งหนึ่งสิ่งใดขึ้นมาใหม่ ย่อมมีการเปลี่ยนแปลงด้วยกันทั้งสิ้น รวมทั้งการปฏิบัติการด้าน EW ผลกระทบประการแรก คือ การปรับปรุงระบบการทำงานของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง รวมถึงการปรับตำแหน่งงานและหน้าที่ความรับผิดชอบของบุคคลและหน่วยงานในปัจจุบันให้สอดคล้องกับการปฏิบัติงานด้าน EW ประการที่สอง คือ งบประมาณที่จะต้องทุ่มลงไปในเครื่องมืออุปกรณ์ และข้อมูลต่าง ๆ ที่จะต้องจัดหามาให้สอดคล้องกับขีดความสามารถที่กองทัพอากาศต้องการ และปัจจัยที่สำคัญที่สุดที่จะต้องเปลี่ยนแปลง คือ แนวความคิดในการปฏิบัติด้าน EW ของบุคลากรในกองทัพอากาศ ที่จะต้องทำความเข้าใจในความจำเป็นที่จะต้องก้าวเข้าไปสู่การรบในยุคใหม่ที่ขึ้นอยู่กับเทคโนโลยีข่าวสารและระบบ

อิเล็กทรอนิกส์ รวมทั้งบุคลากรในหน่วยงานที่เกี่ยวข้องจะต้องปรับตัวและเพิ่มพูนขีดความสามารถของตนเองให้สามารถรองรับเทคโนโลยีที่เกี่ยวข้องในอนาคต หากการพัฒนาด้าน EW ของกองทัพอากาศเป็นไปตามแนวทางยุทธศาสตร์การพัฒนาด้าน EW จะได้รับประโยชน์หลายประการ กล่าวคือ

1. การพัฒนาการสงครามอิเล็กทรอนิกส์เป็นอีกแนวทางหนึ่งที่จะนำกองทัพอากาศไปสู่กองทัพอากาศชั้นนำในภูมิภาค (One of the best Air Force in ASEAN) ตามยุทธศาสตร์การพัฒนากองทัพอากาศที่ได้วางไว้ และสามารถบูรณาการงานด้านการสงครามอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ

2. กองทัพอากาศจะสามารถรองรับการพัฒนาเทคโนโลยีด้านปฏิบัติการสงครามอิเล็กทรอนิกส์ในอนาคตได้อย่างมีประสิทธิภาพ โดยมีหน่วยงานและบุคลากรที่รับผิดชอบตลอดจนมีขีดความสามารถในการพัฒนา วิเคราะห์ และจัดทำข้อมูลต่าง ๆ ที่จำเป็นได้ด้วยตนเอง ลดการพึ่งพาจากต่างประเทศในยามเกิดความขัดแย้ง

3. กองทัพอากาศจะสามารถใช้งานยุทโธปกรณ์ที่มีอยู่ได้อย่างมีประสิทธิภาพ และสามารถรองรับการปฏิบัติงานของอากาศยานที่ติดตั้งระบบสงครามอิเล็กทรอนิกส์ทุกประเภท โดยเฉพาะอย่างยิ่งการจัดทำ Threat Library และ CM Tactics ที่ใช้งานกับเครื่องบิน Gripen JAS 39 C/D ในระยะสั้น และเครื่องบินแบบ อื่น ๆ ในอนาคตได้อย่างดีอีกด้วย

4. กองทัพอากาศจะได้รับการพัฒนาระบบการข่าวที่เน้นในข้อมูลที่จะใช้ในการเอาชนะเครื่องบินและยุทโธปกรณ์ของข้าศึกได้

5. การสงครามอิเล็กทรอนิกส์ที่มีประสิทธิภาพจะเป็นปัจจัยในการทวีกำลังของกำลังทางอากาศ และสามารถลดความสูญเสียของอากาศยานและนักบินในการปฏิบัติการรบ

งานวิจัยที่เกี่ยวข้อง

1. บทวิเคราะห์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ปี พ.ศ.2559 (แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ, ออนไลน์, 2559) “The Information Security Forum (ISF)” เป็นองค์กรที่ไม่แสวงหากำไร มีสมาชิกที่เป็นองค์กรชั้นนำทั่วโลก ได้จัดทำผลสำรวจ วิเคราะห์ และรายงาน “Threat Horizon Report” เพื่อพยากรณ์แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศล่วงหน้าทุก ๆ 2 ปี โดยระบุประเด็นที่ส่งผลกระทบอย่างมีนัยสำคัญต่อองค์กร พร้อมทั้งแนวทางดำเนินการเพื่อป้องกันหรือช่วยลดผลกระทบที่อาจเกิดขึ้นจากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 โดย ISF ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทางไซเบอร์ยังคงมีต่อเนื่องและได้สรุปความเชื่อถือที่องค์กรต้องรักษาไว้ให้ได้ใน 3 ประเด็น ดังนี้

1.1 ไม่มีใครน่าไว้ใจในไซเบอร์อีกต่อไป (No-one Left to Trust in Cyberspace) การจารกรรมไซเบอร์ที่สนับสนุนโดยหน่วยงานภาครัฐ จะกลายเป็นกระแสหลัก การควบคุม Internet ภายในประเทศหรือภูมิภาคจะสร้างความยุ่งยากต่อธุรกิจเนื่องจากการแทรกแซงของภาครัฐ

1.2 ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ (Confidence in Accepted Solutions

Crumbles) โดยผู้ให้บริการจะกลายเป็นช่องโหว่สำคัญ ระบบ Big Data จะกลายเป็นปัญหาหลัก และแอพพลิเคชั่นในมือถือจะกลายเป็นช่องทางหลักที่ถูกเจาะข้อมูลและการเข้ารหัสข้อมูลในระบบจะไม่ได้ผล

1.3 ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Failure to Deliver the Cyber Resilience Promise) ผู้บริหารต้องรับรู้และถึงเวลาที่ต้องระบุข้อมูลวางแนวทางในการดำเนินการ ความแตกต่างด้านทักษะของบุคลากรจะมีช่องห่างกว้างมากขึ้นความมั่นคงปลอดภัยสารสนเทศในปัจจุบันอาจจะไม่เหมาะสมกับบุคลากรรุ่นใหม่

การจารกรรมทางไซเบอร์ (Cyber Espionage) จะทวีความเข้มข้นรุนแรงมากขึ้น ซึ่งผลการสำรวจและข้อมูลจากองค์กรชั้นนำได้สรุปผลการวิเคราะห์พฤติกรรม Incidents ที่เกิดจากภัยคุกคามต่าง ๆ ในรอบ 10 ปี คือ การจารกรรมทางไซเบอร์ (Cyber-Espionage) การโจมตีระบบ (DoS Attacks) โปรแกรมมุ่งร้ายเพื่อก่ออาชญากรรม (Crime Ware) 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) รวมถึงการจารกรรมไซเบอร์ด้วยโปรแกรมและซอฟต์แวร์ที่สนับสนุนพัฒนาขึ้นโดยภาครัฐเพื่อติดตามพฤติกรรมกลุ่มเป้าหมายที่ต้องการจะมีวงกว้างมากขึ้น ดังนั้นแนวโน้มการควบคุมหรือแทรกแซงระบบอินเทอร์เน็ตหรืออาจเรียกได้ว่าปิดประเทศด้านไซเบอร์เฉพาะบางช่องทางที่ต้องการควบคุมจะมีให้เห็นมากขึ้นอย่างที่ประเทศจีนได้สร้างกำแพงเมืองจีนในโลกไซเบอร์อยู่ในขณะนี้ทั้งเพื่อปกป้องพลเมืองตนเองไปผจญการสื่อสารโลกภายนอกและป้องกันคนภายนอกเข้ามาดังนั้นองค์กรทั่วโลกต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลงและผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่

2. ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security (ปริญญา หอมเอนก, ออนไลน์, 2559) ได้สรุปแนวโน้มภัยคุกคามและทิศทางด้านความมั่นคงปลอดภัยในปี 2016 - 2018 ดังนี้

2.1 Cyber Security ไม่ใช่เรื่องเฉพาะฝ่าย IT อีกต่อไปหากเป็นเรื่องที่ต้องนำเข้าที่ประชุม “บอร์ดบริหาร” ขององค์กร

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

2.3 Cyber Threat Intelligence เป็นการเปลี่ยนวิธีการบริหารจัดการความมั่นคง ปลอดภัยจาก “Reactive” เป็น “Proactive”

2.4 แฮ็คเกอร์จะมุ่งหน้าโจมตีไปยังเป้าหมายเฉพาะ แต่มีผลกระทบและสร้างความเสียหายสูงต่อองค์กร

2.5 การโจมตีของแฮ็คเกอร์จะมีลักษณะต่อเนื่องและฝังตัวเป็นระยะเวลานานกว่าองค์กรจะตรวจจับได้ว่าถูกแฮ็ค (Advanced Persistent Threats)

2.6 แฮ็คเกอร์พุ่งเป้าโจมตีองค์กรขนาดใหญ่และมีรัฐบาลให้การสนับสนุนอยู่เบื้องหลัง (State-Sponsored Attack)

2.7 องค์กรจำเป็นต้องมีความสามารถในการตามล่าและติดตามแฮ็คเกอร์ในโลกจริงที่ไม่ใช่เพียงโลกไซเบอร์ และกล่าวเพิ่มเติมว่า “ปัจจุบันนี้แฮ็คเกอร์ระดับประเทศเขาไม่แฮ็คระบบหรือ ปล่อยมัลแวร์แล้วแต่ใช้วิธีฝัง Backdoor มากับอุปกรณ์ IoT เช่น CCTV, IP Camera หรือ Router ตั้งแต่แรกแทน ส่งผลให้แฮ็คเกอร์สามารถเข้าโจมตีระบบผ่านอุปกรณ์หรือสร้างกองทัพซอมบี้ไว้โจมตี DDoS แบบที่ปรากฏในข่าวล่าสุดได้ตามต้องการทันที”

3. สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนาได้ดำเนินโครงการวิจัยระยะสั้นเพื่อตอบโจทย์สถานการณ์การค้าและการพัฒนาในมิติความมั่นคงของอาเซียน เรื่อง ความมั่นคงปลอดภัยทางไซเบอร์กับอุปสรรคทางการค้าในอาเซียน มีวัตถุประสงค์เพื่อศึกษาว่ามาตรฐานหรือกฎหมายเพื่อส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมสำหรับการป้องกันและปราบปรามอาชญากรรมไซเบอร์ และไม่เป็นอุปสรรคทางการค้าต่อการค้าดิจิทัลอาเซียนควรมีลักษณะอย่างไร และเพื่อนำเสนอแนวทางการพัฒนาประชาคมอาเซียนที่สร้างสมดุลระหว่างความมั่นคงกับการค้า

การเติบโตของเทคโนโลยีดิจิทัลในยุคปฏิวัติอุตสาหกรรมครั้งที่ 4 โดยเฉพาะอย่างยิ่งการเกิดขึ้นของโลกออนไลน์หรือไซเบอร์สเปซนั้นส่งผลต่อการใช้ชีวิตของผู้คนยุคนี้ในทุกมิติ ในบริบทของไซเบอร์ ผู้ใช้บริการ หรือผู้ให้บริการ มีความเสี่ยงต่อภัยคุกคามรูปแบบใหม่ที่เรียกว่าภัยคุกคามทางไซเบอร์ ซึ่งผู้ก่อภัยคุกคามมุ่งที่จะสร้างภัยคุกคามให้มีผลกระทบในทางลบต่อคอมพิวเตอร์ ระบบคอมพิวเตอร์ระบบอินเทอร์เน็ตหรือแม้แต่ข้อมูลส่วนบุคคลที่อยู่ในคอมพิวเตอร์หรือระบบดังกล่าว

ผลการศึกษาพบว่า มาตรการสร้างความมั่นคงปลอดภัยทางไซเบอร์ส่งผลกระทบต่อการค้าบริการดิจิทัลที่อยู่บนไซเบอร์สเปซ ซึ่งมีบริบทระหว่างประเทศและไม่มีพรมแดนเป็นข้อจำกัด และการให้บริการอินเทอร์เน็ตหรือ Cyber Space ต้องนึกถึงความสามารถในการทำงานร่วมกัน (Interoperability) และการเปิดรับ (Openness) เป็นหลัก ดังนั้น ความแตกต่างของมาตรการสร้างความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ ย่อมส่งผลให้ผู้ประกอบการบริการดิจิทัลมีต้นทุนที่สูงขึ้นและเป็นอุปสรรคต่อการค้าบริการเสรีระหว่างประเทศอย่างแน่นอน (ความมั่นคงปลอดภัยไซเบอร์ในอาเซียน, 2563)

4. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ : ความท้าทายของกองทัพบก (Cyber Security : A Challenge of Army) (ออนไลน์, 2557) บ่งชี้ว่า ปัจจุบันและแนวโน้มในอนาคตภัยคุกคามด้านไซเบอร์ นับวันจะทวีความเข้มข้นและความรุนแรงมากขึ้นตามลำดับ ทั้งนี้เป็นผลมาจากความเจริญก้าวหน้าในการพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสาร องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ (Cyber Attack) รัฐบาลสหรัฐฯ ได้ตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ดังกล่าว จึงได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐฯ (National Institute of Standards and Technology : NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย

(Policy) การจัดการองค์กร (Organization) และเทคโนโลยี (Technology) เพื่อบริหารความเสี่ยงไซเบอร์ (Cyber Risk Management) ที่ส่งผลกระทบกับหน่วยงานได้อย่างเหมาะสม โดยกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เพื่อนำมาใช้ในการดำเนินการร่วมกันประกอบด้วยกลุ่มหน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม จำแนกเป็น 5 Functions (IPDRR : Identify, Protect, Detect, Respond, Recover) กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สินการควบคุมการเข้าถึงกลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิคและ/หรือกิจกรรมในการบริหารจัดการและข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทางและแนวปฏิบัติที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม ซึ่งกองทัพบกได้เล็งเห็นความสำคัญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เช่นกันจึงได้อนุมัติหลักการให้จัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Centre) ขึ้นการกำหนดกรอบความคิดในการปฏิบัติงาน (Framework) เพื่อสร้างหลักประกันความสำเร็จในการดำเนินการ จึงเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่ง ทั้งนี้เพื่อใช้เป็นแนวทางการปฏิบัติงาน (Guide Line) ให้กับเจ้าหน้าที่ศูนย์ไซเบอร์กองทัพบกและเจ้าหน้าที่อื่น ๆ ที่เกี่ยวข้อง รวมถึงการสร้างความสำนึกความตระหนัก และความรู้เข้าใจของกำลังพลทุกระดับชั้น โดยในชั้นต้นกรอบแนวทางการปฏิบัติงานของศูนย์ไซเบอร์กองทัพบกยังคงยึดถือการดำเนินงานตามหลักหน้าที่พื้นฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology NIST) ทั้ง 5 ประการ (IPDRR : Identify, Protect, Detect, Respond, Recover) จึงต้องการบุคลากรที่จะมาปฏิบัติหน้าที่โดยมีคุณลักษณะของงานประเภทสาขาต่าง ๆ ที่ต้องใช้ความรู้ความสามารถและประสบการณ์เฉพาะในด้านไซเบอร์ 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) การเฝ้าระวังตรวจสอบและวิเคราะห์ไซเบอร์ (Cyber Monitoring and Analysis) การปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations) การตรวจสอบระบบสารสนเทศ (IT Audit) การตรวจพิสูจน์หลักฐานทางดิจิตอล (Digital Forensics) การปฏิบัติการฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response ; CER) การปฏิบัติการกู้คืนระบบ (System Recovery ; SR) เป็นต้น

5. งานศึกษาวิจัยแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ (ณรงค์เวตย์ เรืองจวง, 2560) มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและข้อจำกัดการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ ศึกษาปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ และเพื่อเสนอแนวทางการพัฒนาบุคลากรและปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ ศึกษาและวิเคราะห์ข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไปในด้านสงคราม

ไซเบอร์ นโยบายระดับชาติ นโยบายระดับกองทัพ นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของกองทัพอากาศ และการปฏิบัติงานด้านไซเบอร์ ผลการศึกษาวิจัยพบว่ากองทัพอากาศได้ตระหนักถึงความสำคัญการปฏิบัติงานด้านไซเบอร์ เพื่อเตรียมรับมือกับภัยคุกคามที่อาจจะเกิดขึ้น โดยการจัดหาระบบเทคโนโลยีสารสนเทศ พร้อมอุปกรณ์และระบบป้องกันมาใช้ในการปฏิบัติภารกิจจัดทำแผนงานที่เกี่ยวข้อง รวมถึงพัฒนาบุคลากรด้านไซเบอร์ พร้อมจัดให้มีการตรวจสอบระบบอย่างต่อเนื่อง ในประเด็นสภาพปัญหาและข้อจำกัดในการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ มีดังนี้

5.1 ปัญหาหลักที่สำคัญ ได้แก่ บุคลากรบางส่วนยังละเลยการปฏิบัติตามนโยบายที่เกี่ยวข้อง รวมถึงบุคลากรด้านไซเบอร์มีจำนวนไม่เพียงพอและยังขาดทักษะในการปฏิบัติงาน การจัดการความรู้ยังไม่ครอบคลุมเทคโนโลยีและคู่มือการใช้งานอุปกรณ์ใหม่ มีข้อจำกัดในด้านสถานที่ ระบบเทคโนโลยีเชิงป้องกันที่จัดหามาใช้งานยังมีปัญหาในการติดตั้งใช้งานที่ทำให้ไม่สะดวกต่อการปฏิบัติงานของบุคลากรในการเฝ้าตรวจ ระบบเทคโนโลยีที่จัดหามาใหม่ต้องมีลิขสิทธิ์จากบริษัทผู้ผลิต ทำให้ต้องใช้งบประมาณมากขึ้น

5.2 ปัจจัยที่มีผลกระทบต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติการไซเบอร์ของกองทัพอากาศ มีการปฏิบัติตามองค์ประกอบ 3 ด้าน ดังนี้

5.2.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้อง แม้ว่าได้มีการดำเนินการในหลายด้าน เช่น จัดทำระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ จัดทำโครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ การจัดการแข่งขัน Cyber Operations Contest จัดทำเอกสารคู่มือการปฏิบัติงานและการจัดการองค์ความรู้ เป็นต้น ซึ่งการดำเนินการดังกล่าวนี้หากสามารถดำเนินการได้อย่างครบถ้วนเหมาะสมและทันสถานการณ์จะทำให้การปฏิบัติภารกิจด้านไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

5.2.2 ปัจจัยด้านเทคโนโลยี กองทัพอากาศได้จัดหาระบบเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องปรามมาใช้งาน เช่น ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ระบบศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรองระบบเข้ารหัสข้อมูล และระบบจำลองยุทธทางไซเบอร์ เป็นต้น ซึ่งในการจัดหาเทคโนโลยีมาใช้งานนั้น ต้องดำเนินการจัดหาตามแผนงานที่กำหนดไว้ตามระบบการจัดหาของทางราชการ ซึ่งมีเงื่อนเวลามาเกี่ยวข้อง ขณะที่เทคโนโลยีมีการพัฒนาและปรับตัวอย่างรวดเร็ว จึงมีผลกระทบต่อการจัดการกับเทคโนโลยีใหม่ที่นำมาใช้งาน และต่อเนื่องถึงการพัฒนาบุคลากรที่รับผิดชอบและระบบงบประมาณของกองทัพอากาศ

5.2.3 ปัจจัยด้านบุคลากร กองทัพอากาศได้มีการดำเนินการด้านการจัดการองค์ความรู้เพื่อรองรับการพัฒนาบุคลากร โดยจัดทำหลักสูตรพื้นฐานรองรับผู้ปฏิบัติงานหลักสูตรนายทหารรักษาความปลอดภัยสารสนเทศ และหลักสูตรอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งส่งบุคลากรเข้ารับการฝึกอบรมกับหลักสูตรนอกกองทัพ รวมถึงการจัดการฝึกอบรมเพื่อการเลื่อนระดับความชำนาญให้กับบุคลากรที่มีคุณสมบัติครบถ้วนเพื่อรองรับการพิจารณาเลื่อนยศและเข้าดำรงตำแหน่งที่สูงขึ้น เป็นต้น อีกทั้งมีการสร้างจิตสำนึกในด้านการรักษาความปลอดภัยทางไซเบอร์ให้กับกำลังพลของกองทัพอากาศอย่างต่อเนื่อง เช่นเดียวกับการพัฒนาและเสริมสร้างองค์ความรู้

ทักษะและความชำนาญด้านไซเบอร์ให้ทันสมัยควบคู่กับการผลิตนักรบไซเบอร์ให้มีจำนวนเพียงพอต่อการปฏิบัติภารกิจ

5.3 แนวทางการพัฒนาบุคลากร ต้องจัดให้มีการฝึกอบรม ทบทวน และส่งไปศึกษานอกหน่วยให้กับบุคลากรทุกระดับ ได้แก่ ระดับผู้ปฏิบัติงาน ระดับผู้ตรวจสอบและผู้ที่เป็นวิทยากรให้การอบรมระดับผู้รับผิดชอบดูแลระบบ และระดับเจ้าหน้าที่ทำงานด้านการรักษาความปลอดภัยระบบสารสนเทศ รวมถึงให้มีการจัดทำคู่มือในการปฏิบัติงานด้วย อีกทั้งบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติภารกิจและต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน มีการจัดเตรียมหลักสูตรและทบทวนหลักสูตรที่ใช้ในการฝึกศึกษาและอบรมด้านไซเบอร์อย่างต่อเนื่อง ต้องมีการจัดทำและปรับปรุงการตรวจสอบระบบให้ทันสมัย รวมทั้งให้มีการสุ่มตรวจสอบระบบในภาพรวม หากพบข้อบกพร่องให้แจ้งหน่วยเกี่ยวข้องทราบ เมื่อพบบุคลากรกระทำผิดให้พิจารณาลงทัณฑ์ตามแนวทางที่กองทัพอากาศกำหนด รวมทั้งจัดให้มีการทบทวนความรู้ในการปฏิบัติงาน และการดำเนินการตามแผนงานให้กับผู้รับผิดชอบดูแลระบบที่อยู่ในความรับผิดชอบอย่างต่อเนื่อง

5.4 ปัจจัยที่เกี่ยวข้องต่อการปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ ได้แก่ โครงสร้างการจัดหน่วย ที่ควรพิจารณาให้ปรับโครงสร้างอัตราที่เหมาะสมเพื่อรองรับการปฏิบัติภารกิจและปริมาณงานที่จะเกิดขึ้นในอนาคต ทบทวน ปรับปรุง การจัดทำแผนงานและแนวทางการปฏิบัติที่เกี่ยวข้อง ให้ครอบคลุมการปฏิบัติงานรวมถึงแนวทางการตรวจสอบระบบให้ทันสมัย พร้อมทั้งจัดทำคู่มือการปฏิบัติรองรับสถานการณ์ต่าง ๆ แจกจ่ายให้หน่วยเกี่ยวข้องอีกทั้งควรจัดทำคู่มือการใช้งานระบบอุปกรณ์และโปรแกรมที่ใช้งานอยู่และที่จะจัดหามาใหม่เพิ่มเติม และจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งานในกองทัพอากาศ สร้างแรงจูงใจให้กับผู้ปฏิบัติภารกิจ โดยพิจารณาเงินเพิ่มพิเศษเป็นค่าตอบแทนให้กับผู้ปฏิบัติงานด้านไซเบอร์

5.5 ข้อเสนอแนะของผู้วิจัย มีดังนี้

5.5.1 ควรมีการศึกษาวิจัยเพิ่มเติมในส่วนของโครงสร้างและอัตราของหน่วยงานด้านไซเบอร์ให้สอดคล้องกับงานเชิงป้องกันและป้องปราม

5.5.2 ควรมีการจัดการฝึกศึกษา การอบรม การทบทวน และส่งไปศึกษากับหน่วยนอกให้กับบุคลากรทุกระดับรวมถึงให้มีการจัดทำคู่มือในการปฏิบัติงานอีกทั้งควรบรรจุบุคลากรให้เพียงพอต่อการปฏิบัติภารกิจโดยต้องกำหนดคุณสมบัติบุคลากรแรกเข้าก่อนบรรจุในตำแหน่งด้านไซเบอร์ให้ชัดเจน

5.5.3 ปรับปรุงการจัดทำแผนแม่บท แผนงาน แนวทางการปฏิบัติที่เกี่ยวข้องด้านไซเบอร์ให้ครอบคลุมการปฏิบัติ และจัดให้มีการซักซ้อมการดำเนินการตามแผนงานให้กับผู้เกี่ยวข้องอย่างต่อเนื่อง รวมถึงควรจัดทำระบบการจัดการความรู้ให้ครอบคลุมเทคโนโลยีที่มีใช้งาน

5.5.4 สนับสนุนงบประมาณให้เพียงพอต่อการปฏิบัติภารกิจด้านไซเบอร์

หยาดพิรุณ นาชัยสินธุ์ (2559) ได้ศึกษายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย มีวัตถุประสงค์เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการใช้เป็นเครื่องมือทางยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย และวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรค สถานการณ์ และองค์กร

แห่งการเรียนรู้ เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ด้วยการใช้เทคนิคเดลฟาย สัมภาษณ์เชิงลึก แล้วนำข้อมูลที่ได้มาจัดทำแบบสอบถามเชิงปริมาณ ใช้กับกลุ่มตัวอย่างจำนวน 690 คน จากการวิเคราะห์ข้อมูล ผู้วิจัยได้ปรับปรุงยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของไทย โดยผลการวิจัยที่สำคัญแสดงให้เห็นว่าความก้าวหน้าทางไซเบอร์คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็ว ไม่ว่าจะอยู่ที่ใดในโลกการก่อการร้ายทางไซเบอร์จะใช้เครื่องมือทางเทคโนโลยี ได้แก่ โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือ อื่น ๆ ที่เชื่อมต่อทาง Internet เป็นช่องทางในการก่อการร้าย โดยผู้วิจัยได้นำเสนอยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ประเทศไทยไว้ คือ **ยุทธศาสตร์ READ : CLIP** ประกอบด้วย

ยุทธศาสตร์ที่ 1 Research หรือการเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์

ยุทธศาสตร์ที่ 2 Education หรือการจัดการศึกษาในการสร้างพื้นฐานของประชาชน

ยุทธศาสตร์ที่ 3 Awareness หรือการสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน

ยุทธศาสตร์ที่ 4 Development หรือการพัฒนาความก้าวหน้าทางไซเบอร์

ยุทธศาสตร์ที่ 5 Coordinate หรือการส่งเสริมความร่วมมือของภาครัฐภาคเอกชนและภาคประชาชน

ยุทธศาสตร์ที่ 6 Law หรือการกำหนดใช้กฎหมายทางไซเบอร์ และการบังคับใช้กับประชาชน

ยุทธศาสตร์ที่ 7 Integration หรือการบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect หรือการรับรู้ทางไซเบอร์ร่วมกันเพื่อเตรียมการและปกป้องทางไซเบอร์

สรุป

แม้ว่าปฏิญญาประชาคมการเมืองและความมั่นคงของอาเซียน พ.ศ.2568 กำหนดให้ประเทศสมาชิกอาเซียนร่วมกันป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ (Cybercrime) เพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับภูมิภาคอาเซียน แต่การส่งเสริมพาณิชย์อิเล็กทรอนิกส์ของอาเซียน ได้กำหนดให้มีการเปิดเสรีการค้าสินค้า บริการ และการลงทุนด้านเทคโนโลยีสารสนเทศภายในอาเซียน ดังนั้น ประเทศสมาชิกจำเป็นต้องยกเลิกภาษีและอุปสรรคทางการค้าและอำนวยความสะดวกให้เกิดการเติบโตทางพาณิชย์อิเล็กทรอนิกส์ โดยการออกกฎหมายและระเบียบให้สอดคล้องกับมาตรฐานระหว่างประเทศ

ประเทศสมาชิกอาเซียนควรเลือกมาตรการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพในการปกป้องคุ้มครองภัยคุกคามทางไซเบอร์ที่เป็นอุปสรรคทางการค้าระหว่างประเทศน้อยที่สุด โดยเปิดโอกาสให้เอกชนเลือกรูปแบบมาตรการทางเทคนิคที่เหมาะสมและมีประสิทธิภาพมากที่สุดกับการให้บริการนอกจากนั้นในมิติการออกกฎหมายเพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ภาครัฐควรระบุวัตถุประสงค์ว่าต้องการคุ้มครองอะไรเป็นสำคัญมากกว่าการกำหนดว่าผู้ประกอบการจะต้องดำเนินการอย่างไรเพราะผู้ประกอบการมีความเชี่ยวชาญทางเทคนิคในการออกแบบการให้บริการดิจิทัลที่สร้างความมั่นคงปลอดภัยทางไซเบอร์ตามที่กฎหมายต้องการได้

กรอบแนวคิดของการวิจัย

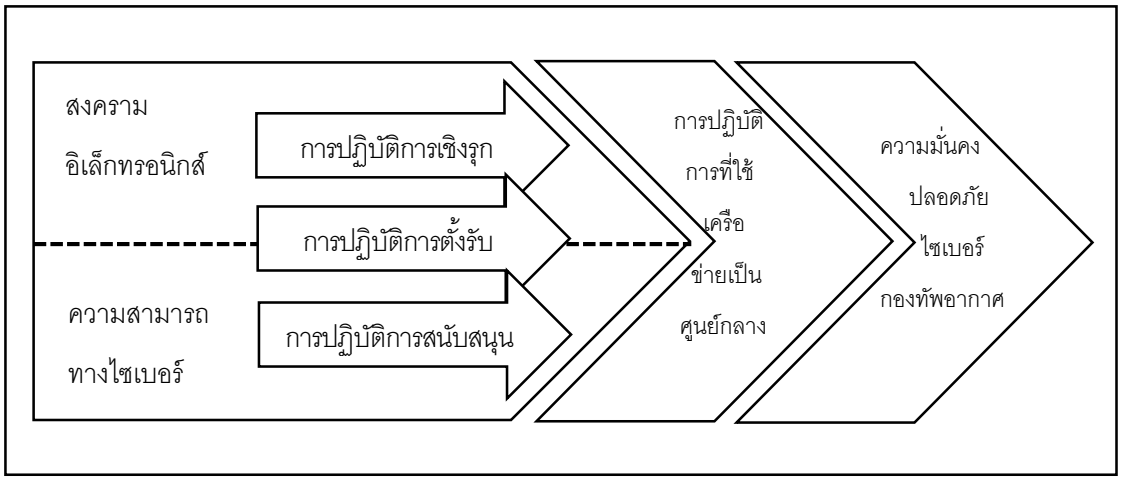
จากพื้นฐานหลักนิยมกองทัพอากาศ ความรูเกี่ยวกับการใช้กำลังทางอากาศที่ถูกต้องจะก่อให้เกิดผลลัพธ์ที่มีผลกระทบอย่างมหาศาลต่อกำลังรบของฝ่ายตรงข้าม กำลังทางอากาศมีลักษณะเฉพาะตัวที่ปฏิบัติให้บรรลุวัตถุประสงค์ดังกล่าวร่วมกับขีดความสามารถด้านการข่าวสารได้เป็นอย่างดี ตลอดจนสามารถกำหนดจังหวะและหนทางปฏิบัติต่าง ๆ ครอบคลุมการใช้กำลังทางทหารได้ทุกระดับของความขัดแย้ง ด้วยธรรมชาติและคุณลักษณะของกำลังทางอากาศสามารถปฏิบัติภารกิจตอบสนองความต้องการได้หลากหลายรูปแบบในทุกมิติของสงคราม กำลังทางอากาศจึงควรมีแนวทางในการใช้งาน ให้สอดคล้องกับหลักปฏิบัติ ได้แก่ รวมการควบคุม แยกการปฏิบัติ การบัญชาการและควบคุมที่เป็นหนึ่ง และ พิจารณาถึงผลกระทบที่เหมาะสมในระดับที่ต้องการ เพราะการเลือกใช้กำลังทางอากาศหากไม่พิจารณาวางแผนอย่างรอบคอบอาจไม่ส่งผลให้เป็นไปตามที่ต้องการถึงขั้นเป็นไปในทางตรงกันข้าม

ความรู้เกี่ยวกับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) หรือ การใช้เทคโนโลยีเครือข่ายในการสร้างความได้เปรียบของข้อมูล ข่าวสารและข่าวกรองสำหรับฝ่ายเรา โดยมีการเชื่อมโยงข้อมูลที่ได้รับจากระบบตรวจจับต่าง ๆ (Sensor) เข้าสู่ระบบควบคุมบังคับบัญชา (Command and Control) นำไปสู่การตัดสินใจของผู้บังคับบัญชาที่ถูกต้อง ปลอดภัย นอกจากนี้ ด้วยความได้เปรียบของข้อมูลข่าวสารดังกล่าว จะนำมาซึ่งความหยั่งรู้สถานการณ์ร่วมกันในทุกระดับของการปฏิบัติการ ส่งผลโดยตรงต่อประสิทธิผลและประสิทธิภาพในการปฏิบัติ การบัญชาการและการควบคุมของกองทัพอากาศจึงมีความสำคัญอย่างมาก โดยเฉพาะการบัญชาการและการควบคุมนภานุภาพ (Air Power) ทั้ง ๓ มิติ ได้แก่ มิติทางอากาศ (Air Domain) มิติไซเบอร์ (Cyber Domain) และมิติอวกาศ (Space Domain) อย่างเป็นระบบและมีการปฏิบัติที่ประสานสอดคล้องกันทุกมิติ ตั้งแต่การตรวจจับ (Sensor) ในทุกมิติ ส่งต่อข้อมูลไปยังระบบควบคุมและบัญชาการ (C2) เพื่อควบคุมและสั่งการนภานุภาพทั้ง ๓ มิติ อันจะทำให้เกิดการทวีกำลังกองทัพอากาศ (Force Multiplier) อย่างเป็นรูปธรรม

ดังนั้น ในระดับยุทธศาสตร์ต้องดำเนินการศึกษาในแนวทางการพัฒนาตามยุทธศาสตร์กองทัพอากาศที่มุ่งเน้นการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) เพื่อให้เข้าใจถึงบริบทของกองทัพอากาศที่เกี่ยวข้องร่วมกับการศึกษาบริบทการพัฒนาขีดความสามารถในมิติไซเบอร์ (Cyber Domain) และศึกษาขีดความสามารถและขอบขีดจำกัดในส่วนสงครามอิเล็กทรอนิกส์ (Electronic Warfare) ที่มีกระบวนการในการดำเนินงานมีลักษณะใกล้เคียงและสอดคล้องกัน ได้แก่ การดำเนินการในลักษณะปฏิบัติการเชิงรุกปฏิบัติการตั้งรับและปฏิบัติการสนับสนุนและลำดับสุดท้าย จะดำเนินการวิเคราะห์เปรียบเทียบและพิจารณาหาแนวทางที่เป็นไปได้ไปสู่ข้อสรุปในการบูรณาการขีดความสามารถทั้งสองด้านที่จะพัฒนาขีดความสามารถทางไซเบอร์ ให้ทวีกำลังความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศและส่งผลต่อความมั่นคงของชาติได้โดยมีหลักฐานทางวิชาการที่ชัดเจนสามารถนำไปใช้ทวีกำลังได้ตามเจตนารมณ์ของหน่วยงาน ซึ่งผู้วิจัยได้กำหนดเป็นกรอบแนวคิดในการวิจัยในครั้งนี้

การศึกษาแนวทางการพัฒนาขีดความสามารถทางไซเบอร์ด้วยการเชื่อมโยงกับขีดความสามารถปฏิบัติการสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศนั้น ในระดับยุทธศาสตร์จะดำเนินการศึกษาในแนวทางการพัฒนาตามยุทธศาสตร์กองทัพอากาศที่มุ่งเน้นการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) เพื่อให้เข้าใจถึงบริบทของกองทัพอากาศที่เกี่ยวข้องร่วมกับการศึกษาบริบทการพัฒนาขีดความสามารถในมิติไซเบอร์ (Cyber Domain) และศึกษาขีดความสามารถและขอบขีดจำกัดในส่วนสงครามอิเล็กทรอนิกส์ (Electronic Warfare) ที่มีกระบวนการในการดำเนินงานมีลักษณะใกล้เคียงและสอดคล้องกัน ได้แก่การดำเนินการในลักษณะปฏิบัติการเชิงรุกปฏิบัติการตั้งรับและปฏิบัติการสนับสนุนและลำดับสุดท้าย จะดำเนินการวิเคราะห์เปรียบเทียบและพิจารณาหาแนวทางที่เป็นไปได้ไปสู่ข้อสรุปในการบูรณาการขีดความสามารถทั้งสองด้านที่จะพัฒนาขีดความสามารถทางไซเบอร์ ให้ทวีกำลังความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศและส่งผลต่อความมั่นคงของชาติได้โดยมีหลักฐานทางวิชาการที่ชัดเจนสามารถนำไปใช้ทวีกำลังได้ตามเจตนารมณ์ของหน่วยงาน ซึ่งผู้วิจัยได้กำหนดเป็นกรอบแนวคิดในการวิจัย ดังแสดง

แผนภาพที่ 2-8 กรอบแนวคิดในการวิจัย



ที่มา : ประมวลโดยผู้วิจัย

สรุป

จากการพิจารณาศักยภาพหรือขีดความสามารถของทั้งมิติไซเบอร์และปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศที่มีอยู่แล้ว ประกอบกับเป้าประสงค์ของภารกิจและกระบวนการในการดำเนินงาน ที่มีลักษณะใกล้เคียงและสอดคล้องกัน คือ มีการดำเนินการในลักษณะเชิงรุก ปฏิบัติการเชิงรับ และปฏิบัติการสนับสนุน โดยผลลัพธ์จากปฏิบัติการสงครามอิเล็กทรอนิกส์ในหลายด้าน น่าจะสามารถนำมาบูรณาการทวีขีดความสามารถทางไซเบอร์ได้อีกด้วย โดยการแสวงประโยชน์ในการเชื่อมโยงจุดเด่นของทั้งสองขีดความสามารถ ซึ่งจะเป็นประโยชน์และสร้างความได้เปรียบด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งในระดับปฏิบัติการทหารและในระดับความมั่นคงของชาติเป็นสำคัญ

บทที่ 3
บทวิเคราะห์ความเกี่ยวข้องระหว่างขีดความสามารถไซเบอร์และสงครามอิเล็กทรอนิกส์ กองทัพอากาศ

การพัฒนาขีดความสามารถสิ่งใดก็ตามวัตถุประสงค์หรือเป้าหมายที่สำคัญที่สุดคือสามารถแก้ไขหรือบรรเทาปัญหาที่เกิดขึ้นได้จริงตามสถานการณ์หรือภัยคุกคามความมั่นคงที่ทันเวลา ดังนั้นการวิเคราะห์บริบทของกองทัพอากาศ การวิเคราะห์สภาพแวดล้อมอย่างรอบด้านโดยเฉพาะการวิเคราะห์และพัฒนาศักยภาพและขีดความสามารถด้านต่าง ๆ ในที่นี้ ได้แก่ ขีดความสามารถไซเบอร์และขีดความสามารถสงครามอิเลคทรอนิกส์ให้มีความพร้อมในการเผชิญกับภัยคุกคาม จึงเป็นเรื่องที่มีความจำเป็นและสำคัญอย่างยิ่ง

บริบทด้านไซเบอร์ของประเทศไทย

ท่ามกลางกระแสโลกาภิวัฒน์และความก้าวหน้าทางเทคโนโลยีทำให้บริบทด้านความมั่นคงของโลกมีความสลับซับซ้อนมากขึ้นมีการแข่งขันที่สูงขึ้นจนนำไปสู่ความขัดแย้งในการแสวงหาประโยชน์และช่วงชิงการครอบครองทรัพยากรธรรมชาติตลอดเวลาทั้งหมดที่กล่าวมานี้ล้วนส่งผลต่อความมั่นคงของรัฐด้านไซเบอร์ทั้งสิ้นโดยมีข้อมูลสำคัญที่รวบรวมมาได้ ดังนี้

1. เทคโนโลยีสารสนเทศและการสื่อสารได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าสู่ยุคดิจิทัลที่มีเศรษฐกิจ สังคมและชีวิตประจำวันของ ประชาชน ที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก

2. การปฏิวัติทางดิจิทัล (Digital Revolution) ทำให้เกิดตัวแปรใหม่ที่ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาลและการให้บริการสาธารณะที่จำเป็น ซึ่งปัจจุบันขึ้นอยู่กับความมั่นคงของโลก ไซเบอร์และโครงสร้างพื้นฐานดิจิทัล อย่างไรก็ตามการสูญเสียความไว้วางใจใน ระบบดิจิทัลจะเป็นภัยคุกคามต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ

3. ฮาร์ดแวร์และซอฟต์แวร์ส่วนใหญ่ที่พัฒนาขึ้นเพื่ออำนวยความสะดวกในสภาพแวดล้อมแบบดิจิทัลที่มีการเชื่อมต่อกันอย่างหนาแน่นยิ่งยวด (Hyperconnected) ได้ส่งผลกระทบต่อประสิทธิภาพ ต้นทุน และขีดความสามารถของอุตสาหกรรมและการใช้ชีวิตอย่างปกติของประชาชน แต่ไม่ได้มีการออกแบบที่มีความปลอดภัยมา ตั้งแต่ต้นอย่างเหมาะสม จึงทำให้ผู้โจมตีไม่ว่าจะเป็นรัฐที่เป็นฝ่ายตรงข้าม องค์กร อาชญากรรม หรือผู้ก่อการร้ายและแม้แต่บุคคลทั่วไปก็สามารถใช้ช่องว่าง ระหว่างความสะดวกและความปลอดภัยในการโจมตีได้ ดังนั้นการลดช่องว่างและ ความเสี่ยงทางไซเบอร์จึงควรได้รับการให้ความสำคัญเป็นอันดับแรก

4. การขยายตัวของอินเทอร์เน็ตที่เชื่อมโยงกับคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มาสู่การใช้งานในระบบอัจฉริยะนั้น เป็นการขยายขอบเขตของการคุกคามทางไซเบอร์ซึ่งระบบและเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเรา เช่น ระบบการ ผลิตไฟฟ้า, ระบบควบคุมการจราจรทางอากาศ, ดาวเทียม, เทคโนโลยีทางการ แพทย์, โรงงานอุตสาหกรรมและระบบการขนส่งต่างมีการเชื่อมต่อกับอินเทอร์เน็ต ที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้

5. ภัยคุกคามด้านไซเบอร์ที่เกิดจากช่องโหว่ที่มีและช่องว่างในขีดความสามารถและการป้องกันของประเทศทำให้รัฐบาลต้องเล็งเห็นถึงความสำคัญอย่างมากเพื่อให้สามารถตอบโต้ได้อย่างเท่าทันต่อภัยคุกคามทางไซเบอร์นี้โดยจำเป็นที่จะต้องมีแนวทางในการป้องกันอย่างรอบด้านเพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและควรมีการแก้ปัญหาในการลงทุนและ การแทรกแซงเพิ่มเติมในภาคธุรกิจและภาคอุตสาหกรรมโดยอาศัยการประเมินดังต่อไปนี้

5.1 ขนาดและลักษณะของภัยคุกคามทางไซเบอร์และช่องโหว่ของประเทศซึ่งหมายความว่าการใช้แนวทางในปัจจุบันอาจจะไม่เพียงพอที่จะทำให้ประเทศปลอดภัย

5.2 แนวทางที่ขึ้นกับตลาด (Market Based Approach) ทำให้เกิดการลงทุนในภาค เอกชนเพื่อสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ แต่ไม่ได้ทำให้เกิดการเปลี่ยนแปลงในระดับที่ต้องการ ดังนั้นรัฐบาลต้องเป็นผู้นำและแทรกแซงโดยตรงโดยการสร้างกลไกด้านการลงทุนและการนำทรัพยากรที่มี อยู่ไปใช้เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์

5.3 การที่รัฐบาลดำเนินการเพียงฝ่ายเดียวเท่านั้น จะไม่สามารถทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ได้ในทุกด้าน ดังนั้นแนวทางสร้างความร่วมมือกับทุก ภาคส่วนจึงเป็นสิ่งจำเป็น

5.4 ประเทศไทยจำเป็นต้องมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตื่นตัวและสนับสนุนทักษะและขีดความสามารถต่างๆ ที่สามารถก้าวให้ทัน และเผชิญกับภัยคุกคามที่กำลังเปลี่ยนแปลงได้

แนวความคิดทางด้านยุทธศาสตร์ด้านไซเบอร์ของประเทศไทย

การพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารด้านเครือข่ายและอินเทอร์เน็ตในยุคปัจจุบันนำมาซึ่งการเกิดขึ้นของภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบการขัดขวาง สกัดกั้นการจารกรรมข้อมูล และการโจมตีเพื่อทำลายล้าง ซึ่งล้วนก่อให้เกิดความเสียหายในวงกว้าง ดังนั้นหลายประเทศจึงมีการจัดตั้งหน่วยงานรับผิดชอบมิติไซเบอร์โดยตรง รวมทั้งกำหนดเป็นมิติหนึ่งในการปฏิบัติการด้านความมั่นคงของชาติ ประเทศไทยได้ให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ โดยสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี ได้กำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564 ใช้เป็นนโยบายระดับชาติฉบับแรกของไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุด ตามสภาวะแวดล้อมที่ปรากฏ (สำนักนายกรัฐมนตรี, 2560) อีกทั้งในยุทธศาสตร์ชาติ 20 ปี ในส่วนยุทธศาสตร์

ด้านความมั่นคง ได้กำหนดประเด็นประการพัฒนาระบบกลไกมาตรการและความร่วมมือระหว่างประเทศ

1. ความเจริญและความมั่นคงปลอดภัยของประเทศขึ้นอยู่กับดิจิทัลมากขึ้นทุกขณะ ซึ่งความท้าทายของสังคมในยุคปัจจุบันคือการสร้างสังคมดิจิทัลที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้และมีองค์ความรู้และขีดความสามารถที่จำเป็นในการสร้างโอกาสและบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ

2. อินเทอร์เน็ตเป็นสิ่งจำเป็นอย่างยิ่ง แต่อย่างไรก็ตามอินเทอร์เน็ตก็ยังคงมีความไม่ปลอดภัยและยังคงมีความพยายามจากผู้ไม่หวังดีอย่างต่อเนื่องที่จะใช้ประโยชน์จากจุดอ่อนที่มีไปในทางที่ผิดในการโจมตีทางไซเบอร์ ซึ่งภัยคุกคามนี้ ไม่สามารถกำจัดได้ทั้งหมดโดยสิ้นเชิง แต่สามารถลดความเสี่ยงได้โดยให้อยู่ใน ระดับที่ทำให้สังคมยังคงดำรงต่อไปได้โดยใช้ประโยชน์จากโอกาสอันมากมายที่ เกิดจากเทคโนโลยีอินเทอร์เน็ต

3. ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Strategy) ที่กำหนดโดยรัฐบาลถือว่าเป็นยุทธศาสตร์ที่มีความสำคัญในลำดับต้นๆ เพื่อที่จะวางแนวทางในการพัฒนาความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นกับ ประเทศ อีกทั้งยังเป็นแนวทางในการพัฒนาบุคลากร, เครื่องมือ และโครงการที่เกี่ยวข้องรวมไปถึงแนวทางการส่งเสริมสนับสนุนงบประมาณ

4. วิสัยทัศน์ที่กำหนดขึ้นต้องเป็นผลให้ประเทศปลอดภัยและสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้และก้าวไปอย่างมั่นใจและประสบความสำเร็จในโลกดิจิทัล

5. เพื่อให้บรรลุวิสัยทัศน์ดังกล่าวรัฐบาลจะต้องดำเนินการให้บรรลุเป้าหมายดังต่อไปนี้

5.1 ป้องกัน – ประเทศจะต้องมีวิธีและเครื่องมือที่จะป้องกันจากภัยคุกคามทางไซเบอร์ที่มีพัฒนาการอยู่ตลอดเวลา เพื่อตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพและทำให้มั่นใจได้ว่า ระบบเครือข่ายและข้อมูลของประเทศจะ ได้รับการคุ้มครองป้องกันและมีความยืดหยุ่น โดยประชาชน ภาคธุรกิจ และ หน่วยงานของรัฐ จะต้องมีความรู้และมีขีดความสามารถในการป้องกันตัวเอง

5.2 ขัดขวาง - ต้องทำให้ประเทศไทยเป็นเป้าหมายที่ยากต่อการโจมตีทางไซเบอร์ทุกรูปแบบซึ่งสามารถตรวจสอบสืบสวนและทำลายการกระทำต่างๆ ที่เข้ามาโจมตีได้โดยทำการไล่ล่าและจับกุมผู้ที่กระทำความความผิด ซึ่งจะต้องมีแนวทางและมาตรการในการจัดการกับผู้กระทำที่ไม่เหมาะสมในโลกไซเบอร์

5.3 พัฒนา - ประเทศไทยมีอุตสาหกรรมที่เกี่ยวกับดิจิทัลที่กำลังเติบโตขึ้นซึ่งรัฐบาลจะต้องสนับสนุนโดยผ่านการวิจัยและพัฒนาทางวิทยาศาสตร์และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์การสร้างบุคลากรที่มีความสามารถในทักษะเฉพาะทางเพื่อตอบสนองต่อความต้องการของทั้งภาครัฐและ เอกชน ซึ่งความเชี่ยวชาญและขีดความสามารถในการวิเคราะห์ที่ทันสมัย จะช่วยให้ประเทศไทยสามารถตอบสนองต่อความท้าทายและเอาชนะภัยคุกคามในอนาคตได้

6. เพื่อเป็นการสนับสนุนเป้าหมายเหล่านี้ประเทศไทยควรจะต้องมีการดำเนินการในระดับนานาชาติและมีมาตรการสนับสนุนในการลงทุนและร่วมเป็นพันธมิตรในการกำหนดทิศทางวิวัฒนาการทางไซเบอร์ในระดับนานาชาติเพื่อช่วยเพิ่มความมั่นคงปลอดภัยไซเบอร์โดยรวมให้แก่ประเทศได้มากที่สุดนอกจากนี้รัฐบาลควรมีการพัฒนาความสัมพันธ์กับพันธมิตรใหม่ๆ ด้วย

เพื่อพัฒนาระดับความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศเหล่านั้นและยังเป็นการปกป้องประเทศไทยอีกด้วย ซึ่งควรทำทั้งในรูปแบบทวิภาคีและพหุภาคีรวมทั้งผ่านทาง ASEAN และ UN

7. เพื่อให้บรรลุผลเหล่านี้ในอีก 5 ปีข้างหน้า (หากกำหนดยุทธศาสตร์ 5 ปี) รัฐบาลควรเข้าไปดำเนินการอย่างจริงจังและใช้การลงทุนที่เพิ่มขึ้นในขณะที่ยังคงสนับสนุนให้อุตสาหกรรมยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัย ไซเบอร์ทั่วทั้งประเทศโดยการร่วมมือกับหน่วยงานที่รับผิดชอบทั้งหน่วยงานภาครัฐและเอกชนเพื่อให้แน่ใจว่าบุคคลทั่วไปภาคธุรกิจ และองค์กรต่างๆ จะมีพฤติกรรมที่เหมาะสมในการใช้งานอินเทอร์เน็ตได้อย่างปลอดภัย โดยมีมาตรการในการแทรกแซง (เมื่อจำเป็นและอยู่ในขอบเขตของอำนาจที่กระทำได้) เพื่อผลักดันให้มีการพัฒนาในระดับชาติโดยเฉพาะอย่างยิ่งในเรื่องเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญของประเทศ (National Critical Infrastructure)

8. รัฐบาลต้องใช้ขีดความสามารถทั้งของรัฐและของภาคอุตสาหกรรมในการพัฒนาและมีมาตรการป้องกันทางไซเบอร์ที่มีประสิทธิภาพได้อย่างจริงจังเพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศ ซึ่งมาตรการเหล่านี้ ได้แก่ การลดรูปแบบการโจมตีแบบฟิชชิ่งทั่วไปที่พบมากที่สุด โดยกรอง IP address ที่น่าสงสัยและทำการบล็อกกิจกรรมออนไลน์ที่เป็นอันตรายปรับปรุงขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานซึ่งจะช่วยเพิ่มความยืดหยุ่นของประเทศในการรับมือกับภัยคุกคามทางไซเบอร์

9. สร้างศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Center (NCSC)) ขึ้น เพื่อเป็นหน่วยงานที่ดูแลเรื่องความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยมีภารกิจในการให้ความรู้หาช่องโหว่ของไซเบอร์และเป็นผู้นำในเรื่องของความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

10.ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ทางทหารของประเทศจะต้องทำงานอย่างใกล้ชิดกับศูนย์ NCSC เพื่อจะทำให้มั่นใจได้ว่ากองทัพของประเทศมีความยืดหยุ่นและมีการป้องกันทางไซเบอร์อย่างแข็งแกร่งที่จำเป็นต่อการรักษาความปลอดภัยและสามารถปกป้องเครือข่ายและแพลตฟอร์มของกองทัพได้ทำให้กองทัพยังคงสามารถดำเนินการและปฏิบัติการรบได้ถึงแม้จะมีภัยคุกคามทางไซเบอร์เกิดขึ้นซึ่งจะทำให้แน่ใจว่ากองทัพสามารถยับยั้งการโจมตีทางไซเบอร์ที่สำคัญในระดับชาติได้

11.นอกจากนี้ควรมีวิธีในการตอบสนองต่อการโจมตีทางไซเบอร์เช่นเดียวกับที่มีอยู่เพื่อโต้ตอบกับการโจมตีในรูปแบบอื่นๆ โดยใช้ขีดความสามารถที่เหมาะสมที่สุด ซึ่งรวมถึงขีดความสามารถด้านการป้องกันทางไซเบอร์มิให้เกิดขึ้นด้วย

12.ควรมีการใช้อำนาจของรัฐในการลงทุน เพื่อจัดการกับปัญหาการขาดแคลน บุคลากรที่มีทักษะทางด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศโดยเริ่มตั้งแต่ระดับโรงเรียนถึงมหาวิทยาลัยจนถึงวัยทำงาน

13.ทำการจัดตั้งศูนย์นวัตกรรมด้านไซเบอร์ เพื่อขับเคลื่อนการพัฒนาผลิตภัณฑ์ทางไซเบอร์ที่ทันสมัย และส่งเสริมให้เกิดบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ ใหม่ๆ ซึ่งรัฐบาลควรจะจัดสรรเงินทุนจากกองทุนเพื่อการป้องกันและนวัตกรรมด้านไซเบอร์ (Defense and Cyber

Innovation Fund) ที่ควรจัดตั้งขึ้นเพื่อสนับสนุนการสร้างนวัตกรรมในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ แก่ประเทศโดยรวม

แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560 - 2564 (แผนแม่บทไซเบอร์, ออนไลน์, 2562) มีสาระสำคัญครอบคลุมแผนงานหลัก 6 แผนงาน ดังนี้

1. แผนการจัดองค์กรด้านไซเบอร์ ให้ กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ดำเนินการจัดตั้ง หน่วยงานไซเบอร์/ ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์

2. แผนการป้องกันระบบโครงสร้างพื้นฐาน โดย กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพเตรียม จัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของตนขึ้นมาเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่จะมาโจมตีระบบโครงสร้างพื้นฐานด้าน เทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูล และให้จัดตั้งทีมจัดการปัญหาฉุกเฉิน ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านปลอดภัย ไซเบอร์ได้อย่างรวดเร็ว และทันเวลา

3. แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกัน สกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้าง ขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่าง ๆ รวมถึงการจัดให้มีการแข่งขันทักษะการ ปฏิบัติการไซเบอร์ (Cyber Contest)

4. แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโนโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตาม ความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวัน จะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว

5. แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาลเพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain)

6. แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ธุรกิจเอกชน และประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน และนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ที่มีพลังอำนาจที่ยิ่งใหญ่ โดยจัดตั้งศูนย์ไซเบอร์ในระดับกระทรวงกลาโหม โดยสำนักงาน ปลัดกระทรวงกลาโหม กรมเทคโนโลยีสารสนเทศและอวกาศ กระทรวงกลาโหม (ทสอ.กห.) โดยจะเชื่อมโยงกับการตั้งศูนย์ Cyber ของ กองบัญชาการกองทัพไทย และ 3 เหล่าทัพ มี ขอบเขตอำนาจหน้าที่ ในการประสานนโยบายไซเบอร์กับระดับชาติ รวมทั้งรับผิดชอบด้านนโยบาย ยุทธศาสตร์ และปฏิบัติงานด้านไซเบอร์ในระดับยุทธศาสตร์ของกระทรวงกลาโหมในภาพรวม จากการที่กองทัพอากาศจัดทำยุทธศาสตร์กองทัพอากาศ 20 ปี รองรับยุทธศาสตร์ของหน่วยเหนือ เพื่อเป็นแนวทางในการพัฒนากองทัพอากาศ

ให้สอดคล้องกับสภาวะแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลงนั้น จะเห็นได้ว่ากองทัพอากาศให้ความสำคัญงานด้านไซเบอร์เป็นอย่างมาก และได้กำหนดการพัฒนาบุคลากรพร้อมให้จัดหาระบบที่เกี่ยวข้องมารองรับการปฏิบัติงานเพื่อป้องกัน ระบบต่าง ๆ ที่มีใช้งานในกองทัพอากาศให้ปลอดภัยจากภัยคุกคามอย่างเป็นรูปธรรม

บริบทกองทัพอากาศ

ยุทธศาสตร์กองทัพอากาศ (ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2563)

ยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ.2561 - พ.ศ.2580) (ฉบับเผยแพร่) ได้ให้ความสำคัญกับการพัฒนากองทัพอากาศใน ทุกด้านอย่างเป็นระบบ ทั้งนี้ เพื่อให้กองทัพอากาศมีขีดความสามารถที่เพียงพอและเหมาะสมในการ ปฏิบัติภารกิจที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพโดยมีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี (พ.ศ.2561 - พ.ศ.2580) ซึ่งมุ่งเน้นขับเคลื่อนประเทศสู่ความ “มั่นคง มั่งคั่ง และยั่งยืน” ยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม และยุทธศาสตร์ทหารกองทัพไทย ซึ่งยุทธศาสตร์ ทหารกองทัพไทย 20 ปี กำหนดวัตถุประสงค์เพื่อเสริมสร้าง ความพร้อมรบของกองทัพไทยในการ ปฏิบัติภารกิจหลักในการป้องกันประเทศ พิทักษ์รักษาและเทิดทูนสถาบันพระมหากษัตริย์ รวมทั้งต้องสามารถสนับสนุนรัฐบาลในการแก้ไขปัญหาสำคัญของชาติ โดยใช้การปฏิบัติการร่วมเชิงรุก เสริมสร้างกองทัพให้เป็นกำลังอเนกประสงค์ที่มีความหลากหลาย พร้อมเผชิญภัยคุกคามทุกรูปแบบ ทั้งนี้ ยังคงยึดถือแนวคิดทางยุทธศาสตร์ จำนวน 3 แนวคิด ตามยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม 20 ปี โดยกำหนดวัตถุประสงค์เฉพาะทางทหารด้านสงครามไซเบอร์ คือ การปฏิบัติการในสงครามไซเบอร์ (Cyber Warfare) เพื่อให้กองทัพไทย มีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ (Cyber Domain) ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติตลอดจนสามารถบูรณาการและให้การสนับสนุน ความมั่นคงไซเบอร์ (Cyber Security) ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ ซึ่งยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทยได้กำหนดแนวทางการปฏิบัติการทางทหารในมิติไซเบอร์ของ กองทัพไทย ทั้งในการเตรียมกำลังและใช้กำลังโดยแยกเป็น 3 ประเด็นยุทธศาสตร์ ได้แก่

1. ยุทธศาสตร์การป้องกันเชิงรุกสำหรับปฏิบัติการในมิติไซเบอร์ เสริมสร้าง พลังอำนาจทางไซเบอร์ของกองทัพไทย (RTARF Cyber Power) เพื่อการปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้ามทั้งที่เป็นรัฐ (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 และสร้างความตระหนักรู้ทางไซเบอร์ (Cyber Awareness) ที่จะนำไปสู่การตัดสินใจของระดับผู้บังคับบัญชาให้เท่าทันต่อสถานการณ์ต่าง ๆ

2. ยุทธศาสตร์การผนึกกำลังป้องกันประเทศสาหรับปฏิบัติการในมิติไซเบอร์ สร้าง ความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติไซเบอร์ของทุกภาคส่วนภายในประเทศอย่างเป็นระบบ

3. ยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับปฏิบัติการในมิติไซเบอร์ เสริมสร้างความร่วมมือในมิติไซเบอร์กับประเทศเพื่อนบ้าน ประเทศสมาชิกอาเซียนและมิตรประเทศทั้งในระดับภูมิภาคและระดับโลก

จากการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารด้านเครือข่ายและ อินเทอร์เน็ตที่มีการพัฒนาอย่างรวดเร็ว รวมทั้งการเกิดขึ้นของภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบ การจารกรรมข้อมูล และการโจมตีเพื่อทำลายล้างล้วนก่อให้เกิดผลกระทบและความเสียหายใน วงกว้าง หลายประเทศมีการจัดตั้งหน่วยงานรับผิดชอบโดยตรง และกำหนดเป็นมิติหนึ่งในการ ปฏิบัติการด้านความมั่นคงของชาติ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศและยุทธศาสตร์ด้าน สงครามไซเบอร์กองทัพไทย กำหนดให้เหล่าทัพต้องมีขีดความสามารถ ดังนี้ การป้องกันภัยคุกคามทางไซเบอร์ พัฒนาและใช้ประโยชน์จากขีดความสามารถทางไซเบอร์ในการปฏิบัติการทางทหาร ร่วมมือ กับหน่วยงานภายในเพื่อการผนึกกำลังป้องกันประเทศเช่นเดียวกับที่กองทัพอากาศกำหนดให้มิติไซเบอร์ มีบทบาท หน้าที่ และภารกิจด้านความมั่นคงโดยกำหนดให้เป็นมิติไซเบอร์ (Cyber Domain) และพัฒนาขีดความสามารถด้านไซเบอร์ให้มีความพร้อมใน การเผชิญกับภัยคุกคามด้านไซเบอร์และสอดคล้องตามยุทธศาสตร์และนโยบายที่เกี่ยวข้อง นอกจากนี้ การพัฒนาสู่กองทัพอากาศดิจิตอล (DAF) และกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (NCAF) จำเป็นต้องพัฒนาระบบเครือข่าย (Network) ให้มีความแข็งแรงและปลอดภัย

ตารางที่ 3-1 ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain)

ทิศทางการพัฒนามิติไซเบอร์ (Cyber Domain)			
2561-2565	2566-2570	2571-2575	2576-2580
⊕ ทบทวนหลักนิยมและพัฒนาแนวความคิดในการปฏิบัติภารกิจด้านไซเบอร์ของ ทอ. ⊕ กำหนดขอบเขตการปฏิบัติภารกิจด้านไซเบอร์ และกำหนดหน่วยรับผิดชอบ ⊕ กำหนดสมรรถนะหลักและทักษะของกำลังพล/นักรบไซเบอร์ ⊕ จัดตั้งหน่วยงานเพื่อดำเนินงานด้านไซเบอร์ ⊕ ปรับปรุงและพัฒนาโครงสร้างพื้นฐานและสิ่งอำนวยความสะดวกด้านไซเบอร์ ⊕ ริเริ่มการทดสอบด้านไซเบอร์และการฝึกร่วม (Bilateral exercise) ⊕ ริเริ่มจัดตั้งศูนย์ฝึกอบรมด้านไซเบอร์ของ ทอ. ⊕ จัดตั้ง Cyber Protection Team (CPT)	⊕ สรรหากำลังพล/นักรบไซเบอร์ ซึ่งมีสมรรถนะหลักและทักษะตามที่กำหนด ทั้งในเชิงปริมาณและคุณภาพ ⊕ ปรับเปลี่ยน Cyber operation center ไปสู่ Cyber intelligence center ⊕ ริเริ่มและบูรณาการการปฏิบัติงานด้านไซเบอร์เข้ากับการฝึกตามความเหมาะสม ⊕ ริเริ่มการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม ⊕ วิจัยและพัฒนาเกี่ยวกับ Internet of things, big data and AI หรือเทคโนโลยีขั้นสูงอื่น ๆ ที่มีศักยภาพในอนาคต ⊕ ส่งเสริมการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ⊕ ดำรงการปฏิบัติงานของ Cyber Protection Team (CPT) และเพิ่มผู้เชี่ยวชาญอย่างต่อเนื่อง	⊕ สิ่งเสริมการเพิ่มขีดความสามารถของกำลังพล/นักรบไซเบอร์ และ Cyber Protection Team (CPT) ⊕ วิจัยและพัฒนาเกี่ยวกับ Quantum computing และ Space/GPS Hacking prevention ⊕ ริเริ่มการนำ AI มาใช้ในการปฏิบัติการด้านไซเบอร์ ⊕ ดำรงการฝึกปฏิบัติการไซเบอร์ในการฝึกร่วม/ผสม ⊕ ส่งเสริมการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ⊕ พัฒนาและดำเนินการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (Incident response plan) ⊕ ทบทวนและประเมินผลหน่วยงานด้านไซเบอร์ และเสนอแนะแนวทางการพัฒนาหน่วยงาน	⊕ ดำเนินงานด้านไซเบอร์อย่างเต็มรูปแบบ และยกระดับขีดความสามารถตามความจำเป็น ⊕ บรรจุนักรบไซเบอร์ในการปฏิบัติงานด้านการรบ ⊕ เริ่มใช้งาน AI และ Quantum computing ใน ทอ. ⊕ ระบบต่างๆ ใน ทอ.มีความแข็งแกร่ง (Cyber Resilience) ⊕ ดำเนินการใช้งาน Big data และ Blockchain เมื่อเหมาะสม

ที่มา : ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2563

กลยุทธ์พัฒนาขีดความสามารถด้านสงครามไซเบอร์ของกองทัพอากาศ (กลยุทธ์ที่ 2.7)

มีวัตถุประสงค์เพื่อพัฒนาขีดความสามารถด้าน สงครามไซเบอร์ของกองทัพอากาศ โดยพัฒนาโครงสร้างพื้นฐาน บุคลากร และองค์ความรู้ เพื่อป้องกัน ภัยคุกคามทางไซเบอร์ และใช้ประโยชน์จากการปฏิบัติการทางไซเบอร์ในการขยายขีดความสามารถการปฏิบัติการทางทหาร รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุกและแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์ มี 4 ตัวชี้วัดความสำเร็จ ดังนี้

1. จำนวนบุคลากรของกองทัพอากาศที่ผ่านการฝึกอบรมด้านสงครามไซเบอร์และได้รับใบรับรองความสามารถ เพื่อให้มีความรู้ความเข้าใจในการปฏิบัติการด้านสงครามไซเบอร์ทั้งเชิงรับและเชิงรุกและมีความพร้อมรับมือกับภัยคุกคามด้านไซเบอร์ ในรูปแบบต่าง ๆ

2. ระดับความสำเร็จในการพัฒนาขีดความสามารถให้ทำงานร่วมกันเป็นชุด ปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team) ตลอดจนการประยุกต์ใช้ ประโยชน์ด้านไซเบอร์ในการปฏิบัติภารกิจของกองทัพอากาศ และการปฏิบัติการร่วม

3. ระดับความสำเร็จในการพัฒนาระบบป้องกัน ติดตาม เฝ้าระวัง แจ้งเตือน และวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ โดยสามารถตรวจพบและแก้ไขปัญหาและ ภัยคุกคามด้านไซเบอร์ได้อย่างรวดเร็วมีประสิทธิภาพ

4. ระดับความสำเร็จในการแลกเปลี่ยนความรู้และความร่วมมือด้านไซเบอร์กับเหล่าทัพและหน่วยงานภายนอกกองทัพอากาศ ตลอดจนหน่วยงานระดับนานาชาติ

กลยุทธ์ย่อยในการดำเนินการ มีดังนี้

1. พัฒนาหลักนิยมการปฏิบัติการในมิติไซเบอร์ของกองทัพอากาศทั้งเชิงรุกและเชิงรับ รวมทั้งปรับปรุงหลักนิยมของกองทัพอากาศในส่วนอื่น ๆ ที่เกี่ยวข้อง เพื่อใช้เป็นพื้นฐานในการ ปฏิบัติการ

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

3. จัดตั้งหน่วยงานเพื่อดำเนินงานด้านไซเบอร์ทั้งมวล ตลอดจนพัฒนา ระบบรวบรวมข้อมูลด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก (Cyber Intelligence) เพื่อจัดทำบัญชีเป้าหมายทางไซเบอร์ โดยเฉพาะเป้าหมายภายในระบบโครงสร้างพื้นฐานสำคัญของรัฐ ระบบโครงสร้างพื้นฐานสำคัญด้านไซเบอร์ทางทหารและเป้าหมายที่มีความอ่อนไหว หรือมีความสำคัญทางยุทธศาสตร์ของฝ่ายตรงข้าม

4. จัดตั้งศูนย์ฝึกอบรมด้านไซเบอร์ของกองทัพอากาศ รวมทั้งการฝึกจำลองยุทธ์ด้านไซเบอร์ และจัดให้มีการฝึกอย่างต่อเนื่อง เพื่อพัฒนาบุคลากรที่เกี่ยวข้องและนักรบไซเบอร์ (Cyber Warrior) ตลอดจนส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Culture) ให้กับกำลังพลกองทัพอากาศทุกระดับเพื่อให้มีความพร้อมในการรับมือภัยคุกคามด้านไซเบอร์ทั้งในปัจจุบันและอนาคต

5. พัฒนาชุดปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team) เพื่อตรวจสอบความมั่นคงปลอดภัยไซเบอร์ เสนอแนวทางการแก้ไข และพร้อมสนับสนุน การปฏิบัติการไซเบอร์ทางการทหาร

6. วิจัยและพัฒนาเทคโนโลยีด้านด้านไซเบอร์ เช่น Internet of Things, Big Data, Artificial Intelligence, Quantum Computing, Block Chain เพื่อนำมาประยุกต์ใช้ให้เหมาะสมในการสร้างความได้เปรียบในการปฏิบัติการของ กองทัพอากาศ

บริบทของสงครามอิเล็กทรอนิกส์ในกองทัพอากาศ

Electronic Warfare หรือ EW คือ การเข้ามาทำลายระบบคอมพิวเตอร์เพื่อสร้างความเสียหายกับข้อมูลในเครื่องคอมพิวเตอร์ ทำให้คอมพิวเตอร์หยุดทำงานเอง และลบข้อมูลในระบบหน่วยความจำ ซึ่งการโจมตีทางอิเล็กทรอนิกส์มีหลายรูปแบบรวมทั้ง การดักฟังสัญญาณ การก่อกวนและโจมตีทำลายเป้าหมาย ซึ่งในปัจจุบันนั้น สงครามอิเล็กทรอนิกส์นับว่าเป็นอีกสมรภูมิหนึ่งที่มีความสำคัญมากในการรบ ฝ่ายใดที่สามารถครองสมรภูมิสงครามอิเล็กทรอนิกส์ได้นั้นก็แทบจะนับได้ว่าเป็นฝ่ายผู้ชนะเพราะว่าในสงครามยุคปัจจุบันนั้น ระบบอิเล็กทรอนิกส์แทบจะเป็นทุกอย่างในสงคราม

สำหรับประเทศไทย จากประวัติศาสตร์สงครามทางอากาศที่ผ่านมาประเทศที่มีระบบสงครามอิเล็กทรอนิกส์ที่ทันสมัยและมีขีดความสามารถในการปฏิบัติการ จะสามารถชิงความได้เปรียบทั้งทางยุทธศาสตร์ ยุทธการ และยุทธวิธีทางการรบ

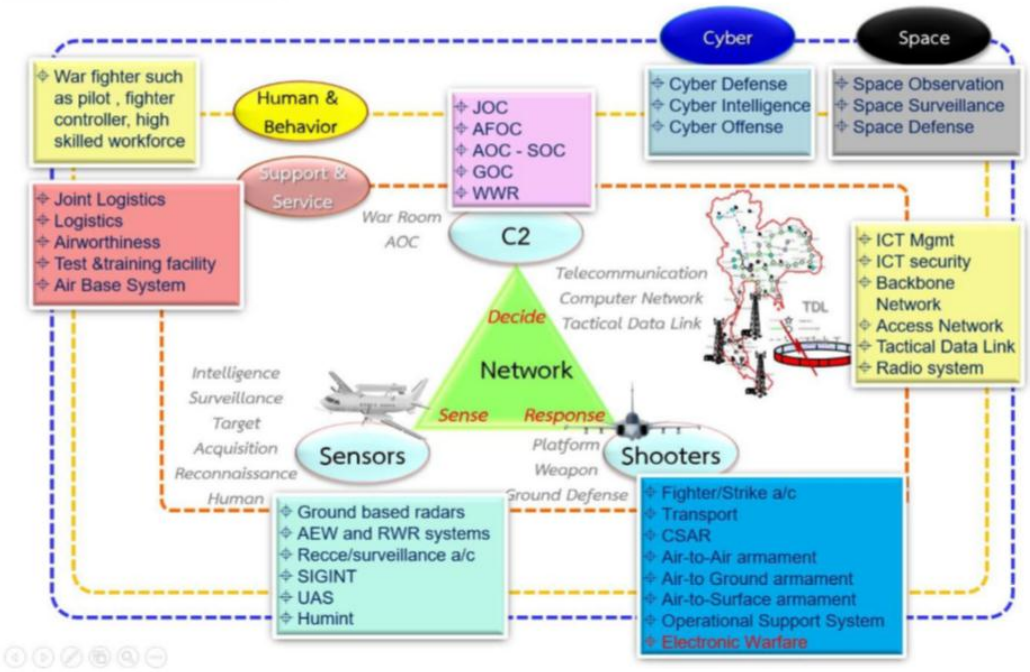
กองทัพอากาศยึดมั่นแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) เนื่องจากเชื่อว่าจะทำให้การปฏิบัติภารกิจของกองทัพอากาศมีประสิทธิภาพสูงสุด ซึ่งเป็นการเพิ่มความรวดเร็วของวงรอบการตัดสินใจ (Observe-Orient-Decide-Act : OODA Loop) โดยการแลกเปลี่ยนข้อมูล ข่าวสาร (Information) และความตระหนักรู้สถานการณ์ (Situation Awareness) ร่วมกันผ่าน ระบบเครือข่าย (Network) ที่มีประสิทธิภาพ ทำให้ผู้บังคับบัญชามีข้อมูลถูกต้อง ครบถ้วน สามารถตัดสินตกลงใจและสั่งการไปยังผู้ปฏิบัติ/หน่วยปฏิบัติ (Shooter) ได้ถูกต้องและทันเวลา นอกจากนี้ ข้อมูลข่าวสารและความตระหนักรู้สถานการณ์ร่วมกันยังช่วยเพิ่มขีดความสามารถให้แก่ผู้ปฏิบัติ/หน่วยปฏิบัติเพิ่มขึ้นเป็นทวีคูณสามารถปฏิบัติภารกิจได้หลากหลาย รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น (ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2563) โดยแบ่งเป็น 3 มิติ ดังนี้

1. มิติทางอากาศ (Air Domain) ประกอบด้วย 1.1 การบัญชาการและควบคุม (Command and Control : C2) 1.2 ระบบตรวจจับ (Sensor) 1.3 ผู้ปฏิบัติ/หน่วยปฏิบัติ (Shooter) 1.4 ระบบเครือข่าย (Network) 1.5 การสนับสนุนและบริการ (Support and Service) และ 1.6 บุคลากรและพฤติกรรมการปฏิบัติงาน (Human & Behavior)

2. มิติไซเบอร์ (Cyber Domain)

3. มิติอวกาศ (Space Domain)

แผนภาพที่ 3-1 การพัฒนาการปฏิบัติงานที่ใช้เครือข่ายเป็นศูนย์กลาง

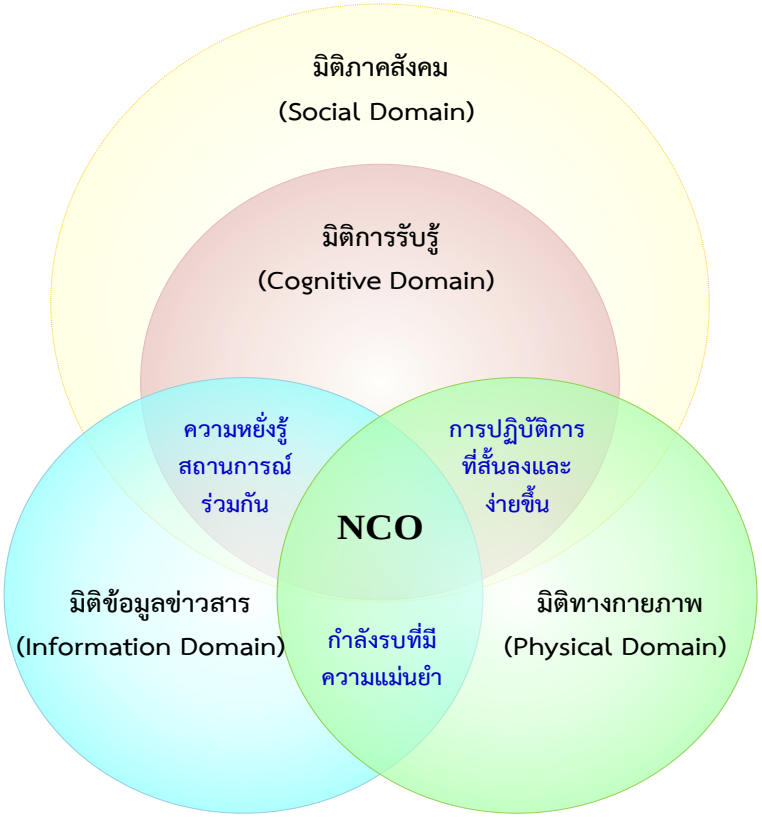


ที่มา : ยุทธศาสตร์กองทัพอากาศ 20 ปี, ออนไลน์, 2563

ทั้งนี้ การพัฒนาขีดความสามารถด้านสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ ถูกระบุไว้ในกลยุทธ์ที่ ๓.๒.๑ การเสริมสร้างขีดความสามารถกองทัพอากาศในส่วนที่เกี่ยวข้องกับ การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางโดยตรง (RTAF NCO Combat Related Function) การพัฒนากองทัพอากาศในส่วนนี้มีเป้าหมายเพื่อพัฒนากองทัพอากาศมุ่งสู่กองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (NCAF) โดยมุ่งเน้นการพัฒนาองค์ประกอบ ในส่วนที่เกี่ยวข้องกับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางโดยตรง (RTAF NCO Combat Related Function) ซึ่งทำหน้าที่ปฏิบัติการในส่วนหน้า (Front Line Operations) รวมทั้งการพัฒนาขีดความสามารถในมิติไซเบอร์ (Cyber Domain) และการ ริเริ่มและวางรากฐานการพัฒนาขีดความสามารถในมิติอวกาศ (Space Domain)

โดยมีการกำหนดกลุ่มเป้าหมายหรือกลุ่มผู้ปฏิบัติสำหรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางโดยตรงตาม “แผนพัฒนาขีดความสามารถการปฏิบัติการที่ใช้เครือข่าย เป็นศูนย์กลางของกองทัพอากาศ” ที่สอดคล้องและเป็นไปในทิศทางเดียวกันกับยุทธศาสตร์ กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) ได้แก่ การพัฒนาบุคลากรที่มีความชำนาญหรือเชี่ยวชาญพิเศษเฉพาะ (Subject Matter Expert : SMEE) ด้าน Electronic Warfare (EW), Tactical Data Link (TDL) , Geographical Data , Air IMINT (Imagery Intelligence) – AIRIX, Software Integration , Cyber Operation และ Space Operation

แผนภาพที่ 3-2 แนวความคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางของกองทัพอากาศ
(Network Centric Operations : NCO)



ที่มา : หลักนิยมกองทัพอากาศ, ออนไลน์, 2563

นอกจากนี้ กองทัพอากาศจะใช้การปฏิบัติการสงครามอิเล็กทรอนิกส์ (Electronic Warfare Operations : EWO) เป็นหนึ่งในการปฏิบัติการหลักในการโจมตีข้าศึกด้วยการใช้การปฏิบัติทางทหารเกี่ยวกับพลังงานแม่เหล็กไฟฟ้า (Electromagnetic) และพลังงานแบบอื่น เพื่อควบคุมแถบความถี่แม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ทั้งยุทธบริเวณของแถบคลื่นแม่เหล็กไฟฟ้า การควบคุมแถบความถี่แม่เหล็กไฟฟ้า ทำให้มีการขยายเครือข่ายจากระบบป้องกันฝ่ายเรา และเพิ่มระบบการต่อต้านฝ่ายตรงข้าม ซึ่งรวมถึงระบบคลื่นวิทยุ สายใยแก้วนำแสง (Optical) และอินฟราเรด การใช้การสงครามอิเล็กทรอนิกส์ (EW) ของกองทัพอากาศ กำหนดกิจสำคัญ ดังนี้

๑. การสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Support : ES) เป็นการใช้สงครามอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับการค้นหา ดักจับ ระบุตัวตน และชี้ตำแหน่งที่ตั้งของแหล่งกำเนิดพลังงานแม่เหล็กไฟฟ้าที่ปล่อยออกมาโดยตั้งใจและไม่ตั้งใจ เพื่อตรวจสอบภัยคุกคามที่เกิดขึ้น

๒. การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection : EP) เป็นการใช้สงครามอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับการป้องกันบุคคล ยุทโธปกรณ์ และระบบอิเล็กทรอนิกส์ต่าง ๆ จากการโจมตีทางอิเล็กทรอนิกส์ของฝ่ายข้าศึก เพื่อให้มีความอยู่รอดสูงในพื้นปฏิบัติการ

๓. การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack : EA) เป็นการใช้สงครามอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับการใช้คลื่นแม่เหล็กไฟฟ้า หรือการควบคุมพลังงาน ในการโจมตีบุคคล ยุทโธปกรณ์ และระบบอิเล็กทรอนิกส์ต่าง ๆ เพื่อทำให้ลดประสิทธิภาพ ไม่สามารถใช้งานอุปกรณ์ได้ หรือทำให้เกิดความเสียหายต่อขีดความสามารถด้านการรบของข้าศึก

ยุคปัจจุบัน ผู้บัญชาการทหารอากาศ ได้มอบนโยบายผู้บัญชาการทหารอากาศ ประจำปี พ.ศ.2563 ให้กำลังพลยึดถือเป็นแนวทางการปฏิบัติ เมื่อ เดือนตุลาคม พ.ศ.2562 สรุปสาระสำคัญที่เกี่ยวข้องกับขีดความสามารถสงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์ ได้ดังนี้

1. การเตรียมกำลังกองทัพอากาศ ในมิติไซเบอร์ (Cyber Domain) ต้องดำเนินการทันทีเนื่องจากเกี่ยวข้องโดยตรงกับความมั่นคงของประเทศและเป็นภารกิจของส่วนราชการกองทัพอากาศ ดังนี้

1.1 นโยบายเฉพาะ ด้านกำลังพล บริหารกำลังพลของกองทัพอากาศ เพื่อรองรับการปฏิบัติในมิติทางไซเบอร์ และมิติทางอวกาศ เพื่อให้มีกำลังพลที่เพียงพอต่อการปฏิบัติงานและพัฒนากำลังพลด้านกฎหมายไซเบอร์

1.2 นโยบายเฉพาะ ด้านกำลังรบ

1.2.1 ข้อ 3.8 พัฒนาระบบบัญชาการและควบคุมให้สามารถรองรับการบัญชาการและควบคุมทั้งมิติทางอากาศ มิติทางไซเบอร์ และมิติทางอวกาศ โดยต้องมีความพร้อมปฏิบัติการตลอดเวลา

1.2.2 ข้อ 3.10 เสริมสร้างขีดความสามารถการปฏิบัติการไซเบอร์ในการควบคุมสั่งการ การปฏิบัติการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ การปฏิบัติการเชิงป้องกันและเชิงป้องปราม และการป้องกันภัยคุกคามทางไซเบอร์ในระบบเครือข่ายเพื่อการยุทธและเครือข่ายสนับสนุน ให้มีความมั่นคงปลอดภัย พร้อมใช้งานทุกพื้นที่ปฏิบัติการ

1.3 นโยบายเฉพาะ ด้านการฝึก ข้อ 4.5 ยกระดับความร่วมมือด้านไซเบอร์ในภูมิภาคอาเซียน และระดับนานาชาติ

1.4 นโยบายเฉพาะ ด้านการศึกษา ข้อ 6.2 โรงเรียนสายวิทยาการที่เกี่ยวข้องทบทวนและปรับปรุงหลักสูตร เพื่อให้ผู้สำเร็จการศึกษามีความพร้อมในมิติทางอากาศ มิติไซเบอร์ และมิติอวกาศ

1.5 นโยบายเฉพาะ ด้านวิทยาการกองทัพอากาศ ข้อ 7.1 เสริมสร้างความรู้ด้านเทคนิคของแต่ละสายวิทยาการ ด้านไซเบอร์ เพื่อให้กำลังพลสามารถปฏิบัติงานได้ตามมาตรฐานสากล และข้อ 7.5 กำหนดมาตรฐานการตรวจด้านจิตเวชให้กับกำลังพลที่ต้องปฏิบัติงานด้านไซเบอร์

2. นโยบายเฉพาะ ด้านกำลังรบ ข้อ 3.3 พัฒนาระบบแจ้งเตือนเรดาร์ภัยคุกคาม (Radar Warning Receiver : RWR) เพื่อให้ผู้ปฏิบัติ/ หน่วยปฏิบัติใช้งานเป็นมาตรฐานเดียวกันในการปฏิบัติการสงครามอิเล็กทรอนิกส์สนับสนุนการปฏิบัติการทางอากาศ

ในยุคปัจจุบัน จากโครงการจัดซื้อเครื่องบิน Gripen 39 C/D เข้าประจำการในกองทัพอากาศ สิ่งที่ประเทศไทยได้รับนอกจากเครื่องบินที่มีสมรรถนะสูง ระบบบัญชาการและควบคุมที่ทันสมัยแล้ว ยังได้รับการรับการถ่ายทอดเทคโนโลยีหลัก (Key Technologies) และการพัฒนาขีดความสามารถของกำลังทางอากาศในด้านสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) การจัดทำฐานข้อมูลทางภูมิศาสตร์ (Geographical Databases: Geo Data) และระบบเชื่อมโยงข้อมูล (Data Link: DL) ในขณะที่ บ. Gripen 39 C/D เป็น บ.ขับไล่ที่มีความทันสมัยในยุค Fighter Generation 4.5 ซึ่งหมายถึง บ.ขับไลในยุคที่ ๔ แต่มีความทันสมัยมากกว่าโดยเฉพาะการมีระบบการตรวจจับที่ดี (Active Electronically Scanned Array: AESA) มีระบบเชื่อมโยงข้อมูลความเร็วสูง (High speed data links) และสามารถใช้อาวุธสมัยใหม่ที่แม่นยำสูง (Latest precision weapons) จึงนับว่าเป็นจุดแข็งของกำลังทางอากาศในยุคปัจจุบัน ที่สามารถสร้างความได้เปรียบทั้งระดับยุทธวิธีถึงระดับยุทธศาสตร์ มีขีดความสามารถในการปฏิบัติภารกิจการสงครามอิเล็กทรอนิกส์ ใน ๓ รูปแบบ คือ ๑) ภารกิจหลัก เช่น การทำลายหรือตัดรอนขีดความสามารถของระบบตรวจจับของข้าศึกด้วยการรบกวน (Jamming) หรือการทำลายด้วยจรวดต่อต้านเรดาห์ (Anti Radiation Missile) การลาดตระเวนทางอิเล็กทรอนิกส์ เพื่อการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ (Electronic Support Measure: ESM) ๒) ภารกิจสนับสนุนหน่วยอื่นเพื่อให้เกิดความปลอดภัยจากอาวุธของฝ่ายตรงข้าม เช่น การบินคุ้มกันทางอิเล็กทรอนิกส์ (Escort Jamming) ๓) การปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อป้องกันตัวเอง (Self-Protection Jamming) ในส่วนของอุปกรณ์ (Equipment) แบ่งเป็น ๒ กลุ่มใหญ่คือ กลุ่มรับข้อมูล ได้แก่ อุปกรณ์ตรวจจับทาง EW (EW picture) อุปกรณ์ตรวจจับอื่น ๆ และระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link) อีกกลุ่มหนึ่งคือ อุปกรณ์ที่วิเคราะห์และใช้ต่อต้านภัยคุกคามต่าง ๆ (Countermeasure Technique) เช่น ชุดประมวลผลกลาง (Mission Central Processor Unit) ชุดควบคุมการปล่อย Chaff/Fair เป็นต้น

หน่วยงานที่รับผิดชอบ สงครามอิเล็กทรอนิกส์ และไซเบอร์ กองทัพอากาศ

การปฏิบัติภารกิจด้านไซเบอร์ของกองทัพอากาศ มีองค์ประกอบหลายส่วน ซึ่งแต่ละส่วนมีความจำเป็นต่อ การปฏิบัติภารกิจอย่างยิ่งยวด 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) การเป็น กองทัพอากาศดิจิทัล (Digital Air Force: DAF) ช่วงที่ 2 (พ.ศ.2555 - 2558) การเป็นกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force: NCAF) และช่วงที่ 3 (พ.ศ.2559 - 2562) ขับเคลื่อนไปสู่การเป็นกองทัพอากาศชั้นนำในภูมิภาคด้วยการปฏิบัติงานแบบใช้เครือข่ายเป็นศูนย์กลางเต็มรูปแบบในการปฏิบัติการรบและการปฏิบัติการที่ไม่ใช่การรบ เพื่อสร้างความพร้อมในการรับมือกับภัยคุกคามทุกรูปแบบได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเอง โดยจุดเน้นสำคัญของประเด็นยุทธศาสตร์ คือ ยุทธศาสตร์ที่ว่าด้วยการเสริมสร้างสมรรถนะ

และความพร้อมในการป้องกันประเทศ ภายใต้การเสริมสร้างนภานุภาพตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) เพื่อให้การดำเนินการภายใต้ NCO เป็นไปอย่างมีประสิทธิภาพ จำเป็นต้องมีและดำรงไว้ซึ่งขีดความสามารถในการปฏิบัติงานที่สอดประสานกัน ระหว่างองค์ประกอบทั้ง 6 ส่วน เพื่อการตัดสินตกลงใจที่ถูกต้องและรวดเร็วของผู้บังคับบัญชาในระบบ บัญชาการและควบคุม ก่อให้เกิดเป็นความได้เปรียบด้านอำนาจกำลังรบ ทั้งนี้ องค์ประกอบที่สำคัญ ในการดำรงไว้ซึ่งขีดความสามารถในการติดต่อสื่อสารอย่างเสรี ได้แก่ ระบบเครือข่าย ซึ่งจำเป็นต้อง มีการรักษาความปลอดภัยจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามในรูปของสงครามไซเบอร์ (Cyber warfare) ซึ่งทวีจำนวนและมีระดับความรุนแรงเพิ่มมากขึ้นทุกขณะอย่างเข้มงวดจริงจัง ทุกส่วนภายใต้ความร่วมมือจากบุคลากรทุกระดับ เนื่องจาก หากระบบเครือข่ายไม่สามารถตอบสนอง ต่อความต้องการใช้งานได้ในเวลาที่ต้องการ ระบบบัญชาการและควบคุมก็จะไม่สามารถปฏิบัติงานได้ อย่างมีประสิทธิภาพ ก่อให้เกิดความไม่สัมฤทธิ์ผลในการปฏิบัติในองค์รวม ดังนั้น จึงจำเป็นที่จะต้องหา แนวทางปฏิบัติเพื่อป้องกันภัยอันเกิดจากการทำสงครามไซเบอร์ จากการที่เทคโนโลยีสารสนเทศพัฒนาขึ้นอย่างรวดเร็ว ในปี 52 กองทัพอากาศ ได้จัดตั้ง กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) เพื่อรับผิดชอบงานดังกล่าว มีหัวหน้าหน่วยในอัตรา พลอากาศตรี ซึ่งมีหน่วยขึ้นตรง คือ กองนโยบายและแผน, กองเทคโนโลยีสารสนเทศ, กองสื่อสารอิเล็กทรอนิกส์, กองสารสนเทศและการสื่อสารทหารอากาศ ต่อมาในปี 57 การดำเนินการด้านไซเบอร์มีความรุนแรงมากขึ้น จึงมีการปรับโครงสร้างและหน้าที่รับผิดชอบของหน่วย ทสส.ทอ. ให้มีความรับผิดชอบมากขึ้น และให้หัวหน้าหน่วยเป็นอัตรา พลอากาศโท โดยการจัดโครงสร้างกองทัพอากาศ ตามพระราชกฤษฎีกาแบ่งส่วนราชการและกำหนดหน้าที่ส่วนราชการกองทัพอากาศ พ.ศ.2557 ตามแผนภาพที่ 3-3 ดังนี้

แผนภาพที่ 3-3 โครงสร้างกองทัพอากาศ

ที่มา : กองทัพอากาศ, ออนไลน์, 2563

ภายใต้โครงสร้างกองทัพอากาศ กำหนดให้กรมเทคโนโลยีสารสนเทศและการสื่อสาร ทหารอากาศเป็นหน่วยงานฝ่ายเสนาธิการ รับผิดชอบเกี่ยวกับงานเชิงนโยบายด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการปฏิบัติการ ไซเบอร์และการปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ มี กองสงครามไซเบอร์ เป็น หน่วยงานรับผิดชอบด้านสงครามไซเบอร์ โดยมีหน่วยงานที่เกี่ยวข้อง คือ กรมสื่อสารอิเล็กทรอนิกส์ ทหารอากาศ (สอ.ทอ.) เป็นหน่วยงานสนับสนุนและซ่อมบำรุงที่รับผิดชอบเกี่ยวกับงานด้านระบบ คอมพิวเตอร์ ระบบเครือข่าย ระบบโทรคมนาคม และการติดต่อสื่อสารเชิงปฏิบัติ มีศูนย์คอมพิวเตอร์ และกองสื่อสารโทรคมนาคม เป็นหน่วยงานรับผิดชอบ รวมถึงมีหน่วยขึ้นตรงของกองทัพอากาศ ที่จะต้องรับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีใช้งานด้วย

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) มีหน้าที่พิจารณาเสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับ การพัฒนา และดำเนินการด้านระบบบัญชาการและควบคุม ระบบเครือข่าย เทคโนโลยีสารสนเทศและ การสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ ปฏิบัติการสงครามอิเล็กทรอนิกส์ และปฏิบัติการ สงครามไซเบอร์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตราภิจการด้านสารสนเทศ สงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ การจัดหน่วย ประกอบด้วย ส่วนบังคับบัญชา แผนกธุรการ สำนักนโยบายและแผน และสำนักระบบบัญชาการและควบคุม สำนักนโยบายและแผน ประกอบด้วย กองนโยบายและแผน กองสื่อสาร อิเล็กทรอนิกส์ และกองเทคโนโลยีสารสนเทศ สำนักระบบบัญชาการและควบคุม ประกอบด้วย กองระบบบัญชาการและควบคุม กองสงครามอิเล็กทรอนิกส์ และกองสงครามไซเบอร์ ประกอบด้วย แผนกสงครามไซเบอร์ แผนกกรรมวิธีข้อมูลสงครามไซเบอร์ แผนกรักษาความปลอดภัยระบบสารสนเทศ แผนกปฏิบัติการสงครามไซเบอร์ และแผนกประเมินผลการสงครามไซเบอร์ ปัจจุบันกองสงครามไซเบอร์ ได้รับอัตราอนุมัติกำลังพล จำนวน 59 อัตรา บรรจุจริง จำนวน 25 คน มีขอบเขตความรับผิดชอบที่สำคัญ คือ การพิจารณาเสนอนโยบาย งานฝ่ายเสนาธิการ ด้านเทคโนโลยีสารสนเทศและการสื่อสารอิเล็กทรอนิกส์ ในขอบเขตเกี่ยวกับ ระบบบัญชาการและ ควบคุม ระบบเครือข่าย คลื่นความถี่ให้ครอบคลุมการปฏิบัติภารกิจของกองทัพอากาศทั้งภายในและ ภายนอกประเทศ เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ การสงครามอิเล็กทรอนิกส์และการสงครามไซเบอร์ บริหารจัดการในฐานะหัวหน้าสายวิทยาการ สารสนเทศและสงครามอิเล็กทรอนิกส์ เกี่ยวกับ การจัดการความรู้ การบริหารการฝึกและศึกษา การบริหารกำลังพลจำพวกทหารสารสนเทศและสงครามอิเล็กทรอนิกส์ ดังแสดงในแผนภาพที่ 3 - 4

แผนภาพที่ 3-4 การจัดหน่วยกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

ที่มา : กองทัพอากาศ, ออนไลน์, 2563

ความพร้อมของกองทัพอากาศ

จากข้อมูลและสารสนเทศที่ได้รับจากการศึกษา ขีดความสามารถด้านสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์ ผู้วิจัยได้ประเมินความพร้อมของกองทัพอากาศในการทวีกำลังของขีดความสามารถทั้งสองด้าน ตามแนวคิด 7S ของ McKinsey (7S McKinsey Framework) สรุปได้ดังนี้

1. ด้านบุคลากร (Staff) กองทัพอากาศมีบุคลากรด้านไซเบอร์ และสงครามอิเล็กทรอนิกส์เพียงพอ เนื่องจากได้รับการผลักดัน และสนับสนุนจากผู้บังคับบัญชาระดับสูงอย่างต่อเนื่องในการบรรจุกำลังพลตามกรอบอัตราที่กองทัพอากาศมีในปัจจุบัน

2. ด้านทักษะความเชี่ยวชาญของบุคลากร (Skill) จากยุทธศาสตร์กองทัพอากาศและนโยบายผู้บัญชาการทหารอากาศ ทำให้เชื่อได้ว่า บุคลากรด้านไซเบอร์ และสงครามอิเล็กทรอนิกส์ได้รับการพัฒนาความรู้และทักษะความเชี่ยวชาญอย่างต่อเนื่องตามเกณฑ์มาตรฐานสากล

3. ด้านรูปแบบ (Style) พิจารณาจากนโยบายผู้บัญชาการทหารอากาศและการแสดงท่าทีในการปกครองบังคับบัญชา ชี้ให้เห็นว่ากองทัพอากาศมีผู้บังคับบัญชาระดับสูงที่ส่งเสริมการดำเนินการด้านไซเบอร์ และสงครามอิเล็กทรอนิกส์เป็นอย่างดี

4. ด้านค่านิยมร่วม (Share Value) กองทัพอากาศมีหลักนิยม “รวมการควบคุม แยกการปฏิบัติ” ซึ่งกำลังพลกองทัพอากาศส่วนใหญ่มีความเข้าใจเป็นอย่างดี ยึดถือปฏิบัติ และมีการย้ำเตือนผ่านหลักสูตรการศึกษาทหารอาชีพ PME ในทุกระดับชั้น นอกจากนี้ ยังมีค่านิยมหลักของกำลังพลกองทัพอากาศ ได้แก่ ความเป็นทหารอากาศ (Airmanship) ความซื่อสัตย์ จงรักภักดี (Integrity and Allegiance) และความรับผิดชอบ (Responsibility) หรือ AIR ซึ่งส่งผลให้ภารกิจมีโอกาสประสบความสำเร็จมากขึ้น

5. ด้านโครงสร้าง (Structure) มีการจัดองค์กรที่เป็นระบบ มีหน่วยรับผิดชอบบังคับบัญชาเรียกว่า หน่วยขึ้นตรงกองทัพอากาศ และแบ่งมอบให้สายวิทยาการ ซึ่งจะเป็นหลักในการบริหารกำลังพล รวมถึงการพัฒนากำลังพล โดยมอบให้หน่วยฝ่ายเสนาธิการ มีหน้าที่ในการเสนอแนะผู้บังคับบัญชา ซึ่งมีการแบ่งมอบอำนาจหน้าที่ชัดเจน

6. ด้านระบบ (System) ภายใต้หลักนิยมกองทัพอากาศ นับว่า กองทัพอากาศมีกระบวนการบริหารจัดการด้านไซเบอร์ และสงครามอิเล็กทรอนิกส์ได้ดีพอควร จะเห็นได้ว่าด้านการปฏิบัติการฯ มีความทับซ้อนกับกรมยุทธการทหารอากาศซึ่งไม่ใช่ผู้รับผิดชอบหลัก ส่วนระบบการบริหารกำลังพลจะมีความทับซ้อนกับกรมกำลังพลทหารอากาศ เป็นต้น ทั้งนี้ ระบบเช่นนี้เป็นระบบเดียวกันกับระบบที่ใช้ในองค์กรขนาดใหญ่ทั่วไป

7. ด้านยุทธศาสตร์ นโยบาย (Strategy) กองทัพอากาศมีหลักนิยม ยุทธศาสตร์ และนโยบายผู้บัญชาการทหารอากาศที่ชัดเจน ต่อการบูรณาการขีดความสามารถของไซเบอร์ และสงครามอิเล็กทรอนิกส์

สรุป

สงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์ มีองค์ประกอบที่เป็นธรรมชาติของสงครามและการใช้ประโยชน์เพื่อหวังผลที่เหนือกว่า มีความแตกต่างกันมากทั้ง องค์ประกอบ เครื่องมือ และประวัติความเป็นมาในอดีต อย่างไรก็ตาม แม้ว่าความสามารถหรือธรรมชาติของสงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์จะมีความแตกต่างกัน แต่แนวคิด ตลอดจนระดับยุทธวิธีที่ใช้ในการรบ มีความเหมือนในบางประเด็น เช่น แนวทางเชิงป้องกัน กับแนวทางเชิงตั้งรับ รวมทั้งระดับยุทธวิธีที่มีความแตกต่างกันในอีกหลายประเด็น

ปัจจุบัน การดำเนินการด้าน สงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์ ในองค์กรส่วนใหญ่ทั้งในและต่างประเทศ รวมทั้งการดำเนินการและแบ่งมอบหน้าที่รับผิดชอบ หรือการกำหนดเป็นภารกิจของหน่วยงานในสังกัดกองทัพอากาศ สงครามไซเบอร์ เป็นความรับผิดชอบของกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ ส่วนสงครามอิเล็กทรอนิกส์เป็นความรับผิดชอบของกรมสื่อสารอิเล็คทรอนิกส์ทหารอากาศ ที่มีหัวหน้าหน่วยรับผิดชอบภารกิจแยกจากกันโดยเด็ดขาด แต่ในระดับยุทธศาสตร์นั้น ย่อมปฏิเสธไม่ได้ว่าภารกิจของสงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์ มีเป้าหมายเดียวกัน ดังนั้น หากสามารถศึกษาโอกาสในการทวีกำลังของสงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์เพื่อนำมาใช้ในกองทัพอากาศได้จะมีประโยชน์อย่างยิ่ง

บทที่ 4
การบูรณาการ การทวีกำลังด้านความมั่นคงปลอดภัยไซเบอร์

การทวีกำลัง จากคุณสมบัติของสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์ เพื่อให้ได้ชัยชนะในการรบตามสภาวะแวดล้อมของโลกในยุคปัจจุบัน ใช้การวิเคราะห์เปรียบเทียบจากข้อมูลในปัจจุบัน และแนวโน้มในอนาคตเพื่อให้ผลการบูรณาการการทวีกำลังด้านความมั่นคงปลอดภัยด้านไซเบอร์สูงสุด และปกปิดช่องโหว่ให้ได้มากที่สุด

แนวทางการดำเนินงาน ขีดความสามารถ และขีดจำกัดของมิติไซเบอร์กองทัพอากาศ

กองทัพอากาศได้กำหนดวิสัยทัศน์องค์กรในการที่จะเป็น“กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ในปี พ.ศ.2562 ด้วยการปฏิบัติงานแบบใช้เครือข่ายเป็นศูนย์กลางเต็มรูปแบบ ในการปฏิบัติการรบและการปฏิบัติการที่ไม่ใช่การรบ เพื่อสร้างรับมือกับภัยคุกคามทุกรูปแบบได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเอง จุดเน้นสำคัญของประเด็นยุทธศาสตร์คือยุทธศาสตร์ที่ว่าด้วยการเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศ ภายใต้การเสริมสร้างนภานุภาพตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) ทั้งนี้ องค์ประกอบในการดำรงไว้ซึ่งขีดความสามารถในการติดต่อสื่อสารอย่างเสรี ได้แก่ ระบบเครือข่าย ซึ่งจำเป็นต้องมีการรักษาความปลอดภัยจากภัยคุกคามทางไซเบอร์โดยเฉพาะภัยคุกคามในรูปของสงครามไซเบอร์ (Cyberwarfare) ซึ่งทวีจำนวนและมีระดับความรุนแรงเพิ่มมากขึ้นทุกขณะ เนื่องจากหากระบบเครือข่ายไม่สามารถตอบสนองต่อความต้องการใช้งานได้ในเวลาที่ต้องการ ระบบบัญชาการและควบคุมก็จะไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ก่อให้เกิดความไม่สัมฤทธิ์ผลในการปฏิบัติในองค์รวม

แนวทางดำเนินงานที่เกี่ยวกับการปฏิบัติการไซเบอร์กองทัพอากาศ

การปฏิบัติการไซเบอร์ของกองทัพอากาศ (Cyber Operations) เป็นการปฏิบัติการภายใต้การบัญชาการและการควบคุมของกองทัพอากาศ เพื่อให้เกิดการทวีกำลังกองทัพอากาศ (Force Multiplier) อย่างเป็นรูปธรรม ตลอดจนการดำรงความพร้อมใช้งานของระบบและข้อมูล/สารสนเทศ (Availability) โดยปฏิบัติการไซเบอร์ของกองทัพอากาศประกอบด้วย ปฏิบัติการหลักทางไซเบอร์ และปฏิบัติการสนับสนุนทางไซเบอร์ ดังนี้

1. การปฏิบัติการหลักทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถทางไซเบอร์ทั้งมวล เพื่อให้บรรลุวัตถุประสงค์ใน/ผ่านมิติไซเบอร์ กำหนดกิจเฉพาะสำคัญ ดังนี้

1.1 การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) เป็นปฏิบัติการเพื่อการป้องกันทางไซเบอร์ มีขั้นตอนการปฏิบัติตามวงรอบการป้องกันทางไซเบอร์ (Defense Cycle) จำนวน 4 ขั้นตอน ดังนี้

1.1.1 การป้องกัน (Protect) หมายถึง การสำรวจสินทรัพย์ทาสารสนเทศ (Information Asset Identification) การตรวจสอบและแก้ไขจุดอ่อน/ช่องโหว่ทางสารสนเทศ (Vulnerability Identification) ในระบบเครือข่ายสารสนเทศของกองทัพอากาศ พร้อมทั้งการเฝ้าระวังและป้องกันไม่ให้เกิดความเสียหายขึ้นกับระบบสารสนเทศที่ใช้งานในส่วนที่รับผิดชอบ

1.1.2 การตรวจจับ (Detect) หมายถึง การเฝ้าระวังการถูกโจมตีหรือการถูกคุกคามทางไซเบอร์ ด้วยการสังเกตสิ่งผิดปกติใด ๆ ที่เกิดขึ้นในการใช้งานระบบสารสนเทศหรือการใช้ซอฟต์แวร์ตลอดจนระบบตรวจจับอื่น ๆ ที่ช่วยในการตรวจจับสิ่งผิดปกติขณะที่ใช้งานและไม่ได้ใช้งานระบบ พร้อมทั้งรายงานเหตุการณ์ความผิดปกติที่ตรวจพบให้กับผู้รับผิดชอบที่เกี่ยวข้อง

1.1.3 การตอบสนอง (React) หมายถึง การปฏิบัติเพื่อแก้ไขปัญหาและระงับเหตุการณ์การล่วงละเมิดการรักษาความปลอดภัยทางไซเบอร์ที่เกิดขึ้นโดยทันทีตามมาตรการปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ขยายผลกระทบต่อไปยังระบบสารสนเทศอื่นที่เกี่ยวข้อง

1.1.4 การฟื้นฟู (Recover) หมายถึง การปฏิบัติเพื่อฟื้นฟูระบบสารสนเทศที่ได้รับผลกระทบทั้งหมด ให้กลับคืนสู่สภาพปกติที่พร้อมใช้งานโดยเร็วที่สุด พร้อมทำการปรับปรุงกระบวนการป้องกันให้มีประสิทธิภาพในการรักษาความปลอดภัยมากยิ่งขึ้น

1.2 การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations : OCO) เป็นปฏิบัติการเพื่อการโจมตีทางไซเบอร์ มีขั้นตอนการปฏิบัติตามวงรอบการโจมตีทางไซเบอร์ (Attack Cycle) จำนวน 5 ขั้นตอน ดังนี้

1.2.1 การรวบรวมข้อมูลเป้าหมาย (Information Gathering) หมายถึง การรวบรวมข้อมูลเป้าหมายเกี่ยวกับโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์และเครื่องมือที่ใช้ วิธีการใช้งาน และข้อมูลของบุคลากร ที่เป็นประโยชน์ในการโจมตี โดยทำการสืบค้นข้อมูลจากกระบวนการทางเทคนิคทุกวิธีที่สามารถปฏิบัติได้ รวมถึงการใช้วิธีวิศวกรรมสังคม (Social Engineering) ด้วย

1.2.2 การตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification) หมายถึง การตรวจสอบหาช่องโหว่หรือการวิเคราะห์ช่องโหว่ของระบบเครือข่ายสารสนเทศของฝ่ายตรงข้าม

1.2.3 การปฏิบัติการโจมตี (Attack) หมายถึง การใช้อาวุธทางไซเบอร์ (Cyber Weapons) ทุกรูปแบบในการเข้าโจมตีระบบเป้าหมาย โดยแสวงประโยชน์จากช่องโหว่ทางไซเบอร์เพื่อเจาะระบบ (Exploitation/Attack) ให้เกิดผลตามที่คาดหวัง ทั้งนี้ปฏิบัติการโจมตียังสามารถปฏิบัติเพื่อให้ได้มาซึ่งข้อมูลข่าวกรองที่ต้องการจากระบบเป้าหมายด้วย

1.2.4 การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) หมายถึง การเปิดช่องโหว่ทิ้งไว้ในระบบเป้าหมาย เพื่อใช้เป็นช่องทางสำหรับการเข้าปฏิบัติการครั้งต่อไป ด้วยวิธีการฝังทางลับ (Backdoor) ไว้ในระบบที่เป็นเป้าหมาย

1.2.5 การลบร่องรอยการโจมตี (Covering Tracks) หมายถึง การลบร่องรอยของการโจมตี หรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบ เพื่อไม่ให้ฝ่ายตรงข้ามสามารถสืบย้อนกลับมาถึงผู้โจมตีได้

1.3. การปฏิบัติการข่าวกรองทางไซเบอร์ (Cyber Intelligence : CI) และการปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ (Cyber Counterintelligence : CCI) ดังนี้

1.3.1 การปฏิบัติการข่าวกรองทางไซเบอร์ (CI) เช่น การรวบรวมข้อมูลข่าวกรองจากแหล่งเปิด (Open-Source Intelligence : OSINT) จากข่าวกรองทางบุคคล (Human Intelligence : HUMINT) จากข่าวกรองทางสัญญาณ (Signal Intelligence : SIGINT) จากข่าวกรองทางภาพ (Image Intelligence : IMINT) และจากข่าวกรองทางภูมิสารสนเทศเชิงพื้นที่ (Geospatial Intelligence : GEOINT) เป็นต้น

1.3.2 การปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ (CCI) เป็นการปฏิบัติการเพื่อป้องกัน ระงับยับยั้ง และลดทอนประสิทธิภาพ การปฏิบัติการข่าวกรองทางไซเบอร์ (CI) ของฝ่ายตรงข้ามที่กระทำต่อฝ่ายเรา

2. การปฏิบัติการสนับสนุนทางไซเบอร์ เป็นการปฏิบัติการที่ใช้ขีดความสามารถด้านไซเบอร์ในการสนับสนุนภารกิจอื่น ๆ เพื่อเอื้ออำนวยให้ภารกิจนั้นสามารถดำเนินการได้อย่างมีประสิทธิภาพ กำหนดกิจเฉพาะสำคัญ ดังนี้

2.1 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support : MIS) เป็นการปฏิบัติการข่าวกรองทางไซเบอร์ (CI) และการปฏิบัติการต่อต้านข่าวกรองทางไซเบอร์ (CCI) ด้วยอุปกรณ์/วิธีทางไซเบอร์ วิธีวิศวกรรมสังคม (Social Engineering) และวิธีอื่น ๆ

2.2 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support : IO Support) เป็นการปฏิบัติการไซเบอร์เชิงป้องกัน (DCO) การปฏิบัติการไซเบอร์เชิงป้องปราม (OCO) และการปฏิบัติการข่าวกรองทางไซเบอร์ (CI)/การปฏิบัติการต่อต้านการข่าวกรองทางไซเบอร์ (CCI) เพื่อสนับสนุนการดำรงขีดความสามารถในการปฏิบัติการข่าวสาร (Information Operations : IO) ในการสร้างสภาวะที่ได้เปรียบเชิงข่าวสารต่อฝ่ายตรงข้าม เช่น การสนับสนุนการปฏิบัติการลวงทางทหาร (Military Deception : MILDEC) การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security : OPSEC) การประกันข่าวสาร (Information Assurance : IA) และการต่อต้านข่าวกรอง (Counter Intelligence) เป็นต้น

3. วงรอบการปฏิบัติด้านไซเบอร์ จากหลักการทั่วไปด้านไซเบอร์วงรอบการปฏิบัติทางไซเบอร์ แบ่งออกเป็น วงรอบการป้องกันทางไซเบอร์ และวงรอบการโจมตีทางไซเบอร์ ดังนี้

3.1 วงรอบการป้องกันทางไซเบอร์ แบ่งการปฏิบัติเป็น 4 ขั้นตอน ดังนี้ การป้องกัน คือ การระวังป้องกันไม่ให้เกิดความเสียหายขึ้นกับระบบสารสนเทศที่ใช้งานการตรวจจับ คือ การเฝ้าระวังการถูกโจมตีหรือการถูกคุกคามทางไซเบอร์ด้วยการสังเกต การใช้ซอฟต์แวร์

ตลอดจน ระบบตรวจจับอื่น ๆ ช่วยในการตรวจจับสิ่งผิดปกติที่เกิดขึ้นในการใช้งานระบบสารสนเทศ การตอบสนอง (React) คือ การปฏิบัติเพื่อแก้ไขปัญหาและระงับเหตุการณ์การล่วงละเมิดการรักษาความปลอดภัยทางไซเบอร์ที่เกิดขึ้นโดยทันทีและการฟื้นฟู (Recover) คือ การปฏิบัติเพื่อฟื้นฟูระบบ สารสนเทศที่ได้รับผลกระทบทั้งหมด ให้กลับคืนสู่สภาพปกติที่พร้อมใช้งานโดยเร็วที่สุด เพื่อปรับปรุงกระบวนการป้องกันให้มีประสิทธิผลในการรักษาความปลอดภัยยิ่งขึ้น

การปฏิบัติตามวงรอบดังกล่าว ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศได้ยึดถือตามแนวทางนี้มาตลอด โดยมีระบบอุปกรณ์ โปรแกรมและบุคลากรในการปฏิบัติงานเฝ้าตรวจ หากมีการพบไวรัสและมัลแวร์จะดำเนินการป้องกันไม่ให้เข้ามาในระบบทันท่วงที หากมีการโจมตีระบบแล้วมีผลกระทบจะมีแผนงานในการดำเนินการฟื้นฟูระบบตามขั้นตอนในปัจจุบัน สามารถป้องกันระบบได้ในระดับหนึ่ง

กรณีบุคลากรภายในกองทัพมีการดำเนินการนำอุปกรณ์มาต่อเชื่อมระบบคอมพิวเตอร์ภายในหน่วย โดยไม่มีการตรวจสอบก่อนใช้งานรวมถึงคอมพิวเตอร์ที่ได้รับการเชื่อมต่อ ไม่มีโปรแกรมป้องกันแต่ไม่ทันสมัยอาจทำให้ระบบติดไวรัสและมัลแวร์ได้ ซึ่งระบบป้องกันที่มีอยู่อาจตรวจพบได้ช้าและอาจจะไม่ทันต่อเหตุการณ์ โดยบุคลากรของกองทัพอากาศต้องดำเนินการตาม ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 และปฏิบัติตามแนวนโยบายและการปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กองทัพอากาศในทุกกรณีรวมถึงในระบบสารสนเทศที่สำคัญทางด้านยุทธการ ต้องดำเนินการให้เป็น ระบบปิดโดยไม่ให้เชื่อมต่อกับระบบอินเทอร์เน็ตภายนอกได้

3.2 วงรอบการโจมตีทางไซเบอร์ วงรอบการโจมตีทางไซเบอร์ แบ่งการปฏิบัติออกเป็น 5 ขั้นตอน ดังนี้ การรวบรวมข้อมูลเป้าหมาย คือ การรวบรวมข้อมูลเป้าหมายด้านโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์และเครื่องมือที่ใช้งาน และข้อมูลต่างวิธีการ ๆ ของบุคลากรที่อาจเป็นประโยชน์ในการโจมตีตรวจสอบหาช่องโหว่ของระบบคือ การตรวจสอบหา ช่องโหว่หรือการวิเคราะห์ช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์เพื่อการโจมตีจากข้อมูลเป้าหมาย การปฏิบัติการโจมตี คือ การใช้อาวุธทางด้านไซเบอร์ทุกรูปแบบในการเข้าโจมตีระบบเป้าหมายเพื่อให้เกิดผลตามที่คาดหวัง การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป คือ การเปิดช่องทิ้งไว้ในระบบที่เข้าโจมตี เพื่อใช้เป็นช่องทางสำหรับการเข้าปฏิบัติการครั้งต่อไป การลบ โจมตี คือ การลบร่องรอยของการโจมตีหรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบ เพื่อไม่ให้สามารถสืบย้อนกลับมาถึงผู้โจมตีได้ ในการโจมตีทางไซเบอร์นี้ยังไม่มีกฎหมายรองรับ จึงไม่มีการดำเนินการอย่างเป็นรูปธรรมในกองทัพอากาศ แต่มีการฝึกบุคลากรของกองทัพอากาศ โดยการจัดการแข่งขัน Cyber Operations Contest อย่างต่อเนื่องทุกปี

เมื่อวิเคราะห์จากข้อมูลแล้ว การดำเนินการของกองทัพอากาศเป็นไปตามวงรอบการปฏิบัติ เมื่อวิเคราะห์ในภาพรวมทั้งด้านเชิงป้องกันและการโจมตี (เชิงป้องปราม) พบว่าบุคลากรยังขาดทักษะการปฏิบัติงาน ด้านการโจมตี (เชิงป้องปราม)

4. ปัจจัยที่ส่งผลต่อการปฏิบัติการไซเบอร์

4.1 ปัจจัยด้านกระบวนการ นโยบาย/แผน และการปฏิบัติที่เกี่ยวข้องการปฏิบัติการไซเบอร์ ต้องมีการตั้งนโยบายและวางแผนการปฏิบัติต่าง ๆ พบว่า

4.1.1 กองทัพอากาศจัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศกองทัพอากาศ พ.ศ.2552 ซึ่งครอบคลุมการปฏิบัติตามกฎหมายรัฐธรรมนูญในปัจจุบัน

4.1.2 โครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศและแผนแม่บทด้านสงครามไซเบอร์ของกองทัพอากาศ สามารถใช้เป็นแนวทางในการพัฒนาระบบการปฏิบัติงานด้านสงครามไซเบอร์ของ ทอ. ซึ่งมีการกำหนดเป้าหมายในการดำเนินการด้านบุคลากร ด้านกระบวนการบริหารจัดการ ด้านเทคโนโลยี และด้านงบประมาณ อย่างชัดเจน สามารถนำมาใช้เป็นแนวทางการปฏิบัติงานเพิ่มเติมได้

4.1.3 การจัดการแข่งขัน Cyber Operations Contest เป็นช่องทางที่จะสรรหาบุคลากรเข้ามาปฏิบัติงานได้ในอนาคต และต้องกำหนดให้มีทีมศึกษาถึงยุทธวิธีที่ผู้เข้าแข่งขันเพื่อนำมาพัฒนาระบบป้องกัน รักษาความปลอดภัยไซเบอร์กองทัพอากาศ

4.2 ปัจจัยด้านบุคลากร ในการปฏิบัติการไซเบอร์บุคลากรถือว่าเป็นปัจจัยที่สำคัญอย่างยิ่ง ดังนั้น ความสามารถในการปฏิบัติงานทั้งการปฏิบัติการไซเบอร์เชิงรับ ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว รวมทั้งสามารถกู้คืนระบบที่เสียหายกลับมาปฏิบัติงานได้โดยไม่กระทบต่อกระบวนการทำงานอื่น ๆ ส่วนการปฏิบัติการไซเบอร์เชิงป้องปราม ต้องอาศัยบุคลากรที่มีความรู้ความสามารถในการค้นช่องโหว่ของระบบ หาจุดอ่อนของเป้าหมาย ซึ่งกองทัพอากาศมีการดำเนินการ ดังนี้

4.2.1 ดำเนินการด้านการฝึก ศึกษาและอบรมบุคลากรด้านไซเบอร์

4.2.1.1 หลักสูตรพื้นฐานรองรับผู้ปฏิบัติงานและผู้บริหารกองทัพอากาศได้จัดทำ หลักสูตรสงครามไซเบอร์ให้กับโรงเรียนจ่าอากาศ กรมยุทธศึกษาทหารอากาศ หลักสูตรสำหรับผู้จบการศึกษาจากโรงเรียนจ่าอากาศฯ หลักสูตรเจ้าหน้าที่เทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ หลักสูตรนายทหารเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์ และมีการให้ความรู้ผู้บริหารระดับกลาง คือหลักสูตรสงครามไซเบอร์สำหรับนักศึกษาโรงเรียนเสนาธิการทหารอากาศ โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ

4.2.1.2 หลักสูตรเฉพาะ การอบรมเกี่ยวกับการประเมินและตรวจสอบ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้กับผู้ปฏิบัติงานด้านรักษาความปลอดภัยสารสนเทศ

4.2.1.3 ส่งบุคลากรเข้ารับการฝึกอบรมกับบริษัทเอกชนและ หน่วยงานภายนอก รวมถึงส่งบุคลากรเข้ารับการการศึกษากับมหาวิทยาลัยและหน่วยงานของรัฐ

4.2.1.4 หลักสูตรเกี่ยวกับสร้างความชำนาญการฝึกอบรมในการเลื่อนระดับความชำนาญให้กับข้าราชการที่มีคุณสมบัติครบเพื่อพิจารณาเลื่อนยศและตำแหน่งที่สูงขึ้น

4.3 ปัจจัยด้านเทคโนโลยี กองทัพอากาศได้ดำเนินการจัดหา ระบบเทคโนโลยีทั้งเชิงป้องกันและเชิงป้องปรามดังนี้ เทคโนโลยีทั้งเชิงป้องกันเช่นระบบบริหารจัดการเครือข่าย ระบบตรวจจับและ ป้องกันการบุกรุกเครือข่าย ระบบป้องกันไวรัสและมัลแวร์ ระบบป้องกันการรั่วไหลของข้อมูล ศูนย์ข้อมูลและศูนย์กู้คืนข้อมูลสำรอง ระบบจำลองการโจมตีในรูปแบบการระดมโจมตีเพื่อให้เครือข่ายปฏิเสธการให้บริการ ระบบบริหารแพทช์ ระบบรักษาความมั่นคงปลอดภัยจดหมายอิเล็กทรอนิกส์ ระบบป้องกันภัยคุกคามสำหรับระบบเครื่องแม่ข่ายแบบคลาวด์ ระบบเข้ารหัสข้อมูล และระบบจำลอง ทางไซเบอร์ เป็นต้น ส่วนเทคโนโลยีเชิงป้องปราม เช่น ระบบเครือข่ายเพื่อการซ่อนพราง ระบบบริหารจัดการช่องโหว่ในระบบคอมพิวเตอร์ และเครือข่ายระบบปฏิบัติการด้านการรักษา ความปลอดภัยเชิงรุก ระบบข่าวกรองทางไซเบอร์ เป็นต้น

อย่างไรก็ตาม การจัดหาเทคโนโลยีมาใช้งานในกองทัพ เป็นการจัดหาเทคโนโลยีตามวงรอบ การปฏิบัติการด้านไซเบอร์ทั้งเชิงป้องกันและเชิงป้องปรามโดยมีการจัดหาตามแผนงานที่กำหนดไว้ใน โครงการพัฒนาสงครามไซเบอร์และการสังเกตการณ์ห้วงอวกาศ และแม่บทด้านสงครามไซเบอร์ของ กองทัพอากาศ

แนวทางการดำเนินภารกิจ ขีดความสามารถและขีดจำกัด การปฏิบัติการสงครามอิเล็กทรอนิกส์กองทัพอากาศ

ในปี ๒๕๕๒ กองทัพอากาศได้กำหนดให้มีการจัดตั้งหน่วยงานที่มีความเกี่ยวข้องกับการสงครามอิเล็กทรอนิกส์ ได้แก่ กองสงครามอิเล็กทรอนิกส์และสารสนเทศ ขึ้นในกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.กองทัพอากาศ) มีหน้าที่ พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนา และดำเนินงานเกี่ยวกับ การสงครามอิเล็กทรอนิกส์ และสงครามสารสนเทศ ของกองทัพอากาศ

กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ มีขอบเขตความรับผิดชอบและหน้าที่ที่สำคัญและสนับสนุนการปฏิบัติการสงครามอิเล็กทรอนิกส์

นอกจากนี้ยังมีหน่วยงานอื่นๆ ภายในกองทัพอากาศที่เกี่ยวข้องกับการปฏิบัติด้านสงครามอิเล็กทรอนิกส์อีก เช่น กรมยุทธการทหารอากาศ กรมข่าวทหารอากาศ กรมควบคุมการปฏิบัติทางอากาศ (แผนกลาดตระเวนอิเล็กทรอนิกส์ กองการลาดตระเวนทางอากาศ), กรมสรรพาวุธทหารอากาศกองทัพอากาศ (กองโรงงานสรรพาวุธ ๕), บน.๔ (ฝูง.๔๐๒ฯ) เป็นต้น

ศักยภาพของกองทัพอากาศที่เกี่ยวกับการปฏิบัติการสงครามอิเล็กทรอนิกส์ได้รับการพัฒนาขึ้นตามสัญญาโครงการจัดซื้อ บ. Gripen 39 C/D ทำให้กองทัพอากาศมีการรับการถ่ายทอดเทคโนโลยีหลัก (Key Technologies) และการพัฒนาขีดความสามารถของกองทัพอากาศในด้านสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) การจัดทำฐานข้อมูลทางภูมิศาสตร์(Geographical Databases: Geo Data) และระบบเชื่อมโยงข้อมูล (Data Link: DL) มีการพัฒนาปรับปรุงในด้านระบบควบคุมการบิน (Avionics) เป็นแบบ Digital fly-by-wire มีระบบการตรวจจับที่ดี (Active Electronically Scanned Array: AESA) มีระบบเชื่อมโยงข้อมูล

ความเร็วสูง(High speed data links) และสามารถใช้อาวุธสมัยใหม่ที่แม่นยำได้ (Latest precision weapons) Generation of Jet Fighter

สรุป แนวทางการปฏิบัติการ EW, ขีดความสามารถ และเป้าหมายของการพัฒนา EW ของ กองทัพอากาศในปัจจุบัน แบ่งออกเป็น ๓ รูปแบบ คือ

๑. ภารกิจหลักที่ได้รับมอบหมายให้ปฏิบัติ EW เช่น การทำลายหรือตัดรอนขีดความสามารถของระบบตรวจจับของข้าศึกด้วยการรบกวน (Jamming) หรือการทำลายด้วยจรวดต่อต้านเรดาห์ (Anti- Radiation Missile) การลาดตระเวนทางอิเล็กทรอนิกส์ เพื่อการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ (Electronic Support Measure: ESM)

๒. ภารกิจที่สนับสนุนหน่วยอื่นเพื่อให้เกิดความปลอดภัยจากอาวุธของฝ่ายตรงข้าม เช่น การบินคุ้มกันทางอิเล็กทรอนิกส์ (Escort Jamming)

๓. การปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อป้องกันตัวเอง (Self-Protection Jamming)

ในปัจจุบันภาพรวมของ กองทัพอากาศ ที่มีขีดความสามารถในการปฏิบัติการสงครามอิเล็กทรอนิกส์ ในระดับผู้ใช้งาน กล่าวคือมีการใช้งาน EW ตั้งแต่ระดับอุปกรณ์ (Equipment) ขึ้นไป แต่ยังมีข้อจำกัดในด้านการพัฒนา การต่อต้านทางสงครามอิเล็กทรอนิกส์ (Countermeasure Development) ด้วยตนเอง เนื่องจากขาดบุคลากร และหน่วยงานที่รับผิดชอบ รวมทั้งปัญหาในการถ่ายทอดเทคโนโลยีของผู้จำหน่ายอุปกรณ์ หรืออากาศยาน

ดังนั้นในอนาคตกองทัพอากาศต้องมีการจัดทำฐานข้อมูลทางสงครามอิเล็กทรอนิกส์ (EW Database) ข้อมูลอิเล็กทรอนิกส์ในพื้นที่การรบ (Electronic Order of Battle: EOB) และห้องสมุดอิเล็กทรอนิกส์ (EW Library) ตลอดจนพัฒนาการต่อต้านทางสงครามอิเล็กทรอนิกส์ (EW Countermeasure Development) ด้วยตัวเองได้ รวมทั้งจำเป็นต้องมีหน่วยงานที่รับผิดชอบในเรื่องนี้โดยตรง และมีบุคลากรที่มีความรู้ความสามารถในการจัดการ รวมทั้งวิเคราะห์ข้อมูลต่าง ๆ ที่เกี่ยวข้องจึงจะทำให้ประสิทธิภาพการดำเนินการสงครามอิเล็กทรอนิกส์สูงขึ้น

เปรียบเทียบคุณสมบัติของสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์

จากคำจำกัดความ คุณสมบัติตลอดจนการใช้สงครามไซเบอร์ และสงครามอิเล็กทรอนิกส์ ในการปฏิบัติการรบหลายรูปแบบ ตามที่ผู้วิจัยได้สืบค้นและทบทวนเอกสารหลักฐานตลอดจนรายงานวิจัยที่เกี่ยวข้อง ทำให้สามารถจำแนก การปฏิบัติการที่มีความเกี่ยวข้องสัมพันธ์กัน ขัดแย้งกัน หรือสามารถทวีกำลังได้ เพื่อประโยชน์ของการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางของกองทัพอากาศ

ผู้วิจัยเปรียบเทียบคุณสมบัติ ของสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์ โดยเฉพาะการปฏิบัติการที่ใช้ในการป้องกัน ตั้งรับ หรือเชิงรุก โดยศึกษาในรายละเอียดของแต่ละปฏิบัติการที่สามารถจัดกลุ่มเดียวกับ หรือแตกต่างกัน เพื่อวิเคราะห์จุดร่วม ที่สามารถนำมาควบรวม ทวีกำลัง หรือ ประเด็นที่มีความแตกต่าง ให้ชัดเจนยิ่งขึ้นในรูปแบบตารางที่ 4-1

ตารางที่ 4-1 เปรียบเทียบคุณสมบัติของสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์

คุณลักษณะของการปฏิบัติการ	การปฏิบัติการไซเบอร์ (Cyber Operation : CO)	การปฏิบัติการสงครามอิเล็กทรอนิกส์ (Electronic Warfare Operations : EWO)
การสนับสนุน	การปฏิบัติการสนับสนุนทางไซเบอร์ ได้แก่ 1) การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support : MIS) 2) การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support : IO Support)	การสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Support : ES) ได้แก่ การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึก และวิเคราะห์
เชิงป้องกัน	การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) 1) การป้องกัน (Protect) 2) การตรวจจับ (Detect) 3) การตอบสนอง (React) 4) การฟื้นฟู (Recover)	การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection : EP) ได้แก่ การลดการถูกตรวจจับได้ด้วย Stealth, RAM Coating หรือ EMCON ของอากาศยาน การใช้เทคนิค Pulse Compression หรือ Frequency Hopping กับเรดาร์ของเรา การใช้เทคนิค Home-on-Jam ในอาวุธปล่อยนำวิถี ปฏิบัติการ Radar Jamming จากอากาศยาน
เชิงรุก	การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations : OCO) ได้แก่ 1) การรวบรวมข้อมูลเป้าหมาย (Information Gathering) 2) การตรวจสอบหาช่องโหว่ของระบบ(Vulnerability Identification) 3) การปฏิบัติการโจมตี (Attack) 4) การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) 5) การลบร่องรอยการโจมตี (Covering Tracks)	การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack : EA) ด้วย 1. มาตรการต่อต้าน ได้แก่ การแพร่กระจายคลื่น (Active) ประกอบด้วยการก่อกวน (Jamming) และการลวง (Deception) แบบไม่แพร่กระจายคลื่น (Passive ECM) ประกอบด้วย 1) ชาฟฟ์ (Chaff) 2) แฟลร์ (Flares) 3) อากาศยานเป้าลวงหรือโดรน (Decoy or Drones)

ตารางที่ 4-1 เปรียบเทียบคุณสมบัติของสงครามไซเบอร์และสงครามอิเล็กทรอนิกส์ (ต่อ)

คุณลักษณะของการปฏิบัติการ	การปฏิบัติการไซเบอร์ (Cyber Operation : CO)	การปฏิบัติการสงครามอิเล็กทรอนิกส์ (Electronic Warfare Operations : EWO)
		2. มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (Electronic Counter Counter Measures: ECCM) **

หมายเหตุ ** มาตรการตอบโต้ สามารถเป็นได้ทั้งปฏิบัติการเชิงรุก และเชิงป้องกัน

ที่มา: ประมวลโดยผู้วิจัย

วิเคราะห์รูปแบบที่เป็นไปได้ในการบูรณาการ

การปฏิบัติการไซเบอร์ของกองทัพอากาศ ประกอบด้วย การป้องกันในมิติไซเบอร์ (Cyberspace Defense) การข่าวกรอง การลาดตระเวน และการเฝ้าตรวจในมิติไซเบอร์ (Cyberspace Intelligence, Surveillance and Reconnaissance) การเตรียมสภาวะแวดล้อมในการปฏิบัติการในมิติไซเบอร์ (Cyberspace Operational Preparation of the Environment) และการป้องปรามในมิติไซเบอร์ (Cyberspace Offense) ผู้วิจัย จึงวิเคราะห์เปรียบเทียบและคัดเลือกแนวทางที่ดีที่สุดในการสนับสนุนปฏิบัติการไซเบอร์ ที่การปฏิบัติการสงครามอิเล็กทรอนิกส์พึงกระทำได้ตามบริบทของกองทัพอากาศ ดังนี้

ตารางที่ 4-2 วิเคราะห์มิติการปฏิบัติการสงครามอิเล็กทรอนิกส์ที่สนับสนุนการปฏิบัติการไซเบอร์

ปฏิบัติการไซเบอร์		**กำลังรบ (+/0/-)**	**ปฏิบัติการสงครามอิเล็กทรอนิกส์**	
เชิงป้องกัน	การป้องกัน	+	การป้องกันทางอิเล็กทรอนิกส์ (EP)	การลดการถูกตรวจจับได้ด้วย Stealth, RAM Coating หรือ EMCON ของอากาศยาน การใช้เทคนิค Pulse Compression หรือ Frequency Hopping กับเรดาร์ของเรา

ตารางที่ 4-2 วิเคราะห์มิติการปฏิบัติการสงครามอิเล็กทรอนิกส์ที่สนับสนุนการปฏิบัติการไซเบอร์ (ต่อ)

ปฏิบัติการไซเบอร์		**กำลังรบ (+/0/-)**	**ปฏิบัติการสงครามอิเล็กทรอนิกส์**	
	การตรวจจับ	+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	ดักรับ
		+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	พิสูจน์ทราบ
	การตอบสนอง	+	การป้องกันทางอิเล็กทรอนิกส์	การใช้เทคนิค Home-on-Jam ในอาวุธปล่อยนำวิถี ปฏิบัติการ Radar Jamming จากอากาศยาน
	การฟื้นฟู	0		
ปฏิบัติการสนับสนุน	สนับสนุนข้อมูลข่าวกรองทางทหาร (MIS)	+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึกวิเคราะห์
	สนับสนุนการปฏิบัติการข่าวสาร (DCO)	+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึกวิเคราะห์
ปฏิบัติการเชิงป้องปราม	การรวบรวมข้อมูลเป้าหมาย	+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึกวิเคราะห์
	การตรวจสอบหาช่องโหว่ของระบบ	+	การสนับสนุนทางอิเล็กทรอนิกส์ (ES)	การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึกวิเคราะห์

ตารางที่ 4-2 วิเคราะห์มิติการปฏิบัติการสงครามอิเล็กทรอนิกส์ที่สนับสนุนการปฏิบัติการไซเบอร์ (ต่อ)

ปฏิบัติการไซเบอร์		**กำลังรบ (+/0/-)**	**ปฏิบัติการสงครามอิเล็กทรอนิกส์**	
	การปฏิบัติการโจมตี (Attack)	+	การโจมตี (EA)	1. มาตรการต่อต้าน (ECM) ได้แก่ 1.1 การแพร่กระจายคลื่น (Active ECM) ประกอบด้วยการก่อกวน (Jamming)
ปฏิบัติการเชิงป้องปราม	การปฏิบัติการโจมตี (Attack)	+	การโจมตี (EA)	1. มาตรการต่อต้าน (ECM) 1.2 การลวง (Deception) แบบไม่แพร่กระจายคลื่น (Passive ECM) ประกอบด้วย 1) ชาฟฟ์ (Chaff) 2) แฟลร์ (Flares) 3) อากาศยานเป้าลวงหรือโดรน (Decoy or Drones)
		+	การโจมตีทางอิเล็กทรอนิกส์	2. มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์
	การเปิดช่องโหว่	0		
	การลบร่องรอยการโจมตี	0		

ที่มา : ประมวลโดยผู้วิจัย

แนวทางการบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์

1. ปฏิบัติการไซเบอร์เชิงป้องกัน สามารถใช้การป้องกันทางอิเล็กทรอนิกส์ การสนับสนุนทางอิเล็กทรอนิกส์ และการป้องกันทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้น ด้านการฟื้นฟู

2. การปฏิบัติการไซเบอร์สนับสนุน สามารถใช้การสนับสนุนทางอิเล็กทรอนิกส์ และการ เพื่อทวีกำลังได้ทุกด้าน

3.การปฏิบัติการไซเบอร์เชิงป้องปราม สามารถใช้ การสนับสนุนทางอิเล็กทรอนิกส์ และโจมตีทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้น ด้านการเปิดช่องโหว่ และด้านการลบร่องรอยการโจมตี

บทที่ 5
สรุปและข้อเสนอแนะ

งานวิจัย เรื่อง การบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศฉบับนี้ มีวัตถุประสงค์ ดังนี้

๑. เพื่อศึกษาแนวทางการดำเนินงาน ขีดความสามารถ และขอบขีดจำกัดของมิติไซเบอรอย่างรอบด้าน

๒. เพื่อศึกษาแนวทางการดำเนินภารกิจ ขีดความสามารถและขอบขีดจำกัดการปฏิบัติการสงครามอิเล็กทรอนิกสอย่างรอบด้าน

๓. เพื่อวิเคราะห์และประมวลผลลัพธ์การบูรณาการเชื่อมโยงขีดความสามารถของทั้งสองด้านเพื่อทวีขีดความสามารถทางไซเบอรใหม เพื่อใหมีความได้เปรียบในความมั่นคงปลอดภัยไซเบอรกองทัพอากาศ

ทั้งนี้ ตอบสนองประเด็นยุทธศาสตร์การเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศของกองทัพอากาศ ตลอดจนสอดคล้องกับกลยุทธ์การพัฒนาขีดความสามารถด้านสงครามไซเบอร์ รวมทั้ง การแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์ ยุคปัจจุบัน การดำเนินการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศมีการพัฒนาก้าวกระโดดจากโครงการจัดซื้อเครื่องบิน Gripen 39 C/D เข้าประจำการในกองทัพอากาศ ทำให้มีระบบการตรวจจับที่ดี (Active Electronically Scanned Array: AESA) มีระบบเชื่อมโยงข้อมูลความเร็วสูง (High speed data links) และสามารถใช้อาวุธสมัยใหม่ที่แม่นยำสูง (Latest precision weapons) จึงนับว่าเป็นจุดแข็งของกำลังทางอากาศในยุคปัจจุบัน สามารถสร้างความได้เปรียบทั้งระดับยุทธวิธีถึงระดับยุทธศาสตร์ มีขีดความสามารถในการปฏิบัติภารกิจการสงครามอิเล็กทรอนิกส์ ใน ๓ รูปแบบ คือ ๑) ภารกิจหลัก เช่น การทำลายหรือตัดรอนขีดความสามารถของระบบตรวจจับของข้าศึกด้วยการรบกวน (Jamming) หรือการทำลายด้วยจรวดต่อต้านเรดาห์ (Anti Radiation Missile) การลาดตระเวนทางอิเล็กทรอนิกส์ เพื่อการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ (Electronic Support Measure: ESM) ๒) ภารกิจสนับสนุนหน่วยอื่นเพื่อให้เกิดความปลอดภัยจากอาวุธของฝ่ายตรงข้าม เช่น การบินคุ้มกันทางอิเล็กทรอนิกส์ (Escort Jamming) ๓) การปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อป้องกันตัวเอง (Self-Protection Jamming)

การดำเนินการดังกล่าวยังสอดรับกับยุทธศาสตร์ทหาร กองทัพไทย ๒๐ ปี ในวัตถุประสงค์เฉพาะทางทหารที่กำหนดให้การปฏิบัติการในสงครามไซเบอร์ (Cyber Warfare) มีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ (Cyber Domain) ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติ ตลอดจนสามารถบูรณาการและให้การสนับสนุนความมั่นคงไซเบอร์

(Cyber Security) ของประเทศในภาพรวมได้อย่างมีประสิทธิภาพ และกำหนดเป็นยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย เพื่อเป็นแนวทางในการปฏิบัติการทางทหารในมิติไซเบอร์กองทัพไทย แยกเป็น ๓ ประเด็นยุทธศาสตร์ได้แก่ ๑) ยุทธศาสตร์การป้องกันเชิงรุกสำหรับปฏิบัติการในมิติไซเบอร์ ๒) ยุทธศาสตร์การผนึกกำลังป้องกันประเทศสำหรับปฏิบัติการในมิติไซเบอร์ และ ๓) ยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับปฏิบัติการในมิติไซเบอร์

ผู้วิจัยได้ตรวจสอบสภาพแวดล้อม ศึกษาทฤษฎีและแนวคิดที่เกี่ยวข้อง ในระดับชาติ ระดับหน่วยงานกองทัพอากาศ ตลอดจนเอกสาร บทความ และงานวิจัยที่เกี่ยวข้องกับการพัฒนาขีดความสามารถไซเบอร์ และสงครามอิเล็กทรอนิกส์ทั้งในและต่างประเทศ เพื่อให้งานวิจัยฉบับนี้มีความถูกต้องสมบูรณ์มากยิ่งขึ้น โดยขอบเขตของงานวิจัยฉบับนี้มุ่นเน้นการศึกษาภารกิจด้านไซเบอร์กองทัพอากาศ ที่สนับสนุนแนวทางการพัฒนาตามยุทธศาสตร์กองทัพอากาศที่มุ่งเน้นการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) เพื่อให้เห็นและเข้าใจถึงบริบทการพัฒนาขีดความสามารถในมิติไซเบอร์ (Cyber Domain) และศึกษาขีดความสามารถและขอบขีดจำกัดในส่วนสงครามอิเล็กทรอนิกส์ (Electronic Warfare) ที่มีกระบวนการในการดำเนินงานมีลักษณะใกล้เคียงและสอดคล้องกัน ได้แก่ การดำเนินการในลักษณะปฏิบัติการเชิงรุก ปฏิบัติการตั้งรับ และปฏิบัติการสนับสนุนเพื่อวิเคราะห์ เปรียบเทียบ และพิจารณาหาแนวทางที่เป็นไปได้ ไปสู่ข้อสรุปในการบูรณาการขีดความสามารถทั้งสองด้าน ที่จะพัฒนาขีดความสามารถทางไซเบอร์ ให้ทวีกำลังความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ และส่งผลต่อความมั่นคงของชาติได้โดยมีหลักฐานทางวิชาการที่ชัดเจนในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ และที่สำคัญที่สุดการวิจัยนี้จะเน้นเฉพาะหลักการหรือเนื้อหาในแต่ละขีดความสามารถ ที่สามารถเปิดเผยได้เท่านั้น โดยใช้การวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับการวิจัยเชิงพรรณนา (Descriptive Research) สรุปได้ดังนี้

สรุป

วัตถุประสงค์การวิจัยข้อที่ 1 การปฏิบัติการไซเบอร์ สรุปได้ดังนี้

กองทัพอากาศมีการปฏิบัติการไซเบอร์ (Cyber Operation : CO) ที่จะนำมาใช้วิเคราะห์และประมวลผลลัพธ์การบูรณาการเชื่อมโยงขีดความสามารถของการปฏิบัติการไซเบอร์และการปฏิบัติการสงครามอิเล็กทรอนิกส์ ดังนี้

1. การปฏิบัติการสนับสนุนทางไซเบอร์ ได้แก่ 1.1) การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support : MIS) และ 1.2) การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support : IO Support)

2. การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) ได้แก่ 2.1) การป้องกัน (Protect) 2.2) การตรวจจับ (Detect) 2.3) การตอบสนอง (React) และ 2.4) การฟื้นฟู (Recover)

3. การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations : OCO) ได้แก่ 3.1) การรวบรวมข้อมูลเป้าหมาย (Information Gathering) 3.2) การตรวจสอบหาช่องโหว่

ของระบบ (Vulnerability Identification) 3.3) การปฏิบัติการโจมตี (Attack) 3.4) การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) และ 3.5) การลบร่องรอยการโจมตี (Covering Tracks)

วัตถุประสงค์การวิจัยข้อที่ 2 การปฏิบัติการสงครามอิเล็กทรอนิกส์ สรุปได้ดังนี้

1. การสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Support : ES) ได้แก่ การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึก และวิเคราะห์

2. การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection : EP) ได้แก่ การลดการถูกตรวจจับด้วย Stealth, RAM Coating หรือ EMCON ของอากาศยาน การใช้เทคนิค Pulse Compression หรือ Frequency Hopping กับเรดาร์ของเรา การใช้เทคนิค Home-on-Jam ในอาวุธปล่อยนำวิถีปฏิบัติการ Radar Jamming จากอากาศยาน

3. การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack : EA) ได้แก่ 3.1) มาตรการต่อต้าน ได้แก่ การแพร่กระจายคลื่น (Active) ประกอบด้วยการก่อกวน (Jamming) และการลวง (Deception) แบบไม่แพร่กระจายคลื่น (Passive ECM) ประกอบด้วย 3.1.1) ชาฟฟ์ (Chaff) 3.1.2) แฟลร์ (Flares) และ 3.1.3) อากาศยานเป้าลวงหรือโดรน (Decoy or Drones) 3.2) มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (Electronic Counter Counter Measures: ECCM)

วัตถุประสงค์การวิจัยข้อที่ 3 การบูรณาการเชื่อมโยงขีดความสามารถ เพื่อทวีกำลังด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ สรุปได้ดังนี้

1. ปฏิบัติการไซเบอร์เชิงป้องกัน สามารถใช้การป้องกันทางอิเล็กทรอนิกส์ การสนับสนุนทางอิเล็กทรอนิกส์ และการป้องกันทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้น ด้านการฟื้นฟู

2. การปฏิบัติการไซเบอร์สนับสนุน สามารถใช้การสนับสนุนทางอิเล็กทรอนิกส์ และการ เพื่อทวีกำลังได้ทุกด้าน

3. การปฏิบัติการไซเบอร์เชิงป้องปราม สามารถใช้ การสนับสนุนทางอิเล็กทรอนิกส์ และโจมตีทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้น ด้านการเปิดช่องโหว่ และด้านการลบร่องรอยการโจมตี

ข้อเสนอแนะ

ข้อเสนอแนะระดับยุทธศาสตร์

1. ให้เพิ่มเติมการปฏิบัติการร่วมเพื่อทวีกำลังระหว่าง การปฏิบัติการไซเบอร์และการปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อเป็นแนวทางดำเนินการอย่างเป็นรูปธรรม ที่สอดคล้องกับยุทธ์ศาสตร์กองทัพอากาศ โดยกำหนดเป็นกลยุทธหลักในการดำเนินการ

2. แต่งตั้งผู้รับผิดชอบดำเนินการตรวจสอบสภาพแวดล้อมรอบด้านอย่างละเอียด ถึงปัจจัยที่ส่งผลต่อระดับความสำเร็จในการดำเนินการ ทรัพยากรที่จำเป็น และคุณประการที่จะเกิดขึ้น ความเสี่ยง จนสามารถนำไปสู่การกำหนดยุทธศาสตร์ดำเนินการได้อย่างเป็นรูปธรรม และ ส่งผลต่อความสัมฤทธิ์ในการปฏิบัติการของกองทัพอากาศ

3. อนุมัติงบประมาณ และแนวทางในการจัดหาบุคลากร เทคโนโลยี เครื่องมือเครื่องใช้ตลอดจนซอฟแวร์ที่จำเป็น

ข้อเสนอแนะระดับยุทธวิธี

1. กำหนดให้มี คณะกรรมการ คณะทำงาน หรือคณะเจ้าหน้าที่ แปลงนโยบายลงสู่การปฏิบัติในรูปแบบของการคร่อมสายงาน และรายงานผลต่อผู้บัญชาการทหารอากาศโดยตรง

2. ปรับปรุงอาคารสถานที่ ให้เหมาะสมในการบรรจุเทคโนโลยีมูลค่าสูง เพื่อให้สามารถใช้งานได้เกิดประโยชน์ต่อกองทัพอากาศระดับสูงสุด

3. พัฒนาองค์ความรู้และบุคลากรกองทัพอากาศ ด้านไซเบอร์ สงครามอิเล็กทรอนิกส์ตลอดจนสนับสนุนให้สร้างงานวิจัยอย่างต่อเนื่อง

ข้อเสนอแนะระดับปฏิบัติการ

1. หัวหน้าหน่วยขึ้นตรงทุกระดับให้ความสำคัญ และกระตุ้นให้ผู้ใต้บังคับบัญชาตระหนักถึงความมั่นคงปลอดภัยไซเบอร์ โดยถือเป็นข้าศึกในยุคปัจจุบัน และกองทัพอากาศอาจถูกโจมตีได้ทุกวินาที

2. ปรับปรุงกฎ ระเบียบ คำสั่งที่เกี่ยวข้องให้สอดคล้องกับยุทธศาสตร์ที่ปรับปรุงขึ้นใหม่

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ศึกษา วิเคราะห์เชิงลึก ด้านความพร้อมและการเตรียมทรัพยากรทุกประเภทของกองทัพอากาศที่จำเป็นในการสนับสนุนด้านสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์

2. ศึกษา วิเคราะห์เชิงลึก การปฏิบัติการสงครามอิเล็กทรอนิกส์ ในแต่ละด้านเพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์ ตลอดจนวิเคราะห์ข้อได้เปรียบ และข้อด้อยที่อาจพบได้จากการปฏิบัติการ

3. ศึกษา โครงการนำร่องการปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์

บรรณานุกรม

ภาษาไทย

หนังสือ

ธันยวัต ชูสงแสง. การกอการรายในมุมมองของสหรัฐอเมริกา. กรุงเทพฯ : กรมขาวทหารอากาศ กองทัพอากาศ, 2547.

นายกรัฐมนตรี, สำนัก. ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564, 2560.

วารสาร และหนังสือพิมพ์

ดลยา เทียนทอง. “ข่อมูลเบื้องตนเกี่ยวกับการกอการราย”การกอการรายรวมสมัย (Contemporary Terrorism). จุลสารความมั่นคงศึกษา, ปีที่ 57 (7–12), 2549.

นงรัตน์ สายเพชร. “ความมั่นคงไซเบอร์ของสหรัฐอเมริกา”. จุลสารความมั่นคงศึกษา. ปีที่ 64 (129 - 130), กันยายน 2556.

พงศธร สัตยเจริญ. “กฎหมายกับการกอการราย”. สารชาวฟา. ปีที่ 46 (2113), 2549.

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

ชัชวาลย์ ชำนิกุล. “**การพัฒนาระบบวิเคราะห์และออกแบบฐานข้อมูลสงครามอิเล็กทรอนิกส์”.** ปัญหาพิเศษ วิทยาศาสตร์มหาบัณฑิต, สาขาเทคโนโลยีสารสนเทศ, ภาควิชาการจัดการเทคโนโลยีสารสนเทศ, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2555.

ธนภัทร กิตติวณิชพันธุ์. **“สมรรถนะของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์.”** วิทยานิพนธ์บริหารธุรกิจมหาบัณฑิต, สาขาวิชาการจัดการ, บัณฑิตวิทยาลัยการจัดการและนวัตกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี, 2560.

หยาดพิรุณ นาชัยสินธุ์. “**ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย”.** ดุษฎีนิพนธ์รัฐศาสตร์ดุษฎีบัณฑิต, สาขาวิชายุทธศาสตร์และความมั่นคง, คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา, 2559.

เอกสารไม่ตีพิมพ์

กลาโหม, กระทรวง. “ยุทธศาสตร์กระทรวงกลาโหม พ.ศ.2560 – 2579”. 2560.

กองทัพบก. “วิชาสงครามอิเล็กทรอนิกส์”. เอกสารอัดสำเนา. ม.ป.ป.

กองทัพเรือ. “หลักสูตร 3111 สงครามอิเล็กทรอนิกส์ (สัญญาบัตร) (Electronic Warfare Curriculum)”. กองฝึกศูนย์ยุทธการและสื่อสาร กองการฝึก กองเรือยุทธการ. 2554.

กองทัพอากาศ. “นโยบายผู้บัญชาการทหารอากาศ ประจำปี พ.ศ.2560 - 2561”. 2559.
กองทัพอากาศ. “นโยบายผู้บัญชาการทหารอากาศ ประจำปี พ.ศ.2563”. 2562.
กองทัพอากาศ. “ยุทธศาสตร์กองทัพอากาศ 20 ปี พ.ศ.2559 - 2580 (ฉบับเผยแพร่)”. 2562.
กองทัพอากาศ. “หลักนิยมกองทัพอากาศ พ.ศ.2562”. 2562.
กองทัพอากาศ. “หลักนิยมพื้นฐานกองทัพอากาศ พ.ศ.2551”. 2551.
กองบัญชาการกองทัพไทย. “แผนที่ยุทธศาสตร์กองทัพไทย พ.ศ.2559 - 2562”. 2559.
เลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, สำนักงาน. ยุทธศาสตร์ชาติ พ.ศ. 2561 - 2580. ราชกิจจานุเบกษา. เล่มที่ 135 ตอนที่ 82ก, 13 ตุลาคม 2561.

ฐานข้อมูลอิเล็กทรอนิกส์

“การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ : ความท้าทายของกองทัพบก (Cyber Security : A Challenge of Army)”. (ออนไลน์). เข้าถึงได้จาก : HTTP://RITTEE1834.BLOGSPOT.COM/2014/08/CYBER-SECURITY-CHALLENGE-OF-ARMY.HTML, 2557.
โกวิท วงศสุรวัฒน. การกอการรายในเมืองกับสงครามกองโจร. (ออนไลน์). เขาถึงไดจาก : HTTP://MATICHON.COM, 2550.
“ความเป็นมาของสงครามอิเล็กทรอนิกส์ ทอ.” (ออนไลน์). เข้าถึงได้จาก : https://sites.google.com/site/wwwdjnonmixcom/tha-ha-nth-har/kheruxng-bin/jas-39-c-d-gripen/bthkhwammimichux, 2563.
“ความมั่นคงปลอดภัย 'ไซเบอร์' ในอาเซียน” (ออนไลน์). เข้าถึงได้จาก : HTTPS://WWW.BANGKOKBIZNEWS.COM/NEWS/DETAIL/865066, 2563.
“คู่มือ CYBER SECURITY สำหรับประชาชน”. (ออนไลน์). เข้าถึงได้จาก : HTTP://WWW.NBTC.GO.TH/NEWS/รวมบทความ-(1)/คู่มือ-CYBER-SECURITY-สำหรับ ประชาชน.ASPX, 2561.
“แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ”. (ออนไลน์). เข้าถึงได้จาก : HTTPS://WWW.ACISONLINE. NET/?P=5040&LANG=TH, 2559.
ปริญญา หอมเอนก. “แนวโน้มภัยคุกคามและทิศทางด้านความมั่นคง ปลอดภัยในปี 2016 – 2018”. ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security (ออนไลน์). เข้าถึงได้จาก : https://www.techtalkthai.com/cdic-2019-threat-landscape-and-cybersecurity-trends-in-2020/, 2563.
พัฒนาธุรกรรมทางอิเล็กทรอนิกส์, สำนักงาน. (องค์การมหาชน). กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. “ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ: ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ”. (ออนไลน์). เข้าถึงได้จาก : HTTPS://WWW.THAICERT.OR.TH/DOWNLOADS/FILES/CYBER_THREATS_TO_THE_NETWORKED_GOVERNMENT.PDF, 2558.

"ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน CYBER SECURITY". (ออนไลน์). เข้าถึงได้จาก : HTTPS:// WWW.TECHTALKTHAI.COM/CDIC-2016-CYBER- SECURITY-THREATS-AND-TRENDS/, 2559.

ศูนยศึกษาการกอการราย. "การตอต่านและการตอบโตการกอการราย". (ออนไลน์). เขาถึงไดจาก : www.geocities.com, 2563.

สรรสิริ สิริสันต์คุปต์, นาวาอากาศเอก. "บทบาท AI เพื่อการทหารในอนาคต The Future Role of AI in the Military". (ออนไลน์). เข้าถึงได้จาก : http://www.cioworldmagazine.com/sansiri-sirisantakupt-future-role-of-ai-in-military, 2563.

Lew. "กระทรวงกลาโหมประเทศญี่ปุ่นยื่นของบประมาณ ด้านไซเบอร์และด้านอวกาศ รวม 1.5 ล้านล้านบาท". (ออนไลน์). เข้าถึงได้จาก : https://www.blognone.com/node/111632, 2563.

"What is an Electronic Warfare?". (ออนไลน์). เข้าถึงได้จาก : https://nniwat.wordpress.com/2010/05/10/what-is-an-, electronic-warfare/, 2563.

ภาษาต่างประเทศ

Books

Thornton, T.P. Terror as a weapon of political agitation. In eckstein. New York: Free Press of Glencoe., 2005.

Journal

Gurr, R. T. "Some Characteristics of Political Terrorism in the 1960s". National Criminal Justice Reference Service. NCJ-56208, 1988.

Research, Report and Thesis

Daud,A. "Cyber–dissent in the middle east: A tool of political resistance". Doctoral dissertation, School of Political and Policy, Claremont Graduate University, 2001.

Kim, S.Y. "Cyber–surveillance: A case study in policy and development". Doctoral dissertation, Faculty in Criminal Justice in partial fulfillment, The City University of New York, 2010.

Snowden, A.M. “The perception of cyber threats and its associative relationship to the protection motivation theory and generational age groups: a Quantitative study”. Doctoral dissertation, Faculty in Business and Technology, Capella University, 2015.

Electronic Data Base

Geocities. “Terrorism studies.” (Online). Available : http://www.geocities.com/terrorismstudies, 2004.

ภาคผนวก

แบบสัมภาษณ์ ผู้บังคับบัญชา และผู้ปฏิบัติงาน ด้านไซเบอร์ และการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้รับการสัมภาษณ์

ยศ ชื่อ สกุล ..... อายุ .....ปี

ระยะเวลาที่ปฏิบัติงานในกองทัพอากาศ .....ปี

ประเภทของงานในด้านที่เกี่ยวข้อง ☐ ด้านไซเบอร์ ☐ การสงครามอิเล็กทรอนิกส์

ระยะเวลาที่ปฏิบัติงานในด้านที่เกี่ยวข้อง (ประสบการณ์ตรง) .....ปี

ลักษณะงาน ☐ ผู้บังคับบัญชาระดับสูง

☐ ผู้บังคับบัญชาระดับหัวหน้าหน่วยขึ้นตรง

☐ ผู้บังคับบัญชาระดับกลาง

☐ ผู้ปฏิบัติงาน

ส่วนที่ 2 ลักษณะงานด้านไซเบอร์ หรือ การสงครามอิเล็กทรอนิกส์

1. ยุทธศาสตร์ นโยบาย แผนงาน โครงการที่เกี่ยวข้อง

.....

.....

.....

2. ลักษณะการกำหนดโครงสร้างหน่วยงานที่รับผิดชอบของกองทัพอากาศ

.....

.....

.....

3. ศักยภาพ สมรรถนะ และสภาพปัจจุบัน

.....

.....

.....

4. ความคิดเห็น หากนำไซเบอร์ และ การสงครามอิเล็กทรอนิกส์ มาใช้สนับสนุนกันและกัน

.....

.....

.....

5. ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

ประวัติย่อผู้วิจัย

ชื่อ นาวาอากาศเอก เสกสัณน์ ไชยมาตย์

วัน เดือน ปีเกิด 28 กุมภาพันธ์ 2509

การศึกษา

โรงเรียนเตรียมทหาร	รุ่นที่ 26
โรงเรียนนายเรืออากาศ	รุ่นที่ 33
ศิษย์การบิน โรงเรียนการบิน	รุ่นที่ น.88-33-2
โรงเรียนนายทหารชั้นผู้บังคับฝูง	รุ่นที่ 86
โรงเรียนเสนาธิการทหารอากาศ	รุ่นที่ 45

วิทยาลัยเสนาธิการทหาร สปท. รุ่นที่ 54

ประวัติการทำงานโดยย่อ

- นักบินประจำกอง ฝูงบิน 531 กองบิน 53
- รองผู้บังคับหมวดบิน 4 ฝ่ายยุทธการ ฝูงบิน 531 กองบิน 53
- ผู้บังคับหมวดบิน 4 ฝ่ายยุทธการ ฝูงบิน 402 กองบิน 4
- นายทหารโครงการ กองการปกครอง โรงเรียนนายทหารชั้นผู้บังคับฝูง
- นายทหารปกครอง กองการปกครอง โรงเรียนนายทหารชั้นผู้บังคับฝูง
- ผู้บังคับกองพันที่ 5 กรมนักเรียนนายเรืออากาศ รักษาพระองค์ โรงเรียนนายเรืออากาศ
- ผู้บังคับฝูงบิน 531 กองบิน 53
- ผู้บังคับฝูงบิน 501 กองบิน 5
- รองผู้บังคับการฝ่ายเทคนิค กองบิน 5
- เสนาธิการกองบิน 5
- รองผู้อำนวยการกองข่าวกรองยุทธศาสตร์ กรมข่าวทหารอากาศ
- ผู้อำนวยการกองปฏิบัติกิจพิเศษ สำหนักยุทธการและการฝึก กรมยุทธการทหารอากาศ
- รองผู้อำนวยการสำนักยุทธการและการฝึก กรมยุทธการทหารอากาศ

ตำแหน่งปัจจุบัน รองผู้อำนวยการสำนักนโยบายและแผน กรมยุทธการทหารอากาศ

สรุปย่อ

ลักษณะวิชา การทหาร

เรื่อง การบูรณาการขีดความสามารถทางไซเบอร์กับปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ

ผู้วิจัย นาวาอากาศเอก เสกสัณน์ ไชยมาตย์ **หลักสูตร** วปอ. **รุ่นที่** 62

ตำแหน่ง รองผู้อำนวยการสำนักนโยบายและแผน กรมยุทธการทหารอากาศ

ความเป็นมาและความสำคัญของปัญหา

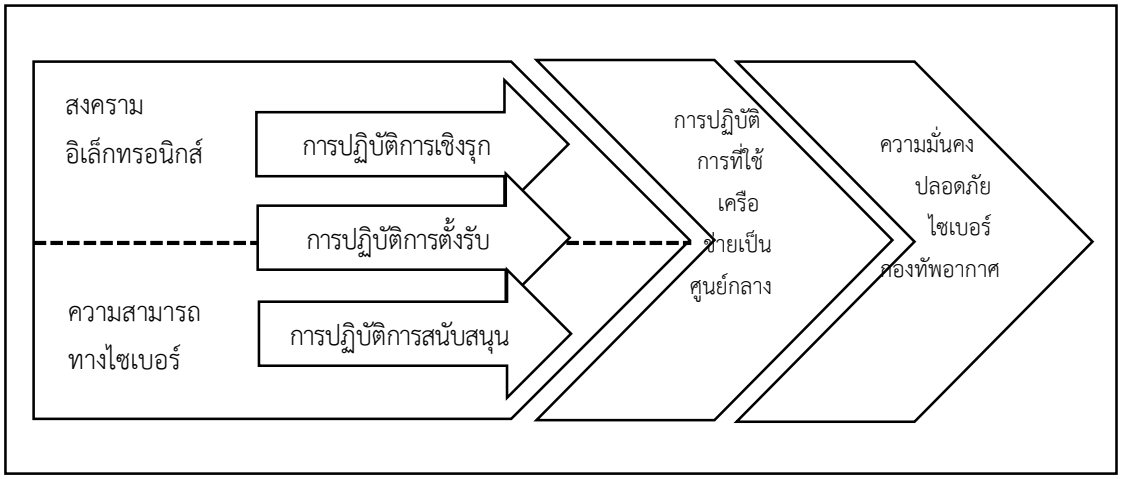
ในท่ามกลางกระแสโลกาภิวัฒน์และความก้าวหน้าทางเทคโนโลยี ทำให้บริบทความมั่นคงของโลกมีการแข่งขันสูงขึ้น จนนำไปสู่ความขัดแย้งในการแสวงหาผลประโยชน์และช่วงชิงการครอบครองทรัพยากรธรรมชาติ ส่งผลกระทบต่อสภาวะแวดล้อมด้านความมั่นคง การพัฒนาทางเทคโนโลยีสารสนเทศและการสื่อสารทั้งด้านเครือข่ายและอินเทอร์เน็ต นำมาซึ่งภัยคุกคามในมิติไซเบอร์ สำหรับประเทศไทยให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ โดยสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี ได้กำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 - 2564 โดยมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุด, ในยุทธศาสตร์ชาติ 20 ปี ด้านความมั่นคง ได้กำหนดประเด็นการพัฒนาระบบ กลไก มาตรการ และความร่วมมือระหว่างประเทศในทุกระดับ เพื่อรักษาผลประโยชน์ของชาติ สามารถป้องกันและแก้ไขปัญหาความมั่นคงรูปแบบใหม่ ภัยคุกคามข้ามชาติ ภัยก่อการร้าย และเสริมสร้างความมั่นคงเทคโนโลยีสารสนเทศและไซเบอร์ไว้ด้วยเช่นกัน (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561) ทั้งนี้ กระทรวงกลาโหมได้กำหนดยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม 20 ปี โดยการพัฒนาและดำรงขีดความสามารถการปฏิบัติการด้านไซเบอร์ให้มีศักยภาพทัดเทียมกับประเทศในภูมิภาค นำไปสู่การกำหนดยุทธศาสตร์ทหารกองทัพไทย 20 ปี ที่กำหนดการปฏิบัติการในสงครามไซเบอร์ (Cyber Warfare ตลอดจนสามารถบูรณาการและให้การสนับสนุนความมั่นคงไซเบอร์ (Cyber Security) ของประเทศในภาพรวมได้อย่างมีประสิทธิภาพ

ในส่วนกองทัพอากาศ ได้กำหนดกลยุทธ์การพัฒนาขีดความสามารถด้านสงครามไซเบอร์ ตามคุณลักษณะที่เหมาะสมกับการใช้กำลังกองทัพอากาศ โดยพัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ และใช้ประโยชน์จากการปฏิบัติการทางไซเบอร์ในการขยายขีดความสามารถการปฏิบัติการทางทหาร รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือกับหน่วยงานภายในและภายนอกประเทศเพื่อป้องกันภัยคุกคามทางไซเบอร์

การปฏิบัติการสงครามอิเล็กทรอนิกส์ เป็นขีดความสามารถที่มีความสำคัญมากในการปฏิบัติการทางทหารในทุกยุคสมัย จนมีคำกล่าวว่า “ฝ่ายใดที่สามารถครองสมรภูมิสงครามอิเล็กทรอนิกส์ได้นั้น ก็แทบจะนับได้ว่าเป็นฝ่ายผู้ชนะ” เป็นขีดความสามารถที่ถูกพัฒนาและนำมาใช้ในภารกิจด้านการทหารตั้งแต่ยุคโรมัน หน่วยงาน กองทัพอากาศ ได้เริ่มมีปฏิบัติการสงครามอิเล็กทรอนิกส์ ในปี 2522 ในบริบทของการสนับสนุนการข่าวกรองเพื่อการตัดสินใจของผู้บังคับบัญชา และจากโครงการจัดซื้อเครื่องบิน Gripen 39 C/D ทำให้กองทัพอากาศ ได้รับการถ่ายทอดเทคโนโลยีหลัก และพัฒนาขีดความสามารถด้านสงครามอิเล็กทรอนิกส์ (Electronic Warfare : EW), การจัดทำฐานข้อมูลทางภูมิศาสตร์ (Geographical Databases : Geo Data) และระบบเชื่อมโยงข้อมูล (Data Link : DL) ที่สามารถสร้างความได้เปรียบทั้งระดับยุทธวิธีถึงระดับยุทธศาสตร์ สอดคล้องกับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) โดยมีการเชื่อมโยงข้อมูลที่ได้รับจากระบบตรวจจับต่าง ๆ (Sensor) เข้าสู่ระบบควบคุมบังคับบัญชา (Command and Control) นำไปสู่การตัดสินใจของผู้บังคับบัญชาที่ถูกต้องปลอดภัย นำมาซึ่งความหยั่งรู้สถานการณ์ร่วมกันในทุกระดับของการปฏิบัติการ ส่งผลโดยตรงต่อประสิทธิผลและประสิทธิภาพในการปฏิบัติ โดยเฉพาะการบัญชาการและการควบคุมนภานุภาพ (Air Power) ทั้ง ๓ มิติ ได้แก่ มิติทางอากาศ (Air Domain) มิติไซเบอร์ (Cyber Domain) และมิติอวกาศ (Space Domain) อันจะทำให้เกิดการทวีกำลังกองทัพอากาศ (Force Multiplier) อย่างเป็นรูปธรรม

เมื่อพิจารณาจากขีดความสามารถทั้งมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ ซึ่งเป็นขีดความสามารถที่มีแนวทางปฏิบัติคล้ายคลึงกัน ผู้วิจัยจึงมีข้อสันนิษฐานว่าผลลัพธ์จากปฏิบัติการสงครามอิเล็กทรอนิกส์ จะสามารถนำมาเสริมสร้างขีดความสามารถทางไซเบอร์ได้ ซึ่งจะเป็นประโยชน์และสร้างความได้เปรียบด้านความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในระดับการปฏิบัติการทางทหารและในระดับความมั่นคงของชาติโดยรวม ผู้วิจัยจึงสนใจที่จะศึกษาแนวทางการพัฒนาขีดความสามารถทางไซเบอร์ด้วยการเชื่อมโยงกับขีดความสามารถการสงครามอิเล็กทรอนิกส์เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศ จึงกำหนดเป็นหัวข้อในการจัดทำเอกสารวิจัยส่วนบุคคลของหลักสูตรการป้องกันราชอาณาจักร ปีการศึกษา 2562 - 2563 (วปอ.62) ฉบับนี้

แผนภาพที่ 1 กรอบแนวคิดของการวิจัย



วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการดำเนินงาน ขีดความสามารถ และขอบขีดจำกัดของมิติไซเบอร์และสงครามอิเล็กทรอนิกส์ทั้งในอดีตและปัจจุบัน

2. เพื่อศึกษาการเชื่อมโยงการดำเนินภารกิจ ขีดความสามารถและขอบขีดจำกัดของมิติไซเบอร์กับการปฏิบัติการสงครามอิเล็กทรอนิกส์

3. เพื่อเสนอแนวทางการบูรณาการเชื่อมโยงขีดความสามารถในมิติไซเบอร์กับสงครามอิเล็กทรอนิกส์ ในการทวีขีดความสามารถเพื่อความได้เปรียบในความมั่นคงปลอดภัยไซเบอร์กองทัพอากาศและความมั่นคงของชาติ

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา

1.1 การวิจัยนี้เน้นการศึกษา วิเคราะห์ เนื้อหา ความสอดคล้องในรูปแบบและกระบวนการในการดำเนินภารกิจด้านไซเบอร์ของกองทัพอากาศ เท่านั้น

1.2 การวิจัยนี้จะศึกษาหลักการหรือแนวคิดที่เป็นไปได้จริงทั้งในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ ในเชิงเปรียบเทียบขีดความสามารถที่มีความสอดคล้องสัมพันธ์และเกื้อกูลกันได้ในเชิงปฏิบัติ

1.3 การวิจัยนี้จะเน้นเฉพาะหลักการหรือเนื้อหาในแต่ละขีดความสามารถที่สามารถเปิดเผยได้เท่านั้น เนื่องจากในขีดความสามารถทั้งสองด้านเป็นหัวข้อที่ดำเนินการเกี่ยวกับภารกิจที่มีความเกี่ยวข้องกับเนื้อหาที่มีชั้นความลับ จึงจำเป็นต้องมีการกลั่นกรองเนื้อหาอย่างรอบคอบและใช้ความระมัดระวังสูง

2. ขอบเขตด้านประชากร

ประชากรที่เกี่ยวข้องในการศึกษาครั้งนี้ ได้แก่ กำลังพลและเจ้าหน้าที่ผู้ปฏิบัติงานด้านไซเบอร์และสงครามอิเล็กทรอนิกส์กองทัพอากาศ ทั้งระดับผู้บังคับบัญชาหน่วย (ผู้บริหาร) และผู้ปฏิบัติงานจริง

วิธีดำเนินการวิจัย

ดำเนินการด้วยระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับการวิจัยเชิงพรรณนา (Descriptive Research) ดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ ดำเนินการโดยการศึกษาจากตำรา คู่มือและเอกสารต่าง ๆ เรื่องมิติไซเบอร์ และภารกิจสงครามอิเล็กทรอนิกส์ ทั้งข้อมูลภายในประเทศและกองทัพมิตรประเทศ

1.2 ข้อมูลปฐมภูมิ ดำเนินการโดยการสัมภาษณ์เชิงลึกผู้บังคับบัญชาหน่วยงานที่เกี่ยวข้องในกองทัพอากาศ ผู้รับผิดชอบงานและผู้ปฏิบัติงานจริง ตลอดจนผู้ชำนาญที่มีความเชี่ยวชาญ

2. การวิเคราะห์ข้อมูล

ดำเนินการวิเคราะห์เนื้อหา (Content Analysis) การวิเคราะห์เปรียบเทียบ (Comparison Analysis) และสังเคราะห์ข้อมูล (Synthesis) จากทฤษฎี หลักการที่เกี่ยวข้อง ทั้งในและต่างประเทศ

3. การนำเสนอข้อมูล

นำเสนอข้อมูลแบบรายงานวิจัยเชิงพรรณนาและวิเคราะห์ ได้ผลงานที่เป็นแนวคิดใหม่ ๆ จากการวิจัย

ผลการวิจัย

ผลการวิจัยจากวัตถุประสงค์การวิจัยข้อที่ 1 การปฏิบัติการไซเบอร์ พบว่า

1. การปฏิบัติการสนับสนุนทางไซเบอร์ ได้แก่ 1.1 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการข้อมูลข่าวกรองทางทหาร (Military Intelligence Support : MIS) และ 1.2 การปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร (Information Operations Support : IO Support)

2. การปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operations : DCO) ได้แก่ 2.1 การป้องกัน (Protect) 2.2 การตรวจจับ (Detect) 2.3 การตอบสนอง (React) และ 2.4 การฟื้นฟู (Recover)

3. การปฏิบัติการไซเบอร์เชิงป้องปราม (Offensive Cyber Operations : OCO) ได้แก่ 3.1 การรวบรวมข้อมูลเป้าหมาย (Information Gathering) 3.2 การตรวจสอบหาช่องโหว่ของระบบ (Vulnerability Identification) 3.3 การปฏิบัติการโจมตี (Attack) 3.4 การเปิดช่องโหว่เพื่อการปฏิบัติครั้งต่อไป (Maintaining Access) และ 3.5) การลบร่องรอยการโจมตี (Covering Tracks)

ผลการวิจัยจากวัตถุประสงค์การวิจัยข้อที่ 2 การปฏิบัติการสงครามอิเล็กทรอนิกส์ พบว่า

1. การสนับสนุนทางอิเล็กทรอนิกส์ (Electronic Support : ES) ได้แก่ การปฏิบัติการค้นหา ดักรับ พิสูจน์ทราบ บันทึก และวิเคราะห์

2. การป้องกันทางอิเล็กทรอนิกส์ (Electronic Protection : EP) ได้แก่ การลดการถูกตรวจจับด้วย Stealth, RAM Coating หรือ EMCON ของอากาศยาน การใช้เทคนิค Pulse Compression หรือ Frequency Hopping กับเรดาร์ของเรา การใช้เทคนิค Home-on-Jam ในอาวุธปล่อยนำวิถี ปฏิบัติการ Radar Jamming จากอากาศยาน

3. การโจมตีทางอิเล็กทรอนิกส์ (Electronic Attack : EA) ได้แก่ 3.1 มาตรการต่อต้าน ได้แก่ การแพร่กระจายคลื่น (Active) ประกอบด้วยการก่อกวน (Jamming) และการลวง (Deception) แบบไม่แพร่กระจายคลื่น (Passive ECM) ประกอบด้วย 3.1.1 ชาฟฟ์ (Chaff) 3.1.2 แฟลร์ (Flares) และ 3.1.3 อากาศยานเป้าลวงหรือโดรน (Decoy or Drones) 3.2 มาตรการตอบโต้การต่อต้านทางอิเล็กทรอนิกส์ (Electronic Counter Counter Measures: ECCM)

ผลการวิจัยจากวัตถุประสงค์การวิจัยข้อที่ 3 การบูรณาการเชื่อมโยงขีดความสามารถเพื่อทวีกำลังด้านความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ พบว่า

1. ปฏิบัติการไซเบอร์เชิงป้องกัน สามารถใช้การป้องกันทางอิเล็กทรอนิกส์ การสนับสนุนทางอิเล็กทรอนิกส์ และการป้องกันทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้นด้านการฟื้นฟู

2. การปฏิบัติการไซเบอร์สนับสนุน สามารถใช้การสนับสนุนทางอิเล็กทรอนิกส์ และการ เพื่อทวีกำลังได้ทุกด้าน

3. การปฏิบัติการไซเบอร์เชิงป้องปราม สามารถใช้ การสนับสนุนทางอิเล็กทรอนิกส์ และโจมตีทางอิเล็กทรอนิกส์ เพื่อทวีกำลังได้เกือบทุกด้าน ยกเว้น ด้านการเปิดช่องโหว่ และด้านการลบร่องรอยการโจมตี

ข้อเสนอแนะ

1. ข้อเสนอแนะระดับยุทธศาสตร์

1.1 ให้เพิ่มเติมการปฏิบัติการร่วมเพื่อทวีกำลังระหว่าง การปฏิบัติการไซเบอร์ และการปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อเป็นแนวทางดำเนินการอย่างเป็นรูปธรรม ที่สอดคล้องกับยุทธ์ศาสตร์กองทัพอากาศ โดยกำหนดเป็นกลยุทธหลักในการดำเนินการ

1.2 แต่งตั้งผู้รับผิดชอบดำเนินการตรวจสอบสภาพแวดล้อมรอบด้านอย่างละเอียด ถึงปัจจัยที่ส่งผลต่อระดับความสำเร็จในการดำเนินการ ทรัพยากรที่จำเป็น และคุณูประการที่จะเกิดขึ้น ความเสี่ยง จนสามารถนำไปสู่การกำหนดยุทธศาสตร์ดำเนินการได้อย่างเป็นรูปธรรม และ ส่งผลต่อความสัมฤทธิ์ในการปฏิบัติการของกองทัพอากาศ

1.3 อนุมัติงบประมาณ และแนวทางในการจัดหาบุคลากร เทคโนโลยี เครื่องมือเครื่องใช้ ตลอดจนซอฟแวร์ที่จำเป็น

2. ข้อเสนอแนะระดับยุทธวิธี

2.1 กำหนดให้มี คณะกรรมการ คณะทำงาน หรือคณะเจ้าหน้าที่ แปลงนโยบายลงสู่การปฏิบัติในรูปแบบของการคร่อมสายงาน และรายงานผลต่อผู้บัญชาการทหารอากาศโดยตรง

2.2 ปรับปรุงอาคารสถานที่ ให้เหมาะสมในการบรรจุเทคโนโลยีมูลค่าสูง เพื่อให้สามารถใช้งานได้เกิดประโยชน์ต่อกองทัพอากาศระดับสูงสุด

2.3 พัฒนาองค์ความรู้และบุคลากรกองทัพอากาศ ด้านไซเบอร์ สงครามอิเล็กทรอนิกส์ตลอดจนสนับสนุนให้สร้างงานวิจัยอย่างต่อเนื่อง

3. ข้อเสนอแนะระดับปฏิบัติการ

3.1 หัวหน้าหน่วยขึ้นตรงทุกระดับให้ความสำคัญ และกระตุ้นให้ผู้ใต้บังคับบัญชาตระหนักถึงความมั่นคงปลอดภัยไซเบอร์ โดยถือเป็นข้าศึกในยุคปัจจุบัน และกองทัพอากาศอาจถูกโจมตีได้ทุกวินาที

3.2 ปรับปรุงกฎ ระเบียบ คำสั่งที่เกี่ยวข้องให้สอดคล้องกับยุทธศาสตร์ที่ปรับปรุงขึ้นใหม่

4. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

4.1 ศึกษา วิเคราะห์เชิงลึก ด้านความพร้อมและการเตรียมทรัพยากรทุกประเภทของกองทัพอากาศที่จำเป็นในการสนับสนุนด้านสงครามอิเล็กทรอนิกส์ เพื่อทวีความได้เปรียบด้านความมั่นคงปลอดภัยไซเบอร์

4.2 ศึกษา วิเคราะห์เชิงลึก การปฏิบัติการสงครามอิเล็กทรอนิกส์ ในแต่ละด้านเพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์ ตลอดจนวิเคราะห์ข้อได้เปรียบ และข้อด้อยที่อาจพบได้จากการปฏิบัติการ

4.3 ศึกษา โครงการนำร่องการปฏิบัติการสงครามอิเล็กทรอนิกส์เพื่อสนับสนุนความมั่นคงปลอดภัยไซเบอร์