ภัยคุกคามทางไซเบอร์ (Cyber threats Intelligence) ความท้าทายงานการข่าวกรองในศตวรรษที่ ๒๑ : แนวทางการกำหนดนโยบายในการพัฒนางานข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของกองทัพบก

โดย

พลตรี ประเสริฐ หมวดเชียงคะ
รองผู้บัญชาการโรงเรียนข่าวทหารบก
กรมข่าวทหารบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕
ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ - ๒๕๖๖

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “ภัยคุกคามทางไซเบอร์ (Cyber threats Intelligence) ความท้าทายงานการข่าวกรอง ในศตวรรษที่ ๒๑ : แนวทางการกำหนดนโยบายในการพัฒนางานข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของกองทัพบก” ลักษณะวิชาการทหาร ของ พลตรี ประเสริฐ หมวดเชียงคะ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕ ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ – ๒๕๖๖

พลโท

(ชาติชาย ชัยเกษม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง ภัยคุกคามทางไซเบอร์ (Cyber threats Intelligence) ความท้าทายงานการข่าวกรองในศตวรรษที่ ๒๑ : แนวทางการกำหนดนโยบายในการพัฒนางานข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของกองทัพบก

ลักษณะวิชา การทหาร

ผู้วิจัย พลตรี ประเสริฐ หมวดเชียงคะ **หลักสูตร** วปอ. **รุ่นที่** ๖๕

การศึกษาวิจัยในครั้งนี้ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ ๓ ข้อ ประกอบด้วย วัตถุประสงค์ที่ ๑ เพื่อศึกษาสภาวะแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้านไซเบอร์ (Cyber Security) และ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง วัตถุประสงค์ที่ ๒ เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ในปัจจุบัน และวัตถุประสงค์ที่ ๓ เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ผลการศึกษาวิจัยที่สามารถตอบวัตถุประสงค์การวิจัย ๓ ข้อดังกล่าวแล้วเบื้องต้นสามารถที่จะสรุปได้ดังนี้

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๑ สรุปได้ว่า ปัจจุบันโลกอยู่ในยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยีทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง บุคคล หรือกลุ่มบุคคลที่ไม่ใช่รัฐ (Non - State Actor) จะเป็นผู้มีบทบาทมีอิทธิพลมากขึ้น ในการดำเนินกิจกรรมที่ส่งผลกระทบต่อความมั่นคง การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศในห้วงปัจจุบัน พบว่าประเด็นความมั่นคงที่จะส่งผลกระทบต่อไทย ได้แก่ การเมืองระหว่างประเทศ, การขยายอิทธิพลและบทบาทของประเทศมหาอำนาจต่อภูมิภาคเอเชียตะวันออกเฉียงใต้, การขยายตัวของความสัมพันธ์ระหว่างประเทศในระดับภูมิภาค, ความขัดแย้งทางดินแดนและการใช้กำลังทางการทหาร, สถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้, การเคลื่อนตัวของภัยคุกคามข้ามชาติ, การย้ายถิ่นฐานของประชากร, ความมั่นคงหลัง COVID – 19 กรมข่าวทหารบกเป็นหน่วยงานด้านข่าวกรองหลักของกองทัพบกจึงต้องมีความพร้อมที่จะรับมือกับภัยคุกคามทุกรูปแบบให้ได้อย่างมีประสิทธิภาพ โดยเฉพาะภัยคุกคามทางบก เช่น ภัยคุกคามทางทหาร

จากประเทศเพื่อนบ้านภัยคุกคามรูปแบบใหม่ และอาชญากรรมข้ามชาติ รวมไปถึงการก่อความไม่สงบในจังหวัดชายแดนภาคใต้การใช้เทคโนโลยีที่ทันสมัยโดยเฉพาะเทคโนโลยี AI จะเป็นปัจจัยส่งเสริมให้การปฏิบัติการ ด้านการข่าวเป็นไปอย่างรวดเร็วถูกต้อง และทันเวลา

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๒ สรุปได้ว่า ในส่วนของ ปัญหา/ความท้าทายในการใช้เทคโนโลยีของกองทัพบกนั้น กองทัพบกมีการใช้ระบบเทคโนโลยีสารสนเทศในการปฏิบัติงานโดยอาจแบ่งประเภทของการนำมาใช้งานใน ๒ แบบ คือ เป็นระบบที่หน่วยดำเนินการพัฒนาขึ้นมาด้วยตนเอง และระบบที่ได้จากการจ้างผู้ประกอบการภายนอกเข้ามาดำเนินการให้ ทั้งนี้จากข้อมูลผลการปฏิบัติงานด้านการข่าวของกองทัพบกที่ผ่านมา มีประเด็นปัญหาของการใช้เทคโนโลยี เพื่อสนับสนุนการปฏิบัติงานที่สำคัญสรุป ได้แก่ ความปลอดภัย, ความท้าทายในเรื่องของ Generation Gap หรือความต่างของอายุและช่วงวัย เนื่องจากเทคโนโลยีนั้นมีการอัพเดต และปรับเปลี่ยนอยู่ตลอดเวลา คนรุ่นเก่าจะเรียนรู้วิธีการใช้เทคโนโลยีได้ยากกว่าคนรุ่นใหม่, ความท้าทายเรื่องความถูกต้องและแม่นยำของเทคโนโลยี, ปัญหาด้านความรู้ความสามารถด้านเทคโนโลยีของกำลังพล, ปัญหาด้านงบประมาณ และปัญหาด้านโครงสร้างหน่วยงานที่ไม่เอื้อต่อการทำงานข่าวที่ต้องการความรวดเร็ว

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๓ สรุปได้ว่า การดำเนินการข่าวกรองไซเบอร์ของ ทบ. ต้องได้รับการปรับปรุง เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นในปัจจุบัน โดย ทบ. ต้องให้ความสำคัญด้วยการใช้กลยุทธ์เชิงรุกในการพัฒนาขีดความสามารถของหน่วยข่าวของกองทัพบกรวมทั้งขีดความสามารถด้านสารสนเทศของหน่วยขึ้นตรงกองทัพบก

การพัฒนาขีดความสามารถของ ทบ. มีความเหมือนและแตกต่างกับการพัฒนาในเรื่องเดียวกันของมิตรประเทศ โดยประเด็นที่เหมือนกัน เช่น รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ ในปัจจุบัน ได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์มาประยุกต์ใช้กับหน่วยงานของตนเอง โดยมีกระบวนการการทำงานหลัก คือ Identify Protect Detect Respond and Recovery โดยมีประเด็นที่ต่างกันเช่น มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ โดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์(Cyber Intelligence) จะเป็นหน้าที่และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด

การพัฒนาต้นแบบ หรือขีดความสามารถด้านการข่าวกรองไซเบอร์ต้องสอดคล้องกับแนวทางการพัฒนา ทบ. ตามแผนที่กำหนด เพื่อให้สอดคล้องกับแนวทางการใช้กำลังและภารกิจของ ทบ. ในอนาคต โดยต้องมีการดำเนินการใน ๔ ด้าน คือ โครงสร้างกำลัง ความพร้อมรบ ความต่อเนื่องในการรบ และความทันสมัย เพื่อให้บรรลุเป้าหมายในการเสริมสร้างขีดความสามารถที่ ทบ. ต้องการ โดยต้องคำนึงถึงปัจจัยแวดล้อมที่เป็นทั้งข้อสนับสนุนและข้อจำกัด เช่น ระยะเวลา งบประมาณ กฎระเบียบและนโยบาย เป็นต้น

ผลการศึกษามีข้อเสนอแนะในเรื่อง ข้อเสนอแนะแนวนโยบายและหลักปฏิบัติ (Policies and Practices), ข้อเสนอแนะด้านการบริหารจัดการข้อมูล, ข้อเสนอแนะด้านศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capability) และข้อเสนอแนะด้านการใช้ประโยชน์จากข้อมูล เพื่อสนับสนุนภารกิจโดยเฉพาะงานด้านการข่าวกรองไซเบอร์ ทั้งนี้ สำหรับการวิจัยในโอกาสต่อไปนั้นสามารถนำข้อมูลที่รวบรวมไว้ในครั้งนี้เป็นข้อมูลพื้นฐานในการดำเนินการศึกษาวิจัยที่เกี่ยวข้องกับงานด้านการทหารอื่น ๆ ได้ เช่น การใช้ BIG DATA และ AI ในการเสริมสร้างขีดความสามารถงานข่าวกรองไซเบอร์ของ ทบ. ในเรื่อง การวางแผนรวบรวมข่าวสาร การรวบรวมข่าวสาร การวิเคราะห์ข่าวกรองไซเบอร์ การใช้และการกระจายข่าวกรองไซเบอร์ การบูรณาการข่าวกรองไซเบอร์ และการประเมินประสิทธิภาพการดำเนินการข่าวกรองไซเบอร์ของหน่วย

Abstract

Title Cyber threats Intelligence challenges in the 21st century : Policy guidelines for developing the Army's Cyber Intelligence (CYBINT) operations.

Field Military

Name Major General Prasert Muadjienga **Course** NDC **Class** 65

In this research study, the researcher has set 3 research objectives as follows: Objective 1: to study the security environment; Especially cyber security and cyber threats that affect security. Objective 2: to study the implementation pattern, status, problems, and obstacles in intelligence operations, especially the Cyber Intelligence of the Royal Thai Army at present, and the third objective is to suggest guidelines for developing the Royal Thai Army's Cyber Intelligence operations. The study can answer the objectives, they are summarized as follows.

The results of the study that answered the 1st research objective can be concluded that the world is currently in an era of change where it is fast and unpredictable. Globalization and technological advancement play a leading role in everything. This leads to a wide range of factors affecting security. Non-State Actors or groups will play a more influential role in the activities that affect the stability. Assessment of threats that affect national security in the present found that security issues that will affect Thailand include international politics, the expansion of the influence and role of superpowers in Southeast Asia, the expansion of regional international relations, territorial conflicts and the use of military force, the unrest situation in the southern border provinces, transnational Threats, illegal Migration and Post-COVID-19 Security. Directorate of Intelligence of The Royal Thai Army is the Army's primary intelligence agency and therefore must be equipped to effectively deal with all forms of threats. Especially land threats such as military threats from neighboring countries, hybrid threats and transnational crime Including the insurgency in the southern border provinces. The use of modern technology, especially AI technology, will be a factor that will promote speedy, accurate, and timely intelligence operations.

The results of the study that answered the 2nd research objective can be concluded that in terms of problems/challenges in the use of technology by the Royal Thai Army. The Royal Thai Army uses information technology systems in its operations. It may be categorized into two types of implementations: a system developed by the unit itself and systems obtained from outsourcing operators to operate. According to the information on the past performance of the Royal Thai Army's intelligence there are issues with using technology to support intelligence operations. The issues include security, generation gap challenges, technology accuracy and precision challenges, personnel technology competency issues, budget issues, and unit structure issues that affect the speed of operations.

The results of the study that answered research objective No. 3 concluded that the cyber intelligence operations of the Royal Thai Army must be improved in order to be able to respond to the increasing cyber threats at present. By using an aggressive strategy to develop the capabilities of the Army's intelligence units, including the information capabilities of the Army subordinate units. There are similarities and differences of cyber intelligence approach between Thailand and partnership countries.

Prototype development of cyber intelligence capabilities must be in line with the Development Guidelines for the Royal Thai Army. Action must be taken in four areas: force structure, combat readiness, combat sustainability, and modernization. To achieve the goal of enhancing the capacity required by the Royal Thai Army, consideration must be given to environmental factors that are both supportive and constrained, such as timelines, budgets, regulations and policies, etc.

The results of the study have recommendations on Policies and Practices, data management, development of Digital Capability for personnel and the use of data to support military missions especially cyber intelligence. As for future research, the findings from this study can be used as firsthand information for conducting other military-related research studies, such as using BIG DATA and AI to enhance capabilities of the Royal Thai Army's cyber intelligence in the area of planning, collection, analysis, distribution of cyber intelligence and evaluating the effectiveness cyber intelligence operations.

คำนำ

รายงานวิจัยเรื่อง “ภัยคุกคามทางไซเบอร์ (Cyber threats Intelligence) ความท้าทายงานการข่าวกรองในศตวรรษที่ ๒๑ : แนวทางการกำหนดนโยบายในการพัฒนางานข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของกองทัพบก” เป็นส่วนหนึ่งของการศึกษาในหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕ ของวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ มีวัตถุประสงค์ ๑. เพื่อศึกษาสภาวะแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้าน Cyber Security และ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง ๒. เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ในปัจจุบัน และ ๓. เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ทั้งนี้ เพื่อนำข้อมูลที่ได้จากการวิจัย นำมาเป็นแนวทางในการพัฒนาระบบงานด้านการข่าวกรองและการต่อต้านการข่าวกรองให้มีประสิทธิภาพมากยิ่งขึ้น

ผู้วิจัยหวังเป็นอย่างยิ่งว่า รายงานวิจัยฉบับนี้ จะก่อให้เกิดประโยชน์ให้กับหน่วยงานด้านการข่าวกรองของกองทัพบก และหน่วยงานอื่น ๆ ทั้งภายในและภายนอกกระทรวงกลาโหม หากรายงานวิจัยฉบับนี้มีความบกพร่องประการใด ผู้วิจัยขออภัยไว้ ณ โอกาสนี้ และยินดีน้อมรับข้อเสนอแนะของทุกท่านเพื่อนำมาปรับปรุงและพัฒนางานวิจัยในโอกาสต่อไป

พลตรี
(ประเสริฐ หมวดเชียงคะ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

กิตติกรรมประกาศ

งานวิจัยฉบับนี้ สำเร็จสมบูรณ์ได้ด้วยความกรุณาอย่างสูงจาก พลโท พงษ์เทพ แก้วไชโย อาจารย์ที่ปรึกษาหลัก และคณาจารย์วิทยาลัยป้องกันราชอาณาจักรทุกท่าน ที่กรุณาให้คำปรึกษา และให้คำแนะนำที่เป็นประโยชน์ต่อการศึกษาวิจัยครั้งนี้

ผู้วิจัยขอขอบคุณ พลตรี จักราวุธ อยู่นาน กำลังพลของกรมข่าวทหารบก ทั้งผู้ที่ปฏิบัติงานและผู้มีประสบการณ์ทั้งงานด้านข่าวกรอง และเทคโนโลยีสารสนเทศและการสื่อสาร โดยกรุณาสนับสนุนข้อมูลและให้ข้อแนะนำอีกทั้งข้อเสนอแนะเพิ่มเติม ซึ่งนับว่าเป็นประโยชน์อย่างยิ่งสำหรับการทำวิจัยในครั้งนี้

พลตรี
(ประเสริฐ หมวดเชียงคะ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันโลกอยู่ในยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยีทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง บุคคล หรือกลุ่มบุคคลที่ไม่ใช่รัฐ (Non - State Actor) จะเป็นผู้มีบทบาทมีอิทธิพลมากขึ้น ในการดำเนินกิจกรรมที่ส่งผลกระทบต่อความมั่นคง นอกจากนี้ระบบความสัมพันธ์ระหว่างประเทศได้เปลี่ยนแปลงไปสู่ความสัมพันธ์ แบบหลายขั้วอำนาจ (Multi - Polar) มีการคานอำนาจ หรือความพยายามในการลดบทบาทนำของประเทศมหาอำนาจมิให้เป็นผู้นำที่ครองความเป็นประเทศมหาอำนาจเพียงผู้เดียว (Hegemon) การเปลี่ยนแปลงดังกล่าวส่งผลให้แต่ละประเทศต่างมุ่งปกป้อง และรักษาผลประโยชน์ของตนเองเป็นสำคัญ และมักรวมกลุ่มพันธมิตรลักษณะเฉพาะกิจขนาดต่าง ๆ เพื่อพิทักษ์ผลประโยชน์ร่วมกัน

พัฒนาการของระบบคอมพิวเตอร์ และการเปลี่ยนแปลงทางด้านเทคโนโลยีที่รวดเร็วในปัจจุบันได้ส่งผลกระทบต่อกิจการ และการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์ และเทคโนโลยีในหลายทศวรรษที่ผ่านมา ทำให้ยุคสมัยปัจจุบันเกิดการปฏิวัติสารสนเทศ (information revolution) ซึ่งเกี่ยวข้องกับการประมวลผล และกระจายสารสนเทศอย่างกว้างขวาง จนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดด และก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “พื้นที่ไซเบอร์” (cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (national security) จึงได้รับผลกระทบจากการปฏิวัติสารสนเทศ และปรากฏการณ์ของพื้นที่ไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “การรักษาความมั่นคงปลอดภัยด้านไซเบอร์” (cyber security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้ง ยังมีผู้กล่าวถึงคุณลักษณะของพื้นที่ไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน ภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (defense) การยับยั้ง (deterrence) และการโจมตี (attack) ในพื้นที่ไซเบอร์มากขึ้น

กองทัพบกกำหนดความรับผิดชอบในการดำเนินงานข่าวกรอง โดยใช้ประเภทของข่าวกรองเป็นหลัก ๓ ประการ คือ งานข่าวกรองทางยุทธศาสตร์ งานข่าวกรองทางยุทธวิธี และงานข่าวกรองเพื่อความมั่นคง โดยขอบเขตความรับผิดชอบงานข่าวกรองเพื่อความมั่นคง เป็นการดำเนินการข่าวกรอง เพื่อสนับสนุนภารกิจของกองทัพบกในการรักษาความมั่นคงของรัฐ การรักษาผลประโยชน์ของชาติ และการพัฒนาประเทศ ตามขอบเขตของภารกิจที่ได้รับมอบ นอกเหนือจากการดำเนินงานข่าวกรองทางยุทธศาสตร์ ข่าวกรองทางยุทธวิธี และข่าวกรองเพื่อความมั่นคง ที่เป็นประเภทหลักของข่าวกรองในการดำเนินการข่าวกรองแล้ว ยังมีการแบ่งประเภทข่าวกรองตามลักษณะของการปฏิบัติงาน ความมุ่งหมายและเครื่องมือข่าวกรอง อีก ๗ ประเภท คือ ข่าวกรองทางบุคคล (Human Intelligence : HUMINT), ข่าวกรองทางสัญญาณ (Signal Intelligence : SIGINT), ข่าวกรองทางการภาพ (Imagery Intelligence : IMINT), ข่าวกรองภูมิสารสนเทศ (Geospatial Intelligence : GEOINT), ข่าวกรองเครื่องมือวัดและสัญญาณแสดง (Measurement and Signature Intelligence : MASINT), ข่าวกรองทางเทคนิค (Technical Intelligence : TECHINT) และข่าวกรองจากแหล่งข่าวเปิด (Open Source Intelligence : OSINT)

เนื่องจากการรวบรวมข่าวสารทั้งปกปิดและเปิดเผย การวิเคราะห์ และการประเมินค่าข่าวสารดังกล่าว เพื่อผลิตเป็นข่าวกรอง คือ สิ่งที่สำคัญยิ่งต่อการประเมินความล่อแหลม และการรับประกันต่อความอยู่รอดของระบบทางการทหาร โดยระเบียบปฏิบัติของการรวบรวมข่าวกรองตามปกติ มิได้กล่าวถึงการผสมกลมกลืนระหว่างเทคโนโลยีกับขีดความสามารถในพื้นที่ไซเบอร์เอาไว้ ภัยคุกคามทางไซเบอร์ จึงเป็นสิ่งที่ท้าทายต่อการวิเคราะห์ความล่อแหลม และผลกระทบต่อความมั่นคง จึงเป็นประเป็นที่น่าสนใจว่าการดำเนินการข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของหน่วยข่าวกรองกองทัพบกจะมีรูปแบบ หรือพัฒนาการอย่างเป็นระบบได้อย่างไร

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาสภาวะแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้านไซเบอร์ (Cyber Security) และ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง

๒. เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ในปัจจุบัน

๓. เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก

ขอบเขตของการวิจัย

๑. ศึกษาข้อมูลเฉพาะโดยเน้นในเรื่อง ข่าวกรองไซเบอร์ (Cyber intelligence)

๒. เอกสารในการศึกษาวรรณกรรมบางส่วนเป็นเอกสารที่มีชั้นความลับของทางราชการ

๓. การสัมภาษณ์ผู้ทรงคุณวุฒิที่มีความรู้ ประสบการณ์เกี่ยวกับงานด้านความมั่นคง การข่าวกรองและการต่อต้านการข่าวกรอง และงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

วิธีดำเนินการวิจัย

การศึกษาวิจัยฉบับนี้ ดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับใช้การวิจัยเชิงพรรณนา (Descriptive Research) ดังนี้

๑. การรวบรวมข้อมูล

๑.๑ ข้อมูลปฐมภูมิ ดำเนินการโดยการรวบรวมจากผลการปฏิบัติราชการ ข้อมูลผลการประชุม และการสัมมนาทางวิชาการของหน่วยงาน รวมทั้งการสอบถามผู้เชี่ยวชาญ และผู้ทรงคุณวุฒิในประเด็นที่กำหนด เช่น ความมั่นคงปลอดภัยทางไซเบอร์ การพัฒนารัฐบาลดิจิทัล การข่าวกรองไซเบอร์ เป็นต้น

๑.๒ ข้อมูลทุติยภูมิ ดำเนินการโดยการศึกษาจากตำราและเอกสารต่าง ๆ การรวบรวมจากแหล่งข้อมูลที่ได้รับการยอมรับ และน่าเชื่อถือ ทั้งหนังสือพิมพ์ บทความ เอกสารวิชาการ เอกสารราชการ นอกจากแหล่งทุติยภูมิ จากแหล่งภาษาไทยแล้ว ยังได้รวบรวมข้อมูลจากแหล่งข้อมูลต่างประเทศด้วย

๒. การวิเคราะห์ข้อมูล : ดำเนินการโดยใช้การวิเคราะห์เนื้อหา (Context Analysis) และการวิเคราะห์ เปรียบเทียบ และสังเคราะห์ข้อมูลทฤษฎี หลักการต่าง ๆ ด้านการข่าวกรอง และความมั่นคง

๓. การนำเสนอข้อมูล : นำเสนอข้อมูลแบบรายงานวิจัยเชิงพรรณนา และวิเคราะห์นำเสนอแนวคิดใหม่ ๆ จากการวิจัย

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทราบถึงสถานการณ์ภัยคุกคามทางไซเบอร์ ที่ส่งผลกระทบต่อความมั่นคง และความพร้อมของกองทัพบก ในการปฏิบัติงานด้านการข่าวกรองเพื่อรับกับภัยคุกคามดังกล่าว

๒. ทราบถึงสภาพอุปสรรค ปัญหาข้อขัดข้องของ งานข่าวกรองไซเบอร์

๓. เพื่อเสนอแนะแนวทางพัฒนาและการใช้งาน งานข่าวกรองไซเบอร์ ที่จะสามารถนำไปใช้สนับสนุนภารกิจกองทัพบกได้ในอนาคต

คำจำกัดความ

ภัยคุกคาม หมายถึง ภาวะหรือสถานการณ์ที่ก่อให้เกิดความไม่มั่นคง ซึ่งเป็นปัญหาที่มีความรุนแรง สลับซับซ้อน หากไม่ดำเนินการแก้ไขจะเกิดผลกระทบในวงกว้างต่อความมั่นคงแห่งชาติ

การบูรณาการด้านการข่าว หมายถึง กระบวนการที่ก่อให้เกิดความสัมพันธ์ของหน่วยงานด้านการข่าวที่รวมตัวกัน

เป็นประชาคมข่าวกรอง โดยปฏิบัติงานร่วมกันในศูนย์ประสานข่าวกรองแห่งชาติ ทั้งนี้การปฏิบัติงานจะมีทั้งการแลกเปลี่ยนข้อมูลข่าวสารและการปฏิบัติการร่วมกันตามห้วงสถานการณ์

การรักษาความมั่นคงปลอดภัยไซเบอร์

หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์

หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่ง หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง

ไซเบอร์ หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

ข่าวกรองไซเบอร์

หมายถึง ข่าวสารต่าง ๆ ที่ได้รับความสนใจและมีความเกี่ยวข้องกับระบบเครือข่าย ระบบสารสนเทศ ที่ผ่านการตรวจสอบวิเคราะห์หรือได้รับพิสูจน์ถึงความน่าจะเป็นและความน่าเชื่อถือ ซึ่งสามารถนำไปใช้ในกระบวนการตัดสินใจได้

บทที่ ๒
การทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง

ในการศึกษาหัวข้อเรื่อง ภัยคุกคามทางไซเบอร์ (Cyber threats Intelligence) ความท้าทายงานการข่าวกรองในศตวรรษที่ ๒๑ : แนวทางการกำหนดนโยบายในการพัฒนางานข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของกองทัพบก ได้มีการนำทฤษฎีและแนวคิดที่เกี่ยวข้องมาใช้เพื่อเป็นแนวทางในการศึกษาดังนี้

๑. ยุทธศาสตร์ชาติ ๒๐ ปี (ด้านความมั่นคง)(พ.ศ. ๒๕๖๑ - ๒๕๘๐)
๒. ยุทธศาสตร์ข่าวกรองแห่งชาติ (พ.ศ. ๒๕๕๘ - ๒๕๖๔)
๓. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๔. แผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม (พ.ศ. ๒๕๖๖ - ๒๕๗๐)
๕. ทฤษฎีด้านการข่าวกรอง (วงรอบข่าวกรอง และข่าวกรองไซเบอร์)
๖. เอกสารวิจัยที่เกี่ยวข้อง
๗. กรอบแนวคิดในการวิจัย
๘. สรุป

ยุทธศาสตร์ชาติ ๒๐ ปี (ด้านความมั่นคง)(พ.ศ. ๒๕๖๑ - ๒๕๘๐)

๑. กล่าวทั่วไป

ยุทธศาสตร์ชาติด้านความมั่นคงมีเป้าหมายสำคัญในภาพรวมระยะ ๒๐ ปี ที่เป็นรูปธรรมชัดเจน คือ “ประเทศชาติมั่นคง ประชาชนมีความสุข” โดยเร่งเสริมสร้างความเข้มแข็งและความรักความสามัคคีปรองดองของคนในชาติ ตลอดถึงการปลุกจิตสำนึกด้านความมั่นคงให้เกิดขึ้นในประชาชนทุกระดับ การพัฒนาระบบงานด้านการข่าวให้มุ่งเน้นการบูรณาการข้อมูลข่าวสารด้านความมั่นคงอย่างเป็นระบบ การพัฒนาปรับปรุงกลไกการขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคง และกลไกในการป้องกันและแก้ไขปัญหาความมั่นคงให้มีเอกภาพ มีประสิทธิภาพ และมีการบูรณาการการดำเนินงานอย่างแท้จริง โดยปัญหาความมั่นคงเร่งด่วนที่จะต้องดำเนินการแก้ไขประกอบด้วย ปัญหาความมั่นคงปลอดภัยในชีวิตและทรัพย์สิน ปัญหายาเสพติด ปัญหาความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ ปัญหาอาชญากรรมทางไซเบอร์ และปัญหาการทุจริตในระบบราชการ

๒. เป้าหมายและประเด็นยุทธศาสตร์ชาติด้านความมั่นคง

๒.๑ เป้าหมายของยุทธศาสตร์ชาติด้านความมั่นคง ประกอบด้วย ๕ เป้าหมายหลัก คือ ประชาชนอยู่ดี กินดี และมีความสุข, บ้านเมืองมีความมั่นคงในทุกมิติ และทุกระดับ, กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชน และภาคประชาชน มีความพร้อมในการป้องกัน และแก้ไขปัญหาความมั่นคง, ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชม และได้รับการยอมรับโดยประชาคมระหว่างประเทศ และการบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ

๒.๒ ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง : ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง ประกอบด้วย ๕ ประเด็นหลัก คือ การรักษาความสงบภายในประเทศ, การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง, การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ, การบูรณาการความร่วมมือด้านความมั่นคงกับอาเซียนและนานาชาติ รวมถึงองค์กรภาครัฐและที่มิใช่ภาครัฐ และการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม

๓. ประเด็นยุทธศาสตร์ การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ

การดำเนินการในประเด็นยุทธศาสตร์นี้ เป็นการดำเนินการเพื่อยกระดับขีดความสามารถของกองทัพ และหน่วยงานด้านความมั่นคงทั้งระบบของประเทศ ให้มีความพร้อมในการป้องกัน และรักษาอธิปไตยของประเทศ รวมทั้งสามารถติดตาม ป้องกัน แก้ไข และรับมือกับปัญหาความมั่นคงทุกมิติทุกรูปแบบ และทุกระดับแบบบูรณาการให้มีความพร้อม และเพียงพอต่อการป้องกันภัยคุกคามทุกมิติ ทุกรูปแบบ และทุกระดับความรุนแรง โดยมีแนวทาง/วิธีการ ในการดำเนินการ ที่สำคัญคือ

๓.๑ การพัฒนาระบบงานข่าวกรองแห่งชาติแบบบูรณาการอย่างมีประสิทธิภาพ : เพื่อให้สามารถติดตาม แจ้งเตือน ระงับยับยั้ง และป้องกันปัญหาและภัยคุกคามได้อย่างมีประสิทธิภาพ สามารถประเมินสถานการณ์ได้ถูกต้อง แม่นยำ และทันเวลา โดยเสริมสร้าง พัฒนา และบูรณาการขีดความสามารถของระบบงานข่าวกรอง หน่วยงานข่าวกรอง และประชาคมข่าวกรองในประเทศให้ทันสมัย ทันสถานการณ์ ทั้งด้านศักยภาพของบุคลากร ยุทโธปกรณ์ เทคโนโลยี และระบบข้อมูลขนาดใหญ่ สามารถครอบคลุมการใช้งานได้อย่างครบถ้วนและต่อเนื่อง มีการบูรณาการข้อมูล และนำผลผลิตด้านข่าวกรองไปใช้ในการบริหารจัดการปัญหา และความมั่นคงของชาติในทุกมิติ และทุกด้าน รวมทั้งให้มีการเสริมสร้างความร่วมมือกับภาคประชาชนในรูปแบบประชารัฐ และประชาคมข่าวกรองต่างประเทศอย่างแน่นแฟ้น

๓.๒ การพัฒนาและผนึกพลังอำนาจแห่งชาติ กองทัพและหน่วยงานความมั่นคง รวมทั้งภาครัฐ และภาคประชาชน ให้พร้อมป้องกันและรักษาอธิปไตยของประเทศ และเผชิญกับภัยคุกคามได้ทุกมิติทุกรูปแบบ และทุกระดับ : เพื่อให้ทรัพยากรที่สำคัญ และจำเป็นทั้งปวงของกองทัพและหน่วยงานความมั่นคง ได้รับการพัฒนา เสริมสร้างศักยภาพ ให้มีความพร้อม รวมทั้งระบบบริหารจัดการในการป้องกันประเทศ และการป้องกันภัยคุกคามทุกมิติ ทุกรูปแบบ และทุกระดับความรุนแรง ตลอดจนการป้องกัน และบรรเทาสาธารณภัย สามารถระดมทรัพยากรได้อย่างเป็นระบบ

และมีขั้นตอนชัดเจน โดยการจัดทำแผนพัฒนา และผนึกกำลังทรัพยากร รวมถึงขีดความสามารถทั้งปวงของกองทัพ หน่วยงานด้านความมั่นคงทั้งภาครัฐ ภาคเอกชน และภาคประชาชน พร้อมพัฒนาคนโครงสร้างกำลังรบ และยุทโธปกรณ์ให้เหมาะสมเพียงพอ และเป็นรูปธรรม สามารถรับมือกับภัยคุกคามได้ทุกมิติ ยกระดับการฝึกร่วมให้เป็นแบบบูรณาการที่ทันสมัย มีความสมบูรณ์ เสริมสร้างความสัมพันธ์ในการปฏิบัติการร่วม และการป้องกันภัยคุกคามด้านความมั่นคงกับเพื่อนบ้าน และมิตรประเทศ มิให้เกิดข้อขัดแย้ง หรือปัญหาเกี่ยวกับเขตแดนทางบก และอาณาเขตทางทะเล พร้อมทั้งมีกลไกแก้ไขปัญหาความเห็นต่าง หรือความขัดแย้ง ตลอดไปจนถึงการส่งเสริมการวิจัย และพัฒนาวิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ การพลังงานทหาร กิจการอวกาศ เทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง เพื่อสร้างหลักประกันให้ประเทศไทยก้าวไปสู่การมีอุตสาหกรรมป้องกันประเทศแบบอัจฉริยะในอนาคต มีเทคโนโลยีเป็นของตนเอง และลดการพึ่งพา หรือนำเข้าจากต่างประเทศได้อย่างเหมาะสม

๓.๓ การพัฒนาระบบเตรียมพร้อมแห่งชาติ และการบริหารจัดการภัยคุกคามให้มีประสิทธิภาพ : เพื่อให้มีความพร้อมเผชิญกับสภาวะไม่ปกติ ภัยคุกคามทุกมิติ ทุกรูปแบบ และทุกระดับ รวมทั้งภัยพิบัติ และภัยคุกคามรูปแบบต่าง ๆ ได้อย่างแท้จริง โดยพัฒนาปรับปรุงนโยบาย แนวทาง ระบบ กลไกการบริหารจัดการ ตลอดถึงแผนการปฏิบัติที่เกี่ยวข้องทั้งปวงให้ชัดเจน มีประสิทธิภาพ ครอบคลุม ผลักดันให้ทุกภาคส่วนมีการฝึกร่วมกันในทุกขั้นตอนอย่างต่อเนื่อง เสริมสร้างความร่วมมือกันอย่างบูรณาการของทุกภาคส่วน ทั้งภายใน และภายนอกประเทศ ยกระดับการแบ่งปันข้อมูล ทรัพยากร การพัฒนาเทคโนโลยี และการฝึกอบรมให้ทุกส่วนรู้จัก และเข้าใจขั้นตอนการปฏิบัติต่าง ๆ ตลอดถึงพัฒนาปรับปรุงกฎหมาย และกระบวนการที่เกี่ยวข้องให้มีความทันสมัยสอดคล้องกับบริบทที่เปลี่ยนแปลงไป

ยุทธศาสตร์ข่าวกรองแห่งชาติ (พ.ศ. ๒๕๕๘ - ๒๕๖๔)

ตามที่สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้ประเมินสถานการณ์ภัยคุกคามความมั่นคง และสถานการณ์ที่เป็นโอกาส ในการเสริมสร้างความมั่นคงในระยะ ๗ ปี (พ.ศ. ๒๕๕๘ - ๒๕๖๔) พบว่า

๑. สถานการณ์โลกในภาพรวมมีแนวโน้มเปลี่ยนแปลงจากระบบขั้วอำนาจเดียวเข้าสู่ระบบหลายขั้วอำนาจส่วนปัญหาการก่อการร้ายยังคงเป็นภัยคุกคามโลก และปัญหาอาชญากรรมข้ามชาติมีแนวโน้มขยายตัวเพิ่มขึ้น

๒. สถานการณ์ในภูมิภาคเอเชียตะวันออกเฉียงใต้จากการรวมตัวเป็นประชาคมอาเซียนในปี ๒๕๕๘ จะเป็นโอกาสอย่างมาก สำหรับสมาชิกอาเซียนในด้านเศรษฐกิจและการค้า แต่ก็ยังอาจจะประสบปัญหาด้านความมั่นคงที่ซับซ้อนมากขึ้น

๓. สถานการณ์ภายในประเทศยังคงมีความรุนแรง และมีแนวโน้มที่จะขยายตัวในประเด็นที่สำคัญ คือ การละเมิดสถาบันพระมหากษัตริย์ ความแตกแยกของคนในชาติ ความไม่สงบ

ในพื้นที่จังหวัดชายแดนภาคใต้ภัยคุมคามข้ามชาติ ภัยคุกคามใหม่ และความมั่นคงทางเทคโนโลยีสารสนเทศ

ดังนั้น จึงได้มีการจัดทำยุทธศาสตร์ข่าวกรองแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔ ขึ้น โดยมีวัตถุประสงค์ เพื่อให้มีงานข่าวกรองที่มีคุณภาพ และแจ้งเตือนภัยคุกคามได้อย่างมีประสิทธิภาพรวมทั้งสนับสนุนโอกาส และผลประโยชน์ในการแข่งขันของไทย และให้เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรองทั้งในประเทศ และต่างประเทศ รวมถึงเครือข่ายภาคเอกชนและประชาชน อีกทั้งเสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรอง อันประกอบด้วย ๓ ยุทธศาสตร์ ได้แก่

๑. ยุทธศาสตร์ข่าวกรองเพื่อเสริมสร้างความมั่นคงที่เป็นแก่นหลักของชาติมี ๓ กลยุทธ์ ประกอบด้วย เสริมสร้างความมั่นคงของสถาบันหลัก, เสริมสร้างความเป็นธรรมและความสมานฉันท์ และเสริมสร้างการแก้ไข และป้องกันปัญหาความไม่สงบ และการใช้ความรุนแรงในจังหวัดชายแดนภาคใต้

๒. ยุทธศาสตร์ข่าวกรองเพื่อป้องกันและแก้ไขภัยคุกคามทั่วไป และเสริมสร้างโอกาสด้านความมั่นคง มี ๖ กลยุทธ์ ประกอบด้วย ป้องกันและแก้ไขภัยคุกคามข้ามชาติ, ป้องกันและแก้ไขภัยคุกคามระบบสารสนเทศ, ป้องกันและแก้ไขภัยคุกคามใหม่, พัฒนาศักยภาพการต่อต้านข่าวกรอง, รักษาและเสริมสร้างผลประโยชน์ของชาติในเวทีความสัมพันธ์ระหว่างประเทศ และการป้องกันประเทศ และประเมินสถานการณ์และแนวโน้มเชิงยุทธศาสตร์เพื่อเสริมสร้างผลประโยชน์และโอกาสของประเทศ

๓. ยุทธศาสตร์สนับสนุนงานข่าวกรอง มี ๔ กลยุทธ์ประกอบด้วย เสริมสร้างศักยภาพงานข่าวกรอง, ส่งเสริมการบูรณาการของประชาคมข่าวกรองให้มีเอกภาพ, พัฒนาความเป็นหุ้นส่วนทางข่าวกรองกับทุกภาคส่วน และสร้างสภาวะแวดล้อมที่เอื้อต่อการทำงานข่าวกรอง กล่าวได้ว่า ยุทธศาสตร์ข่าวกรองแห่งชาติเป็นกรอบที่ให้ความสำคัญ ในการดำเนินงานของประชาคมข่าวกรองและหน่วยราชการอื่น ๆ ที่มิใช่หน่วยข่าว เพื่อให้เกิดเอกภาพในการปฏิบัติให้สอดคล้องเป็นไปในลักษณะบูรณาการมีทิศทางและเป้าหมายเดียวกัน ทั้งนี้ โดยคำนึงถึงความมั่นคงและผลประโยชน์แห่งชาติเป็นเป้าหมายสูงสุด ซึ่งการดำเนินการจะมุ่งต่อเป้าหมายภัยคุกคาม ที่เป็นแก่นหลักของประเทศ เพื่อเสริมความมั่นคงและสภาวะแวดล้อมที่สันติสุข ลดความเสี่ยงจากเป้าหมายภัยคุกคามทุกรูปแบบ เสริมสร้างผลประโยชน์และโอกาสของประเทศ สร้างภูมิคุ้มกันของสังคมทุกระดับ และพัฒนาศักยภาพงานข่าวกรอง

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลใช้บังคับเมื่อวันที่ ๒๘ พฤษภาคม ๒๕๖๒ โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้ สำนักงานคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐ และเอกชน ไม่ว่าในสถานการณ์ทั่วไป หรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

สาระสำคัญของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้แก่

๑. ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วย

๑.๑ นายกรัฐมนตรี เป็นประธานกรรมการ

๑.๒ กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ และเลขาธิการสภาความมั่นคงแห่งชาติ

๑.๓ กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนภาพที่ ๒ - ๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๒. ให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” ประกอบด้วย

๒.๑ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

๒.๒ กรรมการโดยตำแหน่ง ได้แก่ ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคมปลัดกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงสาธารณสุข ผู้บัญชาการตำรวจแห่งชาติ ผู้บัญชาการทหารสูงสุด เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และเลขาธิการคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

๒.๓ กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

๓.๑ การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๓.๒ การสร้างมาตรการและกลไก เพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๓.๓ การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๓.๔ การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๕ การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๖ การพัฒนาบุคลากร และผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐ และเอกชน

๓.๗ การสร้างความตระหนัก และความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๘ การพัฒนาระเบียบ และกฎหมาย เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การรับมือกับภัยคุกคามทางไซเบอร์ : มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้น ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุม หรือกำกับดูแลของตนโดยเร็ว

๕. ลักษณะของภัยคุกคามทางไซเบอร์ : แบ่งออกเป็น ๓ ระดับ ดังต่อไปนี้

๕.๑ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของ ประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง

๕.๒ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่มีการโจมตีระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตี และการโจมตีดังกล่าว มีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ เสียหายจนไม่สามารถทำงาน หรือให้บริการได้

๕.๓ ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ที่มีลักษณะ ล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานจาก ส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ ทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน

แผนภาพที่ ๒ - ๒ ระดับภัยคุกคามทางไซเบอร์

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

แผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม (พ.ศ. ๒๕๖๖ - ๒๕๗๐)

การจัดทำแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กห. พ.ศ. ๒๕๖๖ – ๒๕๗๐ เป็นการดำเนินการโดยปรับปรุงจากการจัดทำแผนปฏิบัติการด้านไซเบอร์เพื่อความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) กระทรวงกลาโหม ซึ่งจะสิ้นสุดในปี ๒๕๖๕ เพื่อให้เกิดความต่อเนื่องในการดำเนินการ และมีแนวทางการดำเนินการที่ชัดเจนเป็นรูปธรรม โดยยึดถือตามอำนาจหน้าที่ของกระทรวงกลาโหมที่กฎหมายกำหนด และแผนระดับที่ ๓ ที่เกี่ยวข้อง การดำเนินการเพื่อให้บรรลุเป้าหมายสำคัญในภาพรวมระยะ ๒๐ ปีที่เป็นรูปธรรมชัดเจน คือ “ประเทศชาติมั่นคง ประชาชนมีความสุข”

โดยประเทศชาติมีความมั่นคงในทุกมิติและทุกระดับ ภายใต้สภาวะแวดล้อมด้านความมั่นคง นั้นได้ยึดถือแนวทางการดำเนินการ หรือแนวความคิดทางยุทธศาสตร์จำนวน ๓ แนวความคิด ได้แก่

๑. การป้องกันเชิงรุก (Active Defence) โดยจัดเตรียมกำลัง เสริมสร้าง พัฒนาและบริหารจัดการทรัพยากรทั้งมวลให้กองทัพ และหน่วยงานด้านความมั่นคง สามารถพึ่งพาตนเองได้ และมีความพร้อมในการบูรณาการร่วมกัน หรือใช้กำลัง เพื่อการป้องปราม การแก้ไข และยุติความขัดแย้ง โดยต้องเป็นฝ่ายได้เปรียบอยู่เสมอ และพร้อมรับสถานการณ์ ทั้งในยามปกติและยามสงคราม ซึ่งการปฏิบัติการทางทหารต้องใช้การปฏิบัติในลักษณะของการปฏิบัติการยุทธ์ร่วมเป็นหลัก

๒. การผนึกกำลังป้องกันประเทศ (United Defence) ด้วยการนำทรัพยากรที่เป็นพลังอำนาจของชาติทุกประเภท ในทุกมิติทั้งด้านการทหาร การเมือง เศรษฐกิจ สังคมจิตวิทยา วิทยาศาสตร์และเทคโนโลยีมาบูรณาการอย่างมีระเบียบแบบแผน และเป็นระบบในภาวะปกติ เพื่อแก้ไขข้อจำกัดของชาติ รวมทั้งชดเชยอำนาจกำลังรบของกองทัพที่มีอยู่อย่างจำกัด และในภาวะสงคราม

๓. การสร้างความร่วมมือด้านความมั่นคง (Security Cooperation) ด้วยการใช้ทรัพยากรในการสนับสนุนรัฐบาล โดยสร้างความร่วมมือกับประเทศเพื่อนบ้าน ประเทศสมาชิกอาเซียน มิตรประเทศประเทศมหาอำนาจต่าง ๆ และองค์การระหว่างประเทศ ทั้งในระดับทวิภาคีและพหุภาคี เพื่อเสริมสร้างความมั่นคงร่วมกัน สร้างบรรยากาศความเป็นมิตร รักษาความเป็นกลาง ลดเงื่อนไข และลดโอกาสที่จะนำไปสู่ความขัดแย้ง รวมทั้งป้องกันมิให้ความขัดแย้งขยายขอบเขตออกไปนอกเหนือการควบคุม โดยยึดมั่นในหลักการแนวความคิดเชิงป้องกัน (Preventive)

ซึ่งแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กห. พ.ศ. ๒๕๖๖ – ๒๕๗๐ แบ่งออกเป็น ๓ แนวทาง ในการดำเนินการ/พัฒนา ดังนี้ การพัฒนาศักยภาพไซเบอร์ กห. โดยการเตรียมกำลังด้านไซเบอร์, การปฏิบัติการไซเบอร์ของ กห. โดยการใช้กำลังด้านไซเบอร์ และความร่วมมือด้านความมั่นคงไซเบอร์โดยการทำความร่วมมือ

ทฤษฎีด้านการข่าวกรอง (วงรอบข่าวกรอง และข่าวกรองไซเบอร์)

๑. วงรอบข่าวกรอง

การให้ได้มาซึ่งข่าวกรอง สามารถนำไปใช้ประโยชน์ในการปฏิบัติภารกิจ มีหลักการ/วิธีการในการดำเนินการที่เรียกว่า “วงรอบข่าวกรอง” โดยคู่มือราชการสนามว่าด้วยหลักนิยมการข่าวกรองของกองทัพบก พ.ศ. ๒๕๖๑ ระบุว่า การดำเนินงานตามวงรอบข่าวกรองมีอยู่ ๔ ขั้นตอน ดังนี้

๑.๑ ขั้นที่ ๑ การวางแผนรวบรวมข่าวสาร เพื่อกำหนดว่าผู้บังคับบัญชา และฝ่ายอำนวยการมีความต้องการข่าวกรองในเรื่องอะไร หน่วยใดจะทำหน้าที่ในการรวบรวมข่าวสาร และจะต้องรายงานให้เราทราบเมื่อใด โดยจะกำหนดออกมาในรูปของความต้องการข่าวกรองของผู้บังคับบัญชาที่แยกออกเป็นหัวข้อข่าวสารสำคัญ (หขส.) ซึ่งเป็นความต้องการข่าวกรองที่สำคัญ และมีความเร่งด่วนสูงกับความต้องการข่าวกรองอื่น ๆ (ตขอ.) ซึ่งเป็นความต้องการข่าวกรองที่มีระดับความสำคัญและความเร่งด่วนที่ต่ำกว่า ทั้งนี้ จะต้องแปลงความต้องการข่าวกรองออกมาให้อยู่ในรูปของรายการข่าวสารเฉพาะเจาะจง หรืออาจเรียกว่ารายการคำสั่ง/คำขอ จากนั้นจะเป็นการพิจารณาใช้หน่วย

หรือเจ้าหน้าที่รวบรวมข่าวสาร โดยคำนึงถึงขีดความสามารถ ความเหมาะสม ความสมดุล และความเพียงพอ นอกจากนั้นแผนรวบรวมข่าวสารยังมีประโยชน์ในการประเมินการปฏิบัติงานด้านการข่าวของหน่วย ว่ามีส่วนใดที่ยังเป็นจุดอ่อนได้อีกด้วย

๑.๒ ขั้นที่ ๒ การรวบรวมข่าวสาร เพื่อให้ได้มาซึ่งข่าวสารที่จะนำไปดำเนินกรรมวิธีผลิตเป็นข่าวกรอง ทั้งนี้ในการรวบรวมข่าวสารนั้น ผู้บังคับบัญชาจะต้องใช้ทุกขีดความสามารถของหน่วยให้ได้มาซึ่งข่าวสารที่จำเป็น ขณะเดียวกันนายทหารข่าวกรองจะต้องทำหน้าที่ในการกำหนดการใช้เครื่องมือรวบรวมข่าวสารทุกประเภทที่อยู่ในอัตราการจัดของหน่วยตนเอง หน่วยเหนือ หน่วยรอง และหน่วยข้างเคียง เพื่อตอบสนองต่อความต้องการข่าวกรองของผู้บังคับบัญชา สำหรับงานข่าวกรองประเภทต่าง ๆ ที่ใช้ในการรวบรวม อาทิ ข่าวกรองทางบุคคล (HUMINT) ข่าวกรองทางสัญญาณ (SIGINT) ข่าวกรองทางการภาพ (IMINT) ข่าวกรองภูมิสารสนเทศ (GEOINT) ข่าวกรองเครื่องมือวัดและสัญญาณแสดง (MASINT) ข่าวกรองทางเทคนิค (TECHINT) และข่าวกรองจากแหล่งข่าวเปิด (OSINT) อย่างไรก็ดี การรวบรวมข่าวสารสำหรับงานข่าวกรองยุทธศาสตร์ งานข่าวกรองเพื่อความมั่นคง และงานข่าวกรองทางยุทธวิธี อาจใช้เครื่องมือที่เหมือนหรือแตกต่างกันไป ตามขีดความสามารถและข้อจำกัดของเครื่องมือรวบรวมข่าวสารนั้น ๆ

๑.๓ ขั้นที่ ๓ การดำเนินกรรมวิธีต่อข่าวสาร กระทำเพื่อทำข่าวสารให้เป็นข่าวกรอง มีการดำเนินการแบ่งเป็น ๓ ขั้น คือ การบันทึก การประเมินค่า และการตีความ ทั้งนี้ ในการตีความนั้นยังมีการแบ่งการดำเนินการแบ่งเป็น ๓ ขั้น คือ การวิเคราะห์ การสนธิ และการอนุมาน

๑.๔ ขั้นที่ ๔ การใช้และการกระจายข่าวกรอง เพื่อส่งไปยังหน่วย หรือเจ้าหน้าที่ที่จะต้องใช้ประโยชน์ได้อย่างทันเวลา ด้วยแบบฟอร์มที่เหมาะสม ทั้งนี้ผู้ใช้ข่าวกรองที่เป็นความเร่งด่วนอันดับแรก คือ ผู้บังคับบัญชา

การปฏิบัติการวงรอบข่าวกรองเป็นงานที่ต่อเนื่อง และงานทั้ง ๔ ขั้น อาจจะเกิดขึ้นพร้อม ๆ กัน เช่น ในขณะที่กำลังรวบรวมข่าวสารอันใหม่จากแหล่งข่าวทั้งปวงอยู่นั้นจะดำเนินกรรมวิธีต่อข่าวสารที่ได้รวบรวมมาก่อนแล้ว เพื่อผลิตเป็นข่าวกรองและกระจายต่อไป นอกจากนั้นในการปฏิบัติการวงรอบข่าวกรอง ตามปกติแล้วจะดำเนินการไปตามลำดับขั้นตอน แต่ในบางกรณีอาจมีการข้ามขั้นตอนได้ เช่น ข่าวสารที่รวบรวมมาได้ อาจจะกระจายไปก่อน โดยที่ยังมิได้ดำเนินกรรมวิธีให้เป็นข่าวกรอง โดยคำนึงถึงความสำคัญของความรวดเร็วทันเวลา ในการถึงมือผู้ใช้มากกว่าความสมบูรณ์ และความถูกต้องของข่าวกรองนั้น

๒. ข่าวกรองไซเบอร์ (Cyber Intelligence)

เนื่องจากการรวบรวมข่าวสารทั้งปกปิด และเปิดเผย การวิเคราะห์ และการประเมินค่าข่าวสารดังกล่าว เพื่อผลิตเป็นข่าวกรอง คือ สิ่งที่สำคัญยิ่งต่อการประเมินความล่อแหลม และการรับประกันต่อความอยู่รอดของระบบทางการทหาร เมื่อระเบียบปฏิบัติของการรวบรวมข่าวกรองตามปกติ มิได้กล่าวถึงการผสมกลมกลืนระหว่างเทคโนโลยีกับขีดความสามารถในพื้นที่ไซเบอร์อย่างปัจจุบันทันด่วน ไปเป็นรูปแบบ และสิ่งที่ท้าทายต่อการวิเคราะห์ความล่อแหลม และความอยู่รอด

ต่อไป ข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) จึงถือกำเนิดขึ้นโดยใช้เป็นหลักการพื้นฐานอย่างหนึ่งของงานด้านการข่าวกรอง

๒.๑ ปัญหาของการใช้คำจำกัดความของคำว่า “ข่าวกรองไซเบอร์”

โดยทั่วไปแล้ว คำว่า “ข่าวกรองไซเบอร์” (cyber intelligence) หมายถึง ภัยคุกคามที่สามารถเกิดขึ้นได้ โดยไม่รู้ตัวในมิติของไซเบอร์ พร้อมกับผลกระทบที่ตามมาอย่างมหาศาล เช่น การทำลายทางกายภาพที่ก่อให้เกิดความวุ่นวาย ทางเศรษฐกิจ เป็นต้น ข่าวกรองไซเบอร์ จึงเป็นการประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรมของฝ่ายตรงข้ามในมิติของไซเบอร์ เพื่อสนับสนุนและแจ้งข่าวสารให้กับการปฏิบัติการเครื่องข่ายของหน่วยทั้งหมด ทั้งในแง่ของการปฏิบัติการเชิงรุก และการปฏิบัติการเชิงรับ แม้ว่าข่าวกรองไซเบอร์ ถือเป็นสิ่งจำเป็นยิ่งต่อการดำเนินกิจกรรมไซเบอร์ของหน่วย ข่าวกรองไซเบอร์ ในฐานะข้อบังคับของมืออาชีพ มีลักษณะของงานเร่งด่วน และจำเป็นต้องอาศัยทักษะเฉพาะด้าน เช่น การผสมผสานความรู้ทางเทคนิค (เช่น การปฏิบัติการบนเครือข่าย (network operations) การติดต่อสื่อสาร (communication) และนิติวิทยาศาสตร์ดิจิทัล (digital forensic) หรือวิศวกรรมย้อนกลับการใช้โปรแกรมที่ไม่พึงประสงค์ที่แฝงมากับข้อมูลที่อยู่บนเครือข่ายคอมพิวเตอร์ (malware reverse engineering) เป็นต้น) และทักษะการวิเคราะห์แบบดั้งเดิม (เช่น การทดสอบสมมุติฐาน (hypothesis) และทางเลือก (alternative) เป็นต้น)

อย่างไรก็ตาม การให้คำจำกัดความเฉพาะให้กับคำว่า “ข่าวกรองไซเบอร์” (cyber intelligence) ถือเป็นเรื่องยาก เพราะหากอยู่ภายใต้สมมุติฐานของข่าวกรองทางสัญญาณ (SIGINT) หมายถึง ข่าวกรองที่ได้รับจากสัญญาณใด ๆ ในขณะที่ข่าวกรองบุคคล หมายถึง ข่าวกรองที่ได้รับจากบุคคลแล้ว ฉะนั้น หากยึดถือแนวทางการให้คำจำกัดอย่างง่าย ๆ ข่าวกรองไซเบอร์ ก็จะหมายถึง ข่าวกรองที่รวบรวมได้จากพื้นที่ไซเบอร์นั่นเอง ทว่าคำว่า “พื้นที่ไซเบอร์” โดยทั่วไปแล้วหมายถึง เทคโนโลยีที่มีการเชื่อมโยงกันเป็นเครือข่าย (interconnected technology) ซึ่งถือเป็นส่วนหนึ่งของพื้นที่ไซเบอร์เท่านั้น ข่าวกรองไซเบอร์ จึงมีขอบเขตที่กว้างขวางมากกว่า โดยครอบคลุมมิติระดับโลกและเป็นพลวัตร (สรรพสิ่งที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง) และมีคุณลักษณะของการใช้แถบอิเล็กตรอนและแม่เหล็กไฟฟ้า โดยมีวัตถุประสงค์เพื่อสร้างสรรค์ (create) จัดเก็บ (store) ปรับเปลี่ยน (modify) แลกเปลี่ยน (exchange) แบ่งปัน (share) คัดเลือก (extract) ใช้ (use) และกำจัด (eliminate) ข่าวสาร รวมถึงการรบกวนทรัพยากรทางกายภาพ ด้วยเหตุนี้ การไร้ซึ่งฉันทามติเกี่ยวกับสิ่งที่ประกอบเป็นพื้นที่ไซเบอร์ ทำให้คำจำกัดความของคำว่า “ข่าวกรองไซเบอร์” ค่อนข้างหลากหลาย และไม่เหมือนกับการรวบรวมข่าวกรองประเภทอื่น ๆ อีกทั้ง ข่าวกรองไซเบอร์ ก็มิได้จำกัดอยู่เฉพาะในหลักนิยมร่วม หรือเหล่าทหารเหล่าใดเหล่าหนึ่งเท่านั้น แนวคิดสำหรับการปฏิบัติการไซเบอร์ จึงเป็นสิ่งที่ได้รับการยอมรับโดยทั่วไปในฐานะที่เป็นขีดความสามารถของเหล่าทัพที่จะดำเนินปฏิบัติการ และดำเนินกลยุทธ์ภายใต้กรอบของคำจำกัดความของพื้นที่ไซเบอร์ของตนเอง พื้นที่ไซเบอร์จึงนับเป็นสิ่งท้าทายสำหรับการปฏิบัติการข่าวกรอง และการปฏิบัติการทางทหารอื่น ๆ อย่างต่อเนื่อง ในขณะที่พื้นที่ไซเบอร์ คือ มิติเสมือนที่มนุษย์สร้างขึ้น การปรับเปลี่ยนและผลกระทบที่เกิดขึ้นในมิตินี้ จึงแสดงให้เห็นถึงลักษณะทางกายภาพภายในพื้นที่ปฏิบัติการได้อย่างชัดเจน โดยเฉพาะในสภาพแวดล้อมที่มีขอบเขตที่แน่นอน และชุดของความสัมพันธ์ที่ซับซ้อนมาก

ยิ่งขึ้น นอกจากนี้แล้ว ด้วยธรรมชาติของการปฏิบัติการ และผลกระทบทางทหารที่มักเกิดขึ้นอย่างทันทีทันใด ทำให้การพิจารณาทางทหารแบบดั้งเดิม โดยอาศัยปัจจัยในเรื่องเวลากลายเป็นสิ่งที่ล้าสมัย ในขณะที่หลักมูลฐานดั้งเดิมของการรวบรวมข่าวกรองยังสามารถนำมาปรับใช้ได้กับข่าวกรองไซเบอร์ ระยะห่างของพื้นที่ไซเบอร์จากพื้นที่ปฏิบัติการทางทหารแบบดั้งเดิม ทำให้ความพยายามที่จะให้คำจำกัดความและอธิบาย เกี่ยวกับข่าวกรองไซเบอร์ภายใต้ความเชื่อมโยงของความคิดแบบดั้งเดิม ในเรื่องข่าวกรองกลายเป็นสิ่งที่ไร้ประโยชน์

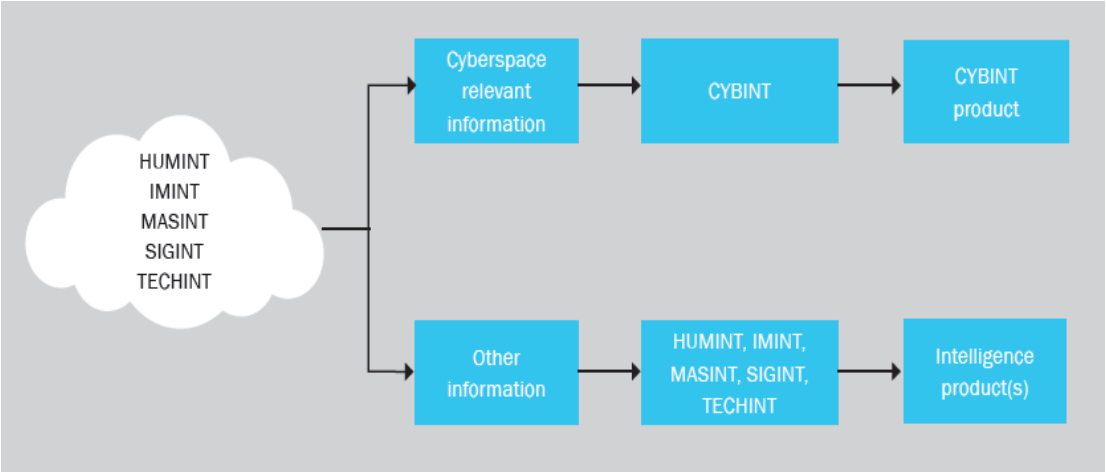
หากเราจะกำหนดคำจำกัดความให้กับข่าวกรองไซเบอร์อย่างง่าย ๆ ว่าเป็นการรวบรวมข่าวกรองจากพื้นที่ไซเบอร์เท่านั้น ความท้าทายที่ยิ่งใหญ่ มิใช่เพียงแค่การรู้แจ้งในสิ่งที่เป็นอันตรายต่อพื้นที่ไซเบอร์เท่านั้น แต่ยังเป็นการกล่าวถึงปัญหาทับซ้อน และความขัดแย้งที่อาจจะเกิดขึ้น กับการให้คำจำกัดความเกี่ยวกับหลักการการรวบรวมข่าวกรองที่มีอยู่แล้วด้วย ในเรื่องข่าวกรองทางสัญญาณ (SIGINT) แล้ว ข้อมูลทางสัญญาณ มีคำจำกัดความที่ชัดเจนของการติดต่อสื่อสารระหว่างบุคคล (โดยให้ความสำคัญกับข่าวกรองทางอิเล็กทรอนิกส์) ในบริบทของข่าวกรองไซเบอร์ เราไม่สามารถให้คำจำกัดความข่าวสาร ที่ได้จากพื้นที่ไซเบอร์อย่างชัดเจนได้ เนื่องจากองค์ประกอบที่แน่นอนที่ถือกำเนิดขึ้นในพื้นที่ไซเบอร์มีความหลากหลายระหว่างพื้นที่ปฏิบัติการ ปัจจัยที่ไม่ทราบเป็นจำนวนมาก และสภาพการณ์ที่สามารถเปลี่ยนแปลงได้ทันทีทันใด ทั้งที่ได้อาศัยความพยายามเพียงเล็กน้อยเท่านั้น นอกจากนี้แล้ว การขาดฉันทามติในเรื่องคำจำกัดความของพื้นที่ไซเบอร์ ข่าวสารที่จะได้รับการพิจารณาว่า เป็นองค์ประกอบอย่างหนึ่งของหลักการรวบรวมข่าวกรองอื่น ๆ ก็สามารถให้คำจำกัดความได้ง่าย ๆ โดยถือเป็นองค์ประกอบอย่างหนึ่งของข่าวกรองไซเบอร์อีกด้วย ตัวอย่างเช่น การดักรับช่องสัญญาณของศูนย์การติดต่อสื่อสารแบบดิจิทัล (digital - communications links) เพื่อรวบรวมข่าวสารในการสร้างศูนย์การสื่อสารระหว่างระบบต่าง ๆ ถือเป็นแนวปฏิบัติอย่างหนึ่งของข่าวกรองทางสัญญาณนั่นเอง ดังนั้น การใช้เทคโนโลยีการเชื่อมต่อระหว่างกันเป็นคำจำกัดความของพื้นที่ไซเบอร์ และข้อเท็จจริงที่ว่าข่าวกรองได้ถูกรวบรวมมาจากการเชื่อมต่อระบบเทคโนโลยีตั้งแต่ ๒ ระบบขึ้นไป จนนำมาซึ่งข่าวกรอง ในปริมณฑลของข่าวกรองไซเบอร์ที่รวบรวมได้จากพื้นที่ไซเบอร์ด้วยเหตุนี้ ข่าวสารใด ๆ ที่รวบรวมได้มาจากการเชื่อมต่อทางเทคนิคก็จะกลายเป็นข่าวกรองไซเบอร์ไปในทันที

การให้คำจำกัดความของข่าวกรองไซเบอร์ โดยอาศัยการใช้แหล่งข่าวกรองเป็นหลัก อาจไม่เหมาะสมกับแหล่งข่าวกรองที่มีความหลากหลายมากนัก ยิ่งไปกว่านั้น ข่าวกรองที่รวบรวมได้จากแหล่งข่าวเหล่านี้ มักใช้ได้เพียงบางส่วน สิ่งที่ไม่น่าเป็นไปได้ คือ การรวบรวม การวิเคราะห์ และการประเมินข่าวกรองไซเบอร์ จะสามารถกระทำได้โดยอาศัยวิธีการอย่างใดอย่างหนึ่ง แต่เพียงอย่างเดียว ตัวอย่างเช่น ข่าวกรองจากบุคคล (HUMINT) ที่นำมาใช้เพื่อการรวบรวมข่าวกรองภัยคุกคามไซเบอร์ ถ้าผู้รวบรวม ข่าวกรองดังกล่าวเป็นสายลับ ดำเนินการรวบรวมข่าวสารอย่างลับ ๆ จากแหล่งข่าวเกี่ยวกับสิ่งที่ล่อแหลมของระบบไซเบอร์แล้ว เราจะถือว่าข่าวกรองนี้เป็น ข่าวกรองจากบุคคล (HUMINT) หรือข่าวกรองไซเบอร์ (CYBINT) เพราะการมีอยู่ของแหล่งข่าวในฐานะมนุษย์ที่ให้การสนับสนุนงานที่ได้รับมอบหมายต่อข่าวกรองจากบุคคล ในขณะเดียวกัน ก็มีการประยุกต์ใช้ข่าวกรอง ในการปฏิบัติการในพื้นที่ไซเบอร์ เพื่อให้การสนับสนุนงานที่ได้รับมอบหมาย

ต่อข่าวกรองไซเบอร์ด้วย ดังนั้น การบูรณาการข่าวกรอง อย่างอื่นเข้ากับข่าวกรองไซเบอร์ ยังไม่อาจเรียกได้ว่า เป็นข่าวกรองไซเบอร์อย่างเต็มปากเต็มคำได้

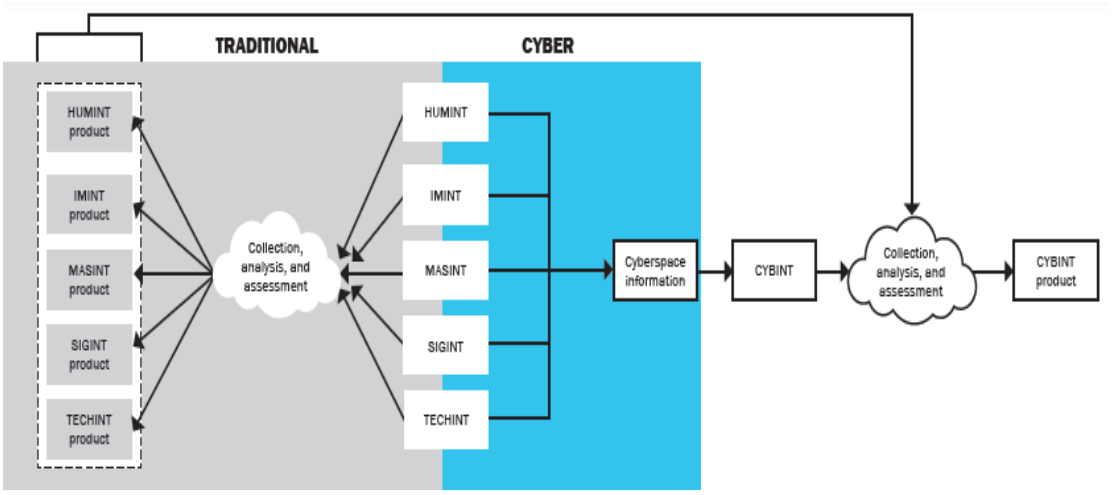
แทนที่จะให้คำจำกัดความของคำว่า “ข่าวกรองไซเบอร์” อย่างง่าย ๆ โดยอาศัยกระบวนการรวมรวม การวิเคราะห์ และการประเมินข่าวสารในพื้นที่ไซเบอร์ เราสามารถให้คำจำกัดความของคำ ๆ นี้ ได้ โดยการหลอมรวมข่าวกรองทั้งหมดที่เกี่ยวข้องกับการปฏิบัติการในพื้นที่ไซเบอร์ ซึ่งได้มาจากหลักการรวบรวมข่าวสารแบบดั้งเดิม เพื่อนำไปสู่ผลผลิตที่ทำให้ผู้บังคับบัญชาทราบและตัดสินใจเกี่ยวกับการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับได้ โดยหลักการรวบรวมข่าวสารแบบดั้งเดิม จะยังคงเป็นกิจกรรมการรวบรวมข่าวกรองอย่างต่อเนื่อง ผลลัพธ์หรือผลผลิตของการดำเนินกรรมวิธีข่าวสารให้เป็นข่าวกรอง ที่เกี่ยวกับพื้นที่ไซเบอร์ หรือการปฏิบัติการในพื้นที่ไซเบอร์สามารถเป็นส่วนหนึ่ง หรือเป็นงานที่ได้รับมอบหมายให้กับข่าวกรองไซเบอร์ ที่ซึ่งมีการหลอมรวมข่าวสารที่ได้จากทุกแหล่ง เพื่อสร้างเป็นผลผลิตที่ตอบสนองความต้องการข่าวสารของผู้บังคับบัญชาได้ดังตัวอย่างในแผนภาพที่ ๒ - ๓ ได้แสดงให้เห็นถึงการใช้พื้นที่ไซเบอร์ที่เกี่ยวข้องกับข่าวสารในระดับสูงจากการรวบรวมข่าวกรอง ในฐานะที่เป็นแหล่งข่าวหนึ่งของข่าวกรองไซเบอร์ และแผนภาพที่ ๒ – ๔ ที่แสดงให้เห็นถึงความแตกต่างระหว่างกระบวนการข่าวกรอง แบบดั้งเดิมกับข่าวกรองไซเบอร์อย่างชัดเจน

แผนภาพที่ ๒ - ๓ การแยกข่าวกรองประเภทต่าง ๆ ที่มีอยู่ เพื่อเป็นปัจจัยป้อน (inputs) เข้าสู่กระบวนการของข่าวกรองไซเบอร์



ที่มา : จุลสารการข่าวกรองทหารบกปีที่ ๑ ฉบับที่ ๑ พฤษภาคม ๒๕๖๕

แผนภาพที่ ๒ - ๔ โครงสร้างที่ใช้สนับสนุนการกำหนดคุณลักษณะข่าวกรองไซเบอร์ในฐานะผลผลิตข่าวกรองจากทุกแหล่งข่าว



ที่มา : จุลสารการข่าวกรองทหารบกปีที่ ๑ ฉบับที่ ๑ พฤษภาคม ๒๕๖๕

ในกระบวนการของข่าวกรองไซเบอร์ (แสดงอยู่ในแถบสีฟ้า) ข่าวสารที่เกี่ยวข้องกับพื้นที่ไซเบอร์จากกิจกรรมต่าง ๆ ของการรวบรวมข่าวกรองแบบดั้งเดิม แต่ละอย่างจะได้รับการตรวจทาน เพื่อจัดทำเป็นข่าวสารในพื้นที่ไซเบอร์ ตั้งแต่ต้น จนจบของกระบวนการ ข่าวสารจากทุกแหล่งจะถูกหลอมรวม เพื่อสร้างเป็นปัจจัยป้อนเข้าสู่กระบวนการของข่าวกรองไซเบอร์ จนกระทั่งสามารถสร้างผลผลิตข่าวกรองไซเบอร์ขึ้นมาได้ ในกระบวนการข่าวกรองแบบดั้งเดิม (แสดงอยู่ในแถบสีเทา) ข่าวกรองที่มีอยู่ ๕ ประเภท และกระบวนการรวบรวมข่าวกรองที่ได้รับการวางแผนมาเป็นอย่างดี จะใช้กระบวนการของข่าวกรองไซเบอร์ เพื่อสร้างเป็นผลผลิตของข่าวกรองไซเบอร์ต่อไป ถ้าผลผลิตสุดท้ายของกระบวนการเหล่านี้เป็นข่าวสารที่เกี่ยวข้องกับพื้นที่ไซเบอร์แล้ว ข่าวสารเหล่านี้จะถูกใช้เป็นปัจจัยป้อนเข้าสู่การหลอมรวมข่าวสารจากทุก ๆ แหล่ง เพื่อสร้างเป็นผลผลิตของข่าวกรองไซเบอร์ทั้งสิ้น

๒.๒ ประโยชน์ของข่าวกรองไซเบอร์ ในฐานะเป็นผลผลิตอย่างหนึ่งของการข่าวกรอง

ข่าวกรองไซเบอร์ (cyber intelligence) เป็นการผลิตและกระบวนการในวงรอบข่าวกรองที่มีการประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรม (ทางเทคนิคและอื่น ๆ) เกี่ยวกับคู่แข่งและฝ่ายตรงข้ามที่เป็นไปได้ในมิติไซเบอร์ คู่แข่ง และ ฝ่ายตรงข้ามเหล่านี้ ประกอบด้วยบุคคลและองค์กรที่ใช้มิติไซเบอร์ เพื่อการก่ออาชญากรรมและกิจกรรมที่เกี่ยวข้องกับ การฉ้อโกง คำว่า “ข่าวกรองไซเบอร์” จึงถูกใช้ใน ๒ นัย ได้แก่

๒.๒.๑ ในบริบทของความมั่นคงแห่งชาติ (national security) และองค์การด้านการป้องกันประเทศ (defense organizations) และเป็นพื้นที่ไซเบอร์ที่ใช้เป็นจุดอ้างอิงสำหรับการรวบรวมและการวิเคราะห์ข่าวกรอง (เช่น ข่าวกรองทางทะเล เป็นต้น)

๒.๒.๒ ข่าวกรองที่เกี่ยวข้องกับความรู้ที่ได้มาจาก การประมวลผล หรือการวิเคราะห์ข้อมูลและข่าวสาร ข่าวกรองนี้จึงมีลักษณะที่แตกต่างจากข้อมูลดิบเกี่ยวกับภัยคุกคาม เช่น ตัวอักษร รหัส และข่าวสารภัยคุกคามที่ยังมิได้รับการประมวลผล เป็นต้น ด้วยเหตุนี้ พันธกิจข่าวกรองสำหรับความมั่นคง ด้านไซเบอร์ หรือการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (cyber security) จึงประกอบด้วย การรวบรวม (collecting) การประมวลผล (processing) การวิเคราะห์ (analyzing)

การสร้างเนื้อหา (contextualizing) และการรายงาน (reporting) ข่าวสารภัยคุกคามให้ผู้มีอำนาจตัดสินใจทราบ เพื่อใช้ข้อมูลและข่าวสารดังกล่าวได้อย่างมีประสิทธิผล

เนื่องจากข่าวกรอง (intelligence) คือ สิ่งที่สำคัญยิ่งต่อการปฏิบัติภารกิจความมั่นคงด้านไซเบอร์ที่มีประสิทธิผล องค์การสนธิสัญญาแอตแลนติกเหนือ หรือกลุ่มนาโต้ (NATO) จึงถือว่า “การข่าวกรอง” (intelligence) และการต่อต้านการข่าวกรอง (counter - intelligence) เป็น ๑ ใน ๕ งานหลักของความมั่นคงแห่งชาติด้านไซเบอร์ ในทำนองเดียวกัน ยุทธศาสตร์ข่าวกรองแห่งชาติของสหรัฐอเมริกา ประจำปี ค.ศ. ๒๐๑๔ ได้กำหนดให้ข่าวกรองไซเบอร์ เป็น ๑ ใน ๔ ความมุ่งหมายหลักที่กำหนดไว้ในภารกิจของประชาคมข่าวกรอง เทียบเท่ากับภารกิจด้านการต่อต้านการก่อการร้าย (counterterrorism) และการต่อต้านการแพร่ขยายของอาวุธทำลายล้างสูง (counter - proliferation) อีกทั้ง กระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา (U.S. Department of Homeland Security) ได้กำหนดให้นักวิเคราะห์ภัยคุกคาม/การต่อต้านการข่าวกรอง (intelligence/counterintelligence analyst) มีกิจ (tasks) และงาน (jobs) ที่สำคัญยิ่งต่อการบรรลุภารกิจที่หลากหลาย จากรายงานประจำปีของกระทรวงความมั่นคงแห่งมาตุภูมิ ค.ศ. ๒๐๑๒ ได้กำหนดให้นักวิเคราะห์ของหน่วยงานเฉพาะกิจนี้ มีทักษะด้านไซเบอร์เอาไว้ว่า “นักวิเคราะห์ภัยคุกคาม/ การต่อต้านการข่าวกรอง จักต้องสามารถใช้ความรู้ในปัจจุบัน และความรู้เชิงลึกเกี่ยวกับการโจมตีที่เปิดเผยตัวออกมา เป้าหมายที่ล่อแหลมมากที่สุด และเป้าหมายที่มีค่าสูง และวิธีการแสวงประโยชน์จากความล่อแหลมทางเทคนิค โดยยกระดับไปสู่การรับรู้สถานการณ์ ในรายละเอียดเกี่ยวกับผู้เล่นที่ประสงค์ร้าย พัฒนาเทคนิคและโปรแกรมที่ใช้เครื่องมือตามปกติ เพื่อตรวจจับการเปลี่ยนแปลงในท้องถิ่น พิสูจน์ทราบปฏิสัมพันธ์ที่ต้องสงสัย เฝ้าระวัง และตอบสนองต่อสิ่งที่ผู้เล่นที่ประสงค์ร้ายจะกระทำ ถ้าจัดตั้งเป็นทีมงานที่ก้าวหน้ายิ่งขึ้น ทีมงานนี้จักต้องสามารถเข้าใจแรงจูงใจ ภาษา การจัดองค์กร และพฤติกรรมทางสังคมของผู้โจมตี รวมถึงกลุ่มบุคคลที่เป็นภัยคุกคาม เพื่อสร้างประวัติทางไซเบอร์ของกลุ่มบุคคล ผู้เล่น และลักษณะของการงาน เพื่อช่วยให้องค์กรสามารถควบคุมสถานการณ์ด้านความมั่นคง และการป้องกันประเทศได้อย่างมั่นใจ”

พันธกิจหลักของข่าวกรองไซเบอร์ มีดังนี้

๑. การพิสูจน์ทราบ (identify) หมายถึง การพัฒนาความเข้าใจขององค์กร เพื่อการจัดการกับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้กับระบบ (systems) เครื่องมือ (assets) ข้อมูล (data) และขีดความสามารถ (capabilities) ของฝ่ายเรา

๒. การพิทักษ์ (protect) หมายถึง การพัฒนาและการใช้เครื่องมือป้องกัน (safeguards) ที่เหมาะสม เพื่อรับประกันในเรื่องการนำส่งการบริการ ของโครงสร้างพื้นฐานที่สำคัญยิ่งของฝ่ายเรา

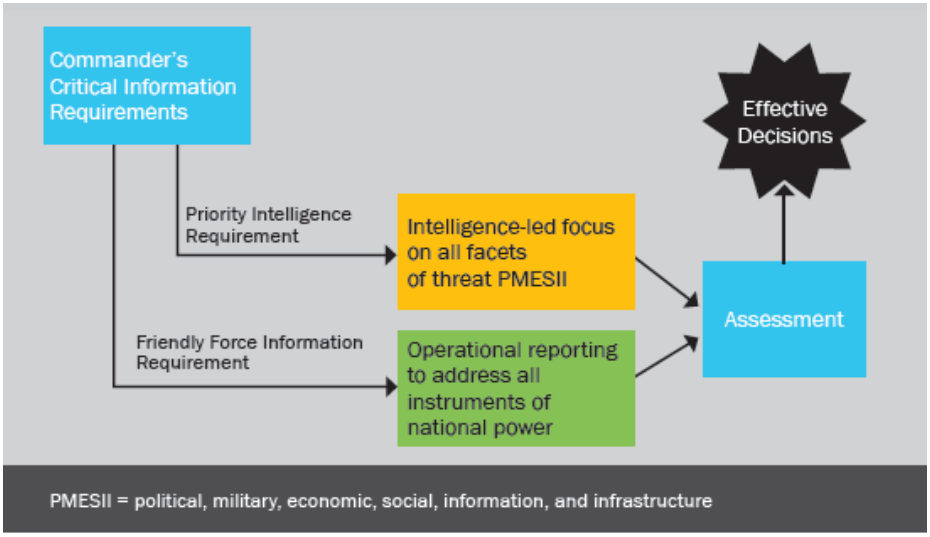
๓. การตรวจจับ (detect) หมายถึง การพัฒนาและใช้กิจกรรมที่เหมาะสม เพื่อพิสูจน์ทราบเหตุการณ์ที่เกิดขึ้น เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๔. การตอบสนอง (respond) หมายถึง การพัฒนาและการใช้กิจกรรมที่เหมาะสม เพื่อการดำเนินการเกี่ยวกับเหตุการณ์ที่ตรวจพบ เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๕. การฟื้นฟู (recovery) หมายถึง การพัฒนาและการใช้กิจกรรมที่เหมาะสม เพื่อปฏิบัติตามแผนการคืนสู่ สภาพเดิมและการฟื้นฟูขีดความสามารถ หรือการบริการใด ๆ ที่ได้รับผลกระทบจากเหตุการณ์ เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

อย่างไรก็ตาม หากมองลึกเข้าไปในพื้นที่ไซเบอร์และการปฏิบัติการไซเบอร์ และความสามารถในการพิสูจน์ทราบ และแสดงความต้องการข่าวสาร ดังตัวอย่างในแผนภาพที่ ๒ – ๕ ความต้องการข่าวสาร (information needs) ได้แสดงบทบาทสำคัญต่อกระบวนการแสวงข้อตกลงใจของผู้บังคับบัญชาได้อย่างมีประสิทธิผลได้อย่างไร ในสถานการณ์ที่ผู้บังคับบัญชา ไม่สามารถแสดงความต้องการข่าวสารเฉพาะเจาะจงสำหรับข่าวกรองไซเบอร์ได้ ความต้องการดังกล่าว อาจอุบัติขึ้นในฐานะผลพลอยได้จากกระบวนการรวบรวมข่าวกรองที่มีอยู่ก็ได้ โดยเฉพาะอย่างยิ่ง เมื่อผู้บังคับบัญชามีความต้องการข่าวสารเฉพาะเจาะจงอย่างหนึ่งอยู่แล้ว ข่าวกรองที่เกี่ยวข้องก็สามารถรับการพิสูจน์ทราบ ค้นหา และป้อนเข้าสู่กระบวนการของข่าวกรองไซเบอร์ โดยเป็นส่วนหนึ่งของความพยายามเชิงโครงสร้างของการรวบรวมข่าวกรองที่มีอยู่แล้วนั่นเอง การดำเนินการเช่นนี้ จึงสามารถลดภาระงานของการรวบรวมข่าวสารสำหรับข่าวกรองไซเบอร์ได้บางส่วน แม้จะไม่ใช่ทั้งหมดของการรวบรวมข่าวกรอง ตามกระบวนการที่มีอยู่แล้วก็ตาม ด้วยเหตุนี้ เมื่องานข่าวกรองไซเบอร์ได้เกิดขึ้นจากกระบวนการรวบรวมข่าวกรองที่มีอยู่ และเป็นส่วนหนึ่งของโครงสร้างข่าวกรองไซเบอร์แล้ว ย่อมเป็นโอกาสให้กระบวนการข่าวกรองทั้งสองประเภท (ข่าวกรองไซเบอร์ และข่าวกรองประเภทอื่น ๆ) ดำเนินการควบคู่กันไปได้ โดยแสวงประโยชน์จากการดำเนินกระบวนการรวบรวมข่าวสารจากทุกแหล่งข่าวที่มีอยู่ และใช้มุมมองในเชิงลึกมากขึ้น โดยมุ่งความสนใจไปที่การตอบสนองต่อความต้องการข่าวสารของผู้บังคับบัญชาเป็นหลัก ดังนั้น การตอบสนองต่อพื้นที่ไซเบอร์ และการให้คำจำกัดความให้กับข่าวกรองไซเบอร์ที่ยากต่อความเข้าใจ จึงไม่ใช่สิ่งที่มีความจำเป็นสำหรับกระบวนการของข่าวกรองไซเบอร์อีกต่อไป ไม่ว่าจะเป็นการรวบรวม การวิเคราะห์ และการประเมินข่าวกรองไซเบอร์สำหรับระบบหรือการปฏิบัติการทางทหาร

แผนภาพที่ ๒ - ๕ การแยกแยะข่าวกรองที่มีอยู่เพื่อจัดทำเป็นปัจจัยป้อนเข้าสู่กระบวนการของข่าวกรองไซเบอร์



ที่มา : จุลสารการข่าวกรองทหารบกปีที่ ๑ ฉบับที่ ๑ พฤษภาคม ๒๕๖๕

ประโยชน์ของข่าวกรองไซเบอร์ในแง่ของความอยู่รอด (survivability) และความล่อแหลม (vulnerability) ซึ่งเกิดจากการรวบรวม และการใช้ข่าวกรองไซเบอร์ โดยเป็นส่วนหนึ่งของกระบวนการแสวงข้อตกลงใจทางทหาร เพื่อให้นักการทหาร สามารถประเมินสิ่งซึ่งเป็นทิศทางของการโจมตี และการโจมตีที่เกี่ยวข้อง จึงอยู่ในรูปแบบ และระบบที่เกี่ยวข้อง ตัวอย่างเช่น ในการใช้ข่าวสาร สิ่งที่เป็นไปได้ ก็คือ การประเมินให้ได้ว่า รูปแบบและระบบดังกล่าวสามารถหลีกเลี่ยงการถูกตรวจจับ หรือจะป้องกันการโจมตีเหล่านี้ได้อย่างไร ระบบที่เกี่ยวข้องจะหลีกเลี่ยงการโจมตี หรือทิศทางการโจมตีนั้นได้ดีเพียงใด ระบบดังกล่าว จะสามารถทนต่อการโจมตีได้มากเพียงใด กล่าวโดยสรุป ระบบดังกล่าวจะสามารถฟื้นฟูตนเองจากการโจมตี และกลับสู่สภาพที่สามารถใช้งานได้เหมือนเดิมได้อย่างไร เป็นต้น โดยอาศัยกระบวนการพัฒนา การใช้ข่าวกรองไซเบอร์ จึงเป็นสิ่งที่อำนวยในเรื่องการออกแบบ และการสร้างสรรค์รูปแบบ และระบบที่อยู่ภายใต้มาตรฐานที่ได้รับการรับรองแล้ว ทั้งในเรื่องความอยู่รอด และความล่อแหลม เพื่อวิวัฒนาการไปเป็นความเปลี่ยนแปลงภัยคุกคามที่ได้รับการประเมินแล้วนั่นเอง

เอกสารวิจัยที่เกี่ยวข้อง

งานวิจัยและเอกสารวิชาการที่เกี่ยวข้องกับ การพัฒนาระบบข่าวกรอง และข่าวกรองไซเบอร์ (Cyber Intelligence) เป็นที่ได้รับความสนใจจากนักวิจัย หน่วยงานราชการ และองค์กรต่าง ๆ เป็นจำนวนมาก โดยมีวัตถุประสงค์และประเด็นที่แตกต่างกันไป ผู้วิจัยนำบทความทางวิชาการและเอกสารการวิจัยที่เกี่ยวข้องมาใช้ในการทบทวนวรรณกรรม ดังนี้

๑. รายงานการศึกษาส่วนบุคคล (Individual Study) เรื่อง ปัจจัยความสำเร็จของสิงคโปร์ “กรณีศึกษา เพื่อประกอบการพัฒนาแนวทางการดำเนินการตาม นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย” : การศึกษานี้ดำเนินการวิเคราะห์ปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการ ดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ช่วงปี ๒๐๑๔ – ปัจจุบัน แล้วนำผลการวิเคราะห์มา เปรียบเทียบกับการดำเนินงานของไทย เพื่อหาแนวทางและข้อเสนอแนะในการพัฒนาการดำเนินการ ตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย โดยการศึกษาจะวิเคราะห์ตามกรอบดัชนีตัวชี้วัดตามที่สหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยแบ่งเป็น ๕ เสาหลัก ได้แก่

๑.๑ ด้านกฎหมาย
๑.๒ ด้านเทคนิค
๑.๓ ด้านองค์กร
๑.๔ ด้านการเสริมสร้างศักยภาพ
๑.๕ ด้านความร่วมมือ

ทั้งนี้ จากการศึกษาพบว่า ปัจจัยหลักที่ทำให้สิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ คือ รัฐบาลสิงคโปร์มีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วย

การใช้เทคโนโลยีดิจิทัลและนวัตกรรม จึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีการดำเนินการอย่างจริงจัง ต่อเนื่อง และเป็นระบบ และดำเนินงานร่วมมือกับทุกภาคส่วนทั้งในประเทศ และระหว่างประเทศ มาตั้งแต่ ปี ๒๕๔๘

๒. เอกสารวิจัยเรื่อง Strategic cyber intelligence โดย Randy Borum, John Felker, Sean Kern, Kristen Dennesen, Tonya Feyes Date: 07/13/2015 งานวิจัยนี้มีวัตถุประสงค์ เพื่อเน้นความสำคัญและบทบาทของข่าวกรองทางไซเบอร์เชิงยุทธศาสตร์ เพื่อสนับสนุนการตัดสินใจที่มีข้อมูลความเสี่ยง ซึ่งนำไปสู่การปรับปรุงวัตถุประสงค์ นโยบาย สถาปัตยกรรม และการลงทุน เพื่อพัฒนาผลประโยชน์ของประเทศ หรือองค์กรในด้านไซเบอร์ในที่สุด ทั้งนี้งานวิจัยค้นพบว่า การลงทุนในเทคโนโลยีไฟร์วอลล์ และระบบตรวจจับการบุกรุกเป็นสิ่งที่เหมาะสม แต่โดยตัวมันเองนั้นยังไม่เพียงพอ การข่าวกรองเป็นองค์ประกอบสำคัญ ข่าวกรองทางไซเบอร์เน้นการป้องกันและการคาดการณ์ เพื่อเน้นความพยายามในการรักษาความปลอดภัยทางไซเบอร์ก่อนที่จะเกิดการโจมตี ข่าวกรองทางไซเบอร์เชิงยุทธศาสตร์สามารถลดความเสี่ยงต่อภารกิจขององค์กรและสินทรัพย์อันมีค่าได้อย่างมาก และรวมถึงเป็นการสนับสนุนการปฏิบัติงานที่ดีขององค์กร

๓. เอกสารวิจัยเรื่อง การพัฒนาการปฏิบัติงานในยุคไทยแลนด์ ๔.๐ กรณีศึกษา : สถาบันการข่าวกรองสำนักข่าวกรองแห่งชาติ โดย สิริกร ชิงดวง ศึกษากระบวนการปฏิบัติงานในยุคไทยแลนด์ ๔.๐ ของสถาบันการข่าวกรอง สำนักข่าวกรองแห่งชาติ ปัญหา ความท้าทายของการนำเทคโนโลยีดิจิทัล, AI (ปัญญาประดิษฐ์), Iot (Internet of Thing) มาใช้ในการปฏิบัติงาน และข้อเสนอแนะในการปฏิบัติงานในยุคไทยแลนด์ ๔.๐ ของสถาบันการข่าวกรองฯ ผลการวิจัยพบว่า ระบบเทคโนโลยีที่ใช้ในการปฏิบัติงานของสำนักข่าวกรองแห่งชาติ (สขช.) มี ๒ แบบ คือ ระบบที่เจ้าหน้าที่ สขช. จัดทำระบบ เขียนระบบเอง และการจ้าง Outsource เข้ามาทำระบบให้ ปัญหาและความท้าทาย ได้แก่

๓.๑ ปัญหาด้านบุคลากร มีความเข้าใจในตัวนโยบายไทยแลนด์ ๔.๐ ที่แตกต่างกันและขาดทักษะการใช้เทคโนโลยี

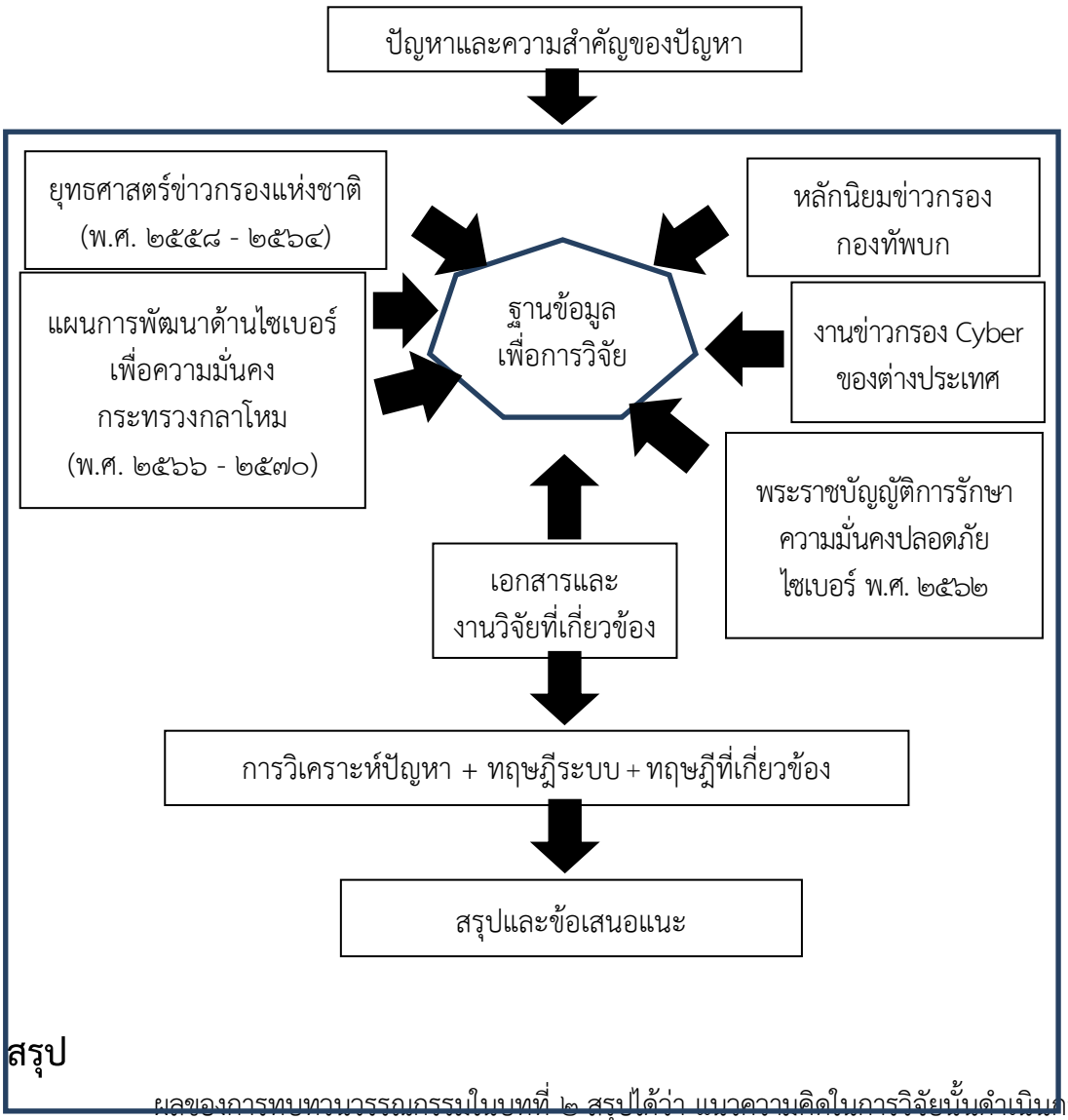
๓.๒ ความต่างของอายุและช่วงวัย Generation Gap

๓.๓ อุปกรณ์และเครื่องมือที่ไม่ทันสมัย มีต้นทุนสูง

๓.๔ ระบบราชการมีโครงสร้างที่ใหญ่และซับซ้อน

และข้อเสนอแนะพบว่า ๑. สิ่งสำคัญที่สุดในการแก้ไขและพัฒนา คือ ทรัพยากรมนุษย์ต้องเริ่มจากการพัฒนาตนเองก่อนที่จะเริ่มพัฒนาไปสู่องค์กร ๒. พัฒนาเทคโนโลยี อุปกรณ์อิเล็กทรอนิกส์ให้ทันสมัยพร้อมต่อการทำงาน ๓. ผู้บริหารต้องมีวิสัยทัศน์ สนับสนุน ในเรื่องการพัฒนาเทคโนโลยีในการทำงานอย่างจริงจัง และมีแนวทางที่ชัดเจนเป็นรูปธรรม ๔. ปฏิรูประบบราชการ ให้เอื้ออำนวยต่อการทำงานด้านการข่าว และ ๕. ต้องตั้งเป้าหมายว่าในอนาคตว่าเป้าหมายหรือทิศทางการทำงานเป็นอย่างไร

กรอบแนวความคิดในการวิจัย



สรุป

ผลของการทบทวนวรรณกรรมในบทที่ ๒ สรุปได้ว่า แนวความคิดในการวิจัยนั้นดำเนินการโดยการศึกษารวบรวมข้อมูลที่เกี่ยวข้องกับข่าวกรองไซเบอร์, การดำเนินงานตามวงรอบข่าวกรอง, ปัญหาการดำเนินงานด้านการข่าวโดยเฉพาะด้านข่าวกรองไซเบอร์ จากนั้นทำการศึกษาวิเคราะห์ ปัญหา สาเหตุ ปัจจัย และความท้าทาย และ นำเสนอการพัฒนา Model ต้นแบบ สำหรับการพัฒนาระบบงานข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก โดยใช้กระบวนการเครื่องมือและทฤษฎีที่เกี่ยวข้อง

บทที่ ๓
รูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก

การศึกษาในบทที่ ๓ เป็นการศึกษาถึง รูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบกโดยมีลำดับการศึกษาดังต่อไปนี้

๑. การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศในห้วงปัจจุบัน

๒. รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศ

๓. รายงานความมั่นคงปลอดภัยทางไซเบอร์ของโลก (Global Cybersecurity Index) โดย International Telecommunication Union (ITU)

๔. สรุป

การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศในห้วงปัจจุบัน

การศึกษานี้มุ่งเน้นไปที่การเสริมสร้างประสิทธิภาพของการปฏิบัติงานด้านการข่าว ดังนั้น จึงเป็นการนำเสนอถึงภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศทั้งทางตรงและทางอ้อม โดยมีสถานการณ์และบริบทความมั่นคงที่สำคัญดังนี้

๑. การเมืองระหว่างประเทศ

การเมืองโลกมีแนวโน้มที่จะเปลี่ยนแปลงไปสู่หลายขั้วอำนาจโดยสหรัฐอเมริกาต้องเผชิญกับการท้าทายจากรัสเซียและจีน ขณะที่การเสริมสร้างความร่วมมือระหว่างสหรัฐอเมริกา ญี่ปุ่น ออสเตรเลีย และอินเดีย ในกรอบ Quadrilateral Security Dialogue (QUAD) จะช่วยสนับสนุนการมีบทบาทนำด้านความมั่นคงของสหรัฐอเมริกาในภูมิภาคเอเชีย นอกจากนี้ การเพิ่มบทบาทของขั้วอำนาจใหม่ทางเศรษฐกิจโลก คือ กลุ่ม BRICS ประกอบด้วย บราซิล รัสเซีย อินเดีย จีน และแอฟริกาใต้ ซึ่งกำลังมีบทบาทในเวทีระหว่างประเทศเพิ่มมากขึ้น และมีท่าทีต้องการมีส่วนร่วมในการกำหนดกรอบกติกาของโลก โดยมีความเคลื่อนไหวที่สำคัญในด้านเศรษฐกิจและการเงินระหว่าง

ประเทศ ซึ่งเป็นการท้าทายและสร้างดุลอำนาจใหม่ และมีแนวโน้มส่งผลต่อการเปลี่ยนแปลงระเบียบโลก ทั้งทางการเมืองและเศรษฐกิจ สภาพการณ์ดังกล่าวส่งผลให้ประเทศไทยต้องดำเนินนโยบายด้วยความอ่อนตัวในการกำหนดท่าที เพื่อรักษาดุลยภาพทางความสัมพันธ์ระหว่างไทยกับประเทศมหาอำนาจต่าง ๆ นอกจากนี้ ปัจจัยความมั่นคงด้านพลังงาน ทรัพยากรธรรมชาติ สิ่งแวดล้อม และภัยธรรมชาติ ถือเป็นปัญหาสำคัญของโลก โดยเฉพาะอย่างยิ่งการแสวงหาแหล่งพลังงานใหม่อาจนำไปสู่ความขัดแย้งระหว่างประเทศ ในขณะที่ปัจจัยด้านสิ่งแวดล้อม อาทิ การเปลี่ยนแปลงของสภาพภูมิอากาศ ซึ่งส่งผลโดยตรงต่อภัยธรรมชาติที่มีระดับความรุนแรงมากขึ้น ทำให้จำเป็นต้องมีความร่วมมือในระดับนานาชาติ เพื่อเผชิญกับภัยพิบัติที่เกิดขึ้น รวมถึงจะนำมาสู่การกำหนดกรอบกติกาใหม่ที่มหาอำนาจอาจเข้ามาแทรกแซงประเทศอื่น ๆ และใช้เป็นมาตรการกีดกันทางการค้า

๒. การขยายอิทธิพลและบทบาทของประเทศมหาอำนาจต่อภูมิภาคเอเชียตะวันออกเฉียงใต้

มีการปรับเปลี่ยนนโยบายที่แสดงให้เห็นถึงแนวโน้มของการแข่งขันและการขยายอิทธิพลของชาติมหาอำนาจ ทั้งในรูปแบบของการใช้พลังอำนาจทางทหารและทางเศรษฐกิจ เพื่อให้ได้มาซึ่งประโยชน์ของตน โดยเฉพาะการแข่งขันระหว่างสหรัฐอเมริกาและจีน ที่ต้องการแสวงหาพันธมิตรในภูมิภาคต่าง ๆ ทั้งประเทศเล็ก และประเทศมหาอำนาจระดับกลาง โดยสหรัฐอเมริกาจะดำเนินยุทธศาสตร์ Indo - Pacific ในขณะที่จีนจะดำเนินยุทธศาสตร์ Belt and Road Initiative (BRI) ซึ่งมีเป้าหมายเชื่อมโยงเศรษฐกิจ ทั้งการค้า การลงทุน และโครงสร้างพื้นฐานระหว่างภูมิภาคเอเชีย แอฟริกา และยุโรป อาจเป็นผลให้จีนพยายามขยายอิทธิพลทางการเมืองและการทูตต่อกลุ่มประเทศอาเซียน เพื่อบรรลุเป้าหมายดังกล่าว และมีแนวโน้มนำไปสู่ความขัดแย้งในภูมิภาคได้ อย่างไรก็ตาม ทิศทางความสัมพันธ์ระหว่างมหาอำนาจที่อยู่ในรูปแบบการสกัดกั้น - พัวพัน การปิดล้อม และการปฏิสัมพันธ์จะส่งผลให้ประเทศต่าง ๆ ทั้งระดับกลางและระดับเล็กจำเป็นต้องดำเนินความสัมพันธ์กับมหาอำนาจต่าง ๆ อย่างสมดุล อนึ่ง ไทยสามารถใช้ข้อได้เปรียบเชิงภูมิศาสตร์ในการเชื่อมโยงนโยบายเศรษฐกิจของประเทศกับประเทศต่าง ๆ ในภูมิภาค โดยเฉพาะโครงการระเบียงเศรษฐกิจภาคตะวันออก (Eastern Economic Corridor : EEC) ที่สามารถเชื่อมโยงกับ BRI ของจีน และการพัฒนาเขตเศรษฐกิจสามฝ่ายอินโดนีเซีย - มาเลเซีย - ไทย (Indonesia - Malaysia - Thailand Growth Triangle : IMT - GT)

พัฒนาการของกลุ่มประเทศอาเซียนจะมีความเชื่อมโยง และรวมตัวกันมากขึ้นภายใต้ “ประชาคมอาเซียน ทั้งด้านการเมือง ความมั่นคง เศรษฐกิจและสังคม” ตามวิสัยทัศน์อาเซียน ค.ศ. ๒๐๒๕ อันจะนำไปสู่การเสริมสร้างพัฒนาการทางการเมืองและเศรษฐกิจของประเทศสมาชิก รวมทั้งเพิ่มโอกาสการติดต่อเชื่อมโยงผ่านเส้นทางคมนาคมในภูมิภาค อย่างไรก็ตาม การเป็นประชาคมเป็นความท้าทาย โดยเฉพาะการที่ประเทศสมาชิกยังมีลักษณะการปกครองและเศรษฐกิจที่แตกต่างกัน การสร้างความเป็นประชาคม และการเปิดกว้างของการติดต่อระหว่างกันอย่างเสรี ทำให้มีความเสี่ยงที่จะเกิดผลกระทบต่อความมั่นคงของชาติ โดยเฉพาะอย่างยิ่งในประเด็นการย้ายถิ่นฐานของประชากรในภูมิภาคการขยายตัวของอาชญากรรมข้ามชาติเศรษฐกิจนอกระบบ ยาเสพติด และการค้ามนุษย์ นอกจากนี้ อาเซียนจะยังคงประสบความท้าทายจากการรักษาดุลยภาพด้านความมั่นคงระหว่างอาเซียนกับมหาอำนาจ รวมถึงประเด็นปัญหาระหว่างประเทศสมาชิกอาเซียนต่อประเด็นข้อพิพาท

ทะเลจีนใต้ อย่างไรก็ตาม ความสัมพันธ์ระหว่างประเทศสมาชิกอาเซียนจะยังมีความเป็นเอกภาพ รวมถึงอาเซียนไม่มีความขัดแย้งภายใน และไม่มีแนวโน้มที่จะเกิดความแตกแยกภายในอาเซียน โดยรวม แม้ว่าสถานการณ์ทางการเมืองและความมั่นคงในเมียนมาจะส่งผลกระทบต่อการเข้าร่วมประชุมระหว่างประเทศในบางโอกาสอยู่บ้าง

๓. ความขัดแย้งทางดินแดนและการใช้กำลังทางการทหาร

ความสัมพันธ์ระหว่างไทยกับประเทศเพื่อนบ้านมีแนวโน้มที่ดี ชายแดนมีความสงบ โดยเฉพาะการใช้กำลังทางการทหารในพื้นที่เป็นไปด้วยความเรียบร้อย ไม่มีแนวโน้มของเหตุการณ์การใช้กำลัง อย่างไรก็ตาม ไทยกับเพื่อนบ้านยังคงประสบปัญหาความไม่เข้าใจ และความหวาดระแวงที่อาจทำให้เกิดความขัดแย้งระหว่างกัน แต่สามารถจำกัดขอบเขต และระดับความรุนแรงให้อยู่เฉพาะในพื้นที่ อันเป็นผลมาจากการเสริมสร้างความสัมพันธ์ และความร่วมมือที่ใกล้ชิดกัน ในทุกระดับและการเสริมสร้างความสัมพันธ์ทางการทูตเชิงป้องกัน รวมถึงทิศทางความร่วมมือของประเทศในภูมิภาคและประชาคมอาเซียน อนึ่ง เมื่อพิจารณาปัจจัยที่เกี่ยวโยงกับสถานการณ์ข้อพิพาทในภูมิภาค สถานการณ์ภายในของประเทศเพื่อนบ้าน และบทบาทของประเทศมหาอำนาจที่เกี่ยวข้องกับภูมิภาค รวมถึงการที่ประเทศไทยมีชายแดนทั้งทางบก และทางทะเลติดกับประเทศเพื่อนบ้านหลายประเทศ โดยยังมีปัญหาความไม่ชัดเจนของเส้นเขตแดน และอาณาเขตทางทะเลระหว่างกัน ตลอดจนมีสิ่งบ่งชี้ถึงการเพิ่มงบประมาณทางทหารของประเทศในภูมิภาค จึงยังคงมีความเสี่ยงที่จะนำไปสู่การใช้กำลังทหารต่อกันหากเกิดความขัดแย้งรุนแรง และไม่มีการบริหารจัดการปัญหาร่วมกันอย่างมีประสิทธิภาพ

๔. การประเมินสถานการณ์ด้านไซเบอร์เพื่อความมั่นคง

๔.๑ สถานการณ์ภัยคุกคามทางไซเบอร์ภายนอกประเทศ

ปัจจุบันโลกอยู่ในยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็ว และไม่แน่นอน ความก้าวหน้าทางเทคโนโลยี ทำให้โลกก้าวเข้าสู่ยุคไร้พรมแดน และอินเทอร์เน็ตได้เข้ามาเป็นส่วนหนึ่งในการดำเนินชีวิตประจำวัน ซึ่งการใช้งานเทคโนโลยีเหล่านั้นอาจแฝงมาด้วยภัยคุกคามทางไซเบอร์ เช่น ไวรัส, มัลแวร์ และโปรแกรมประสงค์ร้ายต่าง ๆ ของผู้ไม่หวังดี โดยมีเป้าหมายเพื่อให้ได้มาซึ่งข้อมูล หรือการจารกรรม หรือสอดแนมข้อมูล, การหวังผลทางการเมือง, การทำลายระบบฐานข้อมูล, การปฏิบัติการข่าวสาร และการค้า รวมถึงการปฏิบัติการใด ๆ ที่ทำให้ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เสียหาย ไม่สามารถใช้งานได้ ซึ่งภัยคุกคามทางไซเบอร์มีแนวโน้มที่ทวีความรุนแรงและซับซ้อนมากขึ้น ทำให้ส่งผลกระทบได้ในหลายลักษณะ ตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจสังคม ความสงบเรียบร้อย และความมั่นคงในประเทศทำให้หลายประเทศพยายามสร้าง และพัฒนาขีดความสามารถด้านไซเบอร์ เพื่อบ่งชี้ว่าประเทศของตนมีศักยภาพที่ก่อให้เกิดความได้เปรียบ และความสามารถด้านเทคโนโลยีและการทหารที่มีความล้ำหน้าในการใช้ไซเบอร์เป็นเครื่องมือหนึ่งของการรบ หรือแม้แต่มีขีดความสามารถในการทำสงครามไซเบอร์ (Cyber Warfare) ซึ่งสถานการณ์เช่นนี้เป็นต้นเหตุแห่งการแข่งขันสะสมและเสริมสร้างศักยภาพด้านไซเบอร์ของหลายประเทศทั่วโลก เพื่อความต้องการเอาชนะ และทำลายซึ่งกันและกัน โดยมีปัจจัยที่เกี่ยวข้อง ได้แก่

๔.๑.๑ สภาพความท้าทายด้านความมั่นคงปลอดภัยทางไซเบอร์ของโลก : ประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยี และความพร้อมทางด้านไซเบอร์ต่างใช้ขีด

ความสามารถทางไซเบอร์ ทั้งโดยทางตรงและทางอ้อม เพื่อให้ได้เปรียบต่อประเทศอื่น เช่น การพยายามให้ได้มาซึ่งข้อมูล หรือการจารกรรมข้อมูลเพื่อวัตถุประสงค์ต่าง ๆ เช่น เพื่อให้ได้เปรียบทางการเมือง หรือทางการทหาร หรือแม้แต่การใช้ขีดความสามารถทางไซเบอร์มุ่งโจมตีต่อระบบสารสนเทศที่ใช้ควบคุมการทำงานของโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ระบบไฟฟ้า, ระบบประปา, ระบบท่อก๊าซ, ระบบสื่อสารโทรคมนาคม และอื่น ๆ เพื่อให้เกิดผลกระทบต่อการใช้ชีวิตอันสงบเรียบร้อยของประชาชน นอกจากนี้ การโจมตีทางไซเบอร์ยังมีอีกหลายรูปแบบ เช่น การสอดแนมข้อมูลผ่านอุปกรณ์ประเภท Internet of Things (IoT), การแพร่ระบาดของไวรัสเรียกค่าไถ่, การทำให้เครื่องแม่ข่ายคอมพิวเตอร์ไม่สามารถให้บริการด้วยการโจมตีแบบ Distributed Denial - of - Service (DDoS) และการแพร่กระจายข้อมูลข่าวสารที่จัดทำขึ้นอย่างแนบเนียน เพื่อหวังผลให้เกิดการตอบสนองต่อข้อมูลข่าวสารนั้นในแนวทางที่ต้องการ เหตุการณ์ดังกล่าวเป็นเพียงตัวอย่างทั่วไปของสถานการณ์ด้านไซเบอร์ในระดับโลกซึ่งจะยิ่งทวีความรุนแรงซับซ้อนและเป็นสาเหตุแห่งอาชญากรรมคอมพิวเตอร์และความขัดแย้งระหว่างประเทศได้ในอนาคต

๔.๑.๒ ภูมิภาคที่มีนัยสำคัญต่อความมั่นคงปลอดภัยทางไซเบอร์ของโลก : ภัยคุกคามทางไซเบอร์เป็นปัญหาเกิดขึ้นได้โดยไม่จำกัดขอบเขตภูมิศาสตร์ หรือไร้พรมแดน ซึ่งจากการจัดอันดับความมั่นคงปลอดภัยไซเบอร์โลกของสหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU โดยพิจารณาจากความพร้อม ๕ ด้านที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือ ด้านกฎหมาย (Legal Measures), ด้านเทคนิค (Technical Measures), การจัดองค์กร (Organizational Measures), การพัฒนาบุคลากร (Capacity Building) และความร่วมมือ (Cooperation) พบว่าประเทศที่มีความพร้อมทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ๓ ลำดับแรก ได้แก่ อังกฤษ, สหรัฐอเมริกา และฝรั่งเศส ตามลำดับ นอกจากนี้จากเหตุการณ์ถูกโจมตีทางไซเบอร์ของประเทศต่าง ๆ จากกลุ่มแฮกเกอร์ที่เปิดเผยตัวตนนั้น พบว่า ส่วนใหญ่เป็นแฮกเกอร์มาจากประเทศในภูมิภาคเอเชียและยุโรป แสดงให้เห็นว่าภูมิภาคเหล่านี้มีนัยสำคัญต่อความมั่นคงปลอดภัยทางไซเบอร์ของโลกอีกด้วย

๔.๑.๓ สภาวะแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของภูมิภาคเอเชียตะวันออกเฉียงใต้ : คุณลักษณะสำคัญประการหนึ่งของไซเบอร์ คือ การแพร่กระจายอย่างรวดเร็วและไร้พรมแดนจึงสามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก และเมื่อพิจารณาถึงปัญหาความขัดแย้งในภูมิภาคเอเชียจะเห็นได้ว่ามีความล่อแหลมอย่างยิ่งที่จะเป็นสาเหตุและนำไปสู่การใช้ขีดความสามารถทางไซเบอร์คุกคามต่อกันความขัดแย้งของหลายประเทศ ในการแย่งชิงกรรมสิทธิ์บนหมู่เกาะในทะเลจีนใต้ หรือแม้แต่การแข่งขันกันของประเทศในกลุ่มเอเชียตะวันออกเฉียงใต้การพยายามขยายผลจากความขัดแย้งตามชายแดน เพื่อให้เกิดภาพลักษณ์ที่เป็นลบต่อประเทศไทย การที่ประเทศไทยมีบทบาทางด้านการเมืองระหว่างประเทศมากขึ้น รวมทั้ง การเป็นศูนย์กลางทางเศรษฐกิจและคมนาคมขนส่งในภูมิภาคอาเซียน การได้รับความสนใจจากประเทศจีนและอินเดีย ในการเข้ามาขยายความสัมพันธ์ทางการค้าการรวมกลุ่มกันเป็นประชาคมเศรษฐกิจอาเซียน การเคลื่อนย้ายแรงงานอย่างเสรีในภูมิภาคตลอดจนกระแสโลกาภิวัตน์ที่เข้มข้นขึ้น ทำให้เกิดการเปลี่ยนแปลงขั้วอำนาจทางเศรษฐกิจเป็นหลายศูนย์ โดยที่อำนาจทางเศรษฐกิจของภูมิภาคเอเชียมีพลังมากขึ้น นอกจากนี้ภูมิภาคเอเชียตะวันออกเฉียงใต้ยังมีปัญหาความขัดแย้งทางวัฒนธรรม หรืออุดมการณ์ร่วมกันของกลุ่มคน และการเชื่อมโยง

ระหว่างกลุ่มก่อการร้ายภายในภูมิภาคกับกลุ่มก่อการร้ายสากลที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้

๔.๒ สถานการณ์ภัยคุกคามทางไซเบอร์ภายในประเทศ

ปัจจุบันรัฐบาลให้ความสำคัญกับการพัฒนา และส่งเสริมทุกภาคส่วนให้มีการนำเทคโนโลยีดิจิทัลมาเป็นองค์ประกอบสำคัญในการขับเคลื่อนการปฏิรูปประเทศไปสู่การเป็นประเทศไทย ๔.๐ เพื่อสร้างระบบเศรษฐกิจและสังคมของประเทศที่ขับเคลื่อนด้วยนวัตกรรมและเทคโนโลยี ทำให้ประเทศไทยมีความเสี่ยงสูงขึ้น จากปัญหาอาชญากรรมคอมพิวเตอร์ อีกทั้งยังต้องเผชิญกับการแข่งขันและการใช้ศักยภาพทางไซเบอร์อย่างกว้างขวางในการหาข่าว การจารกรรมข้อมูล และการโจมตีทางไซเบอร์ (Cyber Attack) จากรัฐหรือบุคคล/กลุ่มบุคคลซึ่งจากการจัดอันดับของสหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU พบว่าประเทศไทยมีความมั่นคงปลอดภัยทางไซเบอร์อยู่ในลำดับที่สูงขึ้น ส่งผลทำให้เป็นอีกประเทศหนึ่งที่มีความเสี่ยงสูงขึ้นที่จะตกเป็นเป้าหมายในการก่อการร้ายทางไซเบอร์ โดยการละเมิดความเป็นส่วนตัวของข้อมูล คือ เป้าหมายหลักในการเกิดภัยคุกคามต่าง ๆ ซึ่งมักจะเป็นการขโมยข้อมูลส่วนบุคคล เพื่อนำไปใช้ในทางที่ผิดกฎหมาย รวมถึง มัลแวร์เรียกค่าไถ่ (Ransomware) มีความรุนแรงยิ่งขึ้น ถึงแม้จะมีระบบรักษาความปลอดภัยที่ดีแล้ว ก็อาจจะถูกโจมตีได้ทำให้ประเทศไทยมีความจำเป็นต้องเร่งรัดในการจัดทำแผนและพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของประเทศเพื่อเป็นการปกป้องรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ซึ่งปัจจุบันปัญหาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศที่เกี่ยวข้อง ได้แก่

๔.๒.๑ ปัญหาในการจัดทำแผนงาน หรือมาตรการป้องกันภัยคุกคามด้านไซเบอร์ : หน่วยงานภาครัฐและเอกชนยังขาดการให้ความสำคัญ และมีมาตรการป้องกันภัยคุกคามทางไซเบอร์ให้สอดรับกับสภาพแวดล้อม และเทคโนโลยีที่เปลี่ยนแปลงไป โดยเฉพาะมาตรฐานและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้รัดกุมรวมถึงแผนรับมือ เพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติเมื่อเกิดเหตุการณ์ทางไซเบอร์ จนทำให้ระบบได้รับความเสียหาย หรือไม่สามารถให้บริการได้

๔.๒.๒ ปัญหาอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) ปัจจุบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นโครงสร้างพื้นฐานสำคัญของประเทศที่ใช้ในการดำเนินงานและให้บริการที่สำคัญ หากระบบโครงสร้างพื้นฐานถูกโจมตีจนไม่สามารถให้บริการได้เป็นวงกว้างจะกระทบกับชีวิต และความปลอดภัยของประชาชนจำนวนมาก ก่อให้เกิดความเสียหายทางด้านเศรษฐกิจและสังคม ซึ่งจะส่งผลต่อความสงบเรียบร้อย และความมั่นคงในประเทศ

๔.๒.๓ ปัญหาความพร้อมของบุคลากรด้านไซเบอร์ : ประเทศไทยยังขาดความพร้อมของบุคลากรด้านไซเบอร์ในระดับนโยบาย, ระดับปฏิบัติและระดับเชี่ยวชาญเฉพาะทางด้านไซเบอร์ อีกทั้งหน่วยงานรัฐและเอกชนยังไม่ได้ให้ความสำคัญกับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และยังมีข้อจำกัดในการสร้างแรงจูงใจให้กับบุคลากรเรื่องการเสริมศักยภาพด้านไซเบอร์ให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศ

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้ทุกประเทศทั่วโลกต่างตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากการสงครามไซเบอร์ ทำให้ทุกประเทศต่างพยายามพัฒนาขีดความสามารถด้านการสงครามไซเบอร์ในเชิงรุกและการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นมาตรการเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม เห็นได้จากประเด็นสำคัญของยุทธศาสตร์ด้านการสงครามไซเบอร์ของประเทศต่าง ๆ ที่สำคัญ มีดังนี้

๑. สหรัฐอเมริกา

๑.๑ สหรัฐอเมริกามองว่าโลกในปัจจุบันถูกเชื่อมโยงเป็นเครือข่าย และล่อแหลมต่อการถูกโจมตีผ่านทางเครือข่าย ด้วยเหตุนี้ ยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกาจะต้องรับประกันในเรื่อง การรักษาความลับ (confidentiality) ความพร้อมใช้งาน (availability) และความสมบูรณ์ของข้อมูล (integrity of data)

๑.๒ สหรัฐอเมริกาขอสงวนสิทธิที่จะใช้เครื่องมือใด ๆ ที่เห็นว่าจำเป็น (เช่น การทูต สารสนเทศ การทหาร และเศรษฐกิจ ฯลฯ) เพื่อตอบโต้กับภัยคุกคามอย่างเหมาะสม และสอดคล้องกับกฎหมายที่มีอยู่หากใช้เครื่องมือดังกล่าวแล้วไม่เป็นผล สหรัฐอเมริกาก็พร้อมที่จะใช้กำลังทหารเมื่อใดก็ได้

๑.๓ การใช้การโจมตีด้านไซเบอร์เป็นเครื่องมือทางการเมือง ได้สะท้อนให้เห็นถึงแนวโน้มที่เป็นอันตรายต่อความสัมพันธ์ระหว่างประเทศ ดังนั้น การสงครามไซเบอร์กับฝ่ายตรงข้ามอาจยกระดับไปสู่สงครามที่มีการใช้กำลังทหารอย่างแท้จริงก็ได้

๒. สหราชอาณาจักร

๒.๑ สหราชอาณาจักรจะจัดการกับอาชญากรรมด้านไซเบอร์ และจะดำเนินการทุกวิถีทาง เพื่อให้สหราชอาณาจักรเป็นประเทศที่มีความปลอดภัยมากที่สุดประเทศหนึ่งในโลกสำหรับการทำธุรกิจในพื้นที่ไซเบอร์

๒.๒ สหราชอาณาจักรจะรับมือกับการโจมตีด้านไซเบอร์ที่ยืดหยุ่นมากขึ้น และจะปกป้องผลประโยชน์ต่าง ๆ ของสหราชอาณาจักรในพื้นที่ไซเบอร์ให้ดียิ่งขึ้น

๒.๓ สหราชอาณาจักรจะช่วยปรับสภาพพื้นที่ไซเบอร์ให้เปิดกว้าง มีเสถียรภาพ และมีชีวิตชีวา เพื่อให้ประชาชนของสหราชอาณาจักรสามารถใช้พื้นที่ไซเบอร์ได้อย่างปลอดภัย และสนับสนุนสังคมที่เปิดกว้าง

๒.๔ ประชาชนของสหราชอาณาจักรจะต้องมีความรู้ ทักษะ และขีดความสามารถที่หลากหลายและจำเป็นต่อการบรรลุจุดมุ่งหมายของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหราชอาณาจักร

๓. สาธารณรัฐประชาชนจีน

๓.๑ จีนเชื่อว่า กฎหมายระหว่างประเทศที่มีอยู่จะต้องได้รับการแก้ไขให้ความชัดเจน หรือสร้างหลักเกณฑ์ขึ้นมาใหม่ ให้สอดคล้องกับพื้นที่ไซเบอร์ในปัจจุบัน โดยเฉพาะในเรื่องสิ่งบ่งชี้ของการโจมตีด้านไซเบอร์ที่เป็นการก่ออาชญากรรมด้านไซเบอร์ และการกำหนดว่า ความเสียหายที่เกิดขึ้นจากการป้องกันตนเองอย่างไร จึงจะถือว่า เป็นการป้องกันตนเองอย่างเหมาะสม และถูกต้องตามกฎหมายระหว่างประเทศ

๓.๒ จีนตระหนักดีว่า สหรัฐอเมริกาและประเทศตะวันตกอื่น ๆ ได้ใช้ให้บริษัทคู่สัญญาด้านกลาโหม เช่น Lockheed Martin, Boeing, Northrop Grumman และ Raytheon เพื่อพัฒนาและใช้อาวุธด้านไซเบอร์ (cyber - weapon) กับทุกประเทศที่เป็นปรปักษ์

๓.๓ รัฐบาลจีนยังคงยึดถือหลักการพื้นฐานเกี่ยวกับพื้นที่ไซเบอร์ ๔ ประการ คือ ๑. หลักการว่าด้วยการเคารพต่อสิทธิและเสรีภาพในพื้นที่ไซเบอร์ โดยเน้นย้ำในเรื่องการเคารพต่อกฎหมายภายในของแต่ละประเทศ เพื่อให้ได้มาซึ่งสิทธิ ในการได้มาและเผยแพร่สารสนเทศ สิทธิมนุษยชน และเสรีภาพพื้นฐานของมนุษย์ ๒. หลักการว่าด้วยความสมดุล โดยถือว่าเทคโนโลยีจะเป็นคุณหรือโทษก็ขึ้นอยู่กับผู้ใช้ ดังนั้น จีนจึงให้ความสำคัญกับความสมดุลระหว่าง “เสรีภาพ” กับ “การควบคุม” “สิทธิ” กับ “ความรับผิดชอบ” และ “ความมั่นคง” กับ “การพัฒนา” ๓. หลักการว่าด้วยการใช้พื้นที่ไซเบอร์อย่างสันติ หลักการนี้จะเกี่ยวข้องกับการปกป้องเทคโนโลยีสารสนเทศของโลก โครงสร้างพื้นฐาน และระบบสารสนเทศทางพลเรือน มิให้ตกเป็นเป้าหมายจากภัยคุกคามหรืออาวุธทางไซเบอร์ และ ๔. หลักการว่าด้วยการพัฒนาอย่างเสมอภาค หลักการนี้ จะกล่าวถึงการแบ่งแยกทางดิจิตอล การคุ้มครองสิทธิและผลประโยชน์ของประเทศที่ด้อยกว่า และคัดค้านต่อการแสวงประโยชน์ในพื้นที่ไซเบอร์ของประเทศที่เหนือกว่าทางเทคโนโลยี เพื่อทำให้ประเทศที่ด้อยกว่าไม่สามารถควบคุมเทคโนโลยีสารสนเทศ และการบริการของตนได้อย่างอิสระ รวมถึงใช้คุกคามต่อเสถียรภาพทางการเมือง เศรษฐกิจ และสังคมของประเทศอื่น

๔. สาธารณรัฐสิงคโปร์

๔.๑ กองทัพสิงคโปร์จัดตั้งกองทัพดิจิตอลและการข่าว (Digital and Intelligence Service : DIS) ขึ้นในไตรมาสที่ ๔ ของปี ๒๕๖๕ ซึ่งกำหนดให้มีสถานะเป็นเหล่าทัพที่ ๔ ของกองทัพสิงคโปร์ นอกเหนือจากเหล่า ทบ., ทร. และ ทอ. เพื่อดูแลความมั่นคงด้านดิจิทัลและการเตรียมการรับมือกับภัยคุกคามทางดิจิทัล โดยเชื่อมโยงกับเหล่าทัพอื่น ด้วยการบูรณาการผ่านระบบ ระบบ (Command, Control, Communication, Computer and Intelligence : C4I) ปฏิบัติการในรูปแบบเครือข่าย รวมทั้งดำเนินการด้านดิจิทัล เชิงรุกให้กองทัพ และการป้องกันทางไซเบอร์ ทั้งนี้ การดำเนินการดังกล่าวสืบเนื่องมาจากการที่กองทัพสิงคโปร์ได้เล็งเห็นความสำคัญด้านดิจิทัลของประเทศ ประกอบกับเหตุการณ์ความขัดแย้งระหว่างยูเครน - รัสเซีย พบว่า มีกลุ่มแฮกเกอร์ของแต่ละฝ่ายใช้เทคโนโลยีด้านดิจิทัลเป็นเครื่องมือโจมตี ซึ่งกันและกัน ทั้งนี้ ตั้งแต่ปี ๒๕๖๔ รัฐบาลสิงคโปร์ได้ออกกฎหมาย เพื่อรับมือกับการแทรกแซงจากต่างชาติ ซึ่งมีผลบังคับให้แพลตฟอร์มโซเชียลมีเดีย และผู้ให้บริการอินเทอร์เน็ตต้องเปิดเผยข้อมูลที่อยู่เบื้องหลังเนื้อหาที่เห็นว่ามีอันตรายและสงสัยว่าต่างชาติเป็นผู้ดำเนินการ นอกจากนี้ DIS ยังให้ความสำคัญต่อการพัฒนาศักยภาพทางเทคโนโลยีดิจิทัล เช่น ระบบ Cloud วิทยาการด้านข้อมูล และปัญญาประดิษฐ์ เป็นต้น ซึ่งถือเป็นวิสัยทัศน์และความพยายามในการเปลี่ยนผ่านไปสู่กองทัพสิงคโปร์ยุคใหม่ภายในปี ๒๕๘๓

๔.๒ เมื่อ ๒๘ ต.ค. ๖๕ กห.สิงคโปร์ ได้จัดงานสถาปนาเหล่า DIS ดังกล่าวขึ้นเป็นเหล่าทัพที่ ๔ โดยมี ประธานาธิบดี Halimah Yacob แห่งสิงคโปร์ เป็นประธานในพิธี ซึ่งการจัดตั้งเหล่า DIS ถือเป็นก้าวสำคัญในการเปลี่ยนแปลงไปสู่กองทัพสิงคโปร์ในยุคต่อไป เหล่าทัพใหม่นี้เป็นการบูรณาการระบบ Command, Control, Communications, Computers and Intelligence (C4I) ที่มีอยู่ และขีดความสามารถด้านไซเบอร์ของกองทัพ ในฐานะหน่วยที่มีหน้าที่โดยเฉพาะกำลังพลเหล่า DIS จะได้รับมอบหน้าที่ในการดูแลความสงบเรียบร้อยและความมั่นคงของสิงคโปร์จากภัยคุกคามที่พัฒนาและซับซ้อนมากขึ้น

๔.๓ การสถาปนาเหล่าทัพที่สี่ของกองทัพสิงคโปร์ (SAF) - Digital and Intelligence Service (DIS) - นับเป็นก้าวสำคัญในการเปลี่ยนแปลงของกองทัพในยุคหน้า หรือ Next Generation SAF เหล่าทัพ DIS นับเป็นการรวมและการบูรณาการของระบบบัญชาการ ควบคุม สื่อสาร คอมพิวเตอร์และการข่าวกรอง (Command, Control, Communications, Computers and Intelligence (C4) ที่มีอยู่ตลอดจนขีดความสามารถทางไซเบอร์ ของกองทัพสิงคโปร์ SAF ในเหล่าทัพที่มีหน้าที่เฉพาะทาง DIS จะยกระดับ การฝึกฝน และการรักษากำลังพลด้านดิจิทัล และดำรงขีดความสามารถด้านดิจิทัลเพื่อบรรลุภารกิจในการปกป้องสันติภาพ และความมั่นคงของสิงคโปร์จากภัยคุกคามที่พัฒนาและซับซ้อนมากขึ้นในขอบเขตงานด้านดิจิทัล

รายงานความมั่นคงปลอดภัยทางไซเบอร์ของโลก (Global Cybersecurity Index) โดย International Telecommunication Union (ITU)

Global Cybersecurity Index เป็นดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมสากล หรือ International Telecommunication Union (ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลก และหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร (The ultimate goal of this initiative is to help foster a global culture of cybersecurity and its integration at the core of ICTs)

ITU เริ่มประเมิน Global Cybersecurity Index หรือ GCI ขึ้นครั้งแรกในปี ๒๕๕๗ โดยจัดทำรายงานครั้งแรกเมื่อเดือนเมษายน พ.ศ. ๒๕๕๘ ในชื่อ The Global Cybersecurity Index and Cyber Wellness Profiles Report เพื่อประเมินความมุ่งมั่นของแต่ละประเทศในการดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยใช้การจัดอันดับ (Ranking) มาเป็นเครื่องมือ สำคัญในการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์

เนื่องจากความมั่นคงปลอดภัยทางไซเบอร์เป็นประเด็นที่ครอบคลุมไปยังแอพพลิเคชั่นที่เกี่ยวเนื่องกับเรื่องกับหลายอุตสาหกรรม หลายภาคส่วน การประเมินความมั่นคงปลอดภัยทางไซเบอร์จึงพิจารณาจากปัจจัยหลักทั้งหมด ๕ ด้าน ได้แก่ มาตรการทางกฎหมาย (Legal Measures), มาตรการทางเทคนิค (Technical Measures), มาตรการการจัดโครงสร้างองค์กร (Organizational

Measures), การพัฒนาศักยภาพบุคลากร (Capacity Building) และการสร้างความร่วมมือ (Cooperation) จากปัจจัยหลัก ๕ ด้านดังกล่าว ประกอบด้วย ๑๗ ปัจจัยย่อย ดังแสดงในตารางที่ ๓ - ๑

ตารางที่ ๓ - ๑ ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ของแต่ละประเทศ

ปัจจัยหลัก	ปัจจัยย่อย
๑. มาตรการทางกฎหมาย (Legal Measures)	๑.๑ กฎหมายอาญา (Criminal Legislation) ที่เกี่ยวกับการควบคุมการกระทำความผิดทางคอมพิวเตอร์
	๑.๒ การมีกฎระเบียบและการปฏิบัติตามกฎระเบียบ (Regulation and Compliance) หมายถึง การมีกฎที่เกี่ยวข้องกับความมั่นคง ปลอดภัยทางไซเบอร์เฉพาะเรื่อง เช่น กฎหมายการใช้ลายเซ็น อิเล็กทรอนิกส์ เป็นต้น
๒. มาตรการทางเทคนิค (Technical Measures)	๒.๑ การจัดตั้งหน่วยงานระดับชาติเพื่อตอบสนองเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (CIRT (Computer Incident Response Team), CERT (Computer Emergency Response Team) หรือ CSIRT (Computer Security incident Response Team))
	๒.๒ มาตรฐาน (Standards)
	๒.๓ การออกใบรับรอง (Certifications)

ตารางที่ ๓ - ๑ ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ของแต่ละประเทศ (ต่อ)

๓. มาตรการด้านโครงสร้าง องค์กร (Organizational Measures)	๓.๑ นโยบาย (Policy)
	๓.๒ แผนด้านการกำกับดูแล (Roadmap for Governance)
	๓.๓ หน่วยงานผู้รับผิดชอบ (Responsible Agency)

	๓.๔ การเทียบเคียงกับหน่วยงานระดับชาติ (National Benchmarking)
๔. การพัฒนาศักยภาพบุคลากร (Capacity Building)	๔.๑ การกำหนดมาตรฐานในการพัฒนาบุคลากร (Standardization Development)
	๔.๒ การพัฒนาบุคลากร (Manpower Development)
	๔.๓ การให้การรับรองแก่ผู้เชี่ยวชาญ (Professional Certification)
	๔.๔ การให้การรับรองหน่วยงาน (Agency Certification)
๕. การสร้างความร่วมมือ (Cooperation)	๕.๑ การสร้าความร่วมมือระหว่างรัฐ (Intra - State Cooperation)
	๕.๒ การสร้างความร่วมมือระหว่างหน่วยงาน (Intra - Agency Cooperation)
	๕.๓ ความร่วมมือภาครัฐและภาคเอกชน (Public - private partnerships (PPP))
	๕.๔ การสร้างความร่วมมือระหว่างประเทศ (International Cooperation)

ที่มา : The World Economic Forum’s Global Cybersecurity Outlook 2023

สรุป

การศึกษาในบทที่ ๓ มีผลการศึกษาสรุปได้ดังนี้ ปัจจุบันโลกอยู่ในยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยี ทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง บุคคล หรือกลุ่มบุคคลที่ไม่ใช่รัฐ (Non - State Actor) จะเป็นผู้มีบทบาทมีอิทธิพลมากขึ้นในการดำเนินกิจกรรมที่ส่งผลกระทบต่อความมั่นคง การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศในห้วงปัจจุบัน พบว่าประเด็นความมั่นคงที่จะส่งผลกระทบต่อไทย ได้แก่ การเมืองระหว่างประเทศ, การขยายอิทธิพลและบทบาทของประเทศมหาอำนาจต่อภูมิภาคเอเชียตะวันออกเฉียงใต้, การขยายตัวของความสัมพันธ์ระหว่างประเทศในระดับภูมิภาค, ความขัดแย้งทางดินแดนและการใช้กำลังทางการทหาร, สถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้, การเคลื่อนตัวของภัยคุกคามข้ามชาติ, การย้ายถิ่นฐานของประชากร, ความมั่นคงหลัง COVID – 19 และภัยคุกคามทางไซเบอร์ ปัจจุบันสถานการณ์ความมั่นคง

ทางไซเบอร์ในต่างประเทศ มีแนวโน้มขยายผลกระทบไปในทุกสาขา อาทิ กลุ่มพลังงาน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการเงิน กลุ่มสาธารณสุข ข้อมูลส่วนบุคคล และด้านการทหาร เป็นต้น ขณะที่ในประเทศไทยก็เผชิญภัยคุกคามทางไซเบอร์ อาทิ การเจาะระบบเว็บไซต์ขององค์กรภาครัฐ การจารกรรมข้อมูล และการโจมตีระบบปฏิบัติการขององค์กรต่าง ๆ รูปแบบภัยคุกคามทางไซเบอร์มีหลากหลาย แต่ที่พบบ่อย ได้แก่ Malware Hacker Ransomware Ddos Phishing และ Spyware เป็นต้น ซึ่งความเสียหายเป็นสิ่งที่ประเมินค่ามิได้ และมีโอกาสที่ความเสียหายจะเพิ่มขึ้นในอนาคต หากไม่มีแนวทางป้องกันผลกระทบจากภัยคุกคามทางไซเบอร์อย่างเหมาะสม กรมข่าวทหารบกเป็นหน่วยงานด้านข่าวกรองหลักของกองทัพบก จึงต้องมีความพร้อมที่จะรับมือกับภัยคุกคามทุกรูปแบบให้ได้อย่างมีประสิทธิภาพ และนำเทคโนโลยี AI มาใช้ให้เกิดประโยชน์ ซึ่งจะเป็นปัจจัยส่งเสริมให้การปฏิบัติการด้านการข่าวเป็นไปอย่างรวดเร็วถูกต้อง และทันเวลา

กองทัพบกมีการนำเทคโนโลยีสารสนเทศมาใช้งานในหลายมิติ อาทิ การติดต่อสื่อสาร การฝึกอบรม การปฏิบัติงานในสำนักงาน การรวบรวบข้อมูลข่าวสาร/การวิเคราะห์ข้อมูล/การกระจายข้อมูลข่าวสาร การจัดทำระบบฐานข้อมูล การควบคุมระบบปฏิบัติการของอาวุธยุทโธปกรณ์ และการอำนวยการ/ควบคุมบังคับบัญชา ในห้องปฏิบัติการ ฯลฯ เป็นต้น ในส่วนของ ปัญหา/ความท้าทายในการใช้เทคโนโลยีของกองทัพบกนั้น กองทัพบกมีการใช้ระบบเทคโนโลยีสารสนเทศในการปฏิบัติงาน โดยอาจแบ่งประเภทของการนำมาใช้งานใน ๒ แบบ คือ เป็นระบบที่หน่วยดำเนินการพัฒนาขึ้นมาด้วยตนเอง และระบบที่ได้จากการจ้างผู้ประกอบการภายนอกเข้ามาดำเนินการให้ ทั้งนี้ จากข้อมูล

ผลการปฏิบัติงานด้านการข่าวของกองทัพบกที่ผ่านมา มีประเด็นปัญหาของการใช้เทคโนโลยีเพื่อสนับสนุนการปฏิบัติงานที่สำคัญสรุป ได้แก่ ความปลอดภัย, ความท้าทายในเรื่องของ Generation Gap หรือความต่างของอายุและช่วงวัย เนื่องจากเทคโนโลยีนั้นมีการพัฒนา และปรับเปลี่ยนอยู่ตลอดเวลา คนรุ่นเก่าจะเรียนรู้วิธีการใช้เทคโนโลยีได้ยากกว่าคนรุ่นใหม่, ความท้าทายเรื่องความถูกต้องและแม่นยำของเทคโนโลยี, ปัญหาด้านความรู้ความสามารถด้านเทคโนโลยีของกำลังพล, ปัญหาด้านงบประมาณ และปัญหาด้านโครงสร้างหน่วยงานที่ไม่เอื้อต่อการทำงานข่าวที่ต้องการความรวดเร็ว

การประเมินสถานการณ์ด้านไซเบอร์เพื่อความมั่นคงของไทยนั้น ประกอบด้วยสถานการณ์ภัยคุกคามทางไซเบอร์ภายนอกประเทศ และสถานการณ์ภัยคุกคามทางไซเบอร์ภายในประเทศ ซึ่งปัจจุบันปัญหาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศที่สำคัญ ๆ ได้แก่

๑. ปัญหาในการจัดทำแผนงานหรือมาตรการป้องกันภัยคุกคามด้านไซเบอร์

๒. ปัญหาอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII)

๓. ปัญหาความพร้อมของบุคลากรด้านไซเบอร์

สำหรับรูปแบบและลักษณะของการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศนั้น ทำการศึกษาใน ๔ ประเทศ สรุปได้ว่า

๑. สหรัฐอเมริกามองว่า โลกในปัจจุบันถูกเชื่อมโยงเป็นเครือข่ายและล่อแหลมต่อการถูกโจมตีผ่านทางเครือข่าย ด้วยเหตุนี้ ยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของ

สหรัฐอเมริกาจะต้องรับประกันในเรื่อง การรักษาความลับ (confidentiality) ความพร้อมใช้งาน (availability) และความสมบูรณ์ของข้อมูล (integrity of data)

๒. สหราชอาณาจักรจะจัดการกับอาชญากรรมด้านไซเบอร์และจะดำเนินการทุกวิถีทาง เพื่อให้สหราชอาณาจักรเป็นประเทศที่มีความปลอดภัยมากที่สุดประเทศหนึ่งในโลก สำหรับการทำธุรกิจในพื้นที่ไซเบอร์

๓. จีนเชื่อว่า กฎหมายระหว่างประเทศที่มีอยู่จะต้องได้รับการแก้ไข ให้ความชัดเจน หรือสร้างหลักเกณฑ์ขึ้นมาใหม่ให้สอดคล้องกับพื้นที่ไซเบอร์ในปัจจุบัน โดยเฉพาะในเรื่องสิ่งบ่งชี้ของการโจมตีด้านไซเบอร์ที่เป็นการก่ออาชญากรรมด้านไซเบอร์ และการกำหนดว่า ความเสียหายที่เกิดขึ้นจากการป้องกันตนเองอย่างไร จึงจะถือว่า เป็นการป้องกันตนเองอย่างเหมาะสมและถูกต้องตามกฎหมายระหว่างประเทศ

๔. กองทัพสิงคโปร์จัดตั้งกองทัพดิจิตอลและการข่าว (Digital and Intelligence Service : DIS) ซึ่งกำหนดให้มีสถานะเป็นเหล่าทัพที่ ๔ ของกองทัพสิงคโปร์ นอกเหนือจากเหล่า ทบ., ทร. และ ทอ. เพื่อดูแลความมั่นคงด้านดิจิทัล และการเตรียม การรับมือกับภัยคุกคามทางดิจิทัล โดยเชื่อมโยงกับเหล่าทัพอื่น ด้วยการบูรณาการผ่านระบบ (Command, Control, Communication, Computer and Intelligence : C4I) ปฏิบัติการในรูปแบบเครือข่าย รวมทั้งดำเนินการด้านดิจิทัลเชิงรุกให้กองทัพ และการป้องกันทางไซเบอร์

และประการสุดท้าย Global Cybersecurity Index เป็นดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมสากล หรือ International Telecommunication Union (ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลก และหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร (The ultimate goal of this initiative is to help foster a global culture of cybersecurity and its integration at the core of ICTs) การศึกษาฉบับนี้สามารถนำแนวคิด Global Cybersecurity Index ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของแต่ละประเทศ มาเป็นเครื่องมือในการวิเคราะห์ปัญหาและข้อเสนอแนะได้

บทที่ ๔
ผลการวิจัย

จากการเก็บรวบรวมข้อมูลทั้งจากแหล่งข้อมูลปฐมภูมิ และข้อมูลทุติยภูมิที่รวบรวมได้จากบทความ ตำราวิชาการ งานวิจัย และเอกสารที่เกี่ยวข้อง ในบทนี้ผู้วิจัยจะนำข้อมูลดังกล่าวมาวิเคราะห์ และกำหนดตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของข่าวกรองทางทหาร โดยใช้หลักการของเหตุผลในเชิงตรรกวิทยาตามกรอบแนวคิด ดังประเด็นต่อไปนี้

วิเคราะห์ปัญหางานข่าวกรองไซเบอร์ของกองทัพบก

สรุป

วิเคราะห์ปัญหางานข่าวกรองไซเบอร์ของกองทัพบก

๑. การวิเคราะห์ SWOT Analysis เพื่อกำหนดแนวทางในการพัฒนาระบบข่าวกรองไซเบอร์

ในส่วนนี้กล่าวถึงสภาพแวดล้อมที่เกี่ยวข้องต่อการกำหนดตัวแบบที่เหมาะสมกับกองทัพบก โดยใช้การวิเคราะห์จากจุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) กำหนดปัจจัยหลักในการวิเคราะห์สิ่งแวดล้อมภายในองค์กรด้วย 4M (Management, Machine, Money และ Man) และใช้การวิเคราะห์ปัจจัยภายนอกที่แสดงถึงโอกาสและอุปสรรคด้วย PEST (Policy, Economic, Social และ Technology) ซึ่งผลการวิเคราะห์สถานการณ์ดังกล่าวจะได้ถูกนำไปกำหนดข้อเสนอเพื่อการพัฒนางานข่าวกรองไซเบอร์ของกองทัพบก ประกอบด้วย การวิเคราะห์ปัจจัยภายใน (Internal Factors) และปัจจัยภายนอก (External Factors) ดังนี้

๑.๑ การวิเคราะห์สภาพแวดล้อมภายใน (Internal Environment) การวิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศภายในของกองทัพบก โดยใช้การวิเคราะห์สภาพแวดล้อมภายในตามหลัก 4M Analysis สามารถสรุปแยกเป็นจุดแข็งและจุดอ่อนสรุปได้ดังนี้

๑.๑.๑ การบริหารจัดการ

<u>จุดแข็ง</u>

มีนโยบายและยุทธศาสตร์ที่ชัดเจนเกี่ยวกับการพัฒนางานด้านไซเบอร์

มีโครงสร้างการจัดหน่วยงานที่รับผิดชอบงานด้านไซเบอร์ที่ชัดเจนในทุกส่วนราชการมีคณะกรรมการ คณะอนุกรรมการคณะทำงานระดับกองทัพบก

จุดอ่อน

โครงสร้างการจัดมีความซับซ้อน มีสายการบังคับบัญชายาวทำให้ต้องใช้เวลาค่อนข้างมากในการดำเนินงานต่าง ๆ

บุคลากรผู้ใช้งานระบบคอมพิวเตอร์บางส่วนยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์

ขาดการบูรณาการข้อมูลร่วมกันระหว่างหน่วยงานรวมทั้งการยืนยันความถูกต้อง สมบูรณ์และเชื่อมโยงเป็นระบบเดียวกัน

ยังไม่มีความชัดเจนในเรื่องข่าวกรองไซเบอร์

๑.๑.๒ อุปกรณ์และระบบ (Machine)

จุดแข็ง

ศูนย์ไซเบอร์ของ ทบ. มีเครื่องมือระบบตรวจจับและป้องกันการโจมตีทางไซเบอร์ที่ครอบคลุมเครือข่ายข้อมูลภายในของแต่ละ นขต.ทบ.

จุดอ่อน

การติดตั้งใช้งานโปรแกรมละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์ส่วนหนึ่งของส่วนราชการ

ระบบงานที่พัฒนาขึ้นเองบางโปรแกรม อาจไม่สอดคล้องตามมาตรฐานการรักษาความปลอดภัยสารสนเทศ

หน่วยงานไม่สนับสนุนเครื่องคอมพิวเตอร์สำหรับใช้ในการปฏิบัติงานไม่เพียงพอ ทำให้ยากต่อการควบคุมความมั่นคงปลอดภัยไซเบอร์

๑.๑.๓ งบประมาณ (Money)

จุดแข็ง

มีการจัดสรรงบประมาณด้านไซเบอร์ และด้านกาข่าวกรองเป็นประจำทุกปี

จุดอ่อน

งบประมาณที่ได้รับไม่เพียงพอต่อการพัฒนาด้านไซเบอร์ และข่าวกรองไซเบอร์

ขาดการวางแผนในการขอรับการสนับสนุนงบประมาณ ที่ทำให้การรักษาความปลอดภัยไซเบอร์มีความไม่ต่อเนื่อง

๑.๑.๔ บุคลากร

จุดแข็ง

บุคลากรด้านการข่าวที่มีความรู้ ประสบการณ์

มีผู้ปฏิบัติงานด้านไซเบอร์จำนวนหนึ่ง

จุดอ่อน

ผู้ใช้งานระบบสารสนเทศส่วนใหญ่ยังขาดความตระหนักรู้ภัยคุกคามทางไซเบอร์

บุคลากรที่มีความรู้ความสามารถระดับสูงที่บรรจุตามหน่วยงานไม่เพียงพอต่อความต้องการ

บุคลากรผู้ใช้งานระบบคอมพิวเตอร์ยังขาดจิตสำนึกด้านการรักษาความปลอดภัยคอมพิวเตอร์

๑.๒ การวิเคราะห์สภาพแวดล้อมภายนอก (External Environment)

การวิเคราะห์สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศภายนอกของ ทบ. โดยใช้การวิเคราะห์สภาพแวดล้อมภายนอก สามารถสรุปแยกเป็นโอกาสและอุปสรรค สรุปได้ดังนี้

๑.๒.๑ นโยบาย กฎระเบียบ (Policy)

<u>โอกาส</u>

นโยบายในระดับรัฐบาลให้ความสำคัญต่อการ ปัญหาในขั้นตอนการตั้งงบประมาณ และการ จัดซื้อปรับไปสู่รัฐบาลดิจิทัล

<u>อุปสรรค</u>

ปัญหาในขั้นตอนการตั้งงบประมาณ และการ จัดซื้อ จัดจ้าง ที่ล่าช้า

ระเบียบราชการไม่เอื้ออำนวยในการปฏิบัติงานในการจัดอุปกรณ์ระบบสารสนเทศที่ทันสมัยเข้ามาใช้งาน

การเปลี่ยนแปลงระดับนโยบายส่งผลต่อการดำเนินงานตามแผนงานโครงการต้องปรับปรุงบ่อยครั้งขาดความต่อเนื่อง

๑.๒.๒ เศรษฐกิจ (Economic)

<u>โอกาส</u>

แนวทางทิศทางเศรษฐกิจรองรับการเติบโตทางด้านเทคโนโลยีดิจิทัลมากขึ้น

<u>อุปสรรค</u>

การระบาดของโควิด - ๑๙ ส่งผลกระทบกับการเติบโตทางด้านเศรษฐกิจและการจัดสรรงบประมาณ

การปรับเปลี่ยนรูปแบบการทำงานที่ใช้ระบบสารสนเทศเข้ามามีส่วนช่วยขับเคลื่อนธุรกิจมากขึ้น จึงเป็นโอกาสเกิดการโจมตีทางไซเบอร์ในรูปแบบใหม่ ๆ

๑.๒.๓ เทคโนโลยีสารสนเทศ (Technology)

<u>โอกาส</u>

ความก้าวหน้าและแนวโน้มของเทคโนโลยีที่เอื้อต่อการนำมาใช้ในหน่วยงาน

มีการนำเทคโนโลยีมาประยุกต์กับงานของกระทรวงได้หลากหลายมากขึ้น

การเข้ามาของเครือข่าย Government Cloud และ Big Data ทำให้มีนวัตกรรม และช่องทางใช้งานเพิ่มขึ้น

<u>อุปสรรค</u>

มีการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็วทำให้ปรับตัวไม่ทัน

ข้อมูลถูกบิดเบือนในเครือข่ายสังคมออนไลน์ (Social Media) ที่สร้างความสับสน ขัดแย้งและความเข้าใจที่ผิดในหลาย ๆ เรื่อง

ภัยคุกคามทางไซเบอร์ในภาพรวมระดับนานาชาติได้ทวีความรุนแรงมากยิ่งขึ้น

๑.๓ แนวทางการกำหนดกลยุทธ

จากการวิเคราะห์จากจุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) ของดำเนินงานที่ผ่านมาซึ่งประกอบด้วยปัจจัยภายในและปัจจัยภายนอกที่ได้รับ นำเข้าสู่การวิเคราะห์ด้วยเครื่องมือ TOWS Matrix ตามขั้นตอนเพื่อกำหนดกลยุทธ์ จำนวน ๔ ด้าน ประกอบด้วย กลยุทธ์เชิงรุก กลยุทธ์เชิงแก้ไข กลยุทธ์เชิงป้องกัน กลยุทธ์เชิงรับ มีรายละเอียดดังนี้

๑.๓.๑ กลยุทธ์เชิงรุก

๑.๓.๑.๑ พัฒนาโครงสร้างพื้นฐานและเทคโนโลยีด้านไซเบอร์อย่างเป็นระบบ ให้สามารถสนับสนุนภารกิจอย่างมีประสิทธิภาพ พร้อมทั้งส่งเสริมหน่วยงานในสังกัดใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อป้องกันการถูกโจมตีทางไซเบอร์

๑.๓.๑.๒ มุ่งเน้นการพัฒนาระบบป้องกันโจมตีทางไซเบอร์ โดยการสร้างความร่วมมือด้านความมั่นคงไซเบอร์ระหว่างหน่วยงาน

๑.๓.๑.๓ เสริมสร้างขีดความสามารถด้านการข่าวกรองไซเบอร์ในทุก ๆ ด้านให้กับหน่วยงานด้านการข่าวของ ทบ.

๑.๓.๒ กลยุทธ์เชิงแก้ไข

๑.๓.๒.๑ พัฒนาการบริหารจัดการงานด้านไซเบอร์ในภาพรวมของ ทบ. ให้มีความเป็นเอกภาพ มีเป้าหมายและแผนระยะยาวที่ชัดเจน เป็นแนวทางการปฏิบัติให้หน่วยในสังกัดมีแนวทางพัฒนาเป็นไปในทิศทางเดียวกัน

๑.๓.๒.๒ พัฒนาการบริหารจัดการกำลังพล ทบ. ที่มีคุณวุฒิประสบการณ์ทำงานด้านไซเบอร์ และเทคโนโลยีที่เกี่ยวข้องให้มีประสิทธิภาพยิ่งขึ้น

๑.๓.๒.๓ การบูรณาการใช้งานกำลังพลระหว่างหน่วยงานมีการถ่ายทอดองค์ความรู้อย่างเป็นระบบ เสริมสร้างขวัญกำลังใจให้กับผู้ปฏิบัติงานอย่างเหมาะสมเพื่อนำไปสู่การพัฒนาองค์ความรู้ด้านไซเบอร์อย่างยั่งยืน

๑.๓.๒.๔ ส่งเสริมความร่วมมือการพัฒนาขีดความสามารถของกำลังพลร่วมกับหน่วยงานภายนอกที่มีความรู้และประสบการณ์

๑.๓.๓ กลยุทธ์เชิงป้องกัน

๑.๓.๓.๑ สร้างบทบาทนำและมีส่วนร่วมในฐานะหน่วยงานด้านความมั่นคงเพื่อสร้างความตระหนักถึงภัยคุกคามสมัยใหม่ เสริมสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการพัฒนาขีดความสามารถในการเฝ้าตรวจ ระวังป้องกัน และแก้ไขปัญหาภัยคุกคาม ตลอดจนเสริมสร้างขีดความสามารถให้มีความพร้อมรักษาอธิปไตยและพิทักษ์รักษาผลประโยชน์ของชาติอย่างเหมาะสม

๑.๓.๓.๒ รักษาสถานภาพระบบสารสนเทศของ นขต.ทบ. ที่ได้รับการรับรองมาตรฐาน ISO 27001 : 2013

๑.๓.๓.๓ ดำรงสภาพการใช้งานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความพร้อมใช้งานสนับสนุนภารกิจได้อย่างมีประสิทธิภาพ มีความคุ้มค่าสูงสุดด้านงบประมาณ

๑.๓.๔ กลยุทธ์เชิงรับ

๑.๓.๔.๑ จัดลำดับความสำคัญ ภารกิจ/แผนงาน/โครงการ/งาน ให้มีความเหมาะสมตามสถานการณ์ เช่น ความสำคัญของภารกิจ ความพร้อมของกำลังพล เครื่องมือ และสถานภาพด้านงบประมาณ

๑.๓.๔.๒ การบูรณาการข้อมูลข่าวสาร เครื่องมือ ให้สามารถใช้งานทรัพยากรร่วมกันระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการลงทุน

๒. วิเคราะห์ Cyber Security ของ ทบ. ตามกรอบ Global Cybersecurity Index ของ International Telecommunication Union (ITU)

จากข้อมูล ITU Global Cybersecurity Index (GCI) ปี ค.ศ. ๒๐๑๔, ๒๐๑๗ และ ๒๐๑๘ พบว่า ประเทศไทยอยู่อันดับ ๗ ในภูมิภาคเอเชียและแปซิฟิก และอยู่ในอันดับที่ ๑๕ ของโลกในปี ค.ศ. ๒๐๑๔ และตกมาเป็นอันดับที่ ๒๐ และ ๓๕ ในปี ค.ศ. ๒๐๑๗ และ ๒๐๑๘ ตามลำดับ แต่หากพิจารณา จากคะแนนรวม ประเทศไทยได้คะแนนรวมเพิ่มขึ้นเป็นลำดับ จาก ๐.๔๑๑๘ ในปี ค.ศ. ๒๐๑๔ เป็น ๐.๗๘๖ ในปี ค.ศ. ๒๐๑๘ แสดงให้เห็นว่าประเทศไทยมีพัฒนาการในการดำเนินนโนบายด้านความ มั่นคงปลอดภัยไซเบอร์อย่างเห็นได้ชัด อย่างไรก็ตาม ข้อมูลจากรายงานในปี ค.ศ. ๒๐๑๔ แต่ละอันดับ จะมีหลายประเทศที่ได้คะแนนเท่ากัน และในรายงานของ ITU ปี ค.ศ. ๒๐๑๗ และ ๒๐๑๘ จะแสดงให้เห็นคะแนนแต่ละตัวชี้วัดเฉพาะ ๑๐ อันดับแรก ทำให้ขาดข้อมูลประกอบการพิจารณาในส่วนของ ประเทศไทยในแต่ละตัวชี้วัด

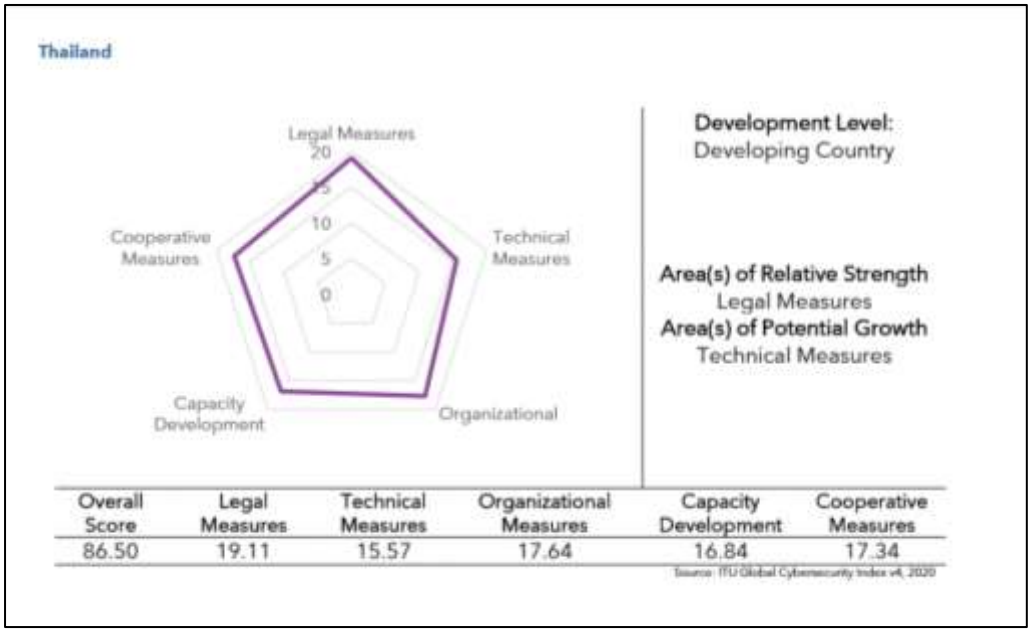
อย่างไรก็ตามในรายงานล่าสุดปี ๒๐๒๐ พบว่า คะแนนรวมของประเทศไทยเพิ่มขึ้นเป็น ๘๖.๕ (๐.๘๖๕) โดยมีอันดับในภูมิภาคที่ ๙ และ อันดับโลกที่ ๔๔ โดยในภาพของประเทศไทยแล้วถือว่ามีพัฒนาการขึ้นมามากแม้นว่าคะแนนในภูมิภาคและโลกจะเพิ่มขึ้นก็ตาม แสดงให้เห็นว่าประเทศต่างๆทั่วโลกมีพัฒนาการที่ดียิ่งขึ้นต่อเนื่อง รายละเอียดคะแนนและอันดับของประเทศไทยในการดำเนินงานด้าน ความมั่นคงปลอดภัยไซเบอร์ปรากฏตาม ตารางที่ ๕

ตารางที่ ๔ - ๑ คะแนนและอันดับของประเทศไทยในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

ปี	ด้าน กฎหมาย	ด้าน เทคนิค	ด้าน องค์กร	ด้าน เสริมสร้างศักยภาพ	ด้าน ความร่วมมือ	คะแนนรวม	อันดับในภูมิภาค	อันดับโลก
2014	0.500	0.3333	0.5000	0.2500	0.5000	0.4118	7	15
2017	NA	NA	NA	NA	NA	0.684	7	20
2018	NA	NA	NA	NA	NA	0.796	7	35
2020*	19.11	15.57	17.64	16.84	17.34	86.5	9	44

ที่มา : ITU Global Cybersecurity Index (GCI) 2014, 2017, 2018 และ 2020

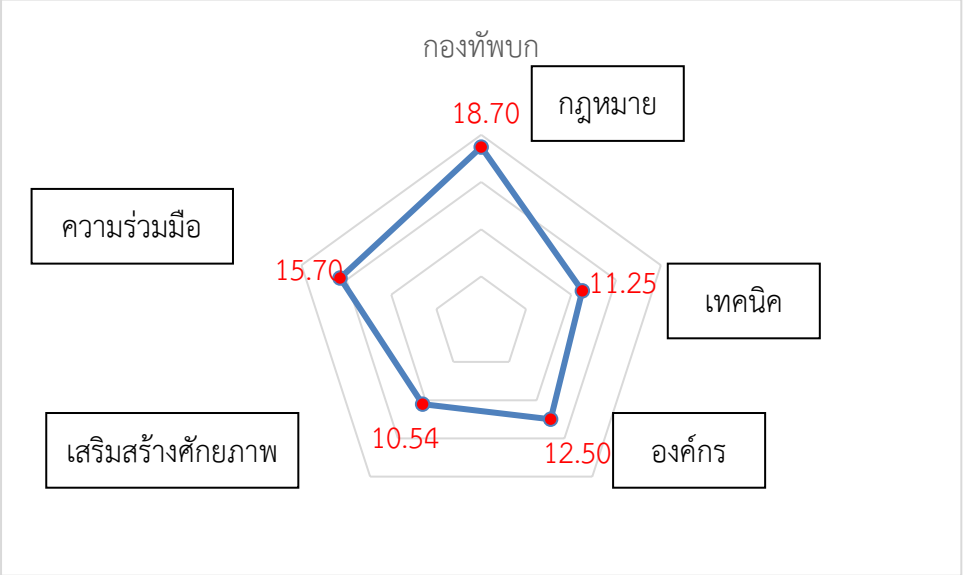
แผนภาพที่ ๔ - ๑ ผลการประเมินในปี ๒๐๒๐



ที่มา : ITU Global Cybersecurity index 2020

ผลจากการศึกษาการดำเนินการของ ทบ. โดย เทคนิคเดลฟาย (การประเมินโดยผู้บริหารและผู้เชี่ยวชาญภายในหน่วยงาน) แบ่งตามตัวชี้วัดทั้ง ๕ ด้าน มีดังนี้

แผนภาพที่ ๔ - ๒ ผลการประเมินการดำเนินงานด้านไซเบอร์ของกองทัพบก ปี ๒๐๒๒



ที่มา : ศูนย์ไซเบอร์กองทัพบก, ๒๕๖๕

ด้านกฎหมาย

ปัจจุบันประเทศไทยได้มีพระราชบัญญัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เช่น

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒

๔. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๕. ร่างพระราชบัญญัติว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและ เท่าเทียมกัน พ.ศ. ....

๖. พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

ด้านเทคนิค

ประเทศไทยมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ที่ทำหน้าที่เพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคง ปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคง ปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและ แนวทางต่าง ๆ

ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่าย อินเทอร์เน็ต ขณะที่ ทบ. ยังมีขีดความสามารถจำกัดในเรื่องนี้ การดำเนินการส่วนใหญ่เป็นเรื่องการรักษาความปลอดภัยและการใช้ประโยชน์จาก internet เท่านั้น

ด้านองค์กร

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลใช้บังคับเมื่อวันที่ ๒๘ พฤษภาคม ๒๕๖๒ โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ รวมทั้งให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดยในส่วนของ ทบ. มีการจัดตั้งศูนย์ไซเบอร์กองทัพบก

ศูนย์ไซเบอร์กองทัพบก มีการปฏิบัติ ๓ เรื่อง คือ

๑. ทำหน้าที่เป็นเสมือน ศูนย์ปฏิบัติการไซเบอร์ เพื่อ เฝ้าระวัง แจ้งเตือน ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ ตลอดจนการพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก เพื่อให้สามารถปฏิบัติการเชิงรุก เพื่อโต้ตอบและโจมตีฝ่ายตรงข้ามได้ในกรณีจำเป็น

๒. เสริมสร้างความรู้ ความเข้าใจ สร้างความตระหนัก ติดตาม กำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ รวมถึงการดำเนินการพิสูจน์หลักฐานทางดิจิตอล

๓. สนับสนุนการปฏิบัติการข่าวสารของกองทัพบก และหน่วยที่เกี่ยวข้อง โดยทำหน้าที่เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ ที่ส่งผลกระทบต่อสถาบัน และความมั่งคงของชาติ การรวบรวม วิเคราะห์ ทิศทาง แนวโน้ม โครงข่ายความสัมพันธ์ของข้อมูล ประเภทสื่อ และกลุ่มเป้าหมาย การติดตาม สืบค้น แหล่งที่มาและเป้าหมาย และการกำหนดมาตรการป้องปราม ตอบโต้ สกัดกั้น รวมถึงการประสานการดำเนินการตามกฎหมาย

ด้านการเสริมสร้างศักยภาพ

ประเทศไทยโดยหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และสภาความมั่นคงแห่งชาติได้ตระหนักถึงความสำคัญ ในการเตรียมบุคลากรที่มีทักษะและความเชี่ยวชาญดังกล่าวโดยมีการจัดหลักสูตรฝึกอบรมด้านนี้ แต่ยังขาดการประสานงานระหว่างหน่วยงานต่าง ๆ โดยเฉพาะอย่างยิ่งการประสานงานกับ สถาบันการศึกษาและภาคธุรกิจและภาคอุตสาหกรรมในการจัดเตรียมบุคลากร และสายงานอาชีพใน ด้านความมั่นคงปลอดภัย ภาคธุรกิจและประชาชนยังขาดความตระหนักรู้ในเรื่องการรักษาความมั่นคง ปลอดภัยไซเบอร์ ทั้งนี้ในส่วนของ ทบ. มีการดำเนินการคล้ายคลึงกัน โดยให้ความสำคัญกับการพัฒนาศักยภาพเจ้าหน้าที่ ในเรื่องของการเข้ารับการศึกษา การฝึกอบรม การเข้าร่วมการแข่งขัน และระบบงาน รวมถึงระบบเครือข่าย อย่างไรก็ตามถือว่าอยู่ในระดับจำกัด ทำให้ไม่สามารถกำหนดทิศทางการพัฒนาขีดความสามารถที่ต้องการได้อย่างเป็นรูปธรรมโดยเฉพาะงานข่าวกรองไซเบอร์

ด้านความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานระหว่างประเทศ

ในส่วนของ ThaiCERT ในฐานะที่เป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งใน ระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/ Forum of Incident Response and Security Teams) จึงมีบทบาทในการประสานงาน ระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้ กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง ในส่วนของ ทบ. มีความร่วมมือด้านการข่าวและด้านไซเบอร์กับ ทบ. มิตรประเทศ ที่สำคัญคือ สหรัฐฯ โดยเป็นลักษณะการแลกเปลี่ยนความรู้และประสบการณ์ (Subject matter experts exchange, SMEE)

๓. เปรียบเทียบรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ

ตารางที่ ๔ – ๒ สรุปผลการรวบรวมข้อมูลเกี่ยวกับรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ

ลำดับ	หัวข้อ	ผลการเปรียบเทียบข้อมูล
	สิ่งที่เหมือนกัน	รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ ในปัจจุบัน ได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทางานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์ มาประยุกต์ใช้กับหน่วยงานของตนเองโดยมีกระบวนการการทางานหลักคือ Identify Protect Detect Respond and Recovery ที่เป็นกรอบแนวคิดในการปฏิบัติที่เป็นที่ยอมรับและนำไปใช้อย่างแพร่หลายทั่วโลก ขณะที่งานข่าวจะเน้น ในเชิงป้องกันมากกว่าเชิงรุก ด้วยการดำเนินการด้านข่าวกรอง ด้านภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) ที่เน้นในการศึกษาว่าภัยคุกคามคือใคร มีเทคนิคและวิธีการโจมตีอย่างไรได้รับการสนับสนุนจากใคร มีหนทางปฏิบัติต่อผู้ที่เป็นเป้าหมายอย่างไร นอกจากนี้ แนวคิดในการพัฒนาขีดความสามารถในด้านไซเบอร์ของไทยยังมีรูปแบบเดียวกันกับอีกหลายประเทศ อาทิ เยอรมนี สิงคโปร์ เป็นต้น โดยมุ่งเน้นในการพัฒนาองค์ประกอบหลัก ๓ ด้าน คือ ด้านบุคลการ (People) ให้มีขีดความสามารถและความพร้อมในการปฏิบัติงานด้านไซเบอร์ ด้านอุปกรณ์และเทคโนโลยี

ตารางที่ ๔ – ๒ สรุปผลการรวบรวมข้อมูลเกี่ยวกับรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ (ต่อ)

ลำดับ	หัวข้อ	ผลการเปรียบเทียบข้อมูล
		(Technology) ให้มีขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์ และการเสริมสร้างความสัมพันธ์กับต่างประเทศ (Enhance Relationship) ในการแบ่งปันองค์ความรู้และสร้างพันธมิตร ในการป้องกันภัยทางไซเบอร์ร่วมกัน
	สิ่งที่ต่างกัน	มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ โดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์ (Cyber Intelligence) จะเป็นหน้าที่และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน โดยจะทางานและบูรณาการข้อมูลกับหน่วยที่ปฏิบัติการด้านไซเบอร์หรือหน่วยงานด้านยุทธการอย่างใกล้ชิด เนื่องจากงานข่าวกรองเป็นงานที่ใช้ความรู้และความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องใช้ประสบการณ์จากการปฏิบัติงานมาเป็นระยะเวลาหนึ่ง จึงจะสามารถวิเคราะห์สถานการณ์ที่อาจจะเกิดขึ้นในอนาคตได้ ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด ไม่ว่าจะเป็นขั้นตอนการระบุภัยคุกคาม การป้องกันและการแจ้งเตือน ไม่ได้มีการแบ่งหน้าที่งานด้านการข่าวในพื้นที่ปฏิบัติการไซเบอร์ให้กับหน่วยงานด้านการข่าวของหน่วย นอกจากนี้ การบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่มีหลักการปฏิบัติ และการดำเนินการที่ชัดเจนเหมือนกับของต่างประเทศ

ที่มา : เอกสารบำรุงความรู้ด้านการข่าวกรองกองทัพบก. ปีที่ ๑ ฉบับที่ ๑, ตุลาคม - ธันวาคม ๒๕๖๕

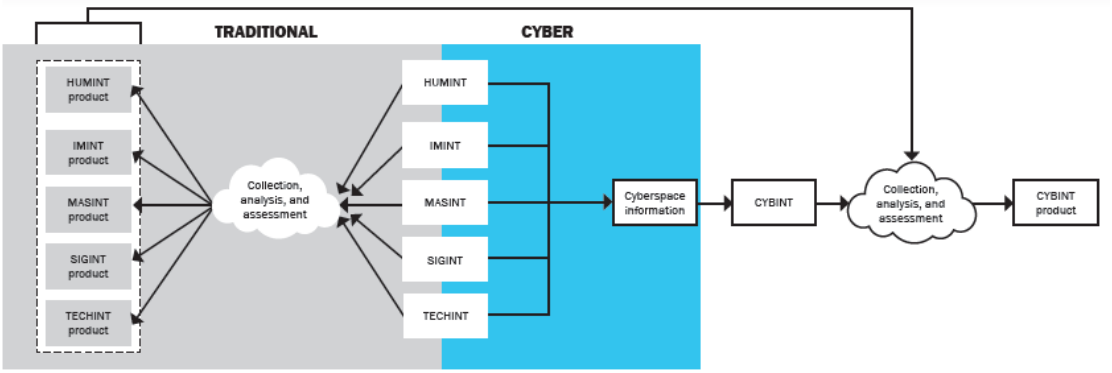
จากการเก็บรวบรวมข้อมูลและการศึกษาตำราวิชาการรวมถึงทบทวนวรรณกรรมที่เกี่ยวข้องพบว่า รูปแบบและลักษณะมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศมีข้อแตกต่างที่สำคัญ คือ การกำหนดหน้าที่และความรับผิดชอบของหน่วยงานด้านไซเบอร์ โดยในประเทศไทยงานทุกงานที่เป็นการปฏิบัติการบนพื้นที่ไซเบอร์ จะอยู่ภายใต้

ความรับผิดชอบของศูนย์ไซเบอร์ หรือหน่วยไซเบอร์ขององค์กรหรือหน่วยงานนั้นทั้งหมด ไม่ได้มีการแบ่งหน้าที่ให้กับหน่วยงานอื่นที่เป็นหัวหน้าสายวิทยาการในงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ขณะที่ต่างประเทศจะมีหลักนิยม และแนวคิดการปฏิบัติที่ชัดเจนในการแบ่งหน้าที่ และความรับผิดชอบที่เหมาะสมต่อกิจของงาน โดยมอบหมายให้แก่หัวหน้าสายวิทยาการในสายงานนั้นเป็นผู้รับผิดชอบ อาทิ หน่วยงานด้านการข่าวมีหน้าที่รับผิดชอบงานข่าวกรองไซเบอร์ ตัวอย่าง คือ กองทัพอากาศสหรัฐฯ ภาคแปซิฟิก (PACAF) มอบหมายให้หน่วยข่าวรับผิดชอบงานข่าวกรองไซเบอร์ โดยสนับสนุนข้อมูลสำคัญให้แก่หน่วยสื่อสารนำไปใช้ในการปฏิบัติทั้งเชิงรุกและเชิงรับ เป็นต้น

๔. กำหนดแนวความคิดในการพัฒนาระบบข่าวกรองไซเบอร์ของ ทบ.

แผนภาพที่ ๔ - ๓ วงรอบข่าวกรองไซเบอร์



ที่มา : เอกสารบำรุงความรู้ด้านการข่าวกรองกองทัพบก. ปีที่ ๑ ฉบับที่ ๑, ตุลาคม - ธันวาคม ๒๕๖๕ หน้า ๒๓

“การข่าวกรองไซเบอร์” คือ กระบวนการตามวงรอบข่าวกรองเพื่อให้ได้มา ซึ่งข่าวกรองไซเบอร์ด้วยการ หลอมรวมข่าวกรองทั้งหมดที่เกี่ยวข้องกับการปฏิบัติการในพื้นที่ไซเบอร์ ซึ่งได้มาจากหลักการรวบรวมข่าวสารจากทุกแหล่ง เพื่อนำไปสู่ผลผลิตที่ทำให้ผู้บังคับบัญชาทราบ และตัดสินใจเกี่ยวกับการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับได้ โดยหลักการรวบรวมข่าวสารแบบดั้งเดิม จะยังคงเป็นกิจกรรมการรวบรวมข่าวกรองอย่างต่อเนื่อง ผลลัพธ์หรือผลผลิตของการดำเนินกรรมวิธีข่าวสารให้เป็นข่าวกรอง ที่เกี่ยวกับพื้นที่ไซเบอร์หรือการปฏิบัติการในพื้นที่ไซเบอร์ สามารถเป็นส่วนหนึ่งหรือเป็นงานที่ได้รับมอบหมายให้กับข่าวกรองไซเบอร์ ที่ซึ่งมีการหลอมรวมข่าวสารที่ได้จากทุกแหล่ง เพื่อสร้างเป็นผลผลิตที่ตอบสนองความต้องการข่าวสารของผู้บังคับบัญชา

กรอบแนวคิดการพัฒนากำลังทางบกในอนาคตของ ทบ. ต้องมีความสอดคล้องต่อสภาวะแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลงไป ในการตอบสนองต่อภัยคุกคามรูปแบบผสม ที่จะเป็นตัวกำหนดภารกิจ หน้าที่ และความรับผิดชอบของ ทบ. ที่จะได้รับมอบหมายให้ปฏิบัติต่อไปในอนาคต โดยมุ่งเน้นการพัฒนากำลังทางบกใน ๔ ด้าน คือ ๑. โครงสร้างกำลัง ๒. ความพร้อมรบ ๓. ความต่อเนื่องในการรบ ๔. ความทันสมัย เพื่อให้บรรลุเป้าหมายในการเสริมสร้างขีดความสามารถที่ ทบ. ต้องการ โดยต้องคำนึงถึงปัจจัยแวดล้อมที่เป็นทั้ง ข้อสนับสนุนและข้อจำกัดต่าง ๆ เช่น ระยะเวลา งบประมาณ กฎระเบียบและนโยบาย เป็นต้น ทั้งนี้ เป้าหมายในการพัฒนาขีดความสามารถของ ทบ. ในงานด้านข่าวกรองไซเบอร์นั้น

ควรอยู่ในกรอบการดำเนินการที่สอดคล้องกับแนวทางการพัฒนา ทบ. คือ เพื่อให้ ทบ. มีสัดส่วนกำลังที่มีความเหมาะสม สามารถปฏิบัติการทางทหารได้ตั้งแต่สภาวะความขัดแย้งระดับต่ำถึงสงคราม และบูรณาการขีดความสามารถทางบกร่วมกับหน่วยงานอื่น ๆ ได้อย่างมีประสิทธิภาพ ตอบสนองต่อเป้าหมายยุทธศาสตร์ชาติในภาพรวม และสามารถรองรับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยมีแนวความคิดในการดำเนินการดังนี้

๔.๑ ด้านโครงสร้างกำลัง (Force Structure) :

หน่วย ขว. ยังคงยึดถือโครงสร้างการจัดหน่วยในปัจจุบัน โดยปรับปรุงอัตราการจัดหน่วยในแต่ละระดับให้เหมาะสม สอดคล้องกับสภาวการณ์ที่เปลี่ยนไป เช่นปรับปรุงภารกิจของหน่วยขึ้นตรงกรมข่าวทหารบก สามารถสนับสนุนหน่วยของ ทบ. ได้ครอบคลุมตามขอบเขตภารกิจที่เพิ่มมากขึ้น และเป็นไปตามยุทธศาสตร์ชาติด้านความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐), แผนปฏิบัติการด้านการพัฒนาศักยภาพของประเทศด้านความมั่นคงระยะที่ ๒ (พ.ศ. ๒๕๖๖ - ๒๕๗๐), แผนปฏิบัติการด้านการปกป้องอธิปไตยและผลประโยชน์ของชาติในภาพรวม ระยะที่ ๒ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) และเป็นไปตามหลักเกณฑ์การพิจารณาปรับปรุงแก้ไขอัตราของ นขต.กห. และเหล่าทัพ ที่จะต้องไม่ทำให้ยอดอัตรากำลังพลแต่ละชั้นยศและงบประมาณรายจ่ายกำลังพลภาครัฐทุกประเภทเพิ่มขึ้น โดยมีแนวคิดในการจัดหน่วย เพื่อสนับสนุนงานข่าวกรองไซเบอร์ ดังนี้

๔.๑.๑ หน่วยในส่วนบัญชาการ : ทบทวนความเหมาะสมของการปฏิบัติงานของ ขว.ทบ. ตามการปรับปรุงโครงสร้างในห้วงที่ผ่านมา และดำเนินการปรับปรุงให้เหมาะสมตามสภาพความเป็นจริง โดยให้เพิ่มภารกิจด้านข่าวกรองไซเบอร์ไปในภารกิจของหน่วยด้วย

๔.๑.๒ หน่วยปฏิบัติงานข่าว :

๔.๑.๒.๑ ปรับปรุงอัตราการจัดหน่วย ขกท., พัน.ขกท. และ หน่วย ขกท.พล.ร.๑๕ ให้มีความอ่อนตัว ทันสมัย สามารถดำรงไว้ซึ่งขีดความสามารถในการปฏิบัติงานข่าวกรอง และการต่อต้านการข่าวกรองสนับสนุนหน่วยปฏิบัติทางยุทธวิธี, งานข่าวกรองความมั่นคง และการติดตามตรวจสอบข่าวสาร การรวบรวมข่าวสารด้วยวิธีพิเศษตามภารกิจที่ได้รับมอบ รวมถึงการรวบรวมข่าวสารที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ จากแหล่งข่าวทางเปิดเป็นหลัก (Open source)

๔.๑.๒.๒ ปรับปรุงอัตรากำลังพลในหน่วย ตข. สนับสนุน ทภ. และ มทบ. ให้สมบูรณ์ โดยให้สอดคล้องตามสภาวการณ์และปริมาณงานในปัจจุบัน และมุ่งเน้นเสริมสร้างขีดความสามารถงานด้าน ตข. ทางไซเบอร์ให้กับหน่วยตามลักษณะภัยคุกคามที่เกิดขึ้น

๔.๒ ด้านความพร้อมรบ (Force Readiness)

๔.๒.๑ ด้านกำลังพล :

๔.๒.๑.๑ พิจารณาความเร่งด่วนในการผลิตและบรรจุกำลังพลเหล่า ขว. ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้กับหน่วยข่าวของ ทบ. และหน่วยที่มีอัตรากำลังพลเหล่า ขว. ตามลำดับความเร่งด่วน

๔.๒.๑.๒ ดำเนินการจัดทำระบบงานด้านกำลังพลของเหล่า ขว. โดยใช้เทคโนโลยีสารสนเทศ เพื่อให้ได้ข้อมูลที่ถูกต้องรวดเร็วสำหรับการบริหารจัดการกำลังพลที่มีประสิทธิภาพ และสนับสนุนการพัฒนาขีดความสามารถด้านข่าวกรองไซเบอร์อย่างมีระบบ

๔.๒.๑.๓ พัฒนาระบบการคัดสรรกำลังพลตามความต้องการของหน่วยที่มีการปฏิบัติภารกิจรวบรวมข่าวสารทางไซเบอร์ และพิจารณากำหนดหลักเกณฑ์การจ่ายเงินค่าตอบแทนให้มีความเหมาะสม

๔.๒.๒ ด้านยุทโธปกรณ์ : พิจารณาความเหมาะสมในการจัดหายุทโธปกรณ์ด้านการข่าว ให้กับ ขกท., พัน.ขกท. และ หน่วย ขกท.พล.ร.๑๕ เพื่อให้หน่วยมีขีดความสามารถตามที่กำหนดไว้ใน อจย. ในห้วงต่อไปอย่างต่อเนื่อง และจัดหาเครื่องมือพิเศษให้กับหน่วยที่มีภารกิจรวบรวมข่าวสารทางไซเบอร์ เพื่อเสริมสร้างให้หน่วยมีขีดความสามารถที่เหมาะสมตามสภาวการณ์ในปัจจุบัน

๔.๒.๓ ด้านการฝึกอบรม :

๔.๒.๓.๑ พัฒนาหลักสูตรการเรียนการสอนของเหล่า ขว. ให้สอดคล้องกับขอบเขตภารกิจที่หน่วยปฏิบัติงานและเทคโนโลยีในปัจจุบัน และพัฒนาระบบการประเมินผลการเรียนการสอนรวมถึงระบบประกันคุณภาพการฝึกอบรมให้มีมาตรฐาน

๔.๒.๓.๒ รวบรวมบทเรียนและพัฒนาหลักสูตรการฝึกอบรมด้านการข่าว ในเรื่องพิเศษเพื่อเสริมสร้างความชำนาญเฉพาะด้านให้แก่กำลังพลเหล่า ขว. โดยมีความเชื่อมโยงเป็นสหวิทยาการ ในเรื่องที่สามารถตอบสนองต่อภัยคุกคามรูปแบบผสม ทั้งในเรื่องการก่อการร้าย/การก่อความไม่สงบ, ไซเบอร์, นิติวิทยาศาสตร์, ข้อมูลชีวภาพ และวัตถุระเบิดแสวงเครื่อง ฯลฯ

๔.๒.๔ ด้านแผนการปฏิบัติ :

๔.๒.๔.๑ จัดทำและพัฒนาแผนปฏิบัติงานด้านการข่าวกรองไซเบอร์ให้สามารถรองรับ ครอบคลุม และสอดคล้องตามกรอบของ กห. และ ทท. ในภาพรวม และแสวงประโยชน์จากความตกลงร่วมกับเหล่าทัพ และหน่วยงานอื่น ๆ ในการใช้ประโยชน์จากเทคโนโลยีและสิ่งอุปกรณ์ ของหน่วยงานนั้น ๆ

๔.๒.๔.๒ พัฒนางานต่อต้านข่าวกรองไซเบอร์ ด้วยการปรับปรุงระบบ รปภ. เครือข่ายและคอมพิวเตอร์ของหน่วยในระดับต่าง ๆ พร้อมทั้งจัดทำมาตรฐานอุปกรณ์ในการรักษาความปลอดภัยไซเบอร์

๔.๒.๔.๓ ขยายเครือข่ายงานข่าวกรองกับหน่วยงานความมั่นคงโดยใช้ประโยชน์จากประชาคมข่าวกรองในทุกระดับและหน่วยข่าวของมิตรประเทศในการบูรณาการด้านการข่าว

๔.๒.๔.๔ สนับสนุนให้ภาคประชาชนที่มีศักยภาพด้านเทคโนโลยีสารสนเทศมีส่วนร่วมในการดำเนินงานด้านการข่าวกรองไซเบอร์ โดยมี ขว.ทบ. เป็นส่วนอำนวยการหลัก

๔.๓ ด้านความต่อเนื่องในการรบ (Sustainability) :

๔.๓.๑ ปรับปรุงอาคาร สถานที่ และการจัดหา สป. ที่จำเป็นให้กับ รร.ขว.ทบ. เพื่อรองรับหลักสูตรการผลิต (นนส.ทบ. เหล่า ขว.), หลักสูตรตามแนวทางรับราชการ และหลักสูตรเสริมสร้างขีดความสามารถพิเศษของเหล่า ขว. (เช่น หลักสูตรข่าวกรองไซเบอร์)

๔.๓.๒ ดำเนินการซ่อมปรับปรุงยุทโธปกรณ์ของหน่วย ขกท., พัน.ขกท. และหน่วย ขกท.พล.ร.๑๕ รวมถึงหน่วยที่มีเครื่องมือพิเศษ โดยเฉพาะเครื่องมือที่สามารถเชื่อมต่อเข้ากับ

เครือข่ายคอมพิวเตอร์และ internet เพื่อให้หน่วยสามารถปฏิบัติงานได้อย่างต่อเนื่องและสนับสนุนการบูรณาการข้อมูลด้านการข่าว

๔.๔ ด้านความทันสมัย (Modernization) :

๔.๔.๑ พัฒนาหลักนิยม : จัดทำและพัฒนาหลักนิยมที่สอดคล้องกับสภาวการณ์ในปัจจุบัน เพื่อให้หน่วย ขว. และหน่วยอื่น ๆ มีแนวทางการปฏิบัติงานที่สามารถรองรับต่อภัยคุกคามทั้งภัยคุกคามทางทหารแบบดั้งเดิมและภัยคุกทางไซเบอร์ ดังนี้

๔.๔.๑.๑ จัดทำ/ปรับปรุงเอกสารและตำราในการฝึกอบรมของเหล่าให้มีความสมบูรณ์และทันสมัยครอบคลุมงานข่าวกรองไซเบอร์

๔.๔.๑.๒ พัฒนาระบบการฝึก ตรวจสอบ และประเมินผลของเหล่าให้มีมาตรฐาน รวมถึงระบบประกันคุณภาพการฝึกอบรมที่สามารถสะท้อนถึงความพร้อมรบของหน่วยในงานด้านข่าวกรองไซเบอร์ได้อย่างแท้จริง โดยการจัดทำคู่มือราชการสนาม, คู่มือการฝึก และระเบียบหลักสูตรการฝึกต่าง ๆ เพื่อพัฒนางานการฝึกหลักตามวงรอบประจำปี ทั้งการฝึกความชำนาญเป็นบุคคลและการฝึกเป็นหน่วยให้ครบสมบูรณ์

๔.๔.๑.๓ แสวงหาความร่วมมือด้านการข่าวกับมิตรประเทศผ่านกลไกคณะทำงานความร่วมมือด้านการทหารที่ ทบ. มีความตกลงกับมิตรประเทศ และที่ ขว.ทบ. มีความร่วมมือแบบทวิภาคีภายใต้อนุมัติหลักการของ ทบ. เพื่อพัฒนาองค์ความรู้ด้านข่าวกรองไซเบอร์ให้มีความเป็นสากลก้าวไปสู่มิติใหม่ของการปฏิบัติงานด้านการข่าวในอนาคต

๔.๔.๒ ด้านเทคโนโลยี : นำเทคโนโลยีสารสนเทศและด้านภูมิสารสนเทศมาสนับสนุนงานด้านการข่าวกรองไซเบอร์ ดังนี้

๔.๔.๒.๑ พัฒนาระบบเฝ้าตรวจชายแดน ให้มีความพร้อมรองรับภัยคุกคามในทุกรูปแบบ สามารถสนับสนุนการบริหารจัดการพื้นที่ชายแดนของ ศปก.ทภ. และ กกล. ป้องกันชายแดนได้อย่างมีประสิทธิภาพ รวมทั้งพิจารณาจัดหายุทโธปกรณ์สมัยใหม่ที่เชื่อมต่อผ่านทางเครือข่ายที่มีความปลอดภัยสูง อย่างคุ้มค่า และเกิดประโยชน์สูงสุด

๔.๔.๒.๒ พัฒนาระบบสารสนเทศด้านการข่าวของ ทบ. ด้วยการจัดทำระบบ Big Data และนำเทคโนโลยี AI มาประยุกต์ใช้ในงานการข่าว และมุ่งสู่การเป็นศูนย์กลางฐานข้อมูลด้านการข่าวของ ทบ. โดยบูรณาการระบบข้อมูล ข่าวสาร ข่าวกรอง ภายใน กห. และหน่วยงานประชาคมข่าวกรองให้สามารถตอบสนองต่อความต้องการข่าวสาร/ข่าวกรองได้ทุกภารกิจ รวมถึงเตรียมการเพื่อรองรับการเชื่อมโยงเครือข่ายและระบบงานด้านการข่าวภายใน กห. ไปสู่ระบบเครือข่ายศูนย์กลาง (Network Centric Information) โดยคำนึงถึงความมั่นคงปลอดภัยทางไซเบอร์

๔.๔.๒.๓ พัฒนางานวิจัยทางทหารของหน่วย/เหล่า ขว. ให้ได้ผลงานที่สามารถนำไปสู่เป้าหมายการพัฒนาขีดความสามารถของหน่วย/เหล่า ให้มีความพร้อมรบ ทันสมัย และส่งเสริมสนับสนุนงานวิจัยและพัฒนาทางทหารที่มุ่งเน้นผลงานด้าน ความปลอดภัยทางไซเบอร์และการข่าวกรองไซเบอร์

สรุป

ผลการศึกษาในบทที่ ๔ สรุปได้ว่า การดำเนินการข่าวกรองไซเบอร์ของ ทบ. ต้องได้รับการปรับปรุงเพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นในปัจจุบัน โดย ทบ. ต้องให้ความสำคัญด้วยการใช้กลยุทธ์เชิงรุกในการพัฒนาขีดความสามารถของหน่วยข่าวของกองทัพบกรวมทั้งขีดความสามารถด้านสารสนเทศของหน่วยขึ้นตรงกองทัพบก

การพัฒนาขีดความสามารถของ ทบ. มีความเหมือนและแตกต่างกับการพัฒนาในเรื่องเดียวกันของมิตรประเทศ โดยประเด็นที่เหมือนกัน ได้แก่ รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ ในปัจจุบัน ได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์มาประยุกต์ใช้กับหน่วยงานของตนเอง โดยมีกระบวนการการทางานหลัก คือ คือ การพิสูจน์ทราบ (Identify), การพิทักษ์ (Protect), การต้องจับ (Detect), การตอบสนอง (Respond) และการฟื้นฟู (Recovery) ที่เป็นกรอบแนวคิดในการปฏิบัติที่เป็นที่ยอมรับ และนำไปใช้อย่างแพร่หลายทั่วโลก ขณะที่งานข่าวจะเน้นในเชิงป้องกันมากกว่าเชิงรุก ด้วยการดำเนินการด้านข่าวกรองด้านภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) ที่เน้นในการศึกษาว่าภัยคุกคาม คือใคร มีเทคนิคและวิธีการโจมตีอย่างไร ได้รับการสนับสนุนจากใคร มีหนทางปฏิบัติต่อผู้ที่เป็นเป้าหมายอย่างไร สำหรับประเด็นที่ต่างกันกับต่างประเทศ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ โดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์ (Cyber Intelligence) จะเป็นหน้าที่ และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน โดยจะทำงานและบูรณาการข้อมูลกับหน่วยที่ปฏิบัติการด้านไซเบอร์ หรือหน่วยงานด้านยุทธการอย่างใกล้ชิด เนื่องจากงานข่าวกรองเป็นงานที่ใช้ความรู้และความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องใช้ประสบการณ์จากการปฏิบัติงานมาเป็นระยะเวลาหนึ่ง จึงจะสามารถวิเคราะห์สถานการณ์ที่อาจจะเกิดขึ้นในอนาคตได้ ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด ไม่ว่าจะเป็นขั้นตอนการระบุภัยคุกคามการป้องกันและการแจ้งเตือน ไม่ได้มีการแบ่งหน้าที่งานด้านการข่าว ในพื้นที่ปฏิบัติการไซเบอร์ให้กับหน่วยงานด้านการข่าวของหน่วย นอกจากนี้ การบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่มีหลักการปฏิบัติ และการดำเนินการที่ชัดเจนเหมือนกับของต่างประเทศ

ในการพัฒนาต้นแบบ หรือขีดความสามารถด้านการข่าวกรองไซเบอร์ต้องสอดคล้องกับแนวทางการพัฒนา ทบ. ตามแผนที่กำหนด เพื่อให้สอดคล้องกับแนวทางการใช้กำลังและภารกิจของ ทบ. ในอนาคต โดยต้องมีการดำเนินการใน ๔ ด้าน คือ โครงสร้างกำลัง ความพร้อมรบ ความต่อเนื่องในการรบ และความทันสมัย เพื่อให้บรรลุเป้าหมายในการเสริมสร้างขีดความสามารถที่ ทบ. ต้องการ โดยต้องคำนึงถึงปัจจัยแวดล้อมที่เป็นทั้งข้อสนับสนุนและข้อจำกัด เช่น ระยะเวลา งบประมาณ กฎระเบียบและนโยบาย เป็นต้น

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การศึกษาวิจัยในครั้งนี้ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ ๓ ข้อ ประกอบด้วย ๑. เพื่อศึกษาสภาวะแวดล้อมแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้านไซเบอร์ (Cyber Security) และภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง ๒. เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ในปัจจุบัน และ ๓. เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ทั้งนี้ ผลการศึกษาวิจัยที่สามารถตอบวัตถุประสงค์การวิจัย ๓ ข้อดังกล่าว สรุปได้ดังนี้

จากกรณีที่สถานการณ์ของโลกปัจจุบันอยู่ในยุคแห่งการเปลี่ยนแปลงที่รวดเร็ว และไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยี ทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง บุคคล หรือกลุ่มบุคคลที่ไม่ใช่รัฐ (Non - State Actor) จะเป็นผู้มีบทบาทมีอิทธิพลมากขึ้นในการดำเนินกิจกรรม ที่ส่งผลกระทบต่อความมั่นคง การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ ในห้วงปัจจุบันพบว่าประเด็นความมั่นคงที่จะส่งผลกระทบต่อไทย ได้แก่ การเมืองระหว่างประเทศ, การขยายอิทธิพลและบทบาทของประเทศมหาอำนาจต่อภูมิภาคเอเชียตะวันออกเฉียงใต้, การขยายตัวของความสัมพันธ์ระหว่างประเทศในระดับภูมิภาค, ความขัดแย้งทางดินแดนและการใช้กำลังทางการทหาร, สถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้, การเคลื่อนตัวของภัยคุกคามข้ามชาติ, การย้ายถิ่นฐานของประชากร, ความมั่นคงหลัง COVID - 19 และภัยคุกคามทางไซเบอร์ ปัจจุบันสถานการณ์ความมั่นคงทางไซเบอร์ในต่างประเทศ มีแนวโน้มขยายผลกระทบไปในทุกสาขา อาทิ กลุ่มพลังงาน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการเงิน กลุ่มสาธารณสุข ข้อมูลส่วนบุคคล และด้านการทหาร เป็นต้น ขณะที่ในประเทศไทย ก็เผชิญภัยคุกคามทางไซเบอร์ อาทิ การเจาะระบบเว็ปไซต์ขององค์กรภาครัฐ การจารกรรมข้อมูล และการโจมตีระบบปฏิบัติการขององค์กรต่าง ๆ รูปแบบภัยคุกคามทางไซเบอร์มีหลากหลาย แต่ที่พบบ่อย ได้แก่ Malware Hacker Ransomware Ddos Phishing

และ Spyware เป็นต้น ซึ่งความเสียหายเป็นสิ่งที่ประเมินค่ามิได้ และมีโอกาสที่ความเสียหายจะเพิ่มขึ้นในอนาคต หากไม่มีแนวทางป้องกันผลกระทบจากภัยคุกคามทางไซเบอร์อย่างเหมาะสม กรมข่าวทหารบกเป็นหน่วยงานด้านข่าวกรองหลัก ของกองทัพบกจึงต้องมีความพร้อมที่จะรับมือกับภัยคุกคามทุกรูปแบบให้ได้อย่างมีประสิทธิภาพ และนำเทคโนโลยี AI มาใช้ให้เกิดประโยชน์ ซึ่งจะเป็นปัจจัยส่งเสริมให้การปฏิบัติการด้านการข่าวเป็นไปอย่างรวดเร็วถูกต้อง และทันเวลา และมีประสิทธิภาพมากขึ้น

กองทัพบกมีการนำเทคโนโลยีสารสนเทศมาใช้งานในหลายมิติ อาทิ การติดต่อสื่อสาร การฝึกอบรม การปฏิบัติงานในสำนักงาน การรวบรวบข้อมูลข่าวสาร/การวิเคราะห์ข้อมูล/การกระจายข้อมูลข่าวสาร การจัดทำระบบฐานข้อมูล การควบคุมระบบปฏิบัติการของอาวุธยุทโธปกรณ์ และการอำนวยการ/ควบคุมบังคับบัญชา ในห้องปฏิบัติการ ฯลฯ เป็นต้น ในส่วนของ ปัญหา/ความท้าทายในการใช้เทคโนโลยีของกองทัพบกนั้น กองทัพบกมีการใช้ระบบเทคโนโลยีสารสนเทศในการปฏิบัติงานโดยอาจแบ่งประเภทของการนำมาใช้งานใน ๒ แบบ คือ เป็นระบบที่หน่วยดำเนินการพัฒนาขึ้นมาด้วยตนเอง และ ระบบที่ได้จากการจ้างผู้ประกอบการภายนอกเข้ามาดำเนินการให้ซึ่งส่งผลต่อการรักษาความปลอดภัยทางไซเบอร์ที่แตกต่างกัน ทั้งนี้จากข้อมูลผลการปฏิบัติงานด้านการข่าวของกองทัพบกที่ผ่านมา มีประเด็นปัญหาของการใช้เทคโนโลยี เพื่อสนับสนุนการปฏิบัติงานที่สำคัญสรุปได้แก่ ความปลอดภัย, ความท้าทายในเรื่องของ Generation Gap หรือความต่างของอายุและช่วงวัย เนื่องจากเทคโนโลยีนั้นมีการพัฒนา และปรับเปลี่ยนอยู่ตลอดเวลา คนรุ่นเก่าจะเรียนรู้วิธีการใช้เทคโนโลยีได้ยากกว่าคนรุ่นใหม่, ความท้าทายเรื่องความถูกต้องและแม่นยำของเทคโนโลยี, ปัญหาด้านความรู้ความสามารถด้านเทคโนโลยีของกำลังพล, ปัญหาด้านงบประมาณ และปัญหาด้านโครงสร้างหน่วยงานที่ไม่เอื้อต่อการทำงานข่าวที่ต้องการความรวดเร็ว

กองทัพบกมีการก่อตั้ง “ศูนย์ไซเบอร์กองทัพบก” เมื่อ ๑ ก.ค. ๕๗ เพื่อรับผิดชอบงานด้านความมั่นคงทางไซเบอร์ ซึ่งมีการวางระบบการจัดการทรัพยากรทางไซเบอร์และเสริมสร้างขีดความสามารถของกำลังพลมาอย่างต่อเนื่อง ศูนย์ไซเบอร์กองทัพบก มิใช่หน่วยขึ้นตรงกับกรมข่าวทหารบก ดังนั้น การดำเนินงานจึงเกี่ยวข้องกับการข่าวกรองไซเบอร์เชิงรับเป็นส่วนใหญ่ โดยใช้ระเบียบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ทบ. ฉบับปี พ.ศ. ๒๕๖๐ เป็นมาตรการควบคุมการปฏิบัติ และได้กำหนดแนวทางการพัฒนาไว้ในแผนแม่บทไซเบอร์กองทัพบก พ.ศ. ๒๕๖๖ - ๒๕๗๐

การประเมินสถานการณ์ด้านไซเบอร์เพื่อความมั่นคงของไทยนั้นประกอบด้วยสถานการณ์ภัยคุกคามทางไซเบอร์ภายนอกประเทศ และสถานการณ์ภัยคุกคามทางไซเบอร์ภายในประเทศ ซึ่งปัจจุบันปัญหาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศที่สำคัญ ๆ ได้แก่ ๑. ปัญหาในการจัดทำแผนงานหรือมาตรการป้องกันภัยคุกคามด้านไซเบอร์ ๒. ปัญหาอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) และ ๓. ปัญหาความพร้อมของบุคลากรด้านไซเบอร์

สำหรับรูปแบบและลักษณะของการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศนั้น ทำการศึกษาใน ๔ ประเทศ สรุปได้ว่า

๑. สหรัฐอเมริกามองว่า โลกในปัจจุบันถูกเชื่อมโยงเป็นเครือข่ายและล่อแหลมต่อการถูกโจมตีผ่านทางเครือข่าย ด้วยเหตุนี้ ยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกาจะต้องรับประกันในเรื่อง การรักษาความลับ (confidentiality) ความพร้อมใช้งาน (availability) และความสมบูรณ์ของข้อมูล (integrity of data)

๒. สหราชอาณาจักรจะจัดการกับอาชญากรรมด้านไซเบอร์และจะดำเนินการทุกวิถีทางเพื่อให้สหราชอาณาจักรเป็นประเทศที่มีความปลอดภัยมากที่สุดประเทศหนึ่งในโลกสำหรับการทำธุรกิจในพื้นที่ไซเบอร์

๓. จีนเชื่อว่า กฎหมายระหว่างประเทศที่มีอยู่จะต้องได้รับการแก้ไขให้ความชัดเจน หรือสร้างหลักเกณฑ์ขึ้นมาใหม่ให้สอดคล้องกับพื้นที่ไซเบอร์ในปัจจุบัน โดยเฉพาะในเรื่องสิ่งบ่งชี้ของการโจมตีด้านไซเบอร์ที่เป็นการก่ออาชญากรรมด้านไซเบอร์ และการกำหนดว่าความเสียหายที่เกิดขึ้นจากการป้องกันตนเองอย่างไร จึงจะถือว่า เป็นการป้องกันตนเองอย่างเหมาะสม และถูกต้องตามกฎหมายระหว่างประเทศ

๔. กองทัพสิงคโปร์จัดตั้งกองทัพดิจิตอลและการข่าว (Digital and Intelligence Service : DIS) ซึ่งกำหนดให้มีสถานะเป็นเหล่าทัพที่ ๔ ของกองทัพสิงคโปร์ นอกเหนือจากเหล่า ทบ., ทร. และ ทอ. เพื่อดูแลความมั่นคงด้านดิจิทัล และการเตรียมการรับมือกับภัยคุกคามทางดิจิทัล โดยเชื่อมโยงกับเหล่าทัพอื่น ด้วยการบูรณาการผ่านระบบ (Command, Control, Communication, Computer and Intelligence : C4I) ปฏิบัติการในรูปแบบเครือข่าย รวมทั้งดำเนินการ ด้านดิจิทัลเชิงรุกให้กองทัพ และการป้องกันทางไซเบอร์

และประการสุดท้าย Global Cybersecurity Index เป็นดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมสากล หรือ International Telecommunication Union (ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลก และหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร (The ultimate goal of this initiative is to help foster a global culture of cybersecurity and its integration at the core of ICTs) การศึกษาฉบับนี้สามารถนำแนวคิด Global Cybersecurity Index ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของแต่ละประเทศ มาเป็นเครื่องมือในการวิเคราะห์ปัญหาและข้อเสนอแนะได้

การดำเนินการข่าวกรองไซเบอร์ของ ทบ. ต้องได้รับการปรับปรุง เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นในปัจจุบัน โดย ทบ. ต้องให้ความสำคัญด้วยการใช้กลยุทธ์เชิงรุกในการพัฒนาขีดความสามารถของหน่วยข่าวของกองทัพบกรวมทั้งขีดความสามารถด้านสารสนเทศของหน่วยขึ้นตรงกองทัพบก

การพัฒนาขีดความสามารถของ ทบ. มีความเหมือนและต่างต่างกับการพัฒนาในเรื่องเดียวกันของมิตรประเทศ โดยประเด็นที่เหมือนกัน เช่น รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ

ในปัจจุบัน ได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์ มาประยุกต์ใช้กับหน่วยงานของตนเองโดยมีกระบวนการการทางานหลัก คือ การพิสูจน์ทราบ (Identify), การพิทักษ์ (Protect), การต้องจับ (Detect), การตอบสนอง (Respond) และการฟื้นฟู (Recovery) ที่เป็นกรอบแนวคิดในการปฏิบัติที่เป็นที่ยอมรับและนำไปใช้อย่างแพร่หลายทั่วโลก ขณะที่งานข่าวจะเน้นในเชิงป้องกันมากกว่าเชิงรุก ด้วยการดำเนินการด้านข่าวกรองด้านภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) ที่เน้นในการศึกษาว่าภัยคุกคามคือใคร มีเทคนิคและวิธีการโจมตีอย่างไรได้รับการสนับสนุนจากใคร มีหนทางปฏิบัติต่อผู้ที่เป็นเป้าหมายอย่างไร สำหรับประเด็นที่ต่างกันกับต่างประเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศโดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์ (Cyber Intelligence) จะเป็นหน้าที่และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน โดยจะทำงาน และบูรณาการข้อมูลกับหน่วยที่ปฏิบัติการด้านไซเบอร์ หรือหน่วยงานด้านยุทธการอย่างใกล้ชิดเนื่องจากงานข่าวกรองเป็นงานที่ใช้ความรู้ และความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องใช้ประสบการณ์จากการปฏิบัติงานมาเป็นระยะเวลาหนึ่ง จึงจะสามารถวิเคราะห์สถานการณ์ที่อาจจะเกิดขึ้นในอนาคตได้ ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด ไม่ว่าจะเป็นขั้นตอนการระบุภัยคุกคามการปูองกันและการแจ้งเตือน ไม่ได้มีการแบ่งหน้าที่งานด้านการข่าวในพื้นที่ปฏิบัติการไซเบอร์ให้กับหน่วยงานด้านการข่าวของหน่วยนอกจากนี้ การบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่มีหลักการปฏิบัติ และการดำเนินการที่ชัดเจนเหมือนกับของต่างประเทศ

ในการพัฒนาต้นแบบ หรือขีดความสามารถด้านการข่าวกรองไซเบอร์ต้องสอดคล้องกับแนวทางการพัฒนา ทบ. ตามแผนที่กำหนดเพื่อให้สอดคล้องกับแนวทางการใช้กำลังและภารกิจของ ทบ. ในอนาคต โดยต้องมีการดำเนินการใน ๔ ด้าน คือ โครงสร้างกำลัง ความพร้อมรบ ความต่อเนื่องในการรบ และความทันสมัย เพื่อให้บรรลุเป้าหมายในการเสริมสร้างขีดความสามารถที่ ทบ. ต้องการ โดยต้องคำนึงถึงปัจจัยแวดล้อมที่เป็นทั้งข้อสนับสนุนและข้อจำกัด เช่น ระยะเวลา งบประมาณ กฎระเบียบและนโยบาย เป็นต้น

ข้อเสนอแนะ

๑. ข้อเสนอแนะเชิงนโยบาย

เนื่องจากปัจจุบันการข่าวกรองทางไซเบอร์มีความสำคัญกับการดำเนินงานข่าวกรองของกองทัพบกเป็นอย่างมาก ในแง่นโยบายควรเน้นดำเนินการในด้านต่างๆ ได้แก่ การยกระดับความสามารถของกำลังพล การสร้างความร่วมมือระหว่างหน่วยทหารและความร่วมมือกับองค์กรภายนอก การวางระบบโครงสร้างพื้นฐานที่มีความปลอดภัย การสร้างกฎ ระเบียบ มาตรฐานการรักษา

ความมั่นคงปลอดภัย การสร้างความเชื่อมั่น และการมุ่งมั่นพัฒนาศักยภาพของหน่วยงานให้มีความพร้อมต่อการปฏิบัติภารกิจ

๒. ข้อเสนอแนะเชิงปฏิบัติ

การพัฒนาขีดความสามารถด้านข่าวกรองไซเบอร์ของ ทบ. นั้น นอกจากเป็นการเสริมสร้างขีดความสามารถตามภารกิจของ ทบ. แล้ว มีข้อเสนอแนะเพิ่มเติมว่า ต้องสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ที่ให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. สำรวจ เก็บรวบรวมข้อมูล วิเคราะห์ และวิจัย เพื่อจัดทำตัวชี้วัด ดัชนีสนับสนุนการพัฒนารัฐบาลดิจิทัลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัล ซึ่งสอดคล้องกับโครงการสำรวจระดับความพร้อมการพัฒนารัฐบาลดิจิทัลหน่วยงานภาครัฐ จึงมีข้อเสนอแนะดังนี้

๒.๑ ข้อเสนอแนะแนวนโยบายและหลักปฏิบัติ (Policies and Practices)

๒.๑.๑ การปรับเปลี่ยนกระบวนการทำงานของหน่วยเป็นดิจิทัลโดยสมบูรณ์

๒.๑.๒ สร้างความเชื่อมั่นต่อระบบการให้บริการภาครัฐว่าปลอดภัยจากภัยคุกคามทางไซเบอร์

๒.๑.๓ จัดทำข้อมูลตามหลักธรรมาภิบาลข้อมูล พร้อมส่งเสริมการเชื่อมโยงแลกเปลี่ยนข้อมูล เปิดเผยข้อมูล และการนำข้อมูลไปใช้ในการวิเคราะห์เชิงนโยบาย

๒.๑.๔ พร้อมเปิดเผยข้อมูลที่ไม่มีชั้นความลับแก่สาธารณะเมื่อมีการร้องขอ

๒.๑.๕ ทบทวน ปรับปรุง และพัฒนากฎหมาย กฎระเบียบ มาตรการที่เอื้อต่อการพัฒนารัฐบาลดิจิทัล

๒.๑.๖ ส่งเสริมศักยภาพและวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่กำลังพล

๒.๑.๗ ส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนในการพัฒนารัฐบาลดิจิทัล

๒.๒ ข้อเสนอแนะด้านการบริหารจัดการข้อมูล : หน่วยขึ้นตรง ทบ. ควรดำเนินการเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐ โดยการดำเนินการดังกล่าวจะต้องเป็นการดำเนินการในด้านเดียวกัน คือ ด้านการแลกเปลี่ยนข้อมูล ด้านการเปิดเผยข้อมูลเปิดภาครัฐ และด้านการวิเคราะห์และใช้ประโยชน์ข้อมูล เช่น

๒.๒.๑ มีการกำหนด สิทธิ หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน

๒.๒.๒ กำหนดสิทธิ หน้าที่ ความรับผิดชอบ ของผู้ครอบครองข้อมูล และผู้ควบคุมข้อมูลตามวงจรชีวิตข้อมูล (create, collect, classify, process/use, store, publish/disclose, inspect, terminate)

๒.๒.๓ มีระบบบริหาร และกระบวนการจัดการ และคุ้มครองข้อมูลตามวงจรชีวิตข้อมูล (create, collect, classify, process/use, store, publish/disclose, inspect, terminate)

๒.๒.๔ มีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล

๒.๒.๕ มีการกำหนดมาตรการ หรือ กระบวนการตรวจสอบ ประเมินคุณภาพข้อมูลได้แก่ ถูกต้อง ครบถ้วน สอดคล้องกัน เป็นปัจจุบัน ตรงความต้องการผู้ใช้ และพร้อมใช้

๒.๒.๖ มีการจัดทำบัญชีรายชื่อข้อมูล (Data Catalog) คำอธิบายข้อมูล (Metadata) และพจนานุกรมข้อมูล (Data Dictionary)

๒.๓ ข้อเสนอแนะด้านการใช้ประโยชน์จากข้อมูลเพื่อสนับสนุนภารกิจโดยเฉพาะงานด้านการข่าวกรองไซเบอร์

๒.๓.๑ การวิเคราะห์ข้อมูลเพื่อใช้ในการอธิบายปัญหาและปรากฏการณ์ (Descriptive Analytic)

๒.๓.๒ การวิเคราะห์ข้อมูลเพื่อใช้ในการอธิบายถึงสาเหตุของสิ่งที่เกิดขึ้น ปัจจัยและความสัมพันธ์ต่าง ๆ (Diagnostic Analytic)

๒.๓.๓ การวิเคราะห์ข้อมูลเพื่อใช้ในการคาดการณ์หรือทำนายสิ่งที่จะเกิดขึ้น (Predictive Analytic)

๒.๓.๔ การวิเคราะห์ข้อมูลเพื่อใช้ในการวิเคราะห์ วางแผนรับมือกับสิ่งที่จะเกิดขึ้นในอนาคต (Prescriptive Analytic)

๓. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

สำหรับการวิจัยในโอกาสต่อไปนั้นสามารถนำข้อมูลที่รวบรวมไว้ในครั้งนี้เป็นข้อมูลพื้นฐานในการดำเนินการศึกษาวิจัยที่เกี่ยวข้องกับงานด้านการทหารอื่นๆได้ เช่น การใช้ BIG DATA และ AI ในการเสริมสร้างขีดความสามารถงานข่าวกรองไซเบอร์ของ ทบ. ในเรื่อง การวางแผนรวบรวมข่าวสาร การรวบรวมข่าวสาร การวิเคราะห์ข่าวกรองไซเบอร์ การใช้และการกระจายข่าวกรองไซเบอร์ การบูรณาการข่าวกรองไซเบอร์ และการประเมินประสิทธิภาพการดำเนินการข่าวกรองไซเบอร์ของหน่วยต่อไป

บรรณานุกรม

ภาษาไทย

หนังสือ

เอกสารศึกษาเฉพาะกรณี เรื่อง แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ , ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, ๒๕๖๐

การจัดการความรู้ (Knowledge Management : KM) เรื่องการจัดทำประมาณการข่าวกรองทางไซเบอร์ระดับยุทธศาสตร์ ระยะสั้น (ฉบับปรับปรุง) โดย กองข่าวกรองเทคนิคและเทคโนโลยีข่าวกรอง สำนักข่าวกรองกรมข่าวทหาร , มิถุนายน พ.ศ.๒๕๖๕

เอกสารไม่ตีพิมพ์

แผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย พุทธศักราช ๒๕๖๒ – ๒๕๖๔

ยุทธศาสตร์ข่าวกรองแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔, สำนักงานสภาความมั่นคงแห่งชาติ (สมช.)

กองทัพไทย. ๒๕๕๘. ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.๒๕๕๘

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

เอกสารวิจัยเรื่อง การพัฒนาการปฏิบัติงานในยุคไทยแลนด์ ๔.๐ กรณีศึกษา : สถาบันการข่าวกรองสำนักข่าวกรองแห่งชาติ โดย สิริกร ชิงดวง , ๒๕๖๒

เอกสารวิจัยเรื่อง Strategic cyber intelligence โดย Randy Borum, John Felker, Sean Kern, Kristen Dennesen, Tonya Feyes Date: ปี ๒๕๕๘

ภาษาต่างประเทศ

Developing maturity modeR. A. Martin, "Making security measurable and manageable", Proc. IEEE Mil. Commun. Conf. (MILCOM), pp. 1-9, 2008.

R. McMillan, Definition: Threat Intelligence, Oct. 2013, [online] Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence.

D. Chismon and M. Ruks, "Threat intelligence: Collecting analysing evaluating", 2015.

W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks", Comput. Security, vol. 72, pp. 212-233, Jan. 2018.

L. Dandurand et al., "Standards and tools for exchange and processing of actionable information", 2014.

J. Steinberger, A. Sperotto, M. Golling and H. Baier, "How to exchange security events? overview and evaluation of formats and protocols", Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM), pp. 261-269, 2015.

F. Menges and G. Pernul, "A comparative analysis of incident reporting formats", Comput. Security, vol. 73, pp. 87-101, Mar. 2018.

C. Wagner, A. Dulaunoy, G. Wagener and A. Iklody, "MISP: The design and implementation of a collaborative threat intelligence sharing platform", Proc. ACM Workshop Inf. Sharing Collab. Security (WISCS), pp. 49-56, 2016.

F. Menges, B. Putz and G. Pernul, "DEALER: Decentralized incentives for threat intelligence reporting and exchange", Int. J. Inf. Security, vol. 20, no. 5, pp. 741-761, 2021.

F. Skopik, G. Settanni and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing", Comput. Security, vol. 60, pp. 154-176, Jul. 2016.

V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies sharing standards and ontologies within cyber threat intelligence", Proc. Eur. Intell. Security Informat. Conf. (EISIC), pp. 91-98, 2017.

C. Sillaber, C. Sauerwein, A. Mussmann and R. Breu, "Data quality challenges and future research directions in threat intelligence sharing practice", Proc. ACM Workshop Inf. Sharing Collab. Security, pp. 65-70, 2016.

D. Schlette, F. Böhm, M. Caselli and G. Pernul, "Measuring and visualizing cyber threat intelligence quality", Int. J. Inf. Security, vol. 20, pp. 21-38, Mar. 2020.

V. G. Li et al., "Reading the tea leaves: A comparative analysis of threat intelligence", Proc. 28th USENIX Security Symp. (USENIX Security), pp. 851-867, 2019.

Berndt and J. Ophoff, "Exploring the value of a cyber threat intelligence function in an organization", Proc. IFIP World Conf. Inf. Security Educ., pp. 96-109, 2020.

D. Preuveneers, W. Joosen, J. B. Bernabe and A. Skarmeta, "Distributed security framework for reliable threat intelligence sharing", Security Commun. Netw., vol. 2020, Aug. 2020.

J. D. Howard and T. A. Longstaff, "A common language for computer security incidents", 1998.

N. H. Ab Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud", Comput. Security, vol. 49, pp. 45-69, Mar. 2015.

Islam, M. A. Babar and S. Nepal, "A multi-vocal review of security orchestration", ACM Comput. Surveys, vol. 52, no. 2, pp. 1-45, 2019.

P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide, Gaithersburg, MD, USA:NIST Spec. Publ, vol. 800, pp. 1-147, 2012.

ประวัติย่อผู้วิจัย

ชื่อ : พลตรี ประเสริฐ หมวดเชียงคะ

วัน เดือน ปีเกิด : ๒ ก.พ. ๑๐

การศึกษา : มัธยมศึกษาปีที่ ๖ รร.อู่ทอง จ.สุพรรณบุรี

: นตท. ๒๖

: จปร. ๓๗

: ปริญญาตรีวิทยาศาสตร์บัณฑิต โรงเรียนนายร้อยพระจุลจอมเกล้า

: ชั้นนายร้อยทหารม้า รุ่นที่ ๓/๓๓

: ชั้นนายพันทหารม้า รุ่นที่ ๒/๓๘

: รร.สธ.ทบ. ชุดที่ ๗๗

: ปริญญาโท รัฐประศาสนศาสตร์ มหาวิทยาลัยรังสิต

: Training Development Course, Australia

: Combined Defence Intelligence Research and Analysis Course, Australia

: Peace Keeping Operation, England

: Command and Staff Officers International Law, Australia

ประวัติการทำงานโดยย่อ

: ผบ.มว.ม.ร้อย ม.ลว.ม.พัน.๒๘

: ผบ.ร้อย ม.ลว.ม.พัน.๒๘

: หน.ฝยก.ขกท.

: หน.แผนกฝึกและศึกษา กผฝ.ขว.ทบ.

: หน.แผนกต่อต้านการก่อการร้าย ฝขว.ศปก.ทบ.

: หน.กองแผนการศึกษาและวิจัย รร.ขว.ทบ.

: ผชท.ทหารบกไทย/อิสลามาบัด, ปากีสถาน, รรก.ผชท.ทหารไทย(ทบ.)/อังการา, ตุรเกีย

: หน.สน.สปข.สปก.ขว.ทบ./หน.สน.๓๒๒

: ผอ.กทบ.สวส.ขว.ทบ.

: รอง ผอ.สวส.ขว.ทบ.

ตำแหน่งปัจจุบัน : รอง ผบ.รร.ขว.ทบ.

สรุปย่อ

ลักษณะวิชา การทหาร

เรื่อง ภัยคุกคามทางไซเบอร์ (Cyber threats intelligence) กับความท้าทายงานการข่าวกรองในศตวรรษที่ ๒๑ : แนวทางการจัดทำนโยบายด้านการพัฒนาการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก

ผู้วิจัย พลตรี ประเสริฐ หมวดเชียงคะ **หลักสูตร** วปอ. **รุ่นที่** ๖๕

ตำแหน่ง รองผู้บัญชาการโรงเรียนข่าวทหารบก

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันโลกอยู่ในยุคแห่งการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วและไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยี ทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง บุคคล หรือกลุ่มบุคคลที่ไม่ใช่รัฐ (Non - State Actor) จะเป็นผู้มีบทบาทมีอิทธิพลมากขึ้น ในการดำเนินกิจกรรมที่ส่งผลกระทบต่อความมั่นคง นอกจากนี้ ระบบความสัมพันธ์ระหว่างประเทศได้เปลี่ยนแปลงไปสู่ความสัมพันธ์ แบบหลายขั้วอำนาจ (Multi - Polar) มีการคานอำนาจ หรือความพยายามในการลดบทบาทนำของประเทศมหาอำนาจมิให้เป็นผู้นำที่ครองความเป็นประเทศมหาอำนาจเพียงผู้เดียว (Hegemon) การเปลี่ยนแปลงดังกล่าวส่งผลให้แต่ละประเทศต่างมุ่งปกป้อง และรักษาผลประโยชน์ของตนเองเป็นสำคัญ และมักรวมกลุ่มพันธมิตรลักษณะเฉพาะกิจขนาดต่าง ๆ เพื่อพิทักษ์ผลประโยชน์ร่วมกัน

พัฒนาการของระบบคอมพิวเตอร์ และการเปลี่ยนแปลงทางด้านเทคโนโลยีที่รวดเร็วในปัจจุบันได้ส่งผลกระทบต่อกิจการ และการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์ และเทคโนโลยีในหลายทศวรรษที่ผ่านมา ทำให้ยุคสมัยปัจจุบันเกิดการปฏิวัติสารสนเทศ (information revolution) ซึ่งเกี่ยวข้องกับการประมวลผล และกระจายสารสนเทศอย่างกว้างขวาง จนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดด และก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “พื้นที่ไซเบอร์” (cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (national security) จึงได้รับผลกระทบ

จากการปฏิวัติสารสนเทศ และปรากฏการณ์ของพื้นที่ไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “การรักษาความมั่นคงปลอดภัยด้านไซเบอร์” (cyber security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้ง ยังมีผู้กล่าวถึงคุณลักษณะของพื้นที่ไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน ภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (defense) การยับยั้ง (deterrence) และการโจมตี (attack) ในพื้นที่ไซเบอร์มากขึ้น

กองทัพบกกำหนดความรับผิดชอบในการดำเนินงานข่าวกรอง โดยใช้ประเภทของข่าวกรองเป็นหลัก ๓ ประการ คือ งานข่าวกรองทางยุทธศาสตร์ งานข่าวกรองทางยุทธวิธี และงานข่าวกรองเพื่อความมั่นคง โดยขอบเขตความรับผิดชอบงานข่าวกรองเพื่อความมั่นคง เป็นการดำเนินการข่าวกรอง เพื่อสนับสนุนภารกิจของกองทัพบกในการรักษาความมั่นคงของรัฐ การรักษาผลประโยชน์ของชาติ และการพัฒนาประเทศ ตามขอบเขตของภารกิจที่ได้รับมอบ นอกเหนือจากการดำเนินงานข่าวกรองทางยุทธศาสตร์ ข่าวกรองทางยุทธวิธี และข่าวกรองเพื่อความมั่นคง ที่เป็นประเภทหลักของข่าวกรองในการดำเนินการข่าวกรองแล้ว ยังมีการแบ่งประเภทข่าวกรองตามลักษณะของการปฏิบัติงานความมุ่งหมายและเครื่องมือข่าวกรอง อีก ๗ ประเภท คือ ข่าวกรองทางบุคคล (Human Intelligence : HUMINT), ข่าวกรองทางสัญญาณ (Signal Intelligence : SIGINT), ข่าวกรองทางการภาพ (Imagery Intelligence : IMINT), ข่าวกรองภูมิสารสนเทศ (Geospatial Intelligence : GEOINT), ข่าวกรองเครื่องมือวัดและสัญญาณแสดง (Measurement and Signature Intelligence : MASINT), ข่าวกรองทางเทคนิค (Technical Intelligence : TECHINT) และ ข่าวกรองจากแหล่งข่าวเปิด (Open Source Intelligence : OSINT) เป็นการดำเนินงานข่าวกรองในรูปแบบใหม่ ซึ่งเป็นผลมาจากความก้าวหน้าทางเทคโนโลยีสารสนเทศ และเริ่มมีบทบาทมากขึ้นกับการข่าวกรองของกองทัพบก

เนื่องจากการรวบรวมข่าวสารทั้งปกปิดและเปิดเผย การวิเคราะห์ และการประเมินค่าข่าวสารดังกล่าว เพื่อผลิตเป็นข่าวกรอง คือ สิ่งที่สำคัญยิ่งต่อการประเมินความล่อแหลม และการรับประกันต่อความอยู่รอดของระบบทางการทหาร โดยระเบียบปฏิบัติของการรวบรวมข่าวกรองตามปกติมิได้กล่าวถึงการผสมกลมกลืนระหว่างเทคโนโลยีกับขีดความสามารถในพื้นที่ไซเบอร์เอาไว้ ภัยคุกคามทางไซเบอร์จึงเป็นสิ่งที่ท้าทายต่อการวิเคราะห์ความล่อแหลม และผลกระทบต่อความมั่นคง จึงเป็นประเด็นที่น่าสนใจว่าการดำเนินการข่าวกรองไซเบอร์ (Cyber Intelligence : CYBINT) ของหน่วยข่าวกรองกองทัพบกจะมีรูปแบบ หรือพัฒนาการอย่างเป็นระบบได้อย่างไร

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาสภาวะแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้านไซเบอร์ (Cyber Security) และ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง

๒. เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรค ในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก ในปัจจุบัน

๓. เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก

ขอบเขตของการวิจัย

๑. ศึกษาข้อมูลเฉพาะโดยเน้นในเรื่อง ข่าวกรองไซเบอร์ (Cyber intelligence)

๒. เอกสารในการศึกษาวรรณกรรมบางส่วนเป็นเอกสารที่มีชั้นความลับของทางราชการ

๓. การสัมภาษณ์ผู้ทรงคุณวุฒิที่มีความรู้ ประสบการณ์เกี่ยวกับงานด้านความมั่นคง การข่าวกรองและการต่อต้านการข่าวกรอง และงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

วิธีดำเนินการวิจัย

การศึกษาวิจัยฉบับนี้ ดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) ร่วมกับใช้การวิจัยเชิงพรรณนา (Descriptive Research) ดังนี้

๑. การรวบรวมข้อมูล

๑.๑ ข้อมูลปฐมภูมิ ดำเนินการโดยการรวบรวมจากผลการปฏิบัติราชการ ข้อมูลผลการประชุม และการสัมมนาทางวิชาการของหน่วยงาน รวมทั้งการสอบถามผู้เชี่ยวชาญและผู้ทรงคุณวุฒิในประเด็นที่กำหนด เช่น ความมั่นคงปลอดภัยทางไซเบอร์ การพัฒนารัฐบาลดิจิทัล การข่าวกรองไซเบอร์ เป็นต้น

๑.๒ ข้อมูลทุติยภูมิ ดำเนินการโดยการศึกษาจากตำราและเอกสารต่าง ๆ การรวบรวมจากแหล่งข้อมูลที่ได้รับการยอมรับและน่าเชื่อถือ ทั้งหนังสือพิมพ์ บทความ เอกสารวิชาการ เอกสารราชการ นอกจากแหล่งทุติยภูมิ จากแหล่งภาษาไทยแล้ว ยังได้รวบรวมข้อมูลจากแหล่งข้อมูลต่างประเทศด้วย

๒. การวิเคราะห์ข้อมูล : ดำเนินการโดยใช้การวิเคราะห์เนื้อหา (Context Analysis) และการวิเคราะห์ เปรียบเทียบ และสังเคราะห์ข้อมูลทฤษฎี หลักการต่าง ๆ ด้านการข่าวกรอง และความมั่นคง

๓. การนำเสนอข้อมูล : นำเสนอข้อมูลแบบรายงานวิจัยเชิงพรรณนา และวิเคราะห์นำเสนอแนวคิดใหม่ ๆ จากการวิจัย

ผลการวิจัย

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ ๑ เพื่อศึกษาสภาวะแวดล้อมด้านความมั่นคง โดยเฉพาะความมั่นคงด้านไซเบอร์ (Cyber Security) และ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่ส่งผลกระทบต่อความมั่นคง มีรายละเอียดผลการศึกษา โดยสรุปดังนี้

จากกรณีที่สถานการณ์ของโลกปัจจุบันอยู่ในยุคแห่งการเปลี่ยนแปลงที่รวดเร็ว และไม่แน่นอน กระแสโลกาภิวัตน์และความก้าวหน้าทางเทคโนโลยี ทำให้โลกก้าวเข้าสู่ยุคที่ระบบข้อมูลดิจิตอลมีบทบาทนำที่สำคัญในทุกสิ่ง และสามารถไหลเวียนไปมาได้ไร้ซึ่งพรมแดน นำมาซึ่งการเชื่อมโยงของปัจจัยที่ส่งผลกระทบต่อความมั่นคงต่าง ๆ อย่างกว้างขวาง ที่ส่งผลกระทบต่อความมั่นคง การประเมินภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศในห้วงปัจจุบัน พบว่าประเด็นความมั่นคงที่จะส่งผลกระทบต่อไทย ได้แก่ การเมืองระหว่างประเทศ, การขยายอิทธิพลและบทบาท

ของประเทศมหาอำนาจต่อภูมิภาคเอเชียตะวันออกเฉียงใต้, การขยายตัวของความสัมพันธ์ระหว่างประเทศในระดับภูมิภาค, ความขัดแย้งทางดินแดนและการใช้กำลังทางการทหาร, สถานการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้, การเคลื่อนตัวของภัยคุกคามข้ามชาติ, การย้ายถิ่นฐานของประชากร, ความมั่นคงหลัง COVID – 19 และภัยคุกคามทางไซเบอร์ ส่งผลกระทบต่อการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยา ในด้านบวกก่อให้เกิดการเชื่อมโยงข้อมูลเป็นเครือข่าย การติดต่อสื่อสาร และการกระจายข่าวสารที่รวดเร็ว ขณะที่ในด้านลบก่อให้เกิด “ภัยคุกคามทางไซเบอร์” ที่กระทบต่อความมั่นคงของแต่ละประเทศ ซึ่งความเสียหายที่เกิดขึ้นอย่างประเมินค่ามิได้ ทำให้หลายประเทศให้ความสำคัญกับ “ความมั่นคงทางไซเบอร์” มากขึ้น ปัจจุบันสถานการณ์ความมั่นคงทางไซเบอร์ในต่างประเทศ มีแนวโน้มขยายผลกระทบไปในทุกสาขา เช่น กลุ่มพลังงาน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการเงิน กลุ่มสาธารณสุข ข้อมูลส่วนบุคคล และด้านการทหาร เป็นต้น ขณะที่ในประเทศไทยได้เผชิญกับภัยคุกคามทางไซเบอร์อาทิ การเจาะระบบเว็ปไซต์ขององค์กรภาครัฐ การจารกรรมข้อมูล และการโจมตีระบบปฏิบัติการขององค์กรต่าง ๆ เป็นต้น โดยรูปแบบภัยคุกคามทางไซเบอร์มีหลากหลาย แต่ที่พบบ่อย ได้แก่ Malware, Hacker, Ransomware, Ddos, Phishing และ Spyware ฯลฯ เป็นต้น กรมข่าวทหารบกเป็นหน่วยงานด้านข่าวกรองหลักของกองทัพบก จึงต้องมีความพร้อมที่จะรับมือกับภัยคุกคามทุกรูปแบบให้ได้อย่างมีประสิทธิภาพ โดยเฉพาะภัยคุกคามทางบก เช่น ภัยคุกคามทางทหารจากประเทศเพื่อนบ้านภัยคุกคามรูปแบบใหม่ และอาชญากรรมข้ามชาติ รวมไปถึงการก่อความไม่สงบในจังหวัดชายแดนภาคใต้ การใช้เทคโนโลยีที่ทันสมัย โดยเฉพาะเทคโนโลยี AI จะเป็นปัจจัยส่งเสริมให้การปฏิบัติการด้านการข่าวกรองเป็นไปอย่างรวดเร็วถูกต้อง ทันเวลา และมีประสิทธิภาพมากขึ้น

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ ๒ เพื่อศึกษารูปแบบการดำเนินการ สถานะ ปัญหาและอุปสรรคในการดำเนินงานด้านการข่าว โดยเฉพาะการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบกในปัจจุบัน สรุปสาระสำคัญ ดังนี้

ในส่วนของ ปัญหา/ความท้าทายในการใช้เทคโนโลยีของกองทัพบกนั้น กองทัพบกมีการใช้ระบบเทคโนโลยีสารสนเทศในการปฏิบัติงาน โดยอาจแบ่งประเภทของการนำมาใช้งานใน ๒ แบบ คือ เป็นระบบที่หน่วยดำเนินการพัฒนาขึ้นมาด้วยตนเอง และระบบที่ได้จากการจ้างผู้ประกอบการภายนอกเข้ามาดำเนินการให้ ทั้งนี้ จากข้อมูลผลการปฏิบัติงานด้านการข่าวของกองทัพบกที่ผ่านมา มีประเด็นปัญหาของการใช้เทคโนโลยี เพื่อสนับสนุนการปฏิบัติงานที่สำคัญ ได้แก่ ความปลอดภัย, ความท้าทายในเรื่องของ Generation Gap หรือความต่างของอายุและช่วงวัย เนื่องจากเทคโนโลยีนั้นมีการพัฒนา และปรับเปลี่ยนอยู่ตลอดเวลา คนรุ่นเก่าจะเรียนรู้วิธีการใช้เทคโนโลยีได้ยากกว่าคนรุ่นใหม่, ความท้าทายเรื่องความถูกต้องและแม่นยำของเทคโนโลยี, ปัญหาด้านความรู้ความสามารถด้านเทคโนโลยีของกำลังพล, ปัญหาด้านงบประมาณ และปัญหาด้านโครงสร้างหน่วยงานที่ไม่เอื้อต่อการทำงานข่าวที่ต้องการความรวดเร็ว

กองทัพบกมีการก่อตั้ง “ศูนย์ไซเบอร์กองทัพบก” เมื่อ ๑ ก.ค. ๕๗ เพื่อรับผิดชอบงานด้านความมั่นคงทางไซเบอร์ ซึ่งมีการวางระบบการจัดการทรัพยากรทางไซเบอร์และเสริมสร้างขีดความสามารถของกำลังพลมาอย่างต่อเนื่อง อย่างไรก็ตาม ศูนย์ไซเบอร์กองทัพบก มิใช่หน่วยขึ้นตรงกับกรมข่าวทหารบก ดังนั้น การดำเนินงานจึงเกี่ยวข้องกับการข่าวกรองไซเบอร์เชิงรับเป็นส่วนใหญ่

โดยใช้ระเบียบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ทบ. ฉบับปี พ.ศ. ๒๕๖๐ เป็นมาตรการควบคุมการปฏิบัติ ขณะที่การพัฒนาในอนาคตได้กำหนดไว้ในแผนแม่บทไซเบอร์ ทบ. พ.ศ. ๒๕๖๖ - ๒๕๗๐

การประเมินสถานการณ์ด้านไซเบอร์เพื่อความมั่นคงของไทยนั้น ประกอบด้วยสถานการณ์ภัยคุกคามทางไซเบอร์ภายนอกประเทศ และสถานการณ์ภัยคุกคามทางไซเบอร์ภายในประเทศ ซึ่งปัจจุบันปัญหาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศที่สำคัญ ๆ ได้แก่

๑. ปัญหาในการจัดทำแผนงานหรือมาตรการป้องกันภัยคุกคามด้านไซเบอร์

๒. ปัญหาอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII)

๓. ปัญหาความพร้อมของบุคลากรด้านไซเบอร์

สำหรับรูปแบบและลักษณะของการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศนั้น ทำการศึกษาใน ๔ ประเทศ สรุปได้ว่า

๑. สหรัฐอเมริกามองว่า โลกในปัจจุบันถูกเชื่อมโยงเป็นเครือข่ายและล่อแหลมต่อการถูกโจมตีผ่านทางเครือข่าย ด้วยเหตุนี้ ยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกาจะต้องรับประกันในเรื่อง การรักษาความลับ (confidentiality) ความพร้อมใช้งาน (availability) และความสมบูรณ์ของข้อมูล (integrity of data)

๒. สหราชอาณาจักรจะจัดการกับอาชญากรรมด้านไซเบอร์และจะดำเนินการทุกวิถีทางเพื่อให้สหราชอาณาจักรเป็นประเทศที่มีความปลอดภัยมากที่สุดประเทศหนึ่งในโลก สำหรับการทำธุรกิจในพื้นที่ไซเบอร์

๓. จีนเชื่อว่า กฎหมายระหว่างประเทศที่มีอยู่จะต้องได้รับการแก้ไขให้ความชัดเจนหรือสร้างหลักเกณฑ์ขึ้นมาใหม่ให้สอดคล้องกับพื้นที่ไซเบอร์ในปัจจุบัน โดยเฉพาะในเรื่องสิ่งบ่งชี้ของการโจมตีด้านไซเบอร์ที่เป็นการก่ออาชญากรรมด้านไซเบอร์ และการกำหนดว่า ความเสียหายที่เกิดขึ้นจากการป้องกันตนเองอย่างไร จึงจะถือว่า เป็นการป้องกันตนเองอย่างเหมาะสมและถูกต้องตามกฎหมายระหว่างประเทศ

๔. กองทัพสิงคโปร์จัดตั้งกองทัพดิจิตอลและการข่าว (Digital and Intelligence Service : DIS) ซึ่งกำหนดให้มีสถานะเป็นเหล่าทัพที่ ๔ ของกองทัพสิงคโปร์ นอกเหนือจากเหล่า ทบ., ทร. และ ทอ. เพื่อดูแลความมั่นคงด้านดิจิทัล และการเตรียม การรับมือกับภัยคุกคามทางดิจิทัล โดยเชื่อมโยงกับเหล่าทัพอื่น ด้วยการบูรณาการผ่านระบบ (Command, Control, Communication, Computer and Intelligence : C4I) ปฏิบัติการในรูปแบบเครือข่าย รวมทั้งดำเนินการด้านดิจิทัลเชิงรุกให้กองทัพ และการป้องกันทางไซเบอร์

และประการสุดท้าย Global Cybersecurity Index เป็นดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมสากล หรือ International Telecommunication Union (ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลก และหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศ

และการสื่อสาร (The ultimate goal of this initiative is to help foster a global culture of cybersecurity and its integration at the core of ICTs) การศึกษาฉบับนี้สามารถนำแนวคิด Global Cybersecurity Index ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของแต่ละประเทศ มาเป็นเครื่องมือในการวิเคราะห์ปัญหาและข้อเสนอแนะได้

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ ๓ เพื่อเสนอแนะแนวทางในการพัฒนาการดำเนินการด้านการข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพบก สรุปสาระสำคัญดังนี้

การดำเนินการข่าวกรองไซเบอร์ของ ทบ. ต้องได้รับการปรับปรุง เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นในปัจจุบัน โดย ทบ. ต้องให้ความสำคัญด้วยการใช้กลยุทธ์เชิงรุกในการพัฒนาขีดความสามารถของหน่วยข่าวของกองทัพบก รวมทั้งขีดความสามารถด้านสารสนเทศของหน่วยขึ้นตรงกองทัพบก

การพัฒนาขีดความสามารถของ ทบ. มีความเหมือนและแตกต่างกับการพัฒนาในเรื่องเดียวกันของมิตรประเทศ โดยประเด็นที่เหมือนกัน ได้แก่ รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ ในปัจจุบันได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์มาประยุกต์ใช้กับหน่วยงานของตนเอง โดยมีกระบวนการการทำงานหลัก คือ การพิสูจน์ทราบ (Identify), การพิทักษ์ (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond) และการฟื้นฟู (Recovery) ที่เป็นกรอบแนวคิดในการปฏิบัติที่เป็นที่ยอมรับ และนำไปใช้อย่างแพร่หลายทั่วโลก ขณะที่งานข่าวจะเน้นในเชิงป้องกันมากกว่าเชิงรุกด้วยการดำเนินการด้านข่าวกรองด้านภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) ที่เน้นในการศึกษาว่าภัยคุกคาม คือใคร มีเทคนิคและวิธีการโจมตีอย่างไรได้รับ การสนับสนุนจากใคร มีหนทางปฏิบัติต่อผู้ที่เป็นเป้าหมายอย่างไร สำหรับประเด็นที่ต่างกันกับต่างประเทศมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ โดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์ (Cyber Intelligence) จะเป็นหน้าที่และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน โดยจะทำงานและบูรณาการข้อมูลกับหน่วยที่ปฏิบัติการด้านไซเบอร์ หรือหน่วยงานด้านยุทธการอย่างใกล้ชิด เนื่องจากงานข่าวกรองเป็นงานที่ใช้ความรู้และความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องใช้ประสบการณ์จากการปฏิบัติงานมาเป็นระยะเวลาหนึ่ง จึงจะสามารถวิเคราะห์สถานการณ์ที่อาจจะเกิดขึ้นในอนาคตได้ ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด ไม่ว่าจะเป็นขั้นตอนการระบุภัยคุกคามการป้องกันและการแจ้งเตือน ไม่ได้มีการแบ่งหน้าที่งานด้านการข่าวในพื้นที่ปฏิบัติการไซเบอร์ให้กับหน่วยงานด้านการข่าวของหน่วย นอกจากนี้ การบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่มีหลักการปฏิบัติและการดำเนินการที่ชัดเจนเหมือนกับของต่างประเทศ

ในการพัฒนาต้นแบบ หรือขีดความสามารถด้านการข่าวกรองไซเบอร์ต้องสอดคล้องกับแนวทางการพัฒนา ทบ. ตามแผนที่กำหนด เพื่อให้สอดคล้องกับแนวทางการใช้กำลังและภารกิจของ ทบ. ในอนาคต โดยต้องมีการดำเนินการใน ๔ ด้าน คือ ๑. โครงสร้างกำลัง ๒. ความพร้อมรบ

๓. ความต่อเนื่องในการรบ ๔. ความทันสมัย เพื่อให้บรรลุเป้าหมายในการเสริมสร้างขีดความสามารถที่ ทบ. ต้องการ โดยต้องคำนึงถึงปัจจัยแวดล้อมที่เป็นทั้งข้อสนับสนุนและข้อจำกัดต่าง ๆ โดยมีแนวความคิดในการดำเนินการ ดังนี้

๑. ด้านโครงสร้างกำลัง (Force Structure) : หน่วย ขว. ยังคงยึดถือโครงสร้างการจัดหน่วยในปัจจุบัน โดยปรับปรุงอัตราการจัดหน่วยในแต่ละระดับให้เหมาะสม สอดคล้องกับสภาวการณ์ที่เปลี่ยนไป เช่นปรับปรุงภารกิจของหน่วยขึ้นตรงกรมข่าวทหารบก สามารถสนับสนุนหน่วยของ ทบ. ได้ครอบคลุมตามขอบเขตภารกิจที่เพิ่มมากขึ้น โดยมีแนวคิดในการจัดหน่วย เพื่อสนับสนุนงานข่าวกรองไซเบอร์ ดังนี้

๑.๑ หน่วยในส่วนบัญชาการ : ทบทวนความเหมาะสมของการปฏิบัติงานของ ขว.ทบ. ตามการปรับปรุงโครงสร้างในห้วงที่ผ่านมา และดำเนินการปรับปรุงให้เหมาะสมตามสภาพความเป็นจริง โดยให้เพิ่มภารกิจด้านข่าวกรองไซเบอร์ไปในภารกิจของหน่วยด้วย

๑.๒ หน่วยปฏิบัติงานข่าว :

๑.๒.๑ ปรับปรุงอัตราการจัดหน่วย ขกท., พัน.ขกท. และ หน่วย ขกท.พล.ร.๑๕ ให้มีความอ่อนตัว ทันสมัย สามารถดำรงไว้ซึ่งขีดความสามารถในการปฏิบัติงานข่าวกรอง และการต่อต้านการข่าวกรองสนับสนุนหน่วยปฏิบัติทางยุทธวิธี, งานข่าวกรองความมั่นคง และการติดตามตรวจสอบข่าวสาร การรวบรวมข่าวสารด้วยวิธีพิเศษตามภารกิจที่ได้รับมอบ รวมถึงการรวบรวมข่าวสารที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ จากแหล่งข่าวทางเปิดเป็นหลัก (Open source)

๑.๒.๒ ปรับปรุงอัตรากำลังพลในหน่วย ตข. สนับสนุน ทภ. และ มทบ. ให้สมบูรณ์ โดยให้สอดคล้องตามสภาวการณ์และปริมาณงานในปัจจุบัน และมุ่งเน้นเสริมสร้างขีดความสามารถงานด้าน ตข. ทางไซเบอร์ให้กับหน่วยตามลักษณะภัยคุกคามที่เกิดขึ้น

๒. ด้านความพร้อมรบ (Force Readiness)

๒.๑ ด้านกำลังพล :

๒.๑.๑ พิจารณาความเร่งด่วนในการผลิตและบรรจุกำลังพลเหล่า ขว. ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้กับหน่วยข่าวของ ทบ. และหน่วยที่มีอัตรากำลังพลเหล่า ขว. ตามลำดับความเร่งด่วน

๒.๑.๒ ดำเนินการจัดทำระบบงานด้านกำลังพลของเหล่า ขว. โดยใช้เทคโนโลยีสารสนเทศ เพื่อให้ได้ข้อมูลที่ถูกต้องรวดเร็วสำหรับการบริหารจัดการกำลังพลที่มีประสิทธิภาพ และสนับสนุนการพัฒนาขีดความสามารถด้านข่าวกรองไซเบอร์อย่างมีระบบ

๒.๑.๓ พัฒนาระบบการคัดสรรกำลังพลตามความต้องการของหน่วยที่มีการปฏิบัติภารกิจรวบรวมข่าวสารทางไซเบอร์ และพิจารณากำหนดหลักเกณฑ์การจ่ายเงินค่าตอบแทนให้มีความเหมาะสม

๒.๒ ด้านยุทโธปกรณ์ : พิจารณาความเหมาะสมในการจัดหายุทโธปกรณ์ด้านการข่าวให้กับ ขกท., พัน.ขกท. และ หน่วย ขกท.พล.ร.๑๕ เพื่อให้หน่วยมีขีดความสามารถตามที่กำหนดไว้ใน อจย. ในห้วงต่อไปอย่างต่อเนื่อง และจัดหาเครื่องมือพิเศษให้กับหน่วยที่มีภารกิจรวบรวมข่าวสารทางไซเบอร์ เพื่อเสริมสร้างให้หน่วยมีขีดความสามารถที่เหมาะสมตามสภาวการณ์ในปัจจุบัน

๒.๓ ด้านการฝึกอบรม :

๒.๓.๑ พัฒนาหลักสูตรการเรียนการสอนของเหล่า ขว. ให้สอดคล้องกับขอบเขตภารกิจที่หน่วยปฏิบัติงานและเทคโนโลยีในปัจจุบัน และพัฒนาระบบการประเมินผลการเรียนการสอน รวมถึงระบบประกันคุณภาพการฝึกอบรมให้มีมาตรฐาน

๒.๓.๒ รวบรวมบทเรียนและพัฒนาหลักสูตรการฝึกอบรมด้านการข่าว ในเรื่องพิเศษเพื่อเสริมสร้างความชำนาญเฉพาะด้านให้แก่กำลังพลเหล่า ขว. โดยมีความเชื่อมโยงเป็นสหวิทยาการ ในเรื่องที่สามารถตอบสนองต่อภัยคุกคามรูปแบบผสม ทั้งในเรื่องการก่อการร้าย/การก่อความไม่สงบ, ไซเบอร์, นิติวิทยาศาสตร์, ข้อมูลชีวภาพ และวัตถุระเบิดแสวงเครื่อง ฯลฯ

๒.๔ ด้านแผนการปฏิบัติ :

๒.๔.๑ จัดทำและพัฒนาแผนปฏิบัติงานด้านการข่าวกรองไซเบอร์ให้สามารถรองรับ ครอบคลุม และสอดคล้องตามกรอบของ กห. และ ทท. ในภาพรวม และแสวงประโยชน์จากความตกลงร่วมกับเหล่าทัพ และหน่วยงานอื่น ๆ ในการใช้ประโยชน์จากเทคโนโลยีและสิ่งอุปกรณ์ของหน่วยงานนั้น ๆ

๒.๔.๒ พัฒนางานต่อต้านข่าวกรองไซเบอร์ ด้วยการปรับปรุงระบบ รปภ. เครือข่ายและคอมพิวเตอร์ของหน่วยในระดับต่าง ๆ พร้อมทั้งจัดทำมาตรฐานอุปกรณ์ในการรักษาความปลอดภัยไซเบอร์

๒.๔.๓ ขยายเครือข่ายงานข่าวกรองกับหน่วยงานความมั่นคง โดยใช้ประโยชน์จากประชาคมข่าวกรองในทุกระดับและหน่วยข่าวของมิตรประเทศในการบูรณาการด้านการข่าว

๒.๔.๔ สนับสนุนให้ภาคประชาชนที่มีศักยภาพด้านเทคโนโลยีสารสนเทศมีส่วนร่วมในการดำเนินงานด้านการข่าวกรองไซเบอร์ โดยมี ขว.ทบ. เป็นส่วนอำนวยการหลัก

๓. ด้านความต่อเนื่องในการรบ (Sustainability) :

๓.๑ ปรับปรุงอาคาร สถานที่ และการจัดหา สป. ที่จำเป็นให้กับ รร.ขว.ทบ. เพื่อรองรับหลักสูตรการผลิต (นนส.ทบ. เหล่า ขว.), หลักสูตรตามแนวทางรับราชการ และหลักสูตรเสริมสร้างขีดความสามารถพิเศษของเหล่า ขว. (เช่น หลักสูตรข่าวกรองไซเบอร์)

๓.๒ ดำเนินการซ่อมปรับปรุงยุทโธปกรณ์ของหน่วย ขกท., พัน.ขกท. และ หน่วย ขกท.พล.ร.๑๕ รวมถึงหน่วยที่มีเครื่องมือพิเศษ โดยเฉพาะเครื่องมือที่สามารถเชื่อมต่อเข้ากับเครือข่ายคอมพิวเตอร์และ internet เพื่อให้หน่วยสามารถปฏิบัติงานได้อย่างต่อเนื่องและสนับสนุนการบูรณาการข้อมูลด้านการข่าว

๔. ด้านความทันสมัย (Modernization) :

๔.๑ พัฒนาหลักนิยม : จัดทำและพัฒนาหลักนิยมที่สอดคล้องกับสภาวการณ์ในปัจจุบัน เพื่อให้หน่วย ขว. และหน่วยอื่น ๆ มีแนวทางการปฏิบัติงานที่สามารถรองรับต่อภัยคุกคามทั้งภัยคุกคามทางทหารแบบดั้งเดิมและภัยคุกทางไซเบอร์ ดังนี้

๔.๑.๑ จัดทำ/ปรับปรุงเอกสารและตำราในการฝึกอบรมของเหล่าให้มีความสมบูรณ์และทันสมัยครอบคลุมงานข่าวกรองไซเบอร์

๔.๑.๒ พัฒนาระบบการฝึก ตรวจสอบ และประเมินผลของเหล่าให้มีมาตรฐาน รวมถึงระบบประกันคุณภาพการฝึกอบรมที่สามารถสะท้อนถึงความพร้อมรบของหน่วย ในงานด้านข่าวกรองไซเบอร์ได้อย่างแท้จริง โดยการจัดทำคู่มือราชการสนาม, คู่มือการฝึก และระเบียบหลักสูตรการฝึกต่าง ๆ เพื่อพัฒนางานการฝึกหลักตามวงรอบประจำปี ทั้งการฝึกความชำนาญเป็นบุคคลและการฝึกเป็นหน่วยให้ครบสมบูรณ์

๔.๑.๓ แสวงหาความร่วมมือด้านการข่าวกับมิตรประเทศผ่านกลไกคณะทำงานความร่วมมือด้านการทหารที่ ทบ. มีความตกลงกับมิตรประเทศ และที่ ขว.ทบ. มีความร่วมมือแบบทวิภาคีภายใต้อนุมัติหลักการของ ทบ. เพื่อพัฒนาองค์ความรู้ด้านข่าวกรองไซเบอร์ให้มีความเป็นสากลก้าวไปสู่มิติใหม่ของการปฏิบัติงานด้านการข่าวในอนาคต

๔.๒ ด้านเทคโนโลยี : นำเทคโนโลยีสารสนเทศและด้านภูมิสารสนเทศมาสนับสนุนงานด้านการข่าวกรองไซเบอร์ ดังนี้

๔.๒.๑ พัฒนาระบบเฝ้าตรวจชายแดน ให้มีความพร้อมรองรับภัยคุกคามในทุกรูปแบบ สามารถสนับสนุนการบริหารจัดการพื้นที่ชายแดนของ ศปก.ทภ. และ กกล.ป้องกันชายแดนได้อย่างมีประสิทธิภาพ

๔.๒.๒ พัฒนาระบบสารสนเทศด้านการข่าวของ ทบ. ด้วยการจัดทำระบบ Big Data และนำเทคโนโลยี AI มาประยุกต์ใช้ในงานการข่าว และมุ่งสู่การเป็นศูนย์กลางฐานข้อมูลด้านการข่าวของ ทบ.

๔.๒.๓ พัฒนางานวิจัยทางทหารของหน่วย/เหล่า ขว. ให้ได้ผลงานที่สามารถนำไปสู่เป้าหมายการพัฒนาขีดความสามารถของหน่วย/เหล่า ให้มีความพร้อมรบ ทันสมัย และส่งเสริมสนับสนุนงานวิจัยและพัฒนาทางทหารที่มุ่งเน้นผลงานด้านความปลอดภัยทางไซเบอร์และการข่าวกรองไซเบอร์

ข้อเสนอแนะ

๑. ข้อเสนอแนะเชิงนโยบาย

เนื่องจากปัจจุบันการข่าวกรองทางไซเบอร์มีความสำคัญกับการดำเนินงานข่าวกรองของกองทัพบกเป็นอย่างมาก ในแง่นโยบายควรเน้นดำเนินการในด้านต่างๆ ได้แก่ การยกระดับความสามารถของกำลังพล การสร้างความร่วมมือระหว่างหน่วยทหารและความร่วมมือกับองค์กรภายนอก การวางระบบโครงสร้างพื้นฐานที่มีความปลอดภัย การสร้างกฎ ระเบียบ มาตรฐานการรักษาความมั่นคงปลอดภัย การสร้างความเชื่อมั่น และการมุ่งมั่นพัฒนาศักยภาพของหน่วยงานให้มีความพร้อมต่อการปฏิบัติภารกิจ

๒. ข้อเสนอแนะเชิงปฏิบัติ

การพัฒนาขีดความสามารถด้านข่าวกรองไซเบอร์ของ ทบ. นั้น นอกจากเป็นการเสริมสร้างขีดความสามารถตามภารกิจของ ทบ. แล้ว มีข้อเสนอแนะเพิ่มเติมว่า ต้องสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ข้อเสนอแนะดังนี้

๒.๑ ข้อเสนอแนะแนวนโยบายและหลักปฏิบัติ (Policies and Practices)

๒.๑.๑ การปรับเปลี่ยนกระบวนการทำงานของหน่วยเป็นดิจิทัลโดยสมบูรณ์

๒.๑.๒ สร้างความเชื่อมั่นต่อระบบการให้บริการภาครัฐว่าปลอดภัยจากภัยคุกคามทางไซเบอร์

๒.๑.๓ จัดทำข้อมูลตามหลักธรรมาภิบาลข้อมูล พร้อมส่งเสริมการเชื่อมโยงแลกเปลี่ยนข้อมูล เปิดเผยข้อมูล และการนำข้อมูลไปใช้ในการวิเคราะห์เชิงนโยบาย

๒.๑.๔ พร้อมเปิดเผยข้อมูลที่ไม่มีชั้นความลับแก่สาธารณะเมื่อมีการร้องขอ

๒.๑.๕ ทบทวน ปรับปรุง และพัฒนากฎหมาย กฎระเบียบ มาตรการที่เอื้อต่อการพัฒนารัฐบาลดิจิทัล

๒.๑.๖ ส่งเสริมศักยภาพและวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่กำลังพล

๒.๑.๗ ส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนในการพัฒนารัฐบาลดิจิทัล

๒.๒ ข้อเสนอแนะด้านการบริหารจัดการข้อมูล : หน่วยขึ้นตรง ทบ. ควรดำเนินการเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐ โดยการดำเนินการดังกล่าวจะต้องเป็นการดำเนินการในด้านเดียวกัน คือ ด้านการแลกเปลี่ยนข้อมูล ด้านการเปิดเผยข้อมูลเปิดภาครัฐ และด้านการวิเคราะห์ และใช้ประโยชน์ข้อมูล เช่น

๒.๒.๑ มีการกำหนด สิทธิ หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของแต่ละส่วนงาน

๒.๒.๒ กำหนดสิทธิ หน้าที่ ความรับผิดชอบ ของผู้ครอบครองข้อมูล และผู้ควบคุมข้อมูลตามวงจรชีวิตข้อมูล (create, collect, classify, process/use, store, publish/disclose, inspect, terminate)

๒.๒.๓ มีระบบบริหาร และกระบวนการจัดการ และคุ้มครองข้อมูลตามวงจรชีวิตข้อมูล (create, collect, classify, process/use, store, publish/disclose, inspect, terminate)

๒.๒.๔ มีการกำหนดนโยบาย/กฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล

๒.๒.๕ มีการกำหนดมาตรการ หรือ กระบวนการตรวจสอบ ประเมินคุณภาพข้อมูลได้แก่ ถูกต้อง ครบถ้วน สอดคล้องกัน เป็นปัจจุบัน ตรงความต้องการผู้ใช้ และพร้อมใช้

๒.๒.๖ มีการจัดทำบัญชีรายชื่อข้อมูล (Data Catalog) คำอธิบายข้อมูล (Metadata) และพจนานุกรมข้อมูล (Data Dictionary)

๒.๓ ข้อเสนอแนะด้านการใช้ประโยชน์จากข้อมูลเพื่อสนับสนุนภารกิจโดยเฉพาะงานด้านการข่าวกรองไซเบอร์

๒.๓.๑ การวิเคราะห์ข้อมูลเพื่อใช้ในการอธิบายปัญหาและปรากฏการณ์ (Descriptive Analytic)

๒.๓.๒ การวิเคราะห์ข้อมูลเพื่อใช้ในการอธิบายถึงสาเหตุของสิ่งที่เกิดขึ้น ปัจจัยและความสัมพันธ์ต่าง ๆ (Diagnostic Analytic)

๒.๓.๓ การวิเคราะห์ข้อมูลเพื่อใช้ในการคาดการณ์ หรือทำนายสิ่งที่จะเกิดขึ้น (Predictive Analytic)

๒.๓.๔ การวิเคราะห์ข้อมูลเพื่อใช้ในการวิเคราะห์ วางแผนรับมือกับสิ่งที่จะเกิดขึ้นในอนาคต (Prescriptive Analytic)

๓. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

สำหรับการวิจัยในโอกาสต่อไปนั้นสามารถนำข้อมูลที่รวบรวมไว้ในครั้งนี้เป็นข้อมูลพื้นฐานในการดำเนินการศึกษาวิจัยที่เกี่ยวข้องกับงานด้านการทหารอื่น ๆ ได้ เช่น การใช้ BIG DATA และ AI ในการเสริมสร้างขีดความสามารถงานข่าวกรองไซเบอร์ของ ทบ. ในเรื่อง การวางแผนรวบรวมข่าวสาร การรวบรวมข่าวสาร การวิเคราะห์ข่าวกรองไซเบอร์ การใช้และการกระจายข่าวกรองไซเบอร์ การบูรณาการข่าวกรองไซเบอร์ และการประเมินประสิทธิภาพการดำเนินการข่าวกรองไซเบอร์ของหน่วยต่อไป