เอกสารวิจัยส่วนบุคคล

เรื่อง

ชื่อเอกสารวิจัย แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ใน กองทัพอากาศ

โดย

นาวาอากาศโท บุรีรัตน์ เข็มทอง

หลักสูตรเสนาธิการทหารอากาศ

รุ่นที่ ๖๖ ปีการศึกษา ๒๕๖๕

โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ

กองทัพอากาศ

ดอนเมือง กรุงเทพมหานคร

หนังสือรับรอง

คณะกรรมการเอกสารวิจัยโรงเรียนเสนาธิการทหารอากาศได้ตรวจและรับรองว่าเอกสารวิจัยส่วนบุคคล เรื่อง แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ของ นาวาอากาศโท บุรีรัตน์ เข็มทอง นายทหารนักเรียน โรงเรียนเสนาธิการทหารอากาศ รุ่นที่ ๖๖ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรเสนาธิการกิจ ประจำปีการศึกษา ๒๕๖๕

พลอากาศตรี
(ปิยะกิตติ์ สุทธิวัฒน์ธนากูล)
ผู้บัญชาการโรงเรียนเสนาธิการทหารอากาศ

นาวาอากาศเอก
(ภิญโญ ศรีวิริยะ)
ที่ปรึกษาเอกสารวิจัยโรงเรียนเสนาธิการทหารอากาศ

นาวาอากาศเอก
(สุวิทย์ ไท้ทอง)
อาจารย์ผู้รับผิดชอบเอกสารวิจัยโรงเรียนเสนาธิการทหารอากาศ

บทคัดย่อ

เอกสารวิจัยเรื่อง	แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ
ชื่อนักศึกษา	นาวาอากาศโท บุรีรัตน์ เข็มทอง
ที่ปรึกษา	นาวาอากาศเอก ภิญโญ ศรีวิริยะ
อาจารย์ผู้รับผิดชอบ	นาวาอากาศเอก สุวิทย์ ไท้ทอง

เอกสารวิจัยเรื่อง แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ จัดทำขึ้น โดยมีวัตถุประสงค์เพื่อสร้างแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศเพื่อวิเคราะห์ขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ในกองทัพอากาศ พร้อมนำเสนอ ตัวแบบของแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศที่สอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยกำหนดขอบเขตการวิจัยด้านเนื้อหาที่เกี่ยวข้องกับข่าวกรองไซเบอร์ในกองทัพอากาศ ที่รับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศเท่านั้นการวิจัยครั้งนี้ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพเพื่อพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เชิงแนวคิด (Conceptual) และรวบรวมข้อมูลที่ได้จากบทความตาราวิชาการงานวิจัยและ เอกสารที่เกี่ยวข้อง (Documentary Research) ตามยุทธศาสตร์และนโยบายระดับชาติ ตลอดจนกองทัพอากาศ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และข่าวกรองไซเบอร์ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของแนวทางข่าวกรองไซเบอร์ของต่างประเทศเปรียบเทียบกับแนวทางของกองทัพอากาศไทยในปัจจุบัน ผลการวิจัยพบว่าขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่จำเป็น คือ การระบุถึงภัยคุกคามและหนทางปฏิบัติของฝ่ายตรงข้าม การจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อสนับสนุนการปฏิบัติการไซเบอร์เชิงรุก และเชิงรับทั้งนี้ ผู้วิจัยได้นำเสนอรูปแบบการพัฒนาวงรอบการปฏิบัติการข่าวกรองทางไซเบอร์ ตามแนวทาง DIAMOND MODELที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ผู้วิจัยมีข้อเสนอแนะเกี่ยวกับแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ คือ ผู้บังคับบัญชาจะต้องให้ความสำคัญโดยหน่วยงานด้านการข่าว ควรมีบทบาทนำในการปฏิบัติ โดยพัฒนาขีดความสามารถของผู้ปฏิบัติงานข่าวกรองไซเบอร์ในระดับยุทธการ และยุทธวิธี ให้มีทักษะทั้งด้านการข่าวกรองและการปฏิบัติการไซเบอร์ควบคู่กันและควรมีการผนึกกำลัง ระหว่างหน่วยงานข่าวกรองไซเบอร์ภายใน

กระทรวงกลาโหมและหน่วยงานภายนอกรวมทั้งมิตรประเทศ โดยกำหนดให้มีการแลกเปลี่ยนข้อมูลข่าวกรองไซเบอร์ในทุกภาคส่วนให้สามารถแลกเปลี่ยนข้อมูลข่าวสาร และช่วยเหลือซึ่งกันและกันในกรณีที่เกิดสถานการณ์วิกฤตทางไซเบอร์ได้

Abstract

Research Title guideline for developing cyber intelligence capabilities in the Royal Thai Airforce

Name Wing Commander Burirat Khemthong

Research Consultant Group Captain Pinyo Sriwiriya

Research Advisor Group Captain Suwit Thithong

The objectives of this research were to study capabilities of cyber intelligence in supporting cyber security measures and the practice of cyber intelligence of the Royal Thai Air Force, to analyze capabilities of the cyber intelligence in the Royal Thai Air Force, and to present a model of cyber intelligence in the Royal Thai Air Force that is in accordance with national strategies and policies. The research was framed with the cyber intelligence in the Royal Thai Air Force according to the national strategies and policies.

The research conducted the qualitative approach, using primary data, i.e., articles from textbooks, research papers and related documents; The data was analyzed with the critical approach. The research found that cyber intelligence in the Royal Thai Air Force had capabilities were identifying threats and practice, building cyber security database, preparing cyber environment, and cyber targeting to support proactive measures. This research presented Diamond model. The Diamond model is the cyber intelligence model that is in accordance with the cyber security of Royal Thai Air Force The research suggested that the executive officers should focus on cyber intelligence. The intelligence units should play an important role in implementation and the Royal Thai Air Force should improve the structure of the intelligence units and improve the cyber intelligence officers in the operational and strategic levels. The officers should be skillful in intelligence and cyber practice. Furthermore, there should be collaboration among the cyber intelligence units of the Ministry of Defence, other units, and other

countries. This could be done by linking database to every unit in order to exchange intelligence and assist each other in case of cyber emergency situation.

คำนำ

การศึกษาวิจัยเรื่อง “แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ” มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ให้ทราบถึงขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ และนำเสนอตัวแบบของแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่สามารถรับมือกับ ภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยมุ่งหวังให้ สามารถนำไปใช้เป็นตัวแบบแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ของหน่วยงาน หรือสถาบันศึกษาที่เกี่ยวข้องกับความมั่นคง หรือนำไปประยุกต์ใช้ในการศึกษาและปรับปรุงให้ตัวแบบ มีความสมบูรณ์และเหมาะสมต่อไป

ผลงานวิจัยฉบับนี้ ได้รับการสนับสนุนด้วยดีจากผู้บังคับบัญชา คณาจารย์ และเจ้าหน้าที่ของโรงเรียนเสนาธิการทหารอากาศทุกท่านที่ได้ให้ความกรุณา เอื้อเฟื้อตลอดระยะเวลา ที่ผู้วิจัยเข้ารับการศึกษาอบรม จึงขอขอบพระคุณทุกท่านไว้ ณ โอกาสนี้ และผู้วิจัยหวังเป็นอย่างยิ่งว่า ผลงานวิจัยฉบับนี้ จะเป็นประโยชน์ต่อการเสริมสร้างขีดความสามารถ และการพัฒนาข่าวกรองไซเบอร์ของกองทัพอากาศต่อไป

(ลงชื่อ) นาวาอากาศโท

(บุรีรัตน์ เข็มทอง)

นายทหารนักเรียนโรงเรียนเสนาธิการทหารอากาศ รุ่นที่ ๖๖

มิถุนายน ๒๕๖๕

กิตติกรรมประกาศ

ขอขอบคุณโรงเรียนเสนาธิการทหารอากาศ ที่ได้จัดหลักสูตรให้มีการทำวิจัยนี้ รวมทั้งคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทความรู้ แนวคิด และแนวทาง อย่างเต็มความสามารถ

ขอขอบคุณ นาวาอากาศเอก สุวิทย์ ไท้ทอง อาจารย์ผู้รับผิดชอบเอกสารวิจัย ที่คอยเมตตาให้คำแนะนำ ตรวจสอบ กำกับดูแล ตลอดจนติดตามความก้าวหน้าในการวิจัยอย่างสม่ำเสมอ และขอขอบคุณ นาวาอากาศเอก ภิญโญ ศรีวิริยะ ที่ปรึกษาเอกสารวิจัย ที่กรุณาให้คำปรึกษา คำชี้แนะตลอดจน ผู้บังคับบัญชา ข้าราชการ ในศูนย์ไซเบอร์ กองทัพอากาศ ที่คอยสนับสนุนทำให้เอกสารวิจัยฉบับนี้สำเร็จลุล่วงด้วยดี

ขอขอบคุณ พลอากาศตรี พงษ์สวัสดิ์ จันทสาร เจ้าของผลงานเอกสารวิจัย หลักสูตรการป้องกันราชอาณาจักรรุ่นที่ ๖๐ ปีการศึกษา ๒๕๖๑ ผู้ซึ่งจุดประกายความคิดในการทำเอกสารวิจัยฉบับนี้

ขอขอบคุณเพื่อนนายทหารนักเรียนหลักสูตรเสนาธิการทหารอากาศรุ่นที่ ๖๖ ที่เป็นเพื่อนร่วมคิด เป็นมิตรร่วมทาง ในระหว่างจัดทำเอกสารวิจับฉบับนี้ และสุดท้ายที่สำคัญที่สุดคือ ครอบครัวอันประกอบด้วย มารดา และภรรยา ที่คอยให้กำลังใจเป็นอย่างดี ในการจัดทำเอกสารวิจัยฉบับนี้

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญภาพ

บทที่ ๑
บทนำ

๑. ความสำคัญและที่มาของปัญหาวิจัย

(Cyber Space) กลายเป็นศัพท์ใหม่ที่ได้รับการยอมรับในสังคมโลกอย่างรวดเร็ว และเป็นสิ่งที่จำเป็นต้องเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้ ไซเบอร์สเปซ คือเครือข่ายอินเทอร์เน็ตที่เป็นโครงสร้างพื้นฐานหลัก และมีคอมพิวเตอร์รวมถึงอุปกรณ์ทุกอย่างเชื่อมต่อเข้ากับระบบเครือข่ายอินเทอร์เน็ตและระบบเครือข่ายย่อยขององค์กร[๑]โดยรวมถึงเครือข่ายย่อยส่วนบุคคล และไม่จำเป็นต้องเป็นเครื่องคอมพิวเตอร์ ซึ่งรวมอุปกรณ์ที่เชื่อมต่อกับอินเตอร์เน็ต Internet of Things (IoT) อาทิเช่น กล้องวงจรปิด อุปกรณ์ไฟฟ้าที่ใช้ในครัวเรือน เป็นต้น ดังนั้นข้อมูลจำนวนมหาศาลจึงเดินทางไปในมิติไซเบอร์เพื่อตอบสนองความสะดวกสบาย รวดเร็ว การแลกเปลี่ยนข้อมูลข่าวสาร การลดความซับซ้อนของการทำงาน และการใช้บริการข้อมูลต่าง ๆ

อย่างไรก็ตาม ปริมาณการใช้งานรวมถึงจำนวนผู้ใช้ที่เพิ่มขึ้น กลับเปิดโอกาสให้กับกลุ่มมิจฉาชีพที่มุ่งแสวงหาผลประโยชน์จากการก่ออาชญากรรมทางไซเบอร์(hacker)เพิ่มขึ้นด้วยเช่นกัน จากที่กล่าวมานั้นคือภัยคุกคามทางไซเบอร์(Cyber Threat) ซึ่งมีความสำคัญในยุคปัจจุบัน เพราะมีแนวโน้มความรุนแรงที่ส่งผลกระทบต่อชีวิตและทรัพย์สินมากขึ้นตามลำดับอย่างหลีกเลี่ยงไม่ได้ นอกจากนี้ยังส่งผลกระทบต่อระบบโครงสร้าง พื้นฐานสำคัญของประเทศ (critical infrastructure) ได้แก่ กลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เช่น กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค กลุ่มสาธารณสุข เป็นต้น ส่งผลกระทบต่อความมั่นคงปลอดภัยของประเทศในภาพรวม จะเห็นได้ว่า ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามรูปแบบใหม่ ที่เน้นกระทำต่อ ระบบอินเทอร์เน็ตและระบบเครือข่ายคอมพิวเตอร์ ทำให้ประชาคมโลกเริ่มตื่นตัวและตระหนักถึงภัยคุกคามดังกล่าว

ตัวอย่าง ภัยคุกคามทางไซเบอร์ที่โจมตีโครงสร้างพื้นฐานสำคัญในระดับโลก เช่น เหตุการณ์ทาง ไซเบอร์ที่เพิ่งเกิดขึ้นคือ บริษัท Colonial Pipeline ฝั่งตะวันออกของสหรัฐอเมริกาโดนโจมตีด้วยโปรแกรมประสงค์ร้ายเรียกค่าไถ่(ransomware) โดยยึดข้อมูลเกือบ ๑๐๐ กิกะไบต์เป็นประกัน[๒]ทำให้ระบบการขนส่งน้ำมันผ่านท่อลำเลียงล่ม ต้องปิดทำการและกลับมาใช้การขนส่งสำรอง ซึ่งหาก hacker มุ่งทำลายระบบการขนส่งน้ำมันอาจทำให้เกิดอันตรายต่อชีวิตพนักงานของบริษัท Colonial Pipeline และประชาชนบริเวณโดยรอบได้

---

[๑] (๒๐๑๘). “Joint Publication ๓-๑๒ cyberspace operations”. accessed ๒๐๒๑, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/.

ในระดับประเทศ โรงพยาบาลสระบุรีได้ตกเป็นเป้าหมายของการโจรกรรมข้อมูลด้วยโปรแกรมประสงค์ร้ายเรียกค่าไถ่[๒] ทำให้แพทย์และพยาบาลทำงานล่าช้าลงเนื่องจากไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้ โดยทางโรงพยาบาลสระบุรีได้ออกมาประกาศผู้ใช้บริการโรงพยาบาลทุกคนทราบว่าระบบคอมพิวเตอร์ของโรงพยาบาลกำลังถูกเข้ารหัสข้อมูลทำให้ไม่สามารถเข้าถึงข้อมูลผู้ป่วยที่อยู่ในเซิร์ฟเวอร์ได้ ซึ่งข้อมูลซึ่งถูกเข้ารหัสนั้นล้วนเป็นข้อมูลผู้ป่วยในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษา และวินิจฉัยโรคเป็นอย่างมาก ซึ่งในเหตุการณ์นี้อาจทำให้มีผู้เสียชีวิตได้ เนื่องจากความล่าช้าในการรักษา ในกองทัพอากาศ ศูนย์ข้อมูลคอมพิวเตอร์ สอ.ทอ.ถูกแฮกเกอร์โจมตีระบบฐานข้อมูลควบคุม บริหารจัดการบัญชี ทำให้ข้อมูล Username/Password ทอ.รั่วไหล[๓] และถูกเรียกค่าไถ่ส่งผลกระทบต่อการปฏิบัติงานด้วยระบบเทคโนโลยีสารสนเทศของกองทัพอากาศ

จากเหตุการณ์ข้างต้น แสดงให้เห็นว่าภัยคุกคามทางไซเบอร์มีความรุนแรงในทุกระดับ ดังนั้นเพื่อเป็นการรับมือกับภัยคุกคามทางไซเบอร์ กระทรวงกลาโหมจึงได้อนุมัติให้จัดตั้งศูนย์ไซเบอร์ขึ้นในทุกเหล่าทัพ

ในส่วนกองทัพอากาศ ได้ตระหนักถึงความจำเป็นในการหาวิธีการป้องกันและรับมือกับภัยคุกคามดังกล่าวอย่างเป็นรูปธรรม จึงได้จัดตั้ง ศูนย์ไซเบอร์กองทัพอากาศ และกำหนดให้มีกิจการมิติไซเบอร์ ในยุทธศาสตร์ ๒๐ ปี โดยมุ่งพัฒนาขีดความสามารถด้านการปฏิบัติการไซเบอร์ของกองทัพอากาศ พัฒนาเทคโนโลยี โครงสร้างพื้นฐาน โครงสร้างองค์กร บุคลากร และองค์ความรู้ เพื่อป้องกันภัยคุกคามทางไซเบอร์ ตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ (Cyber Security)[๔] รวมทั้งการเตรียมความพร้อมในการปฏิบัติการเชิงรุก และแสวงหาความร่วมมือกับหน่วยงานทั้งภายในและภายนอกประเทศ เช่น การประชุมประชาคมไซเบอร์ การฝึกการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนภายนอกประเทศ เช่น การประชุมผู้เชี่ยวชาญทางไซเบอร์ระหว่างไทยอเมริกา และมิตรประเทศรอบบ้าน เพื่อแลกเปลี่ยนองค์ความรู้ไซเบอร์ เพื่อนำมาประยุกต์ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งหากถูกโจมตีทางไซเบอร์ต่อระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ก็สามารถรับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ และสามารถกู้คืนระบบและฟื้นตัวให้สามารถกลับมาใช้งานตามปกติได้อย่างรวดเร็ว

กองทัพอากาศ ได้นำการปฏิบัติการไซเบอร์[๕]มาปรับใช้เป็นหลักนิยมการปฏิบัติการไซเบอร์ของกองทัพอากาศ หรือ (Cyber Conops) ซึ่งประกอบด้วย การปฏิบัติการข่าวกรองไซเบอร์ การ

---

[๒] (๑๐ ก.ย. ๒๕๖๓) “แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง ๖.๓ หมื่นล้านบาท”, สืบค้นเมื่อ ๒๕๖๕ https://www.thairath.co.th/news/local/central/1926912

[๓] “สรุปผลการตรวจสอบเหตุการณ์ข้อมูล Username/Password ทอ.รั่วไหล”ก.ค.๒๕๖๓.

[๔] “Cyber Security”.accessed 2021, http://www.rdpb.go.th/MediaUploader/File/10166/CyberSecurity

[๕] SCOTT JASPER.(2020) “RUSSIAN CYBER OPERATIONS”

ปฏิบัติ การไซเบอร์เชิงป้องปราม การปฏิบัติการไซเบอร์เชิงป้องกัน[๖] กล่าวคือ การปฏิบัติการข่าวกรองไซเบอร์ มีเป้าหมายเพื่อ วางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับเพื่อให้ประสบความสำเร็จในการปฏิบัติการไซเบอร์ **ซึ่งมีหลักการมาจาก**ง**านข่าวกรองใน**ปฏิบัติการทางทหารมักใช้เทคโนโลยีด้านการข่าวที่มีมิติไซเบอร์เป็นสื่อกลางในการค้นหา รวบรวม ดักฟัง ขโมยข้อมูลของฝ่ายตรงข้าม เพื่อช่วงชิงความได้เปรียบในเรื่องข้อมูลข่าวสารเพื่อประกอบการตัดสินใจของผู้บังคับบัญชา โดยมุ่งพัฒนาระบบรวบรวมข้อมูลด้านการปฏิบัติการลาดตระเวนในมิติไซเบอร์ของข้าศึก เพื่อจัดทำบัญชีเป้าหมายทางไซเบอร์

งานข่าวกรองไซเบอร์ หรือ(Cyber Intelligence)[๗] มีการปฏิบัติเช่นเดียวกับงานข่าวกรองในมิติอื่นๆ โดยมีรูปแบบและวงรอบข่าวกรอง กล่าวคือ การอำนวยการ การรวบรวม การประมวลผล การวิเคราะห์ การเผยแพร่ใช้ประโยชน์ และการเสนอแนะ ซึ่งหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ คือ การระบุถึงภัยคุกคามและหนทางปฏิบัติของฝ่ายตรงข้าม การจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ การจัดทำเป้าหมายทางไซเบอร์เพื่อสนับสนุนการปฏิบัติการไซเบอร์เชิงป้องปราม และการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ หรือ (Intelligence Preparation of the Cyber Environment: IPCE) ตัวอย่าง การดำเนินงานที่ผ่านมา คือการจัดทำแฟ้มบัญชีเป้าหมายทางไซเบอร์ เพื่อสนับสนุนข้อมูลในทำเนียบกำลังรบของประเทศตรงข้าม ด้วยเหตุนี้ผู้วิจัยจึงมีความสนใจที่จะศึกษาวิจัย เรื่อง “แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ” เพื่อศึกษาวิเคราะห์ หาแนวทางพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่สมควรจะต้องได้รับการพัฒนาอย่างเป็นรูปธรรม ซึ่งการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพและประสบความสำเร็จนั้น จำเป็นอย่างยิ่งที่จะต้องมีงานข่าวกรองไซเบอร์ที่เข้มแข็ง ซึ่งถือเป็นความท้าท้ายใหม่ของกองทัพอากาศ ที่ยังขาดบุคลากรและองค์ความรู้ ในการพัฒนาข่าวกรองไซเบอร์ในระดับกลาโหม ผู้วิจัยจึงมีความสนใจในการศึกษาวิจัยเพื่อจัดทา “แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ” เพื่อให้หน่วยงานและบุคคลที่เกี่ยวข้อง สามารถนำไปใช้ประโยชน์ต่อไป

๒. วัตถุประสงค์การวิจัย

สร้างแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

---

[๖] “หลักนิยมการปฏิบัติการไซเบอร์”๒๕๖๓.

[๗] (2013). “Joint Publication 2-0 joint intelligence”.accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

๓. คำถามการวิจัย

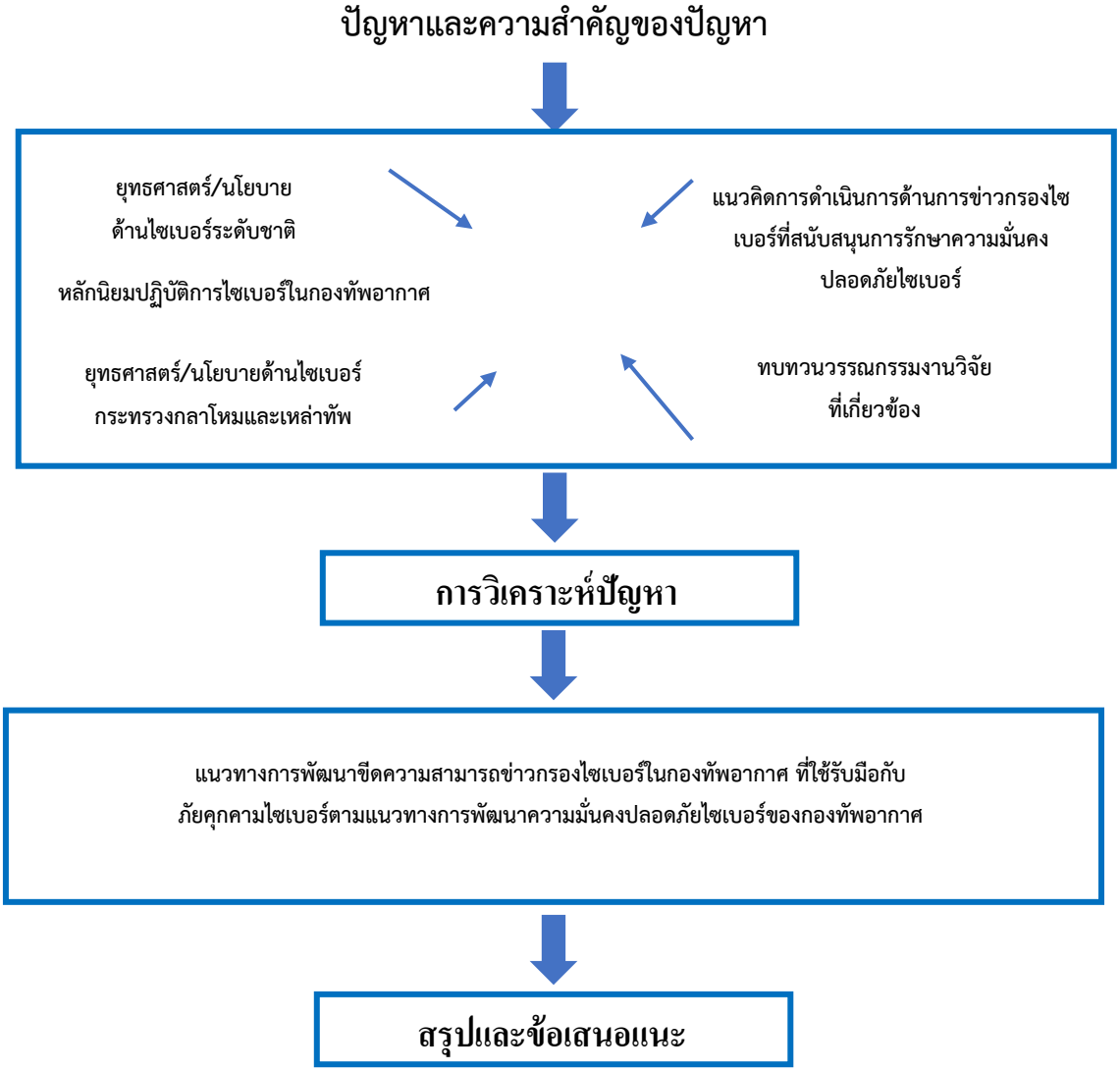
การพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศมีแนวทางอย่างไร

๔. ขอบเขตของการวิจัย

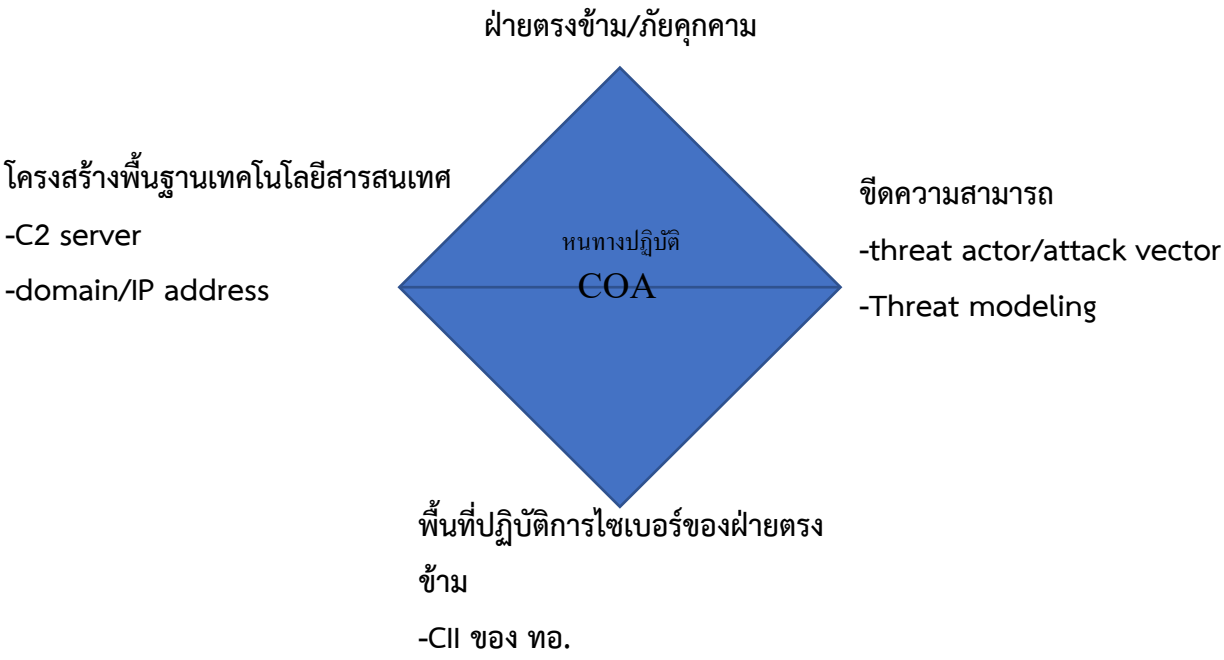
การวิจัยครั้งนี้มุ่งเน้นศึกษายุทธศาสตร์และนโยบายที่เกี่ยวข้องกับข่าวกรองไซเบอร์ในกองทัพอากาศ ที่รับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศเท่านั้น

๕. วิธีการวิจัย

ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ เพื่อพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เชิงแนวคิด (Conceptual) และรวบรวมข้อมูลที่ได้จากบทความตาราวิชาการงานวิจัย และ เอกสารที่เกี่ยวข้อง (Documentary Research) ตามยุทธศาสตร์และนโยบายระดับชาติ ตลอดจนกองทัพอากาศ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และข่าวกรองไซเบอร์ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของแนวทางข่าวกรองไซเบอร์ของต่างประเทศเปรียบเทียบกับแนวทางของกองทัพอากาศไทยในปัจจุบัน


ปัญหาและความสำคัญของปัญหา
ยุทธศาสตร์/นโยบาย
ด้านไซเบอร์ระดับชาติ
หลักนิยมปฏิบัติการไซเบอร์ในกองทัพอากาศ
ยุทธศาสตร์/นโยบายด้านไซเบอร์
กระทรวงกลาโหมและเหล่าทัพ
แนวคิดการดำเนินการด้านการข่าวกรองไซ
เบอร์ที่สนับสนุนการรักษาความมั่นคง
ปลอดภัยไซเบอร์
ทบทวนวรรณกรรมงานวิจัย
ที่เกี่ยวข้อง
การวิเคราะห์ปัญหา
แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่ใช้รับมือกับ
ภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ
สรุปและข้อเสนอแนะ

๖. กรอบแนวคิดวิจัย



๗. ประโยชน์ที่คาดว่าจะได้รับ

๗.๑. ทราบแนวทางการพัฒนาข่าวกรองไซเบอร์ของกองทัพอากาศ

๗.๒. สามารถกำหนดขีดความสามารถข่าวกรองไซเบอร์ที่จำเป็นของงานข่าวกรองไซเบอร์ในกองทัพอากาศ

๗.๓. นำไปใช้รับมือกับภัยคุกคามทางไซเบอร์ในอนาคต ที่สอดคล้องกับแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ

๘. คำนิยามศัพท์เฉพาะ

ไซเบอร์ หมายถึง กิจกรรมที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ การสื่อสารข้อมูลคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์

ความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการและการดำเนินการเพื่อปกป้องป้องกัน การส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายใน

ระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อย ภายในประเทศ และความมั่นคงทางเศรษฐกิจ

ภัยคุกคามทางไซเบอร์ หมายความว่า หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

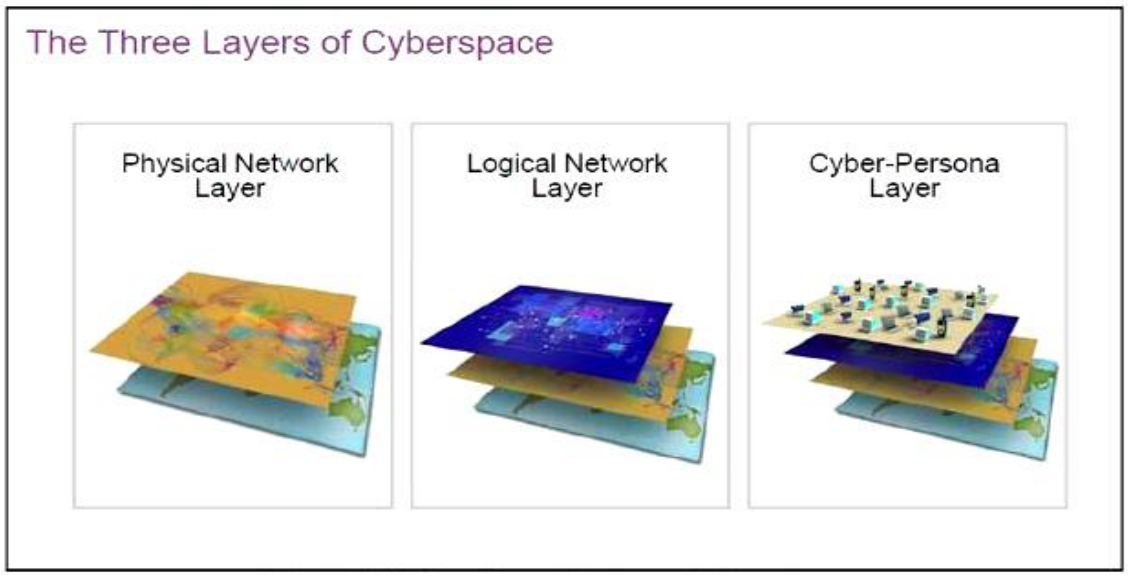
บทที่ ๒
การทบทวนวรรณกรรม

๑. แนวทางข่าวกรองไซเบอร์ของต่างประเทศเปรียบเทียบกับแนวทางของกองทัพอากาศไทยในปัจจุบัน

งานข่าวกรองไซเบอร์ (Cyber Intelligence) ถือเป็น กลไกหลักที่มีบทบาทสำคัญ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วย ซึ่งแนวความคิดในการปฏิบัติ ด้านการข่าวในมิติของไซเบอร์นั้น เป็นการดำเนินวงรอบข่าวกรอง เช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ โดยจะต้อง ดำเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ และจะต้องคัดสรรกำลังพลที่มีความรู้ทั้งในด้านการข่าวและการปฏิบัติการ ไซเบอร์มาปฏิบัติภารกิจดังกล่าว ซึ่งถือเป็นเรื่องที่ยากลำบาก

Joint Publication 3 - 12(R) Cyberspace Operations (5 Feb 2013) ได้กล่าวถึงกระบวนงานข่าวกรองไซเบอร์ ซึ่งมีส่วนสำคัญในการสนับสนุนการปฏิบัติการทางไซเบอร์ทั้งเชิงรับและเชิงรุก และเป็นการดำเนินการร่วมกันทั้งหน่วยข่าวในระดับกลาโหมและหน่วยข่าวระดับชาติทั้งภาครัฐและเอกชน เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรวดเร็วกว่าภัยคุกคามทางทหารซึ่งเป็นภัยคุกคาม ในรูปแบบเดิม ดังนั้นข่าวกรองที่ได้รับจากหลายภาคส่วนจะช่วยในการวิเคราะห์ ระบุสิ่งบอกเหตุ เพื่อทาให้ทราบถึงหนทางการปฏิบัติทางไซเบอร์ของฝ่ายตรงข้าม สำหรับการปฏิบัติการด้านการข่าวในมิติของไซเบอร์นั้น เป็นการดำเนินตามวงรอบข่าวกรอง เช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ ซึ่งจะดาเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ รวมทั้งการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการทางไซเบอร์เพื่อใช้ในการวางแผนสาหรับการปฏิบัติการไซเบอร์ สำหรับการปฏิบัติการข่าวในมิติทางไซเบอร์จะดำเนินการในทุกระดับชั้น ของมิติทาง ไซเบอร์[๘] ประกอบด้วย

๑. Physical Network Layer
๒. Logical Network Layer
๓. Cyber-Persona Layer



ภาพที่ ๑ การแบ่งระดับชั้นต่าง ๆ ในมิติไซเบอร์

ที่มา : Joint Publication ๓ – ๑๒ Cyberspace Operations, Online, ๒๐๑๘

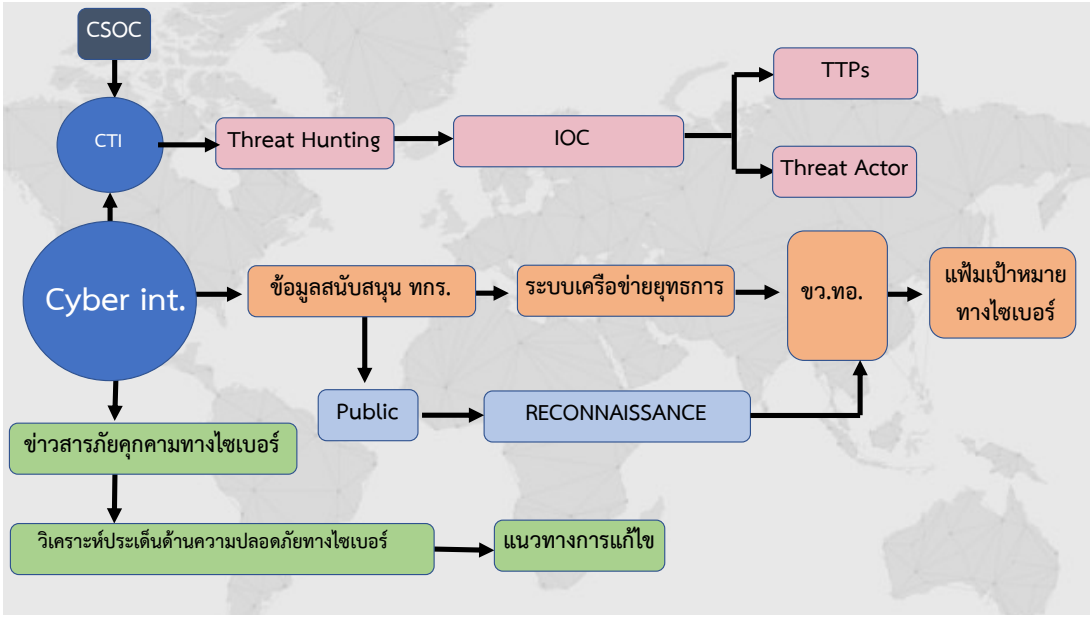
กระบวนการวงรอบข่าวกรองในการปฏิบัติการไซเบอร์ ประกอบด้วย

๑. การวางแผนรวบรวมข่าวสาร
๒. การรวบรวมข่าวสาร รวมทั้งการปฏิบัติการเฝ้าตรวจและการลาดตระเวน
๓. กระบวนการประมวลผลข้อมูลและแสวงหาประโยชน์
๔. การวิเคราะห์ข้อมูลและดาเนินกรรมวิธีผลิตข่าวกรอง
๕. การกระจายข่าวกรอง
๖. การประเมินผลคุณภาพและประสิทธิภาพของข่าวกรอง

ในระดับยุทธการ ข่าวกรองไซเบอร์เชิงเทคนิค (Cyber Threat Intelligence : CTI) ใช้ระบุเทคนิคยุทธวิธี หรืออาวุธทางไซเบอร์ของฝ่ายตรงข้าม เช่นข้อมูลภัยคุกคาม ไซเบอร์ รวมทั้งขีดความสามารถ (Capabilitiy) โดยนำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์(Cyber Threat Target Folder) เพื่อเตรียมการปฏิบัติการไซเบอร์เชิงรุก ส่วนการปฏิบัติการเชิงรับจะให้ความสนใจกับภัยคุกคามไซเบอร์ เพื่อเตรียมการระวังป้องกัน เนื่องจากภัยคุกคามไซเบอร์ ไม่มีขอบเขต ทางภูมิศาสตร์จะเป็นใครก็ได้ทั่วทุกมุมโลก ไม่จำเป็นต้องมีประเด็นขัดแย้งหรือมีพรมแดนติดกับประเทศไทย เช่น กรณีการปล่อยมัลแวร์เรียกค่าไถ่ Wanna Cry โดยเกาหลีเหนือ[๘] กองทัพอากาศก็ได้รับผลกระทบ ทั้ง

[๘] (๒๕๖๐).“พบเกาหลีเหนืออาจพัวพันเหตุมัลแวร์โจมตีทั่วโลก ”. สืบค้นเมื่อ ๒๕๖๕, https://www.bbc.com/thai/international-39931940

ที่ไม่ใช่ เป้าหมายที่เกาหลีเหนือจะโจมตี ดังนั้น การป้องกันภัยคุกคามที่เกิดขึ้นจึงเริ่มต้นจากการหาข่าวภัยคุกคามไซเบอร์ทั่วโลก ทั้งที่มีรัฐชาติสนับสนุนหรือกลุ่มองค์กรอิสระ โดยติดตามข่าวสารจาก APT (Advanced Persistent Threat Groups) ที่วิเคราะห์โดยบริษัทด้านการป้องกันภัยคุกคาม ทางไซเบอร์ขั้นสูง โดยนำข่าวสารที่ได้มาวิเคราะห์และพิสูจน์ทราบเจตนารมณ์ ขีดความสามารถ รูปแบบการโจมตีของกลุ่มต่าง ๆ พร้อมกับการสำรวจตนเอง (Self Assessment) เพื่อป้องกันช่องโหว่ของระบบที่อาจถูกโจมตี หรือได้รับผลกระทบจากการโจมตีเหล่านั้น



ภาพที่ ๒ การปฏิบัติการข่าวกรองไซเบอร์ในกองทัพอากาศ

การปฏิบัติการข่าวกรองไซเบอร์ในกองทัพอากาศในปัจจุบัน ประกอบด้วย

๑. ภัยคุกคาม (Threat) สามารถระบุและตรวจสอบได้ว่าภัยคุกคามคือใคร ทราบถึงขีดความสามารถและหนทางปฏิบัติของภัยคุกคาม

๒. การรวบรวมข่าวสาร (Collection) เมื่อเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (IPCE) แล้วจะทำให้ทราบว่ายังขาดข้อมูลข่าวสาร/ข่าวกรองใดที่กระทบต่อการวิเคราะห์ภัยคุกคาม และทำให้สามารถรวบรวมข้อมูลข่าวสาร/ข่าวกรองในพื้นที่ปฏิบัติการได้อย่างเหมาะสม

๓. การกำหนดเป้าหมาย (Targeting) เมื่อทราบถึงคุณลักษณะสำคัญของสภาพแวดล้อมการปฏิบัติการและภัยคุกคามแล้ว จะทำให้การกำหนดเป้าหมายเพื่อตอบโต้ภัยคุกคามที่ทำการโจมตีฝ่ายเรานั้น ทำได้ง่ายขึ้น และตรงตามเจตนารมณ์ของผู้บังคับบัญชา

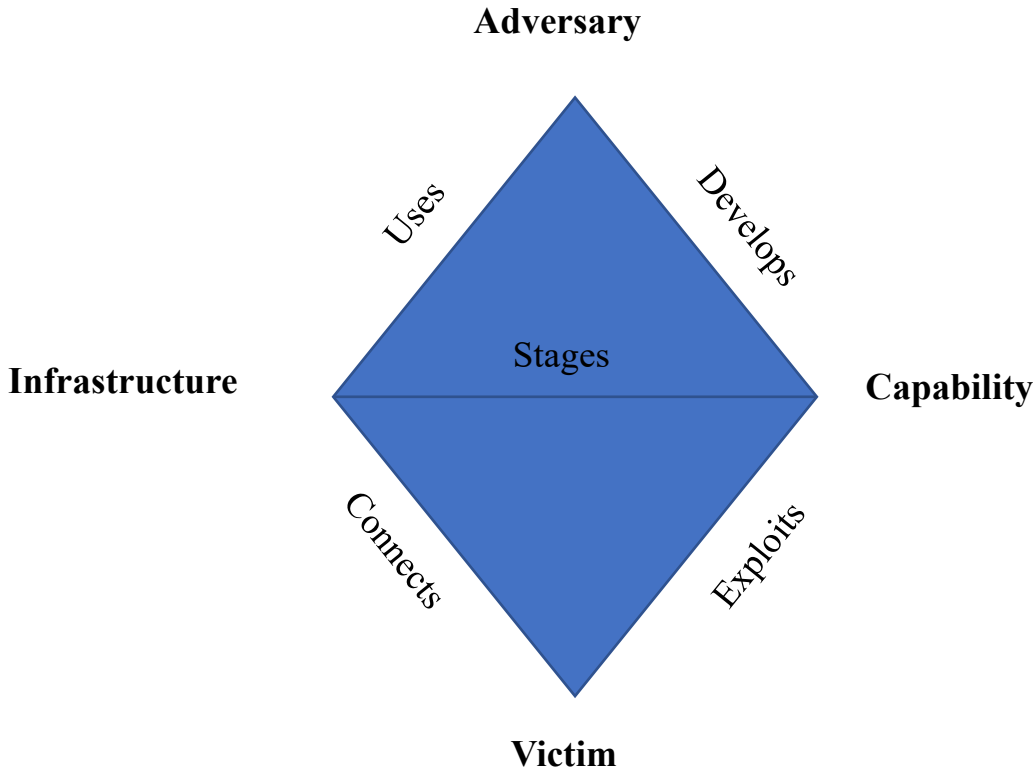
การดำเนินงานด้านข่าวกรองไซเบอร์ของกองทัพอากาศในปัจจุบันจะเป็นการประสานความร่วมมือระหว่าง กรมข่าวทหารอากาศ และศูนย์ไซเบอร์กองทัพอากาศ โดยกรมข่าวทหารอากาศมีหน้าที่ ติดตามสถานการณ์ ภัยคุกคามไซเบอร์ในระดับยุทธศาสตร์ และส่งข้อมูลให้ศูนย์ไซเบอร์กองทัพอากาศดำเนินการข่าวกรองไซเบอร์

๒. แนวทางการการประยุกต์ใช้การปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF กับการข่าวกรองไซเบอร์ในกองทัพอากาศ

จากการทบทวนวรรณกรรม การปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF และ SWOT Analysis การข่าวกรองไซเบอร์ในกองทัพอากาศทำให้ผู้วิจัยเข้าใจภาพแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่ใช้รับมือกับภัยคุกคามดังกล่าว โดยสิ่งที่กรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี กำหนดความต้องการในการป้องกันและรับมือกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ คือ การสร้างขีดความสามารถข่าวกรองไซเบอร์ ทั้งนี้ การที่งานด้านการข่าวกรองไซเบอร์จะสามารถสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเราทราบก่อนที่ภัยคุกคามต่าง ๆ จะทำการโจมตีทางไซเบอร์นั้น จำเป็นต้องทราบและสามารถระบุสภาพแวดล้อมของการปฏิบัติการให้ได้ก่อน และเมื่อทราบถึงคุณลักษณะสำคัญและ ผลกระทบของสภาพแวดล้อมการปฏิบัติการที่มีต่อฝ่ายเราแล้ว งานด้านการข่าวจะทราบว่าภัยคุกคามหรือศัตรูของฝ่ายเรานั้นคือใคร มีจุดมุ่งหมายอะไร มีขีดความสามารถ และมีหนทางปฏิบัติอย่างไร

USAF ได้ใช้กรอบแนวคิด ‘diamond model’ เพื่อช่วยจำแนกสิ่งที่ต้องการและดำเนินการตรวจสอบการเข้าควบคุมเครื่องเป้าหมายของ USAF โดยใช้ข้อมูลการค้นพบเพื่อสร้างข่าวกรองไซเบอร์และใช้ประโยชน์จากข้อมูลดังกล่าวเพื่อช่วยในการสอบสวนต่อไป ‘diamond model’ เป็นกรอบแนวคิดเพื่อสร้างตัวบ่งชี้ ดังนี้

ฝ่ายตรงข้าม –ผู้โจมตี, เป้าหมาย
โครงสร้างพื้นฐาน – คอมพิวเตอร์ โดเมน บัญชี ที่ถูกบุกรุกซึ่งใช้เป็นพร็อกซี ฯลฯ
ขีดความสามารถ – ชุดเครื่องมือ วิธีการ
เหยื่อ – ตัวชี้วัดของการถูกเข้าควบคุมเครื่อง, เป้าหมาย
สอดคล้องกับดำเนินการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการทางไซเบอร์



ภาพที่ ๓ กรอบแนวคิด ‘diamond model’

ที่มา: United States Air Force Cyberspace Threat Intelligence Process Overview[๙]

กระบวนการ

๑. ตรวจสอบภัยคุกคามเปรียบเทียบกับฐานข้อมูลข้อมูลในระบบจัดเก็บข้อมูลด้านการข่าวไซเบอร์เพื่อบ่งชี้ภัยคุกคาม

๒. ตรวจสอบขีดความสามารถของภัยคุกคามและตัวชี้วัดของการถูกเข้าควบคุมเครื่อง

๓. นำข้อมูลการรายงานภัยคุกคามเพื่อระบุ ขีดความสามารถภัยคุกคาม

๔. วิเคราะห์ขีดความสามารถภัยคุกคาม เพื่อหาแหล่งที่มา

[๙] United States Air Force Cyberspace Threat Intelligence Process

๕. หาแหล่งที่มาจากการเชื่อมต่อเครือข่ายภายนอกและค้นหาเบาะแสแวดล้อมเพื่อช่วยในการระบุแหล่งที่มา

๖. กำหนดขอบเขต/กำหนดการตอบสนองภัยคุกคาม/กำหนดการปฏิบัติการป้องปราม

๓. SWOT Analysis การข่าวกรองไซเบอร์ในกองทัพอากาศ

วิธีการ SWOT Analysis เพื่อค้นหาจุดแข็ง จุดอ่อน โอกาส และภัยคุกคาม และนำผลที่ได้มาปรับปรุงข้อบกพร่องและพัฒนา ซึ่งจะช่วยเสริมสร้างขีดความสามารถด้านข่าวกรองไซเบอร์ของ ทอ. ให้มีประสิทธิภาพมากยิ่งขึ้น

ปัจจัยภายใน (Internal Factor)

๑. จุดแข็ง (Strength)

มีการกำหนดยุทธศาสตร์กองทัพอากาศ ในการเป็น “One of the Best Air Forces in ASEAซึ่งทำให้ทอ.ต้องมีการเสริมความพร้อมในการปฏิบัติในทุกด้าน

๑.๑ ผู้บังคับบัญชาระดับสูงให้ความสำคัญกับการปฏิบัติการด้านข่าวกรองไซเบอร์

๑.๒ มีบุคลากรหลักที่มีความรู้ความสามารถด้านงานข่าวกรองไซเบอร์

๑.๓ มีหน่วยงานระดับนโยบายและปฏิบัติงานด้านข่าวกรองไซเบอร์

๑.๔ มีแผนเฉลิมอากาศที่จะปรับปรุงให้ครอบคลุมถึงการปฏิบัติการด้านข่าวกรองไซเบอร์

๑.๕ มีการพัฒนาบุคลากรด้วยการจัดแข่งขันปฏิบัติการด้านไซเบอร์ (Cyber Operations Contest)

๒. จุดอ่อน (Weakness)

๒.๑ ขาดเทคโนโลยีที่จะใช้ในงานด้านข่าวกรองไซเบอร์ที่ครอบคลุมและเพียงพอ

๒.๒ บุคลากรด้านงานข่าวกรองไซเบอร์ยังไม่เพียงพอกับความต้องการ และขาดงบประมาณในการพัฒนา

๒.๓ การจัดหาอุปกรณ์และเทคโนโลยีทันสมัยต้องพึ่งพาหน่วยงานภายนอก และต่างประเทศ

๒.๔ ขาดกรอบแนวความคิดในการปฏิบัติ (Concept of Operations)

ปัจจัยภายนอก (External Factor)

๓. โอกาส (Opportunity)

๓.๑ เทคโนโลยีด้านข่าวกรองไซเบอร์ ในรูปแบบ Open Source มีมากขึ้นและสามารถนำมาประยุกต์ใช้งานได้

๓.๒ องค์ความรู้ด้านงานข่าวกรองไซเบอร์จากแหล่งต่าง ๆ มีมากขึ้น

๓.๓ ภาครัฐให้ความสำคัญงานข่าวกรองไซเบอร์

๓.๔ ได้รับความร่วมมือที่ดีกับหน่วยงานภายในและภายนอก ทอ. รวมทั้งจากต่างประเทศ

๔. อุปสรรค (Threat)

๔.๑ ในหลายประเทศมีการพัฒนาขีดความสามารถด้านไซเบอร์เชิงรุก (Cyber Offensive Capability) ซึ่งยากต่อการตรวจจับ และวิเคราะห์หาแหล่งที่มา

๔.๒ ภัยคุกคามด้านไซเบอร์มีการพัฒนาขีดความสามารถสูงขึ้นจึงสามารถเกิดขึ้นได้ทั้งจากระดับบุคคล องค์กร และรัฐต่อรัฐทำให้การพิสูจน์ทราบยุ่งยากและใช้เวลามากขึ้น

การจัดกลุ่มผลการวิเคราะห์ (SWOT Matrix)

๑. จุดแข็ง-โอกาส จัดทำแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เพื่อสนับสนุนแนวคิดการปฏิบัติการไซเบอร์ ได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเองให้มากที่สุด

๒. จุดแข็ง-อุปสรรค พัฒนาระบบเทคโนโลยีด้านข่าวกรองไซเบอร์ และจัดทำฐานข้อมูลด้านการข่าว ไซเบอร์ โดยสนธิการข่าวทั้งที่เปิดเผยและไม่เปิดเผย

๓. จุดอ่อน-โอกาส พัฒนาให้มีศูนย์กลางแลกเปลี่ยนด้านข่าวทางไซเบอร์ให้พร้อมตอบสนองกับภัยคุกคาม และสร้างความร่วมมือกับหน่วยงานใน กห. หน่วยงานภาครัฐ และหน่วยงานระหว่างประเทศ

๔. จุดอ่อน-อุปสรรค กำหนดแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศที่เป็นรูปธรรม

จากการวิเคราะห์สภาวะแวดล้อม ซึ่งประกอบด้วยปัจจัยภายใน (จุดแข็ง จุดอ่อน) ปัจจัยภายนอก(โอกาสและภัยคุกคาม) สามารถสรุปประเด็นยุทธศาสตร์ด้านข่าวกรองไซเบอร์ของกองทัพอากาศ ที่ต้องดำเนินการได้ดังนี้

๑. เสริมขีดความสามารถในการปฏิบัติการข่าวกรองไซเบอร์ในกองทัพอากาศ

๑.๑ มีกระบวนการปฏิบัติการด้านข่าวกรองไซเบอร์ และนำข้อมูลข่าวสารที่ได้รับไปร่วมในการกำหนดแผน

๑.๒ มีแผนงานและการดำเนินการด้านกำลังพลพร้อมเรียกไซเบอร์ที่เป็นรูปธรรม มีการขึ้นทะเบียน และการตอบแทนที่เหมาะสม

๒. สร้างความร่วมมือระหว่างหน่วยงานเพื่อผนึกกำลังเสริม

๒.๑ มีการฝึกร่วม/ผสม การข่าวกรองไซเบอร์อย่างต่อเนื่อง ทั้งในระดับการตัดสินใจและระดับปฏิบัติ

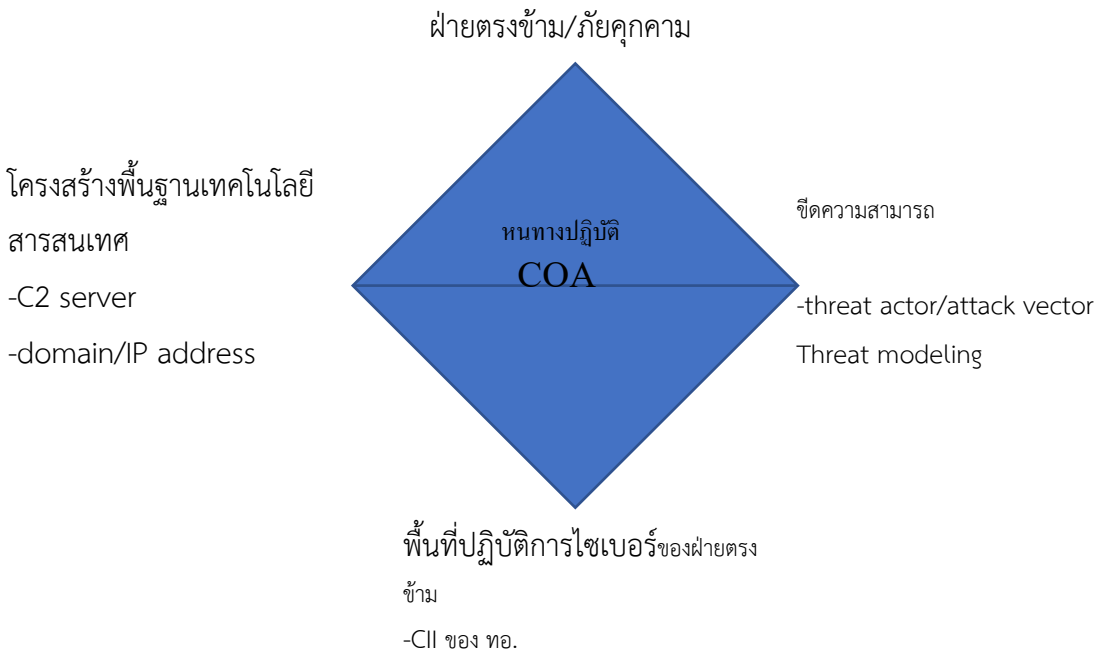
๒.๒ มีการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคามกับหน่วยงานภาครัฐ เอกชน ทั้งในและต่างประเทศ ที่รวดเร็ว เหมาะสม ถูกต้องและปลอดภัย

๒.๓ ส่งเสริม สนับสนุนให้มีผลผลิตของการวิจัยและพัฒนาที่สามารถนำไปปฏิบัติการข่าวกรองทางไซเบอร์ ภายใต้มาตรการควบคุมและการรักษาความลับที่เข้มงวด

๒.๔ มีความร่วมมือด้านข่าวกรองไซเบอร์กับประเทศพันธมิตร

๒.๕ ใช้ศักยภาพของผู้เชี่ยวชาญด้านข่าวกรองไซเบอร์ รวมทั้งขีดความสามารถของกำลังพลจากทุกภาคส่วนนำมาบูรณาการ

กรอบแนวคิดวิจัย



สรุป การปฏิบัติการด้านข่าวกรองไซเบอร์ของกองทัพอากาศ ในปัจจุบันไม่สามารถปฏิบัติภารกิจสนับสนุนทางไซเบอร์ได้อย่างสมบูรณ์ เนื่องจากปัญหาด้านอุปกรณ์ที่ใช้ในการปฏิบัติภารกิจไม่เอื้ออำนวยต่อการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ ไม่สามารถนำข้อมูลด้านไซเบอร์ไปใช้ในการสนับสนุนการปฏิบัติทางอากาศให้สามารถปฏิบัติการโดยใช้เครือข่ายเป็นศูนย์กลางได้ โดยเฉพาะข้อมูลภัยคุกคามด้านไซเบอร์ที่จะนำมาประกอบการตัดสินใจของผู้บังคับบัญชา และนอกจากนี้ ยังขาดระบบวิเคราะห์ข่าวกรองไซเบอร์ที่วิเคราะห์ หาแหล่งที่มาของโปรแกรมประสงค์ร้าย (Malware) ที่ยากต่อการตรวจจับ และสามารถฝังตัวเป็น BOTNET สำหรับใช้ในการโจมตีแบบ Distributed Denial of Service

บทที่ ๓
วิธีดำเนินการวิจัย

ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ เพื่อพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เชิงแนวคิด (Conceptual) และรวบรวมข้อมูลที่ได้จากบทความตำราวิชาการงานวิจัย และ เอกสารที่เกี่ยวข้อง (Documentary Search) ตามยุทธศาสตร์และนโยบายระดับชาติ ตลอดจนกองทัพอากาศ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และข่าวกรองไซเบอร์ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของแนวทางข่าวกรอง ไซเบอร์ของต่างประเทศเปรียบเทียบกับแนวทางของกองทัพอากาศไทยในปัจจุบัน ข้อมูลที่ใช้ในการวิจัยนำมาจากการศึกษาวรรณกรรมที่เกี่ยวข้อง

ขั้นตอนการดำเนินการวิจัย

๑. ศึกษาแนวคิด ทฤษฎี ที่เกี่ยวข้องกับการพัฒนาขีดความสามารถข่าวกรองไซเบอร์

๒. ศึกษารูปแบบหลักนิยมการปฏิบัติการไซเบอร์ของกองทัพอากาศประกอบกับแนวทางข่าวกรองไซเบอร์ในกองทัพอากาศปัจจุบันจากวรรณกรรมที่เกี่ยวข้อง

๓. วิเคราะห์ข่าวกรองไซเบอร์ในกองทัพอากาศในปัจจุบันเพื่อหาแนวทางที่เหมาะสมสำหรับพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

๔. เปรียบเทียบแนวทางการปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF กับการปฏิบัติข่าวกรองไซเบอร์ในกองทัพอากาศโดยใช้เครื่องมือ benchmark

๕. สรุปแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

๑. ศึกษาแนวคิด ทฤษฎี ที่เกี่ยวข้องกับการพัฒนาขีดความสามารถข่าวกรองไซเบอร์

การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE)

๑. ติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคาม และแจ้งเตือนฝ่ายให้เราทราบ (การสร้างความตระหนักรู้สถานการณ์ (Situation Awareness : SA)

๒. รวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนามาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคคลหรือกลุ่มบุคคลที่เฝ้าระวังทั้งภายในและภายนอกประเทศ

๓. จัดเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation Of The Cyber Environment : IPCE) ซึ่งประกอบด้วย ๔ ขั้นตอน คือ

๓.๑. การระบุสภาพแวดล้อมของการปฏิบัติการ(Determine The Operational Environment)

๓.๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ(Determine Influences On The Environment)

๓.๓. การระบุตัวภัยคุกคาม (Determine TheThreat Actors)

๓.๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม(Determine The Threat Scenarios)

๔. การวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคาม เพื่อใช้สำหรับการวางแผนปฏิบัติการไซเบอร์

๕. จัดทำเป้าหมายทางไซเบอร์ เมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้าม หรือภัยคุกคาม การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ เป็นกระบวนการวิเคราะห์อย่างต่อเนื่องและเป็นระบบ มุ่งเน้นการศึกษาและทำความเข้าใจกับสภาพแวดล้อม ของพื้นที่ปฏิบัติการในมิติทางไซเบอร์ ระบุถึงขีดความสามารถและหนทางปฏิบัติของฝ่ายตรงข้าม โดยมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ นอกจากนี้การรวบรวมข้อมูลเกี่ยวกับ ภัยคุกคามไซเบอร์ หรือการรวบรวมและแบ่งปันข่าวกรองภัยคุกคามไซเบอร์ ถือเป็นอีกกระบวนการหนึ่งที่จะทำให้การจัดทำฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ประสบผลสำเร็จ

๒. ศึกษารูปแบบหลักนิยมการปฏิบัติการไซเบอร์ของกองทัพอากาศประกอบกับแนวทางข่าวกรองไซเบอร์ในกองทัพอากาศปัจจุบันจากวรรณกรรมที่เกี่ยวข้อง

๒.๑ แนวคิดการปฏิบัติการไซเบอร์ ทอ.

๒.๑.๑ ปฏิบัติการไซเบอร์เชิงรับ ระวังป้องกันและตรวจจับการบุกรุก สืบค้นจุดอ่อนและซ่องโหว่ในระบบไซเบอร์ของฝ่ายเรา รวมทั้งการสำรองและกู้คืนระบบกรณีถูกโจมตีทางไซเบอร์จากฝ่ายตรงข้าม

๒.๑.๒ ปฏิบัติการไซเบอร์เชิงรุก เพื่อดักรับข้อมูลการใช้งานทางไซเบอร์ การก่อกวนระบบคอมพิวเตอร์ จำกัดเสรีภาพในการใช้งาน และทำให้เครื่องคอมพิวเตอร์แม่ข่ายปฏิเสธการให้บริการหรือหยุดการทำงาน รวมถึงสามารถจารกรรมข้อมูลของฝ่ายตรงข้ามได้ในระดับหนึ่ง โดยระวังป้องกันและรักษาความปลอดภัยระบบสารสนเทศของหน่วยและระบบ ให้ปฏิบัติตามระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒ หรือฉบับที่มีผลบังคับใช้อย่างเคร่งครัด

๒.๑.๓ ปฏิบัติการข่าวกรองไซเบอร์ มีเป้าหมายเพื่อวางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับเพื่อให้ประสบความสำเร็จในการปฏิบัติการเชิงรับ

๒.๒ เรื่องของภัยคุกคาม (Threat) สามารถระบุและตรวจสอบได้ว่าภัยคุกคามคือใคร ทราบถึงขีดความและหนทางปฏิบัติของภัยคุกคาม

๒.๓ การรวบรวมข่าวสาร (Collection) เมื่อเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (IPCE) แล้วจะทำให้ทราบว่ายังขาดข้อมูลข่าวสาร/ข่าวกรองใดที่กระทบต่อการวิเคราะห์ภัยคุกคามและทำให้สามารถรวบรวมข้อมูลข่าวสาร/ข่าวกรองในพื้นที่ปฏิบัติการได้อย่างเหมาะสม

๒.๔ การกำหนดเป้าหมาย (Targeting) เมื่อทราบถึงคุณลักษณะสำคัญของสภาพแวดล้อม การปฏิบัติการและภัยคุกคามแล้ว จะทำให้การกำหนดเป้าหมายเพื่อตอบโต้ภัยคุกคามที่ทำการโจมตีฝ่ายเรานั้นทำได้ง่ายขึ้นและตรงตามเจตนารมณ์ของผู้บังคับบัญชา การดำเนินงานด้านข่าวกรองไซเบอร์ของกองทัพอากาศในปัจจุบันจะเป็นการประสานความร่วมมือระหว่าง กรมข่าวทหารอากาศ และศูนย์ไซเบอร์กองทัพอากาศ โดยกรมข่าวทหารอากาศมีหน้าที่ ติดตามสถานการณ์ภัยคุกคามไซเบอร์ในระดับยุทธศาสตร์ และส่งข้อมูลให้ศูนย์ไซเบอร์กองทัพอากาศดำเนินการข่าวกรองไซเบอร์

๓. วิเคราะห์ข่าวกรองไซเบอร์ในกองทัพอากาศในปัจจุบันเพื่อหาแนวทางที่เหมาะสมสำหรับการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

การวิเคราะห์ข้อมูลผู้วิจัยพบว่าข่าวกรองไซเบอร์ (Cyber Intelligence) เป็นกลไกสำคัญโดยงานข่าวกรองไซเบอร์ แบ่งออกเป็น ๓ ระดับ คือ ข่าวกรองยุทธศาสตร์ ข่าวกรองยุทธการ และข่าวกรองยุทธวิธี และต้องใช้ บุคลากรที่เชี่ยวชาญทั้งในด้านงานข่าวกรองและด้านการปฏิบัติการไซเบอร์ ทั้งนี้การดำเนินงานข่าวกรองไซเบอร์ ของกองทัพอากาศในปัจจุบันยังไม่มีหลักนิยมหรือแนวความคิดในการปฏิบัติที่ชัดเจน การดำเนินงานจึงเป็น ลักษณะของการประสานความร่วมมือแลกเปลี่ยนหรือสนับสนุนข้อมูลระหว่างหน่วยงานด้านการข่าวกับหน่วยงานไซเบอร์เป็นหลัก โดยหน่วยข่าวส่วนใหญ่จะสนับสนุนข้อมูลข่าวกรองยุทธศาสตร์เพื่อแจ้งเตือน ให้ทราบถึงสถานการณ์หรือเบื้องหลังเหตุการณ์การโจมตีทางไซเบอร์ ส่วนหน่วยไซเบอร์จะเป็น ผู้ดำเนินการข่าวกรองยุทธการและข่าวกรองยุทธวิธีเอง เนื่องจากมีความเชี่ยวชาญด้านเทคโนโลยีที่ใช้ในการรวบรวมข่าวสารและการวิเคราะห์ภัยคุกคามไซเบอร์

๓.๑ เพื่อช่วยในการระบุแหล่งที่มา ทำให้หาแหล่งที่มาจากการเชื่อมต่อกับเครือข่ายภายนอกและ ตรวจสอบช่องโหว่โครงสร้างพื้นฐานวิกฤตของ ทอ. เพื่อปรับปรุงกระบวนการป้องกันภัยคุกคามทางไซเบอร์

๓.๒ เพื่อช่วยกำหนดขอบเขต/กำหนดการตอบสนองภัยคุกคาม

๓.๒.๑ จัดเก็บข้อมูลในระบบจัดเก็บข้อมูลด้านการข่าวกรองด้านการปฏิบัติการในมิติไซเบอร์ของข้าศึก

๓.๒.๒ จัดทำบัญชีเป้าหมายทางไซเบอร์ โดยเฉพาะเป้าหมายภายในระบบโครงสร้างพื้นฐานวิกฤต และเป้าหมายที่มีความอ่อนไหว หรือมีความสำคัญทางยุทธศาสตร์ของฝ่ายตรงข้าม

๓.๓ เพื่อส่งข่าวกรองไซเบอร์ให้ส่วนปฏิบัติการไซเบอร์ในตอบโต้เพื่อบรรลุเป้าหมายตามคำสั่งที่ได้รับ

๔. เปรียบเทียบแนวทางการปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF กับการปฏิบัติข่าวกรองไซเบอร์ในกองทัพอากาศโดยใช้เครื่องมือ benchmark

ผู้วิจัยใช้การ Process Benchmarking เป็นการเปรียบเทียบแนวทางการปฏิบัติการข่าวกรองไซเบอร์จากหน่วยงานด้านไซเบอร์ของ USAF กับการปฏิบัติข่าวกรองไซเบอร์ในกองทัพอากาศ เพื่อนำไปสู่แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ รายละเอียดตามผนวก จ

๕. สรุปแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

ขีดความสามารถในการการระบุตัวข้าศึกหรือภัยคุกคามไซเบอร์เพื่อหาหนทางปฏิบัติของข้าศึกหรือภัยคุกคามทางไซเบอร์บนพื้นที่ปฏิบัติการไซเบอร์ของฝ่ายตรงข้ามซึ่งข้อมูลเกี่ยวกับข้าศึกสามารถนำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์เพื่อเตรียมการปฏิบัติการไซเบอร์

การทำงานข่าวกรองไซเบอร์ควรจำแนกขีดความสามารถของงานข่าวกรองไซเบอร์ในแต่ละระดับ ซึ่งนอกจากขีดความสามารถในการวิเคราะห์ข้าศึกหรือภัยคุกคาม หนทางปฏิบัติ พื้นที่ปฏิบัติการและสภาพแวดล้อมที่ส่งผลกระทบแล้ว งานข่าวกรองไซเบอร์ต้องมีขีดความสามารถในการระบุให้ได้ถึงเครื่องมือ รูปแบบและวิธีการที่ข้าศึกนำมาใช้ในการโจมตี ข่าวกรองไซเบอร์ต้องมีขีดความสามารถในการสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับ

นอกจากนี้ การจัดทำฐานข้อมูลและการแลกเปลี่ยนข่าวกรองภัยคุกคามทางไซเบอร์ (cyber threat intelligence sharing plateform) ถือเป็นแนวคิดสำคัญ เนื่องจากห้วงมิติไซเบอร์ไม่มีการแบ่งพรมแดนและอาณาเขตชัดเจน บางครั้งภัยคุกคามไซเบอร์ที่ต้องการจะโจมตีเป้าหมายหนึ่ง อาจส่งผลกระทบต่อบุคคลหรือรัฐที่ไม่ใช่เป้าหมายของการโจมตีนั้นได้เช่นกัน ดังนั้นการจัดทำฐานข้อมูลและการแลกเปลี่ยนร่วมกันในทุกๆ หน่วยงานจึงถือว่ามีความจำเป็น อย่างไรก็ตาม ปัจจุบันการปฏิบัติการไซเบอร์ของกองทัพอากาศ อยู่ภายใต้ความรับผิดชอบของศูนย์ไซเบอร์กองทัพอากาศ ดังนั้นเมื่อเกิดกรณีที่ต้องการข้อมูลข่าวสาร ข่าวกรองไซเบอร์ จึงมีเพียงแต่การส่งคำขอข้อมูลและประสานไปยังหน่วยข่าวกรองไซเบอร์ ให้การสนับสนุนข่าวกรองตามที่ ศูนย์ไซเบอร์กองทัพอากาศต้องการเท่านั้น

บทที่ ๔
ผลการวิเคราะห์ข้อมูล

ในส่วนของวรรณกรรมเอกสารที่เกี่ยวข้องกับการการปฏิบัติการด้านข่าวกรองไซเบอร์ ผู้วิจัยได้ทบทวน วรรณกรรมยุทธศาสตร์ไซเบอร์ของต่างประเทศและหน่วยงานด้านไซเบอร์ของ USAF การแสวงหาความร่วมมือ ระหว่างประเทศมักถูกกำหนดไว้เป็นกลไกสำคัญในการผนึกกำลังทางด้านไซเบอร์รวมถึงการลดความขัดแย้งระหว่างประเทศ ผลการวิจัยพบว่า แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ มุ่งสนใจข้อมูลเกี่ยวกับข้าศึกหรือภัยคุกคาม หนทางปฏิบัติของข้าศึกหรือภัยคุกคาม พื้นที่ปฏิบัติการ ขีดความสามารถ รวมถึง ผลกระทบของการถูกโจมตีโดยเฉพาะพื้นที่ปฏิบัติการในมิติไซเบอร์ ผู้วิจัยจึงสรุปได้ว่า การแจ้งเตือนเพื่อสร้าง ความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเรา การวิเคราะห์หนทางปฏิบัติของภัยคุกคาม ดังนั้น ในการนี้ผู้วิจัยได้นำรูปแบบการพัฒนาวงรอบการปฏิบัติการข่าวกรองทางไซเบอร์ ตามแนวทาง DIAMOND MODEL เพื่อ

๑. ตรวจสอบภัยคุกคามไซเบอร์เปรียบเทียบกับฐานข้อมูลภัยคุกคามไซเบอร์ในระบบจัดเก็บข้อมูลด้าน การข่าวกรองไซเบอร์เพื่อบ่งชี้ภัยคุกคามไซเบอร์

๒. นำข้อมูลการรายงานภัยคุกคามไซเบอร์มาวิเคราะห์เพื่อระบุรูปแบบและวิธีการที่ข้าศึกนำมาใช้ในการโจมตี

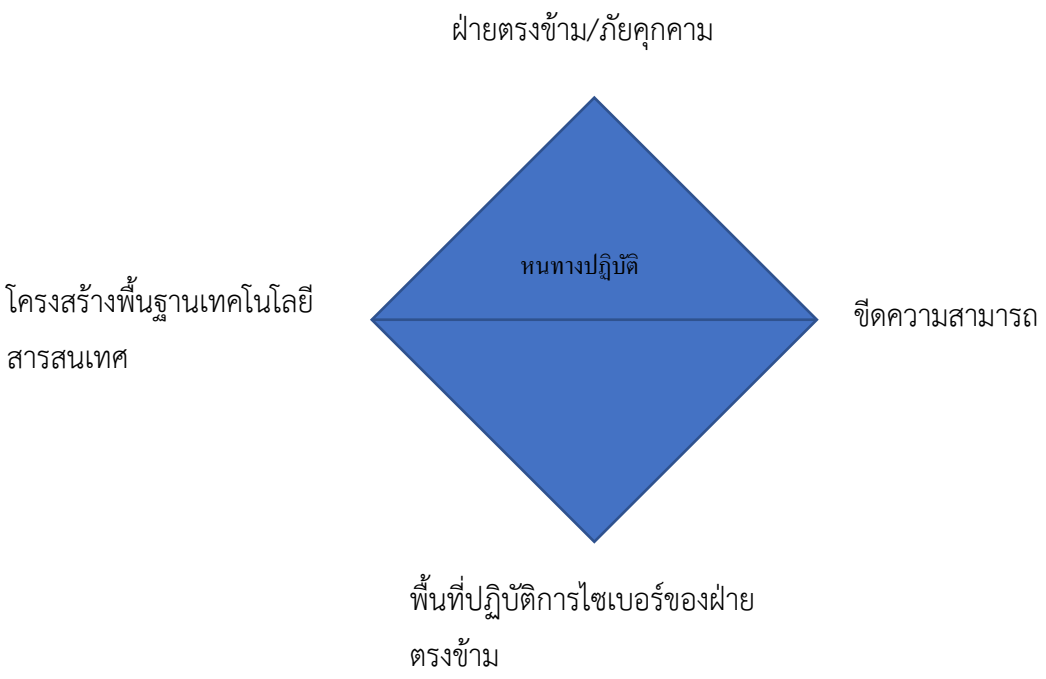
๓. ตรวจสอบขีดความสามารถของภัยคุกคามไซเบอร์ตามผลการวิเคราะห์และตัวชี้วัดของการถูกเข้าควบคุมระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ

๔. วิเคราะห์ขีดความสามารถของภัยคุกคามไซเบอร์หาแหล่งที่มาและค้นหาเบาะแสและหาผลกระทบร้ายแรงต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศวิกฤตของกองทัพอากาศ เพื่อระงับยับยั้ง ขัดขวาง ควบคุม หรือทำลายผู้ที่มีส่วนเกี่ยวข้องในการโจมตีทางไซเบอร์เพื่อเป็นการป้องปรามการโจมตีทางไซเบอร์ของข้าศึก

สรุปผลการวิจัย ผลการวิจัยนี้นอกจากได้ศึกษาวิเคราะห์แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์เพื่อพร้อมรับมือภัยคุกคามไซเบอร์ในกองทัพอากาศ โดยค้นคว้าการพัฒนาหลักนิยมยุทธศาสตร์ไซเบอร์ของต่างชาติและหน่วยงานด้านไซเบอร์ของ USAF (ตามรายละเอียดในเอกสารวิจัยในการทบทวนวรรณกรรมที่เกี่ยวข้อง) ยังสามารถสรุป แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ โดยแนวทางดังกล่าวนี้มีความสอดคล้องกับยุทธศาสตร์ชาติในภาพรวมและมีการรองรับจาก แนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องอย่างเด่นชัดดังนี้

แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ

จากการศึกษาข้อมูลในการทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง ผู้วิจัยเสนอแนวทางการพัฒนาตามตัวแบบที่ แสดงในภาพที่ ๔



บทที่ ๕
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

๑. สรุปผลการวิจัย

การวิจัยครั้งนี้ ผู้วิจัย ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ เพื่อพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เชิงแนวคิด (Conceptual) และรวบรวมข้อมูลที่ได้จากบทความตำราวิชาการงานวิจัยและ เอกสารที่เกี่ยวข้อง (Documentary Search) ตามยุทธศาสตร์และนโยบายระดับชาติ ตลอดจนกองทัพอากาศ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และข่าวกรองไซเบอร์ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของแนวทางข่าวกรองไซเบอร์ของต่างประเทศเปรียบเทียบกับแนวทางของกองทัพอากาศไทยในปัจจุบัน

๒. การอภิปรายผล

ผลการวิจัยในครั้งนี้ สามารถอภิปรายผลในเรื่องของแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ จากการทบทวนวรรณกรรมยุทธศาสตร์ไซเบอร์ของต่างประเทศและหน่วยงานด้านไซเบอร์ของ USAF เพื่อการวิเคราะห์ขีดความสามารถที่จำเป็น ของงานข่าวกรองทางไซเบอร์ในกองทัพอากาศ จนนำมาสู่การนำเสนอแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบาย ได้ตรงตามวัตถุประสงค์การวิจัย กล่าวคือ กองทัพอากาศมีบทบาทสำคัญ ในการขับเคลื่อนปฏิรูปกองทัพด้านไซเบอร์อย่างต่อเนื่องตลอดหลายปีที่ผ่านมา ให้สอดรับกับยุทธศาสตร์ชาติ (ด้านความมั่นคง) และยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นการเสริมสร้างขีดความสามารถและความพร้อมในการปฏิบัติการไซเบอร์ มุ่งเน้นการพัฒนาองค์ประกอบที่สำคัญทั้งการพัฒนาโครงสร้างพื้นฐาน และเทคโนโลยีสารสนเทศ ตลอดจนการสร้างความตระหนักรู้ทางไซเบอร์ให้กับหน่วยขึ้นตรงกองทัพอากาศที่มีระบบเทคโนโลยีสารสนเทศ และสร้างความร่วมมือ ทางไซเบอร์ทั้งในและต่างประเทศ จนนำไปสู่การพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์ เพื่อให้มีพลังอำนาจทางไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง

งานข่าวกรองทางไซเบอร์ถือเป็นกลไกหลักสำคัญ และเป็นกุญแจแห่งความสำเร็จในการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อวิเคราะห์ถึงแนวทางการพัฒนาข่าวกรองไซเบอร์ในกองทัพอากาศ ผลการวิจัยพบว่า ขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ใน

กองทัพอากาศ ไม่แตกต่างจากงานข่าวกรองในพื้นที่ปฏิบัติการอื่น ๆ ได้แก่ การติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคาม และแจ้งเตือนฝ่ายเราให้ทราบ การรวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำมาวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคาม เพื่อใช้สาหรับการวางแผนการปฏิบัติการไซเบอร์เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม

อย่างไรก็ตาม แม้ว่าแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศไม่แตกต่างจากงานข่าวกรองในพื้นที่ปฏิบัติการอื่น ๆ แต่ในมิติไซเบอร์นั้น เป็นการปฏิบัติการบนระบบเครือข่ายคอมพิวเตอร์ที่ไม่มีขอบเขตที่ชัดเจนเหมือนกับพื้นที่ทางบก ทางทะเล และอากาศ รวมทั้งทักษะที่จำเป็นต้องใช้ในการปฏิบัติการนั้นไม่ได้ใช้ความสามารถและประสบการณ์ ทางด้านการข่าวกรองเพียงอย่างเดียว แต่ต้องอาศัยทักษะทางด้านระบบเครือข่ายคอมพิวเตอร์ซึ่งต้องมี ความรู้ความเข้าใจ และประสบการณ์งานด้านไซเบอร์ตลอดจนเครื่องมืออุปกรณ์ Software ต่าง ๆ ที่ใช้สำหรับงานด้านไซเบอร์ โดยการพัฒนาขีดความสามารถที่จำเป็นสำหรับงานข่าวกรองทางไซเบอร์สามารถแบ่งออกเป็น ขีดความสามารถทางด้านการข่าวกรอง และขีดความสามารถทางด้านไซเบอร์ ซึ่งปัจจุบันบุคลากรภายในกองทัพอากาศที่ปฏิบัติงานในส่วนของงานด้านการข่าวและด้านไซเบอร์จะมีทักษะและขีดความสามารถเฉพาะ ในด้านนั้น ๆ จึงเป็นอุปสรรคต่อการพัฒนางานข่าวกรองไซเบอร์ในปัจจุบัน

การวิจัยครั้งนี้ ได้แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ ที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายของกองทัพอากาศ คือ ซึ่งประกอบด้วย ๔ ขั้นตอน คือ

๑. การระบุสภาพแวดล้อมของการปฏิบัติการ(Determine The Operational Environment)

๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ(Determine Influences On The Environment)

๓. การระบุตัวภัยคุกคาม (Determine The Threat Actors)

๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม ที่เหมาะสมและสอดคล้องกับกระบวนการแสวงข้อตกลงใจ ทางทหาร (MDMP Process) ที่ใช้เป็นเครื่องมือในการประมาณสถานการณ์ ข่าวกรองสนับสนุนการวางแผนการยุทธ์ จึงสามารถนำมาประยุกต์ใช้ในการสนับสนุนการปฏิบัติการไซเบอร์ได้อย่างเหมาะสม ทั้งนี้แนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ จะมุ่งเน้นการป้องกันภัยคุกคามทาง ไซเบอร์ที่ส่งผลต่อระบบเครือข่ายในการควบคุมบัญชาการและ ควบคุมการรับส่งข้อมูลของฝ่ายตรงข้าม รวมทั้งสนับสนุนมาตรการการ

รักษาความมั่นคงปลอดภัยทางไซเบอร์ ของกองทัพอากาศตามที่ได้รับมอบหมาย โดยเป็นการปฏิบัติการไซเบอร์เชิงรับ

๓. ข้อเสนอแนะ

๑. ผู้บังคับบัญชาของหน่วยในทุกระดับชั้นควรให้ความสำคัญในการพัฒนาบุคลากร ระบบเครือข่าย และอุปกรณ์ให้มีความพร้อมในการรองรับการปฏิบัติงานด้านการข่าวกรองไซเบอร์

๒. ควรมีการผนึกกำลังระหว่างหน่วยข่าวกรองไซเบอร์ภายในกระทรวงกลาโหมและ หน่วยงานภายนอก รวมทั้งมิตรประเทศ

๓. ข่าวกรองไซเบอร์ในทุกระดับทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี หน่วยรับผิดชอบงานด้านการข่าวควรมีบทบาทหน้าที่ในการปฏิบัติ เพราะเป็นศูนย์กลางในการบูรณาการข้อมูล เพื่อผลิตเป็นข่าวกรองสนับสนุนงานยุทธการ ทั้งนี้กองทัพควรปรับโครงสร้างหน่วยข่าวเพื่อให้สามารถรองรับ การปฏิบัติการด้านข่าวกรองไซเบอร์ และพัฒนาขีดความสามารถของผู้ที่จะปฏิบัติงานด้านการข่าวกรองไซเบอร์ ในระดับยุทธการและยุทธวิธี ให้มีทักษะทั้งด้านการข่าวกรองและการปฏิบัติการไซเบอร์ควบคู่กัน

๔. ระบบเครือข่ายของแต่ละหน่วยงานภายในกระทรวงกลาโหมควรกำหนดให้มีการเชื่อมโยงข้อมูลบนมาตรฐานเดียวกันเพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลข่าวสารทางไซเบอร์ที่รวดเร็วและทั่วถึง ซึ่งในเบื้องต้นหน่วยที่มีขีดความสามารถทางด้านไซเบอร์สูง ควรให้การสนับสนุนหน่วยที่กำลังเริ่มต้นหรือ มีขีดความสามารถน้อยกว่า เพื่อให้เกิดการบูรณาการข้อมูลและการป้องกันภัยคุกคามทางไซเบอร์ร่วมกัน นอกจากนี้ควรมีการเชื่อมโยงระบบกับเครือข่ายทางไซเบอร์ในทุกภาคส่วนให้สามารถแลกเปลี่ยนข้อมูล ข่าวสารและช่วยเหลือซึ่งกันและกันในกรณีที่เกิดสถานการณ์วิกฤตทางไซเบอร์ได้

๕. สำหรับข้อเสนอแนะในการวิจัยครั้งต่อไป ผู้วิจัยเห็นว่าควรนำแนวทางการพัฒนาขีดความสามารถข่าวกรองไซเบอร์ในกองทัพอากาศ เชิงแนวคิดจากเอกสารวิจัยฉบับนี้ไปขยายผลต่อในการจัดทำแนวคิดในการปฏิบัติการข่าวกรองไซเบอร์ในกองทัพอากาศ เพื่อให้เกิดผลอย่างเป็นรูปธรรมและสามารถให้การปฏิบัติการข่าวกรองไซเบอร์สามารถ สนับสนุนงานยุทธการและการปฏิบัติการไซเบอร์ในระดับกองทัพและเหล่าทัพต่าง ๆ ได้ อย่างไรก็ตาม ผู้วิจัยมีข้อเสนอแนะเพิ่มเติมว่า การนำข้อมูลในเอกสารวิจัยฉบับนี้ไปเป็นแนวความคิดในการทำวิจัย ในประเด็นอื่นต่อไป ควรจะตรวจสอบและศึกษาถึงสภาพแวดล้อมของการปฏิบัติการ ณ เวลานั้นด้วย เนื่องจากพื้นที่ปฏิบัติการหรือมิติทางไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่ตลอดเวลา จึงอาจทำให้ ต้องมีการปรับปรุงเปลี่ยนแปลงแนวคิดของการจัดทำตัวแบบของงานข่าวกรองไซเบอร์ให้เหมาะสม

บรรณานุกรม

ภาษาไทย

พลอากาศตรี พงษ์สวัสดิ์ จันทสาร.(๒๕๖๑). “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร”

สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี,สืบค้นเมื่อ ๒๕๖๕https://www.bbc.com/thai/international-57052951

แฮ็กโรงพยาบาล-รีดค่าไถ่ เรียกถึง 6.3 หมื่นล้านบาท, ๑๐ ก.ย. ๒๕๖๓, สืบค้นเมื่อ ๒๕๖๕ https://www.thairath.co.th/news/local/central/1926912

สรุปผลการตรวจสอบเหตุการณ์ข้อมูล Username/Password ทอ.รั่วไหล”(๒๕๖๓).

“หลักนิยมการปฏิบัติการไซเบอร์”(๒๕๖๓).

“พบเกาหลีเหนืออาจพัวพันเหตุมัลแวร์โจมตีทั่วโลก ” .(๒๕๖๐). สืบค้นเมื่อ ๒๕๖๕, https://www.bbc.com/thai/international-39931940

ภาษาอังกฤษ

“Joint Publication 3-12 cyberspace operations” ,(2018). accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/.

“Joint Publication 2-0 joint intelligence”,(2013).accessed 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

“SCOTT JASPER.(2020) “RUSSIAN CYBER OPERATIONS”

“Cyber Security”.accessed 2021, http://www.rdpb.go.th/MediaUploader/File/10166/CyberSecurity

ภาคผนวก

ผนวก ก คำจำกัดความ

คำจำกัดความด้านไซเบอร์

เพื่อให้เกิดความเข้าใจในแนวทางที่สอดคล้องกัน และเพื่อความสะดวกในการอ้างอิงสำหรับการศึกษาและใช้เป็นกรอบในการดำเนินการด้านสงครามไซเบอร์ของ ทอ. จึงได้กำหนดคำจำกัดความหรือคำนิยามศัพท์ด้านไซเบอร์ ดังนี้

๑. การกระทำโดยรัฐ (State Actor) หมายถึง การปฏิบัติในมิติไซเบอร์ใบลักษณะที่เป็นภัยคุกคามโดยมีรัฐให้การสนับสนุนหรือสั่งการ

๒. การกระทำที่มิได้ดำเนินการโดยรัฐ (Non-state Actor) หมายถึง การปฏิบัติในลักษณะที่เป็นภัยคุกคาม โดยปราศจากการสนับสนุนหรือสั่งการจากรัฐ

๓. การตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Audit) หมายถึง การตรวจสอบการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยไม่กำหนดวิธีการหรือขั้นตอนที่จะดำเนินการตรวจสอบ เพื่อให้ได้ผลการตรวจสอบตามความเป็นจริง

๔. การโจมตีทางไซเบอร์ (Cyber Attack) หมายถึง การโจมตีต่อฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้ามด้วย

๕. การทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Distributed Denial of Service: DDoS) หมายถึง การขัดขวางหรือก่อกวนระบบเครือข่ายหรือ Server จนทำให้ทรัพยากรของเครื่องเป้าหมายที่ถูกโจมตีหมดไป หรือเครือข่ายนั้น ๆ ไม่สามารถทำงานได้ตามปกติ

๖. การรับรองความสามารถด้านไซเบอร์ทางทหาร (Cyber Defense Certification) หมายถึง ระบบการพัฒนาขีดความสามารถของนักรบไซเบอร์ ประกอบด้วยการทดสอบความสามารถทางไซเบอร์ด้านทฤษฎีและปฏิบัติ ซึ่งจำเป็นต่อการปฏิบัติงานในมิติไซเบอร์ โดยแบ่งเป็นระดับที่แตกต่างกันตามขอบเขตความรับผิดชอบและลักษณะงาน เพื่อให้กระทรวงกลาโหมมีนักรบไซเบอร์ที่เพียงพอทั้งในเชิงปริมาณและเชิงคุณภาพ ตามมาตรฐานของกระทรวงกลาโหม

๗. การหลอกลวงทางอินเทอร์เน็ต (Phishing) หมายถึง การล่อลวงทางอินเทอร์เน็ตชนิดหนึ่ง ที่พยายามหลอกผู้ใช้งาน โดยการสร้างอีเมล์ หรือหน้าเว็บไซต์ปลอมขึ้นมาเพื่อหวังผลในการให้ผู้ใช้งานเกิดความสับสน และทำธุรกรรมต่าง ๆ บนเว็บไซต์ปลอมที่ถูกสร้างขึ้นนั้น โดยข้อมูลต่าง ๆ ที่ผู้ใช้งานได้กรอกบนหน้าเว็บไซต์ปลอมเหล่านี้ จะถูกดักข้อมูลและบันทึกไว้เพื่อใช้ในการปลอมแปลงและเข้าถึงข้อมูลของผู้เสียหายโดยที่ไม่ได้รับอนุญาต ส่วนการหลอกลวงแบบเจาะจงเป้าหมาย (Spear

Phishing) คือ รูปแบบการหลอกลวงของข้อความอีเมล์ที่เฉพาะเจาะจง ซึ่งอาจดูเสมือนว่านายจ้าง หรือเพื่อนร่วมงานส่งข้อความอีเมล์ให้คนในองค์กร

๘. การสืบสวนทางไซเบอร์ (Cyber Forensics/Computer Forensics) หมายถึง กระบวนการสกัดข้อมูลข่าวสารจากคอมพิวเตอร์และสื่อบันทึกข้อมูลแบบดิจิทัล เพื่อให้ได้มาซึ่งหลักฐานทางดิจิทัล เพื่อใช้ในการดำเนินคดีด้านอาชญากรรมไซเบอร์

๙. การแสวงประโยชน์จากช่องโหว่ (Exploitation) หมายถึง การนำเทคนิคการปฏิบัติในมิติไซเบอร์ มาดำเนินการกับช่องโหว่ หรือใช้ช่องโหว่เป็นทางผ่าน เพื่อให้เกิดผลตามที่ต้องการ

๑๐. ความตระหนักรู้ทางไซเบอร์ (Cyber Awareness, Cyberspace Domain Awareness) หมายถึง ความเข้าใจอย่างถูกต้องเกี่ยวกับสภาวะแวดล้อมและภัยคุกคามในมิติไซเบอร์ในห้วงเวลาหนึ่งหรือตามห้วงเวลาที่ต้องการ มีความเกี่ยวข้องตั้งแต่ระดับบุคคล องค์กร ซึ่งสามารถส่งผลกระทบต่อความมั่นคงของชาติหรือผลประโยชน์แห่งชาติ

๑๑. ความพร้อมในการรับมือทางไซเบอร์ (Cyber Resilience) หมายถึง ความสามารถในการรับมือและฟื้นฟูกลับคืนสู่สภาพปกติโดยเร็วที่สุด หลังจากการถูกโจมตีทางไซเบอร์

๑๒. ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หมายถึง หลักการ มาตรการ กระบวนการ แนวทางปฏิบัติ เพื่อปกป้องมิติไซเบอร์จากการโจมตีทางไซเบอร์ มักใช้ในบริบทด้านพลเรือน

๑๓. โครงสร้างพื้นฐานวิกฤตของ ทอ. (RTAF Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งสำหรับการปฏิบัติในมิติไซเบอร์ หากถูกโจมตีทางไซเบอร์หรือแสวงประโยชน์จาก ช่องโหว่ จะเกิดผลเสียหายร้ายแรงต่อความสำเร็จของการปฏิบัติภารกิจของ ทอ.เช่น ระบบควบคุมบังคับบัญชา ระบบฐานข้อมูลข่าวกรอง ระบบสนับสนุนการตัดสินใจทางยุทธศาสตร์ ระบบสื่อสารโทรคมนาคม ระบบสื่อสารทางยุทธวิธี ระบบป้องกันทางอากาศ เป็นต้น

๑๔. โครงสร้างพื้นฐานวิกฤตของชาติ (National Critical Infrastructure) หมายถึง ระบบสาธารณูปโภคที่สำคัญยิ่งของรัฐ ซึ่งใช้ระบบสารสนเทศในการควบคุมการปฏิบัติงาน มักใช้ในการให้บริการประชาชน เช่น ระบบการจ่ายกระแสไฟฟ้า ระบบการบริหารจัดการน้ำ ระบบบริการด้านการเงิน ระบบการให้บริการอินเทอร์เน็ต ระบบการสื่อสารทั้งภาคพื้นดินและดาวเทียม ระบบกิจการวิทยุและโทรทัศน์ ระบบการขนส่งมวลชน ระบบควบคุมการจราจรทางบกและทางอากาศ เป็นต้น

๑๕. ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่อง ซึ่งถูกนำมาใช้เพื่อให้ได้ผลตามที่ต้องการ

๑๖. ไซเบอร์ (Cyber) หมายถึง สิ่งที่เกี่ยวข้องหรือสัมพันธ์กับอินเทอร์เน็ต ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition: SCADA) ระบบควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Embedded Systems) เป็นต้น

๑๗. นักรบไซเบอร์ (Cyber Warrior) หมายถึง บุคคลหรือกลุ่มบุคคลซึ่งปฏิบัติงานในมิติไซเบอร์ โดยเน้นการปฏิบัติในลักษณะการโจมตีทางไซเบอร์ หรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม ประกอบด้วยผู้ปฏิบัติงานด้านนโยบาย/ยุทธศาสตร์ รวมทั้งผู้ปฏิบัติงานเชิงเทคนิค

๑๘. โปรแกรมประสงค์ร้าย (Malware) หมายถึง โปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Browser แบ่งออกได้หลากหลายประเภท เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) การแอบดักจับข้อมูล (Spyware) คีย์ล๊อกเกอร์ (Key Logger) ดังนี้

๑๘.๑ ไวรัส (virus) หมายถึง โปรแกรมที่สามารถติดต่อจากอีกไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

๑๘.๒ เวิร์ม (worm) หมายถึง โปรแกรมที่สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ผ่านทางเครือข่าย เวิร์ม สามารถทำอันตรายให้กับระบบ

๑๘.๓ โทรจัน (Trojan) หมายถึง โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่ทำงานโดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับจดหมายอิเล็กทรอนิกส์

๑๘.๔ การแอบดักจับข้อมูล (Spyware) หมายถึง โปรแกรมที่ถูกออกแบบมาให้คอยติดตามบันทึกข้อมูลส่วนบุคคล รายงานข้อมูลการใช้งานของผู้ใช้แต่ละคนบนอินเทอร์เน็ต หรือทำการเปลี่ยนการตั้งค่าของโปรแกรมบราวเซอร์ใหม่ ซึ่งก่อให้เกิดความรำคาญ และทำให้ประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ช้าลง

๑๘.๕ คีย์ล๊อกเกอร์ (Key Logger) หมายถึง สปายแวร์ประเภทหนึ่งที่ทำหน้าที่บันทึกข้อมูลการกดแป้นคีย์บอร์ดของผู้ใช้ ข้อมูลที่จัดเก็บจะถูกส่งผ่านอินเทอร์เน็ต เพื่อใช้ก่ออาชญากรรมในรูปแบบต่างๆ ได้

๑๙. มิติไซเบอร์ (Cyberspace) หมายถึง มิติที่มีการประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์และหลักการด้านสเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ในการจัดเก็บ แก้ไข หรือแลกเปลี่ยนข้อมูลบนโครงสร้างพื้นฐานทางกายภาพ

๑๙.๑ อิเล็กทรอนิกส์ (Electronics) หมายถึง หลักการที่เกี่ยวข้องกับการออกแบบวงจรไฟฟ้า (Circuits) โดยใช้ทรานซิสเตอร์ (Transistors) และไมโครชิป (Microchips) รวมไปถึง

หลักการที่เกี่ยวข้องกับพฤติกรรมและการเคลื่อนที่ของอิเล็กตรอนในสารกึ่งตัวนำ (Semiconductor) ตัวนำ (Conductor) สุญญากาศ หรือก๊าซ

๑๙.๒ สเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) หมายถึง หลักการที่เกี่ยวข้องกับช่วงหรือแถบคลื่นแม่เหล็กไฟฟ้าซึ่งมีความยาวที่แตกต่างกัน ใช้ในด้านการสื่อสารโทรคมนาคมแบบต่าง ๆ ตามคุณสมบัติของแต่ละช่วงคลื่น

๑๙.๓ การปฏิบัติในมิติไซเบอร์ (Cyberspace Operations) หมายถึง การดำเนินการโดยใช้ขีดความสามารถทางไซเบอร์ในมิติไซเบอร์ เพื่อให้บรรลุวัตถุประสงค์ที่ตั้งไว้

๒๐. ยุทธภัณฑ์ทางไซเบอร์ (Cyber Weapon) หมายถึง ระบบชุดของยุทโธปกรณ์ หรือชุดคำสั่งทางคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ซึ่งใช้ในการโจมตีทางไซเบอร์หรือแสวงประโยชน์จากช่องโหว่ ในมิติ ไซเบอร์ของฝ่ายตรงข้าม

๒๑. สงครามไซเบอร์ (Cyber warfare) หมายถึง การปฏิบัติในมิติไซเบอร์ซึ่งมีมูลเหตุหรือวัตถุประสงค์ทางการเมืองหรือทางทหาร โดยนำเทคนิคการปฏิบัติในมิติไซเบอร์มาใช้ป้องกัน รวมทั้งโจมตีหรือแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒๒. เหตุคุกคามทางไซเบอร์ (Cyber Incident) หมายถึง เหตุการณ์ (Event) ที่ไม่เป็นไปตามนโยบายหรือมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจบ่งบอกถึงการถูกโจมตีทางไซเบอร์หรือการถูกแสวงประโยชน์จากช่องโหว่ ได้แก่ ความพยายามเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต (Unauthorized Access) เหตุการณ์ขัดขวางหรือทำให้ระบบสารสนเทศไม่สามารถใช้งานได้ (Disruption or Denial of Service) หรือเหตุการณ์พยายามเปลี่ยนแปลงข้อกำหนดทางเทคนิคของระบบสารสนเทศ เป็นต้น

๒๓. USAF คือ United States Air Force

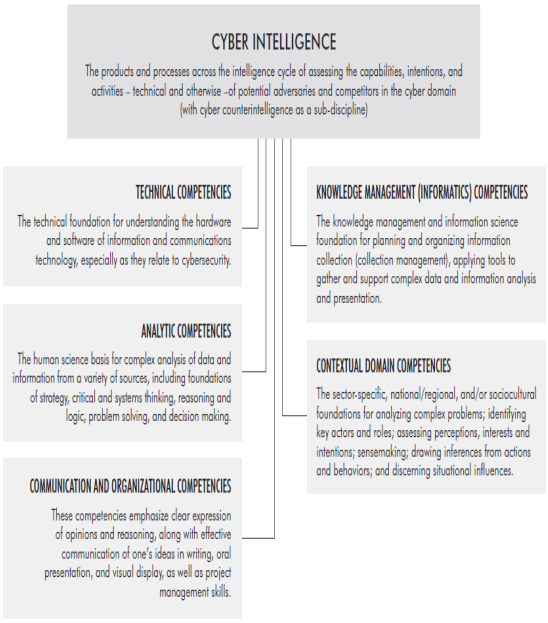
ผนวก ข ผลงานวิจัยที่เกี่ยวข้อง

นาย Jay Mcallister ได้ทาการศึกษาเรื่องการประยุกต์กระบวนการคิดเชิงวิพากษ์ เพื่อนำมาใช้ กับงานข่าวกรองไซเบอร์ สรุปว่านักวิเคราะห์ในทุกระดับควรอุทิศเวลาให้กับการพัฒนาวิธีการคิด โดยการลงลึกไปถึงกระบวนการทำงานของจิตใจมนุษย์ เพื่อปรับปรุงทักษะการวิเคราะห์ ซึ่งผู้วิจัยพบว่า หลักวิธีเช่นนี้ไม่ต่างกับการวิเคราะห์ข่าวกรองชนิดอื่นๆ

นาย Robert M. Lee ทำการศึกษางานข่าวกรองไซเบอร์เพื่อบรรยายในหลักสูตรบัณฑิตศึกษา ด้านความมั่นคงและปลอดภัยทางไซเบอร์ สรุปว่าขั้นตอนแรกในการเข้าใจงานข่าวกรองไซเบอร์ คือ การเข้าใจวงรอบข่าวกรองทั้งในด้านยุทธวิธี เทคนิค และขั้นตอนการปฏิบัติ ซึ่งการดาเนินการข่าวกรอง ประเภทต่าง ๆ มีอยู่นานก่อนที่จะเกิดงานข่าวกรองไซเบอร์ โดยเฉพาะด้านการตัดสินตกลงใจทางทหารที่ ผู้บังคับบัญชา ต้องการทราบเจตนารมณ์ของฝ่ายตรงข้ามเพื่อเลือกยุทธศาสตร์ที่ดีกว่าในสนามรบหรือ เตรียมตัวให้พร้อมสาหรับการโจมตี รวมถึงการป้องกันอย่างเหมาะสม เพราะฉะนั้นการเริ่มศึกษาข่าวกรอง ไซเบอร์สามารถเริ่มได้จากการศึกษาแนวทางข่าวกรองทหาร

เครือข่าย Intelligence and National Security Alliance ระบุว่า ข่าวกรองไซเบอร์ คือ การประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรมของข้าศึก ในห้วงมิติทางไซเบอร์ (Cyber Domain) เพื่อสนับสนุนการแจ้งเตือน การโจมตี และการป้องกันภัยคุกคาม ซึ่งเป็นผลผลิตที่ได้จากการดำเนิน วงรอบข่าวกรองโดยมีขีดความสามารถที่จำเป็น ได้แก่

๑. ความเข้าใจในเรื่องของระบบฮาร์ดแวร์ ซอฟท์แวร์ ระบบสารสนเทศและการสื่อสาร
๒. ทักษะการคิดวิเคราะห์
๓. การนำเสนอ รายงาน ให้ความเห็นที่เป็นเหตุเป็นผล
๔. การบริหารจัดการวางแผนรวบรวมข้อมูลข่าวกรอง
๕. ความเข้าใจในภารกิจ และบริบทของหน่วยงาน เช่น ผู้แสดงหลัก กลุ่มผลประโยชน์



ภาพที่ ๕ ขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์

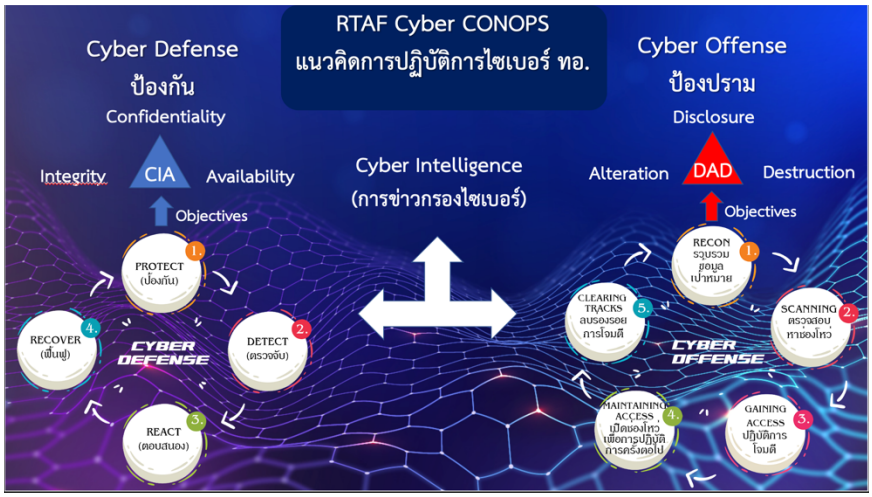
ที่มา : CTI –EU | Bonding EU Cyber Threat Intelligence ENISA, Online, 2017

ภาพที่ ๖ ขีดความสามารถและทักษะที่จำเป็นของนักวิเคราะห์ข่าวกรองทางไซเบอร์

ที่มา : Information Security Education Carnegie Mellon University, Online, 2017

ผนวก ค หลักนิยมการปฏิบัติการไซเบอร์ในกองทัพอากาศ

แนวความคิดทั่วไป



ภาพที่ ๗ แนวคิดการปฏิบัติการไซเบอร์ ทอ.

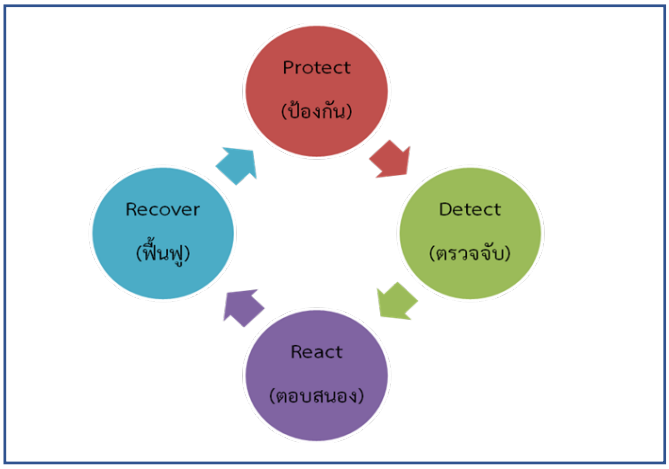
ที่มา : RTAF Cyber CONOPS

แนวคิดการปฏิบัติการไซเบอร์ ทอ.

๑.๑ ปฏิบัติการไซเบอร์เชิงรับ ระวังป้องกันและตรวจจับการบุกรุก สืบค้นจุดอ่อนและช่องโหว่ในระบบ ไซเบอร์ของฝ่ายเรา รวมทั้งการสำรองและกู้คืนระบบกรณีถูกโจมตีทางไซเบอร์จากฝ่ายตรงข้าม

๑.๒ ปฏิบัติการไซเบอร์เชิงรุก เพื่อดักรับข้อมูลการใช้งานทางไซเบอร์ การก่อกวนระบบคอมพิวเตอร์ จำกัดเสรีภาพในการใช้งาน และทำให้เครื่องคอมพิวเตอร์แม่ข่ายปฏิเสธการให้บริการหรือหยุดการทำงาน รวมถึงสามารถจารกรรมข้อมูลของฝ่ายตรงข้ามได้ในระดับหนึ่ง โดยระวังป้องกันและรักษาความปลอดภัยระบบสารสนเทศของหน่วยและระบบ ให้ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๕๒ หรือฉบับที่มีผลบังคับใช้อย่างเคร่งครัด

๑.๓ ปฏิบัติการข่าวกรองไซเบอร์ มีเป้าหมายเพื่อ วางแผน รวบรวม วิเคราะห์ ข่าวกรองเพื่อสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับเพื่อให้ประสบความสำเร็จในการปฏิบัติการเชิงรับ มีการปฏิบัติดังนี้



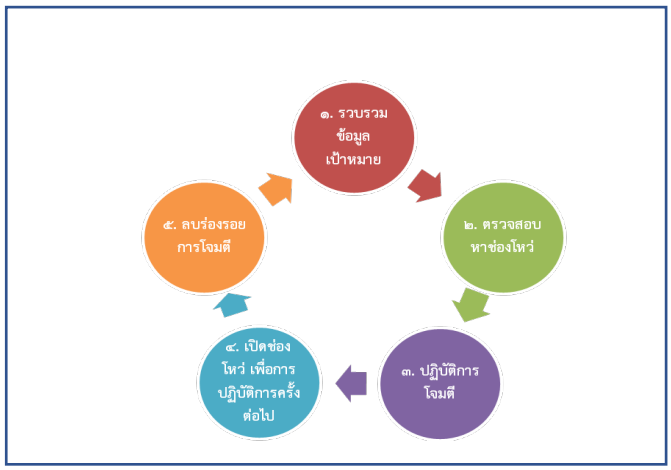
ภาพที่ ๘ วงรอบการปฏิบัติ Cyber Defense

การป้องกัน เน้นย้ำให้ นกข.ต้องระวังป้องกันระบบไซเบอร์ที่ตนเองรับผิดชอบตามแนวทางของระเบียบฯ และนโยบายด้านความมั่นคงฯ ที่เกี่ยวข้อง โดยมีทีมชุดปฏิบัติการด้านสงครามไซเบอร์ เป็นผู้รับผิดชอบในการประเมินมาตรการรักษาความมั่นคงปลอดภัย

การตรวจจับ เน้นย้ำให้ นกข.ผู้รับผิดชอบการระวังป้องกัน ต้องเฝ้าระวัง และรายงานเหตุการณ์ล่วงละเมิดความมั่นคงปลอดภัยด้านไซเบอร์ให้ทันเวลา เพื่อให้สามารถตอบสนองและแก้ไขได้ทันท่วงที

การตอบสนอง เน้นย้ำให้ นกข.ต้องปฏิบัติการแก้ปัญหาการล่วงละเมิด การรักษาความมั่นคงปลอดภัย ไซเบอร์ โดยทันทีตามมาตรการที่เหมาะสม เพื่อป้องกันระบบสารสนเทศ ไม่ให้ส่งผลกระทบกับระบบบัญชาการและควบคุม รวมทั้งระบบอื่นที่เกี่ยวข้อง ตลอดจนระงับเหตุล่วงละเมิดการรักษาความมั่นคงปลอดภัยไซเบอร์

การฟื้นฟู เน้นย้ำให้ นกข.ต้องปฏิบัติการฟื้นฟูระบบที่ได้รับผลกระทบทั้งหมดเพื่อให้กลับคืนสู่สภาพปกติพร้อมใช้งานโดยเร็วที่สุด และปรับปรุงกระบวนการป้องกันให้ดียิ่งขึ้น เชิงป้องปราม/ตอบโต้ มีการปฏิบัติดังนี้



ภาพที่ ๙ วงรอบการปฏิบัติ Cyber Attack

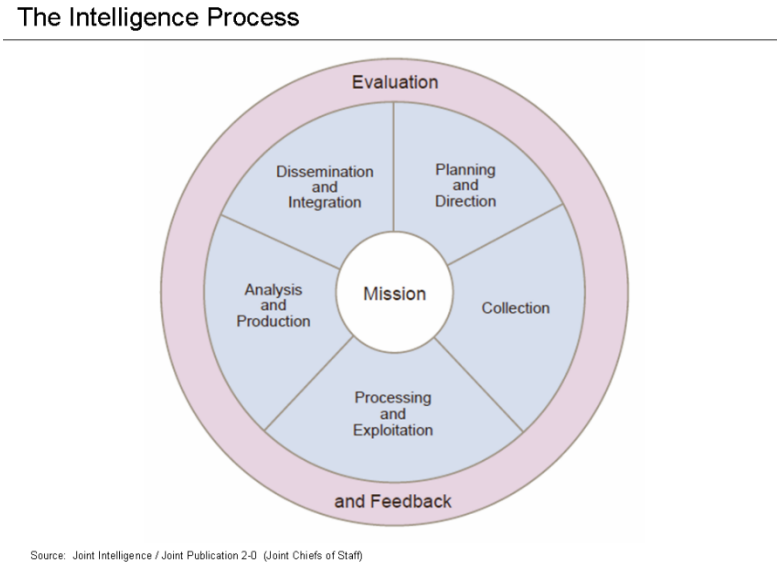
การรวบรวมข้อมูลเป้าหมาย ต้องปฏิบัติอย่างจริงจังในกระบวนการรวบรวมข้อมูลเกี่ยวกับเป้าหมายในทุกด้าน เพื่อใช้ในการวิเคราะห์หาช่องโหว่

การตรวจสอบหาช่องโหว่ ต้องปฏิบัติอย่างจริงจังในการวิเคราะห์หาช่องโหว่ โดยใช้ข้อมูลจากการรวบรวมเป้าหมาย เพื่อเตรียมการโจมตีตามช่องโหว่ที่ค้นพบ

ปฏิบัติการโจมตี ต้องวางแผนและดำเนินการโจมตี เพื่อให้บรรลุเป้าหมายตามคำสั่งที่ได้รับ โดยขั้นตอนนี้ต้องดำเนินการแบบพราง เพื่อไม่ให้สืบย้อนมาถึงเราได้

การเปิดช่องโหว่ เพื่อการปฏิบัติการครั้งต่อไป ให้ปฏิบัติโดยการฝังทางลับ (Backdoor) เพื่อการเข้าปฏิบัติการในครั้งต่อไป

ลบร่องรอยการโจมตี ให้ปฏิบัติโดยการ กลบเกลื่อน ร่องรอย เพื่อไม่ให้สืบย้อนมาถึงหน่วยงาน ทอ.ได้



ภาพที่ ๑๐ วงรอบการปฏิบัติ intelligence

วงรอบข่าวกรอง กล่าวคือ การอำนวยการ การรวบรวม การประมวลผล การวิเคราะห์ การเผยแพร่ใช้ประโยชน์ และการเสนอแนะ

ผนวก ง การวิเคราะห์ขีดความสามารถด้านไซเบอร์ของกองทัพอากาศ

การวิเคราะห์สภาวะแวดล้อม (SWOT Analysis)

การปฏิบัติการทางอากาศที่ประสบความสำเร็จอย่างปลอดภัย เป็นความคาดหวังของ ทอ.ทุกประเทศทั่วโลก ซึ่งงานที่สนับสนุนความสำเร็จเหล่านั้นส่วนหนึ่งคือการปฏิบัติการไซเบอร์ ทั้งเชิงรุกและเชิงรับ เพื่อสนับสนุนการปฏิบัติการทางอากาศให้สามารถปฏิบัติได้อย่างเต็มขีดความสามารถ ลดทอนประสิทธิภาพ หรือหยุดการปฏิบัติส่วนหนึ่งส่วนใดของฝ่ายตรงข้าม ซึ่งจำเป็นต้องวิเคราะห์สภาวะแวดล้อมขององค์กรด้วยวิธีการ SWOT Analysis เพื่อค้นหาจุดแข็ง จุดอ่อน โอกาส และภัยคุกคาม และนำผลที่ได้มาปรับปรุงข้อบกพร่องและพัฒนา ซึ่งจะช่วยเสริมสร้างขีดความสามารถด้านไซเบอร์ของ ทอ. ให้มีประสิทธิภาพมากยิ่งขึ้น

๑. การวิเคราะห์สภาวะแวดล้อม (SWOT Analysis)

๑.๑ ปัจจัยภายใน (Internal Factor)

๑.๑.๑ จุดแข็ง (Strength)

๑.๑.๑.๑ มีการกำหนดยุทธศาสตร์กองทัพอากาศ ในการเป็น “One of the Best Air Forces in ASEAN” ซึ่งทำให้ ทอ.ต้องมีการเสริมความพร้อมในการปฏิบัติในทุกด้าน

๑.๑.๑.๒ ผู้บังคับบัญชาระดับสูงให้ความสำคัญกับการปฏิบัติการด้านสงครามไซเบอร์

๑.๑.๑.๓ มีบุคลากรหลักที่มีความรู้ความสามารถด้านไซเบอร์

๑.๑.๑.๔ มีหน่วยงานระดับนโยบายและปฏิบัติด้านสงครามไซเบอร์

๑.๑.๑.๕ มีระเบียบที่เอื้อกับการปฏิบัติการเชิงรับ

๑.๑.๑.๖ มีแผนเฉลิมอากาศที่จะปรับปรุงให้ครอบคลุมถึงการปฏิบัติการด้านไซเบอร์

๑.๑.๑.๗ ศูนย์ข้อมูล ทอ. ได้การรับรองมาตรฐาน ISO ๒๗๐๐๑

๑.๑.๑.๘ มีการอบรมด้าน Cyber Security ในหลักสูตรต่าง ๆ ของ ทอ.

๑.๑.๑.๙ มีการพัฒนาบุคลากรด้วยการจัดแข่งขันปฏิบัติการด้านไซเบอร์ (Cyber Operations Contest)

๑.๑.๒ จุดอ่อน (Weakness)

๑.๑.๒.๑ ขาดเทคโนโลยีที่จะใช้ในการป้องกันด้านสงครามไซเบอร์ที่ครอบคลุมและเพียงพอ

๑.๑.๒.๒ บุคลากรด้านเชิงรุกและเชิงรับยังไม่เพียงพอกับความต้องการและขาดงบประมาณในการพัฒนา

๑.๑.๒.๓ การจัดหาอุปกรณ์และเทคโนโลยีทันสมัยต้องพึ่งพาหน่วยงานภายนอก และต่างประเทศ

๑.๑.๒.๔ มาตรฐานในการกำหนดอุปกรณ์ด้าน Cyber security ยังไม่สมบูรณ์

๑.๑.๒.๕ บุคลากรในระดับผู้ใช้ยังขาดจิตสำนึกด้าน Cyber Security

๑.๑.๒.๖ ขาดหน่วยงานที่เป็นศูนย์กลางในการบูรณาการด้าน Cyber Security เพื่อรับมือกับภัยคุกคามด้านไซเบอร์ที่สามารถตอบสนองได้ทันเวลา

๑.๑.๒.๗ การรักษาความมั่นคงปลอดภัยของระบบที่อยู่นอกเครือข่าย ทอ. ยังไม่ปลอดภัยจากนักเจาะระบบ เช่น สน.ผชท.ทอ.ต่างประเทศ และการฝึก/ร่วม ผสม ต่างประเทศ เป็นต้น

๑.๑.๒.๘ การติดตั้งเครือข่าย การให้บริการอินเตอร์เน็ตยังไม่ครอบคลุม ทำให้มีการเชื่อมต่ออินเตอร์เน็ต ที่หลากหลาย ยากต่อการควบคุม

๑.๑.๒.๙ ขาดมาตรการในการควบคุมการเชื่อมต่อและการใช้งานเครือข่ายสารสนเทศ

๑.๑.๒.๑๐ ระบบสารสนเทศบางหน่วยยังขาดระบบสำรองเพื่อการให้บริการที่ต่อเนื่อง เมื่อเกิดเหตุภัยพิบัติ ทำให้การฟื้นฟูไปสู่สภาพปกติใช้เวลานาน

๑.๑.๒.๑๑ ภัยคุกคามที่เกิดจากภายใน ทอ. ทั้งที่ตั้งใจและไม่ตั้งใจ

๑.๑.๒.๑๒ ผู้ใช้งานบางกลุ่มขาดจิตสำนึกในการใช้สื่อสังคมออนไลน์และระบบประมวลผลแบบกลุ่มเมฆ (Cloud Computing)

๑.๑.๒.๑๓ ขาดงบประมาณสนับสนุนที่ต่อเนื่อง

๑.๑.๒.๑๔ ขาดกรอบแนวความคิดในการปฏิบัติ (Concept of Operation) ด้านเทคโนโลยีสารสนเทศและการสื่อสารโทรคมนาคม รวมทั้งการปฏิบัติด้านสงครามไซเบอร์

๑.๒ ปัจจัยภายนอก (External Factor)

๑.๒.๑ โอกาส (Opportunity)

๑.๒.๑.๑ ภาครัฐให้ความสำคัญกับการพัฒนาด้านสงครามไซเบอร์ ทั้งเชิงรุกและ เชิงรับ รวมทั้งมีนโยบายกำหนดให้หน่วยงานด้านความมั่นคงเป็นหน่วยงานหลักใน ด้านเชิงรุก

๑.๒.๑.๒ เทคโนโลยีด้านสงครามไซเบอร์ ในรูปแบบ Open Source มีมากขึ้นและสามารถนำมาประยุกต์ใช้งานได้หลายด้าน

๑.๒.๑.๓ องค์ความรู้ด้านสงครามไซเบอร์จากแหล่งต่าง ๆ มีมากขึ้น

๑.๒.๑.๔ ภาครัฐให้ความสำคัญในเรื่องเศรษฐกิจดิจิทัล (Digital Economy) และกฎหมายด้านไซเบอร์

๑.๒.๑.๕ ได้รับความร่วมมือที่ดีกับหน่วยงานภายในและภายนอก ทอ. รวมทั้งจากต่างประเทศ

๑.๒.๒ อุปสรรค (Threat)

๑.๒.๒.๑ ในหลายประเทศมีการพัฒนาขีดความสามารถด้านไซเบอร์เชิงรุก (Cyber Offensive Capability) ซึ่งยากต่อการป้องกัน

๑.๒.๒.๒ ภัยคุกคามจากภายนอกมีวิวัฒนาการที่ก้าวหน้าทำให้มีความเสี่ยงจากการถูกดักจับข้อมูลและการถูกเจาะระบบ

๑.๒.๒.๓ ขาดกฎหมายและข้อตกลงระหว่างประเทศเพื่อลงโทษผู้กระทำความผิดด้านไซเบอร์ภายนอกราชอาณาจักร ต่อความมั่นคงของประเทศ

๑.๒.๒.๔ ภัยคุกคามด้านไซเบอร์สามารถเกิดขึ้นได้ทั้งจากระดับบุคคล องค์กร และรัฐต่อรัฐทำให้การพิสูจน์ทราบยุ่งยากและใช้เวลามากขึ้น

๑.๓ การจัดกลุ่มผลการวิเคราะห์ (SWOT Matrix)

๑.๓.๑ จุดแข็ง-โอกาส จัดทำแนวทางการพัฒนาด้านสงครามไซเบอร์ เพื่อสนับสนุนแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเองให้มากที่สุด โดยมีขีดความสามารถในการป้องปรามและตอบโต้

๑.๓.๒ จุดแข็ง-อุปสรรค พัฒนาระบบความมั่นคงปลอดภัยไซเบอร์ และจัดทำฐานข้อมูลด้านการข่าวสงครามไซเบอร์ ที่มีผลกับความมั่นคงของประเทศ โดยสนธิการข่าวทั้งที่เปิดเผยและไม่เปิดเผย

๑.๓.๓ จุดอ่อน-โอกาส พัฒนา ทอ.ให้มีศูนย์กลางด้านสงครามไซเบอร์ให้พร้อมตอบสนองกับภัยคุกคาม และสร้างความร่วมมือกับหน่วยงานใน กห. หน่วยงานภาครัฐ และหน่วยงานระหว่างประเทศ

๑.๓.๔ จุดอ่อน-อุปสรรค กำหนดแนวความคิดในการปฏิบัติภารกิจสงครามไซเบอร์ที่เป็นรูปธรรม รวมทั้งกำหนดแนวความคิดในการปฏิบัติด้านเทคโนโลยี

สารสนเทศ และแนวความคิดในการปฏิบัติด้านการสื่อสารโทรคมนาคม และเร่งพัฒนาทางด้านเทคโนโลยีและบุคลากรให้ทัดเทียมกับประเทศเพื่อนบ้าน

จากการวิเคราะห์สภาวะแวดล้อม ซึ่งประกอบด้วยปัจจัยภายใน (จุดแข็ง จุดอ่อน) ปัจจัยภายนอก(โอกาสและภัยคุกคาม) สามารถสรุปประเด็นยุทธศาสตร์ด้านสงครามไซเบอร์ของ ทอ. ที่ต้องดำเนินการได้ดังนี้

๑) พัฒนาประสิทธิภาพในการป้องกัน

๒) เสริมขีดความสามารถในการป้องปรามและตอบโต้

๓) สร้างความร่วมมือระหว่างหน่วยงานเพื่อผนึกกำลัง

๒. ขีดความสามารถด้านสงครามไซเบอร์ที่พึงประสงค์ของกองทัพอากาศ

เป้าหมายของการดำเนินงานด้านไซเบอร์คือ การเตรียมความพร้อมให้สามารถปฏิบัติการสงครามไซเบอร์ เพื่อตอบสนองภารกิจ ทอ.ทั้งปวง โดยให้มีการรักษาความมั่นคงปลอดภัยสารสนเทศของ ทอ. เพื่อให้ใช้งานได้อย่างเสรี และสามารถป้องปรามและตอบโต้ภัยคุกคามได้อย่างมีประสิทธิผลและประสิทธิภาพ โดยการผนึกกำลังกัฐหน่วยงานทั้งในและนอกประเทศ ฉะนั้นเพื่อให้บรรลุวัตถุประสงค์ด้านไซเบอร์ในการป้องกันประเทศของ ทอ.จำเป็นต้องดำเนินการตามขีดความสามารถที่ต้องการและแนวทางดำเนินการ ได้แก่ขีดความสามารถในการป้องกัน ขีดความสามารถในการป้องปรามและตอบโต้ และขีดความสามารถในการผนึกกำลัง ดังนี้

๒.๑ ขีดความสามารถในการป้องกัน

๒.๑.๑ โครงสร้างและการบังคับบัญชาที่เหมาะสม

๒.๑.๑.๑ มีหน่วยงานและมีการกำหนดขอบเขตความรับผิดชอบ อำนาจหน้าที่ การสนับสนุนซึ่งกันและกัน ทั้งในระดับนโยบาย/ยุทธศาสตร์และระดับปฏิบัติ เพื่อเป็นแนวทางให้กับทุกหน่วยงานที่เกี่ยวข้องได้ยึดถือปฏิบัติได้อย่างถูกต้อง

๒.๑.๑.๒ มีกลไกที่เอื้ออำนวยต่อการสื่อสารสองทางอย่างมีประสิทธิภาพระหว่างระดับนโยบาย/ยุทธศาสตร์กับระดับปฏิบัติ และบูรณาการการจัดสรรทรัพยากร เพื่อสนับสนุนความต้องการของระดับปฏิบัติอย่างรวดเร็ว เพียงพอและคุ้มค่า

๒.๑.๑.๓ มีคณะกรรมการระดับ ทอ.ที่รับผิดชอบด้านสงครามไซเบอร์เพื่อรวมการควบคุมแยกการปฏิบัติ รวมทั้งมีหน่วยงานที่รับผิดชอบการนำผลการพิจารณาและการตัดสินใจของคณะกรรมการสงครามไซเบอร์ไปสู่การกำหนดแผนงานและการปฏิบัติอย่างถูกต้อง

๒.๑.๒ การบริหารทรัพยากรมนุษย์ด้านไซเบอร์อย่างครบวงจรในทุกระดับตามนโยบาย ผบ.ทอ.ในเรื่องการพัฒนาขีดความสามารถการปฏิบัติการด้านสงครามไซเบอร์ โดยเฉพาะการส่งเสริมและพัฒนากำลังพลด้านไซเบอร์ให้มีความพร้อมในการปฏิบัติการตามมาตรฐานสากล ดังนี้

๒.๑.๒.๑ มีการผลิตผู้ปฏิบัติงานไซเบอร์ในโรงเรียนทหารให้มีความสามารถทั้งการป้องกันและการโจมตีระบบเครือข่ายคอมพิวเตอร์ได้เป็นอย่างน้อย และมีทักษะทางด้านระบบคอมพิวเตอร์ที่จำเป็น

๒.๑.๒.๒ มีการฝึกร่วม/ผสม การป้องกันไซเบอร์ในทุกระดับเพื่อทดสอบแนวคิดทฤษฎีการปฏิบัติด้านไซเบอร์ และเป็นโอกาสในการพัฒนาความสัมพันธ์ทั้งในระดับผู้ฝึกและระดับหน่วยงาน

๒.๑.๒.๓ มีมาตรการรักษา ตอบแทน และจูงใจให้ผู้ปฏิบัติงานด้านไซเบอร์

๒.๑.๓ การรักษาความมั่นคงปลอดภัยไซเบอร์ต่อระบบสารสนเทศด้านการรบและระบบสารสนเทศด้านการสนับสนุน รวมทั้งระบบการบริหารความเสี่ยงที่มีประสิทธิภาพ ดังนี้

๒.๑.๓.๑ มีการจัดทำสถาปัตยกรรมระบบด้านไซเบอร์ ซึ่งแสดงถึงองค์ประกอบของการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานไซเบอร์เพื่อให้ทราบจุดอ่อน หรือจุดล่อแหลมที่ต้องปกป้องจากภัยคุกคามไซเบอร์

๒.๑.๓.๒ มีแผนการบริหารความเสี่ยงที่เหมาะสม และพร้อมปฏิบัติ

๒.๑.๓.๓ มีความสามารถด้านนิติวิทยาศาสตร์ทางดิจิตอลเพื่อสนับสนุนการป้องกันภัยคุกคามจากไซเบอร์

๒.๑.๓.๔ ต้องมีมาตรฐาน ระเบียบ ข้อบังคับ เพื่อใช้เป็นแนวทางการรักษาความมั่นคงปลอดภัยระบบเครือข่ายการสื่อสารและระบบสารสนเทศ

๒.๑.๓.๕มีหลักนิยม กฎการใช้กำลังไซเบอร์ กฎเกณฑ์ ที่สอดคล้องกับกฎหมายในประเทศและระหว่างประเทศที่เกี่ยวข้อง

๒.๒ ขีดความสามารถในการป้องปรามและตอบโต้

๒.๒.๑ มีกระบวนการปฏิบัติการด้านข่าวกรองไซเบอร์ และนำข้อมูลข่าวสารที่ได้รับไปร่วมในการกำหนดแผน หรือร่วมแสวงข้อตกลงใจทางทหาร

๒.๒.๒ มีแผนงานและการดำเนินการด้านกำลังพลพร้อมเรียกไซเบอร์ที่เป็นรูปธรรม มีการขึ้นทะเบียน และการตอบแทนที่เหมาะสม

๒.๒.๓ มีกระบวนการตอบสนองต่อสถานการณ์/ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์อย่างทันท่วงที

๒.๒.๔ สามารถปฏิบัติการตอบโต้แบบเร่งด่วนในลักษณะการเข้าระงับเหตุหรือคลี่คลายสถานการณ์เพื่อให้เกิดสภาพหรือเงื่อนไขทางทหารที่ฝ่ายเราต้องการ

๒.๒.๕ ส่งเสริม สนับสนุนให้มีผลผลิตของการวิจัยและพัฒนาที่สามารถนำไปปฏิบัติการทางสงครามไซเบอร์ ภายใต้มาตรการควบคุมและการรักษาความลับที่เข้มงวด

๒.๓ ขีดความสามารถในการผนึกกำลัง

๒.๓.๑ มีการฝึกร่วม/ผสมการป้องกันไซเบอร์อย่างต่อเนื่อง ทั้งในระดับการตัดสินใจ และระดับปฏิบัติ

๒.๓.๒ มีการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคามกับหน่วยงานภาครัฐ เอกชน ทั้งในและต่างประเทศ ที่รวดเร็ว เหมาะสม ถูกต้องและปลอดภัย

๒.๓.๓ ร่วมดำเนินการในการรับมือภัยคุกคามทางไซเบอร์ระดับชาติ

๒.๓.๔ มีความร่วมมือด้านไซเบอร์กับประเทศพันธมิตร

๒.๓.๕ ใช้ศักยภาพของผู้เชี่ยวชาญด้านคอมพิวเตอร์ การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมทั้งขีดความสามารถของกำลังพลจากทุกภาคส่วนนำมาบูรณาการ เพื่อป้องกันและตอบโต้การทำสงครามไซเบอร์

ผนวก จ การเปรียบเทียบ (Benchmarking)

การเปรียบเทียบ (Benchmarking) คือกระบวนการที่ใช้ในการพัฒนาคุณภาพงาน เป็นกระบวนการวัดเปรียบเทียบและพัฒนาการปฏิบัติงานขององค์กรอย่างเป็นระบบ (ชะนวนทอง ธนสุกาญจน, 2542)

ประเภทของ Benchmarking

การทำ Benchmarking สามารถแบ่งได้ ๔ ประเภท ดังนี้คือ

๑. Internal Benchmarking เป็นการเปรียบเทียบภายในองค์กร โดยมีวัตถุประสงค์เพื่อการกระจายข้อมูล หรือความรู้ไปยังกลุ่มอื่น ๆ ภายในองค์กร การทำ Benchmarking ในลักษณะนี้จะเป็นการสนับสนุนให้เกิดการใช้ข้อมูล หรือกระบวนการติดต่อสื่อสารภายในองค์กร ทำให้เกิดการใช้ทรัพยากรภายในองค์กรให้เกิดประโยชน์สูงสุด และเป็นการดูวิธีการทำงานที่ดีภายในองค์กร

๒. Competitive Benchmarking เป็นการเปรียบเทียบกับองค์กรที่เป็นคู่แข่งขันกัน ทำงานลักษณะเหมือนกัน ทำให้องค์กรสามารถพิจารณาได้ว่าองค์กรของตนเมื่อเปรียบเทียบกับ คู่แข่งขันแล้วเป็นอย่างไรและเป็นการดูวิธีการทำงานที่ดีในระดับต่างองค์กร

๓. Functional Benchmarking เป็นการเปรียบเทียบองค์กรเป้าหมายที่ไม่ใช่คู่แข่งขัน โดยตรง การทำ Benchmarkingในลักษณะนี้ จะมีการถ่ายทอดความรู้ และทักษะต่างๆ อยู่เพียงด้านเดียวและเป็นการดูวิธีการทำงานที่ดีในระดับต่างองค์กรที่ไม่ใช่คู่แข่งขัน

๔. Process Benchmarking เป็นการเปรียบเทียบกระบวนการต่างๆ ในการทำงานและระบบในการดำเนินงานขององค์กรที่ดีที่สุด จากองค์กรประเภทต่างๆ ที่มีลักษณะในการดำเนินงานที่เหมือนหรือคล้ายกัน ซึ่งจะนำไปสู่การพัฒนาในการดำเนินงานและสู่การผลิตที่สูงขึ้น หรือด้านการลดต้นทุนค่าใช้จ่ายลง ขั้นตอนในการทำเบ็นช์มาร์ค พีรศักดิ์ วรสุนทโรสถ (๒๕๔๒) ได้กล่าวถึงขั้นตอนในการทำเบ็นช์มาร์ค ใช้วงจรของ PDCA ของ เดมมิ่ง (Deming) อันเป็นรากฐานของการปรับปรุงกระบวนการต่าง ๆ รวมทั้งการ เรียนรู้หาสาเหตุและแก้ไขปัญหาได้อย่างมีระบบ และมีประสิทธิภาพ ตลอดจนสามารถตอบ ปัญหาหลักๆกวางๆได้ทุกจุดคือ P : Plan ขั้นการวางแผน D : Do ขั้นการค้นคว้าวิจัยและเก็บข้อมูล C : Check ขั้นทำการวิเคราะห์หาสาเหตุของข้อแตกต่างขององค์กร และองค์กรเป็นแบบอย่าง A : Act ลงมือปฏิบัติและปรับปรุงกระบวนการใหม่และแก้ไขข้อบกพร่องต่าง ๆ และกลับไปทำเช่นเดียวกันในด้านอื่นๆ เพราะเป็นกระบวนการต่อเนื่อง

ประวัติย่อผู้วิจัย

ยศ,ชื่อ	นาวาอากาศโท บุรีรัตน์ เข็มทอง
วัน เดือน ปี เกิด	๒๑ พ.ค.๒๕๒๙
สถานที่เกิด	จังหวัด กรุงเทพฯ
ที่อยู่ปัจจุบัน	๙๔/๓๑ รามอินทรา ก.ม.๒ เขตบางเขน แขวง อนุสาวรีย์ กรุงเทพฯ
ประวัติการศึกษา	มัธยมศึกษาปีที่ ๓ ปี ๒๕๔๓ โรงเรียนเตรียมทหาร ปี ๒๕๔๕ ปริญญาตรี โรงเรียนนายเรืออากาศ ปี ๒๕๕๑ หลักสูตรศิษย์การบิน ปี ๒๕๕๑ หลักสูตรนายทหารชั้นผู้บังคับฝูง รุ่นที่ ๑๒๙ ปี ๒๕๖๐ โครงการศึกษา Blackhat and Defcon 2019 USA. Cyber Security Fundamentals course UNSW Institute (Professional Education Courses) 2019 Cyber Security Boot Camp course UNSW Institute (Professional Education Courses) 2021 Strategies and Capabilities For Cyber Challenges (Professional Military Education) 2021
ประวัติการทำงาน	นักบินประจำหมวดบิน ๑ ฝ่ายยุทธการ ฝูงบิน ๒๐๓ ปี ๒๕๕๒- ๒๕๕๙ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร กองบังคับการกองบิน ๒ ปี ๒๕๕๖๐- ๒๕๖๒ หัวหน้าแผนกยุทธการและสนับสนุน กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ ปี ๒๕๖๓- ปัจจุบัน