การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร

โดย

พลอากาศตรี พงษ์สวัสดิ์ จันทสาร
ผู้อำนวยการสำนักนโยบายและแผน กรมข่าวทหารอากาศ
กองทัพอากาศ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๐
ประจำปีการศึกษา พุทธศักราช ๒๕๖๐ – ๒๕๖๑

บทคัดย่อ

เรื่อง การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร
ลักษณะวิชา การทหาร
ผู้วิจัย พลอากาศตรี พงษ์สวัสดิ์ จันทสาร **หลักสูตร** วปอ. **รุ่นที่** ๖๐

เอกสารวิจัยเรื่อง การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อศึกษาบทบาทของงานข่าวกรองที่สนับสนุนมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการดำเนินงานด้านการข่าวกรองไซเบอร์ของกองทัพไทย เพื่อวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร พร้อมนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยกำหนดขอบเขตการวิจัยด้านเนื้อหาที่เกี่ยวข้องกับงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารตามยุทธศาสตร์และนโยบายระดับชาติ โดยเฉพาะการสัมภาษณ์กลุ่มประชากรที่เป็นผู้บริหารและผู้เชี่ยวชาญด้านไซเบอร์และด้านการข่าวกรองของกองทัพไทย ใช้ระยะเวลาในการวิจัยรวมทั้งสิ้น ๕ เดือน ตั้งแต่เดือนมกราคมถึงพฤษภาคม ๒๕๖๑

การวิจัยครั้งนี้ ใช้วิธีดำเนินการวิจัยเชิงคุณภาพโดยอาศัยข้อมูลทุติยภูมิจากบทความตำราวิชาการงานวิจัยและเอกสารที่เกี่ยวข้องและข้อมูลปฐมภูมิจากการสัมภาษณ์กลุ่มผู้บริหารและผู้เชี่ยวชาญนำมาวิเคราะห์ตามแนวทางวิพากษ์วิธี ผลการวิจัยพบว่างานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารมีหลักการเหมือนกันกับงานข่าวกรองในมิติอื่น ๆ โดยใช้รูปแบบและวงรอบข่าวกรองเดียวกันและการดำเนินการต้องมีเอกภาพโดยอาศัยการบูรณาการความร่วมมือ ส่วนหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ คือ การระบุถึงภัยคุกคามและหนทางปฏิบัติของฝ่ายตรงข้าม การจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ และการจัดทำเป้าหมายทางไซเบอร์สนับสนุนมาตรการตอบโต้เชิงรุก ทั้งนี้ ผู้วิจัยได้นำเสนอตัวแบบการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment: IPCE) ของนาย Rob Dartnall เป็นตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

ผู้วิจัยมีข้อเสนอแนะเกี่ยวกับการพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร คือ การพัฒนางานข่าวกรองไซเบอร์เป็นเรื่องที่ผู้บังคับบัญชาจะต้องให้ความสำคัญโดยหน่วยงานด้านการข่าวควรมีบทบาทนำในการปฏิบัติและกองทัพไทยควรมีการปรับโครงสร้างหน่วยข่าวให้สามารถรองรับการปฏิบัติการดังกล่าว โดยพัฒนาขีดความสามารถของผู้ปฏิบัติงานข่าวกรองไซเบอร์ในระดับยุทธการและยุทธวิธี ให้มีทักษะทั้งด้านการข่าวกรองและการปฏิบัติการไซเบอร์ควบคู่กันและควรมีการผนึกกำลังระหว่างหน่วยข่าวกรองไซเบอร์ภายในกระทรวงกลาโหมและหน่วยงานภายนอกรวมทั้งมิตรประเทศ โดยกำหนดให้มีการเชื่อมโยงข้อมูลบนมาตรฐานเดียวกันในทุกภาคส่วนให้สามารถแลกเปลี่ยนข้อมูลข่าวสารและช่วยเหลือซึ่งกันและกันในกรณีที่เกิดสถานการณ์วิกฤตทางไซเบอร์ได้

ABSTRACT

Title Development of Cyber Intelligence in the Aspect of Military Intelligence
Field Military
Name Air Vice Marshal Pongsawat Jantasarn **Course** NDC **Class** 60

The objectives of this research were to study the role of intelligence in supporting cyber security measures and the practice of cyber intelligence of the Royal Thai Armed Forces, to analyze roles and necessary capabilities of the cyber intelligence in the aspect of military intelligence, and to present a model of cyber intelligence in the aspect of military intelligence that is in accordance with national strategies and policies. The research was framed with the cyber intelligence in the aspect of military intelligence according to the national strategies and policies. The process of interviewing executive officers and cyber and intelligence experts of the Royal Thai Armed Forces was five months, from January to May 2018.

The research conducted the qualitative approach, using secondary data, i.e., articles from textbooks, research papers and related documents; and primary data, i.e., interviews of the executive officers and experts. The data was analyzed with the critical approach. The research found that cyber intelligence in the aspect of military intelligence had the same principles with intelligence in other aspects: using the same pattern and intelligence cycle and requiring integrity in practice. Such practice needs integration in cooperation and necessary capabilities of cyber intelligence. The necessary capabilities were identifying threats and practice, building cyber security database, preparing cyber environment, and cyber targeting to support proactive measures. This research presented Rob Dartnell's Intelligence Preparation of the Cyber Environment (IPCE). The IPCE is the cyber intelligence model in the aspect of military that is in accordance with the cyber security of Thailand.

The research suggested that the executive officers should focus on cyber intelligence. The intelligence units should play an important role in implementation and the Royal Thai Armed Forces should improve the structure of the intelligence units and improve the cyber intelligence officers in the operational and strategic levels. The officers should be skillful in intelligence and cyber practice. Furthermore, there should be collaboration among the cyber intelligence units of the Ministry of Defence, other units, and other countries. This could be done by linking database to every unit in order to exchange intelligence and assist each other in case of cyber emergency situation.

คำนำ

การศึกษาวิจัยเรื่อง “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร” มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ให้ทราบถึงหน้าที่และขีดความสามารถข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร และนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร ที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยมุ่งหวังให้สามารถนำไปใช้เป็นตัวแบบในการจัดทำแนวความคิดในการปฏิบัติด้านข่าวกรองไซเบอร์ของหน่วยงานหรือสถาบันศึกษาที่เกี่ยวข้องกับความมั่นคง หรือนำไปประยุกต์ใช้ในการศึกษาและปรับปรุงให้ตัวแบบมีความสมบูรณ์และเหมาะสมกับยุคสมัยต่อไป

ผลงานวิจัยฉบับนี้ ได้รับการสนับสนุนด้วยดีจากผู้บังคับบัญชาและผู้เชี่ยวชาญทั้งในด้านการปฏิบัติการไซเบอร์และด้านการข่าวกรองของกองทัพไทย ซึ่งได้กรุณาให้คำปรึกษาแนะนำและการให้สัมภาษณ์ อันเป็นข้อมูลและองค์ความรู้ให้ผู้วิจัยสามารถนำมาใช้ประโยชน์ ตลอดจนคณาจารย์และเจ้าหน้าที่ของวิทยาลัยป้องกันราชอาณาจักรทุกท่านที่ได้ให้ความกรุณา เอื้อเฟื้อตลอดระยะเวลาที่ผู้วิจัยเข้ารับการศึกษาอบรม จึงขอขอบพระคุณทุกท่านไว้ ณ โอกาสนี้ และผู้วิจัยหวังเป็นอย่างยิ่งว่าผลงานวิจัยฉบับนี้ จะเป็นประโยชน์ต่อการเสริมสร้างขีดความสามารถ และการพัฒนางานข่าวกรองไซเบอร์ของกองทัพไทยต่อไป

พลอากาศตรี

(พงษ์สวัสดิ์ จันทสาร)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๐
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ภัยคุกคามทางไซเบอร์ (Cyber Threat) เป็นภัยคุกคามรูปแบบใหม่ ที่เน้นกระทำต่อระบบอินเทอร์เน็ต และระบบเครือข่ายคอมพิวเตอร์ ทำให้ประชาคมโลกเริ่มตื่นตัวและตระหนักถึงภัยคุกคามดังกล่าวมากขึ้นในห้วง ๕ ปีที่ผ่านมา (พ.ศ.๒๕๕๖ - ๒๕๖๐) เนื่องจากปัจจุบันสังคมโลกอยู่ในยุค โลกาภิวัตน์ (Globalization) ที่โลกมีการเชื่อมโยงถึงกันและมีการเปลี่ยนแปลงอย่างรวดเร็วด้วยระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ (ไซเบอร์) ที่มีความทันสมัยและเข้ามามีบทบาทสำคัญในการพัฒนาประเทศด้านต่าง ๆ ได้แก่ การเมือง เศรษฐกิจ สังคม การทหาร และระบบสาธารณูปโภคของประเทศ รวมถึงการเข้าไปมีบทบาทในภาคเอกชนตลอดจนเกี่ยวพันกับการใช้ชีวิตประจำวันของบุคคลทั่วไป อาทิ การทำการค้า การทำธุรกรรม และการติดต่อสื่อสาร ฯลฯ ทำให้ภัยคุกคามทางไซเบอร์ ส่งผลกระทบต่อความมั่นคงในทุกระดับตั้งแต่ในระดับประชาคมโลก ภูมิภาค ประเทศชาติ และลงมาถึงประชาชน

ทั้งนี้ เมื่อวันที่ ๑๑ พฤษภาคม ๒๕๖๐ นายแดเนียล โคตส์ ผู้อำนวยการข่าวกรองแห่งชาติสหรัฐฯ (DNI) ได้เสนอประมาณการภัยคุกคามของประชาคมข่าวกรองสหรัฐฯ ต่อคณะกรรมาธิการด้านข่าวกรองของวุฒิสภาสหรัฐฯ ระบุว่า ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามความมั่นคงอันดับ ๑[๑] เหนือการก่อการร้ายและอาวุธที่มีอานุภาพทำลายล้างสูง (WMD) โดยอ้างอิงจากขีดความสามารถของฝ่ายตรงข้ามที่มีความเชี่ยวชาญเพิ่มขึ้นในการใช้พื้นที่ปฏิบัติการทางไซเบอร์โจมตีหน่วยงานรัฐและผลประโยชน์ของสหรัฐฯ เมื่อห้วงปี ๒๕๕๙ ขณะที่รายงานความเสี่ยงโลกประจำปี ๒๕๖๐ ของ World Economic Forum[๒] พบว่ามีอัตราการขยายตัวของภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างต่อเนื่องและก่อให้เกิดความเสียหายต่อสังคมโลกมากยิ่งขึ้น โดยก่อนหน้านี้ระหว่างปี ๒๕๕๒ – ๒๕๕๓ ระบบคอมพิวเตอร์ในโครงการนิวเคลียร์อิหร่านถูกไวรัสคอมพิวเตอร์

---

[๑]Daniel R Coats. “Worldwide Threat Assessment of the Us Intelligence Community”. (Statement for the Record Senate Select Committee on Intelligence. 11 May 2017).

[๒]World Economic Forum. “The Global Risks Report 2017 12Th Edition”. (Online). Available : http : //www3.weforum.org/docs/GRR17_Report_web.pdf, 2017.

ชื่อว่า “Stuxnet” โจมตีและไม่สามารถปฏิบัติการต่อไปได้ ซึ่งปัจจุบันยังไม่สามารถยืนยันได้ว่าใครหรือรัฐใดอยู่เบื้องหลังการโจมตีครั้งนี้ ในส่วนของภาคเอกชนและบุคคลสำคัญในระดับประเทศอย่างบริษัทโซนี่ พิกเจอร์ส และ นางฮิลารี คลินตัน อดีตรัฐมนตรีว่าการกระทรวงการต่างประเทศสหรัฐฯ ต่างเคยถูกนักเจาะระบบคอมพิวเตอร์ (Hacker) ทำการเจาะเข้าฐานข้อมูลของบริษัท และบัญชีจดหมายอิเล็กทรอนิกส์ส่วนตัวเมื่อปี ๒๕๕๗ และปี ๒๕๕๙ ตามลำดับ ก่อนจะทำการจารกรรมข้อมูลสำคัญหรือข้อมูลมีที่ชั้นความลับ (Cyber Espionage)[๓] ออกมาเผยแพร่ต่อสาธารณะ และล่าสุดเมื่อวันที่ ๑๑ ตุลาคม ๒๕๖๐ ข้อมูลด้านความมั่นคงของกระทรวงกลาโหมออสเตรเลียจำนวนมาก รวมถึงข้อมูลที่เกี่ยวข้องกับการจัดซื้อเครื่องบินแบบ F-35 และ เครื่องบินแบบ P-8 ถูกจารกรรมผ่านระบบเครือข่ายของบริษัทเอกชนคู่สัญญาของกระทรวงกลาโหมออสเตรเลีย ซึ่งเหตุการณ์ทั้งหมดที่กล่าวมานอกจากจะสร้างความเสียหายต่อภาพลักษณ์ของตัวบุคคลและหน่วยงานที่เกี่ยวข้องแล้วยังเป็นการสร้างความเสียหายต่อเศรษฐกิจและผลประโยชน์แห่งชาติอีกด้วย

จากเหตุผลข้างต้น แสดงให้เห็นว่าภัยคุกคามทางไซเบอร์มีความอันตรายต่อทุกระดับชั้น จึงส่งผลให้นานาประเทศตระหนักถึงความจำเป็นในการหาวิธีการป้องกันและรับมือกับภัยคุกคามนี้อย่างจริงจัง ด้วยการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) โดยมีหลายประเทศที่ดำเนินมาตรการอย่างเป็นรูปธรรม อาทิ สหรัฐฯ ซึ่งกำหนดยุทธศาสตร์ด้านไซเบอร์ ๒ ประการ คือ

๑. การป้องกันโครงสร้างพื้นฐานระบบสารสนเทศสำคัญ

๒. การสร้างระบบนิเวศน์หรือสภาพแวดล้อมทางไซเบอร์ให้แข็งแกร่ง

โดยมอบหมายให้กระทรวงความมั่นคงแห่งมาตุภูมิ และกระทรวงกลาโหมสหรัฐฯ เป็นหน่วยงานรับผิดชอบสำคัญ โดยกระทรวงกลาโหมสหรัฐฯ ได้จัดตั้งหน่วย Cyber Command ขึ้นมารองรับนโยบายดังกล่าว และกำหนดให้พื้นที่ปฏิบัติการบนไซเบอร์ (Cyberspace Domain) เป็นหนึ่งในพื้นที่ปฏิบัติการทางทหารนอกเหนือจากพื้นที่ทางบก อากาศ ทะเล และอวกาศ สำหรับรัสเซียมีการดำเนินการออกกฎหมายที่บังคับให้ผู้ให้บริการ Web Server ต้องติดตั้งตัวควบคุมและสกัดกั้นข้อมูลเข้า-ออก และมีการเพิ่มบทลงโทษทางกฎหมายต่อผู้ที่ก่ออาชญากรรมทางไซเบอร์ รวมถึงมอบหมายให้หน่วยงานด้านความมั่นคงทุกหน่วยต้องติดตามสถานการณ์เมื่อมีการโจมตีทางไซเบอร์ (Cyber Attack)[๔] ด้านจีนมีการเพิ่มหมวดที่เกี่ยวข้องกับอำนาจอธิปไตยทางไซเบอร์ในกฎหมายความมั่นคงแห่งชาติเมื่อเดือนกรกฎาคม ๒๕๕๘ และมีการจัดตั้ง National Computer Network Emergency Response Technical Team (Cncert) ทำหน้าที่ตรวจจับและตอบโต้การโจมตีทางไซเบอร์

---

[๓] การจารกรรมข้อมูลบนเครือข่ายคอมพิวเตอร์ หรือผ่านทางอินเทอร์เน็ต โดยใช้วิธีการค้นหาช่องโหว่ที่มีอยู่ในระบบและทำการแสวงประโยชน์จากช่องโหว่ที่ตรวจพบ ด้วยการเจาะเข้าผ่านทางช่องโหว่นั้น

[๔] การกระทำหรือการดำเนินกิจกรรมใดผ่านมิติทางไซเบอร์โดยรัฐ องค์กร กลุ่ม หรือบุคคลที่มุ่งหวังให้ระบบเครือข่ายคอมพิวเตอร์ ระบบข้อมูลข่าวสาร และระบบโครงสร้างพื้นฐานของฝ่ายตรงข้ามถูกขัดขวาง ทำลาย ควบคุม เปลี่ยนแปลง และไม่สามารถดำเนินการได้เป็นปกติ

สำหรับอาเซียนนั้น สิงคโปร์ถือเป็นประเทศที่มีการเตรียมความพร้อมมากที่สุดด้วยการจัดตั้งศูนย์ปฏิบัติการป้องกันภัยทางไซเบอร์ (Cyber-Defence Operations Hub : CDOH) ในการดำเนินภารกิจป้องกันระบบเครือข่ายคอมพิวเตอร์ การตรวจจับ และการตอบโต้ต่อการโจมตีทางไซเบอร์ตลอด ๒๔ ชม. ภายใต้ความร่วมมือกับหลายองค์กร

ในส่วนของไทยพบว่าระหว่างปี ๒๕๕๗ - ๒๕๕๙ ต้องรับมือกับภัยคุกคามจากไซเบอร์มากกว่า ๓,๐๐๐ ครั้งต่อปี ขณะที่ในปี ๒๕๖๐ รับมือกับภัยคุกคามดังกล่าวจำนวน ๒,๖๒๔ ครั้ง โดยภัยคุกคามที่พบมากที่สุดในปัจจุบัน ๓ อันดับแรกคือ การบุกรุกระบบ การฉ้อโกง และการโจมตีสภาพความพร้อมใช้งานของระบบ[๕] จากเหตุผลดังกล่าวส่งผลให้ร่างยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (พ.ศ.๒๕๖๐ - ๒๕๗๙) ได้ระบุให้ความมั่นคงทางไซเบอร์เป็นหนึ่งในประเด็นที่ทุกภาคส่วน โดยเฉพาะหน่วยงานด้านความมั่นคงต้องให้ความสำคัญ เนื่องจากไซเบอร์จะถูกนำมาใช้เป็นโครงสร้างพื้นฐาน ระบบการบริหารจัดการสาธารณะและระบบสาธารณูปโภคมากขึ้นในอนาคต ดังที่รัฐบาลนำไซเบอร์มาเพิ่มขีดความสามารถขององค์กรในการขับเคลื่อนประเทศตามนโยบาย Thailand 4.0 ขณะที่ประชาชนจะใช้ช่องทางไซเบอร์ในการติดต่อสื่อสาร การทำธุรกรรมทางการเงิน และเคลื่อนไหวในประเด็นต่าง ๆ เพิ่มขึ้น ซึ่งจะทำให้ภัยคุกคามทางไซเบอร์จะมีความซับซ้อนและรุนแรงมากกว่าในอดีต และมีแนวโน้มว่าอาจถูกใช้เป็นฐานในการโจมตีประเทศอื่น ๆ ดังนั้น เพื่อรับมือกับภัยคุกคามดังกล่าวไทยจึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ ลงในนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ - ๒๕๖๔ โดยมุ่งเน้นไปที่การเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศทั้งภายในประเทศและระหว่างประเทศ สนับสนุนการสร้างเครือข่ายขององค์กรและผู้เชี่ยวชาญในด้านการรักษาความมั่นคงทางไซเบอร์ ซึ่งปัจจุบันไทยมีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ๒ แห่ง คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) และศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (G-Cert) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ นอกจากนี้รัฐบาลยังได้จัดทำร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดให้มีหน่วยงานหลักในการรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และทำการบูรณาการประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง เรียกว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) เรียกโดยย่อว่า “กปช.” (ปัจจุบันอยู่ระหว่างการรับฟังความคิดเห็นและยังไม่มีผลบังคับใช้) ทั้งยังมีการปรับปรุงกลไกการบังคับใช้กฎหมายให้สามารถลดภัยคุกคามที่มีต่อความมั่นคงทางไซเบอร์ได้ (พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐) สำหรับหน่วยงานด้านความมั่นคงตั้งแต่ในระดับกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพต่าง ๆ

---

[๕] ไทยเซิร์ต. “สถิติภัยคุกคาม”. (ออนไลน์). เข้าถึงได้จาก : Https : // www.Thaicert.or.th/ Statistics/ Statistics. Html, ๒๕๖๐.

ได้มีการจัดตั้งหน่วยงานภายในเพื่อดูแลเกี่ยวกับปัญหาภัยคุกคามด้านไซเบอร์ อาทิ กองสงครามเครือข่าย กรมยุทธการทหาร ศูนย์ไซเบอร์กองทัพบก กองสงครามไซเบอร์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ และกรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ เป็นต้น

ทั้งนี้ จากการศึกษาค้นคว้าเกี่ยวกับมาตรฐานที่เป็นข้อกำหนดสำหรับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management System : ISMS) เช่น ISO ISO/IEC 27001 ของยุโรป และกรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework ของสหรัฐอเมริกา ที่นานาประเทศยึดถือเป็นมาตรฐานและกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พบว่างานข่าวกรองเป็นองค์ประกอบที่สำคัญในกระบวนการโดย “ข่าวกรองภัยคุกคามไซเบอร์ Cyber Threat Intelligence (CTI)” เป็นรูปแบบของข่าวกรองที่แพร่หลายและเป็นที่รู้จักกันดีในกลุ่มองค์กรหรือหน่วยงานต่าง ๆ ทั่วโลกที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่ง CTI เป็นการนำข้อมูลที่รวบรวมได้จากเครือข่ายมาวิเคราะห์ร่วมกับฐานข้อมูลของการโจมตีที่รู้จักเพื่อให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ สิ่งนี้เป็นจุดเริ่มต้นที่จะนำเอาแนวคิดของข่าวกรองไซเบอร์จากภาคความมั่นคงเข้ามาใช้ในภาคอุตสาหกรรมมากขึ้น นอกจากนี้ พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ รองประธานกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (รองประธาน กสทช.) และประธานกรรมการกิจการโทรคมนาคม ยังได้กล่าวไว้เมื่อวันที่ ๒๑ ธันวาคม ๒๕๕๙ ว่า “การเชื่อมโยงแลกเปลี่ยนข้อมูลข่าวสารด้านการข่าวกรองไซเบอร์ระหว่างประเทศ ของสำนักงานความมั่นคงไซเบอร์แห่งชาติของแต่ละประเทศด้วยศูนย์ปฏิบัติการไซเบอร์ เป็นอีกหนึ่งในปัจจัยแห่งความสำเร็จ ซึ่งในเครือข่าย Cyber Security ระดับนานาชาติจะสามารถช่วยในการค้นหาเป้าหมาย แหล่งต้นตอ การโจมตีได้อย่างรวดเร็ว ทันเวลา และยังมีการแจ้งเตือนแนวโน้มที่จะถูกโจมตีได้อีกด้วย” จึงเป็นเครื่องยืนยันถึงความจำเป็นและความสำคัญของงานข่าวกรองในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีบทบาทในการช่วยผลักดันและสนับสนุนให้การรักษาความมั่นคงทางไซเบอร์ประสบผลสำเร็จ

จากการศึกษาค้นคว้าข้อมูลของผู้วิจัยดังที่ปรากฏในเนื้อหาข้างต้น ประกอบกับหน้าที่ในปัจจุบัน ซึ่งดำรงตำแหน่งผู้อำนวยการสำนักนโยบายและแผน กรมข่าวทหารอากาศ (ผอ.สนผ.ขว.ทอ.) ที่มีความเกี่ยวข้องกับงานด้านการข่าวกรองโดยตรงและมีส่วนในการพิจารณา เสนอนโยบาย วางแผนและดำเนินการด้านนโยบายและแผนงานด้านการพัฒนางานด้านข่าวกรองไซเบอร์ (Cyber Intelligence) ของกองทัพอากาศ เพื่อตอบสนองนโยบายผู้บัญชาการทหารอากาศ ประจำปี ๒๕๖๐ – ๒๕๖๑ และขับเคลื่อนยุทธศาสตร์กองทัพอากาศ ๒๐ ปี[๖] จึงมีความเห็นว่า “การข่าวกรองไซเบอร์” ซึ่งถือเป็นกลไกสำคัญในการรับมือกับภัยคุกคามทางไซเบอร์นั้น เป็นเรื่องที่มีความสำคัญอย่างยิ่งในยุคปัจจุบันและถือเป็นเรื่องใหม่

---

[๖] กองทัพอากาศ. “นโยบายผู้บัญชาการทหารอากาศ ประจำปีพุทธศักราช ๒๕๖๐ – ๒๕๖๑”. “ยุทธศาสตร์ ทอ. ๒๐ ปี ประจำปีพุทธศักราช ๒๕๖๐ – ๒๕๗๙”. (ออนไลน์). เข้าถึงได้จาก : http : //www.rtaf.mi.th, ๒๕๖๑.

ที่ยังขาดแคลนผู้เชี่ยวชาญและองค์ความรู้ และมีความจำเป็นเร่งด่วนที่จะต้องดำเนินการอย่างเป็นรูปธรรม แต่อย่างไรก็ตาม ด้วยสถานการณ์โลกได้เปลี่ยนแปลงไปจากเดิมและวิวัฒนาการด้านข่าวกรองไซเบอร์มีการพัฒนาไปอย่างมาก โดยมีปัจจัยหลายประการที่เอื้อให้ผู้วิจัยพิจารณาเห็นว่า แนวทางการดำเนินงานและการปฏิบัติการด้านข่าวกรองไซเบอร์ในองค์กรต่าง ๆ อาจยังไม่มีเพียงพอต่อการรับมือกับสถานการณ์ภัยคุกคาม เนื่องจากนโยบายรวมถึงแนวความคิดและทฤษฎีในการปฏิบัติการด้านข่าวกรองไซเบอร์ในระดับต่าง ๆ ยังคงขาดความชัดเจนโดยเฉพาะหน่วยงานด้านความมั่นคงที่มีหน้าที่รับผิดชอบในการป้องกันภัยคุกคามโดยตรง ด้วยเหตุนี้ผู้วิจัยจึงมีความสนใจที่จะศึกษาวิจัยเรื่อง “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร” เพื่อศึกษาวิเคราะห์ถึงหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทการข่าวทหาร ที่สมควรจะต้องได้รับการพัฒนาอย่างเป็นรูปธรรมและนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยมุ่งหวังให้สามารถนำไปใช้เป็นตัวแบบในการการจัดทำแนวความคิดในการปฏิบัติด้านข่าวกรองไซเบอร์ของหน่วยงานหรือสถาบันศึกษาที่เกี่ยวข้องกับความมั่นคง หรือนำไปประยุกต์ใช้ในการศึกษาและปรับปรุงให้ตัวแบบมีความสมบูรณ์และเหมาะสมกับยุคสมัยต่อไป

สรุปการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพและประสบความสำเร็จนั้น จำเป็นอย่างยิ่งที่จะต้องมีงานข่าวกรองไซเบอร์ที่เข้มแข็ง ซึ่งถือเป็นความท้าท้ายใหม่ของประเทศไทยและอีกหลายประเทศ ที่ยังขาดบุคลากรและองค์ความรู้ในการพัฒนาข่าวกรองไซเบอร์ในระดับชาติ ผู้วิจัยจึงมีความสนใจในการศึกษาวิจัยเพื่อจัดทำ “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร” เพื่อให้หน่วยงานและบุคคลที่เกี่ยวข้องสามารถนำไปใช้ประโยชน์ต่อไป

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ

๒. เพื่อศึกษาวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร

๓. เพื่อนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ

ขอบเขตของการวิจัย

ด้านเนื้อหา

การวิจัยครั้งนี้มุ่งเน้นศึกษายุทธศาสตร์และนโยบายระดับชาติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนนิยามและขอบเขตข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยเท่านั้น

ด้านประชากร

การศึกษานี้มุ่งศึกษาความคิดเห็นของบุคลากร เฉพาะที่เกี่ยวข้องกับงานด้านการปฏิบัติการไซเบอร์และการข่าวทหารเท่านั้น โดยกลุ่มบุคลากรดังกล่าวประกอบด้วย

๑. กลุ่มผู้บริหารที่มีส่วนในการกำหนดนโยบายในด้านความมั่นคงไซเบอร์และการข่าวกรองของกองทัพไทย จำนวน ๓ คน

๒. กลุ่มผู้เชี่ยวชาญทั้งในด้านการปฏิบัติการไซเบอร์และด้านการข่าวกรองของกองทัพไทย จำนวน ๔ คน

รวมทั้งสิ้นจำนวน ๗ คน

ด้านเวลา

การศึกษานี้ผู้วิจัยได้ใช้ระยะเวลาในการดำเนินการวิจัยตั้งแต่เดือนมกราคม - พฤษภาคม ๒๕๖๐ รวมระยะเวลาทั้งสิ้น ๕ เดือน

วิธีดำเนินการวิจัย

๑. ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ โดยอาศัยข้อมูลปฐมภูมิจากการสัมภาษณ์ (Interview) และข้อมูลทุติยภูมิที่รวบรวมได้จากบทความ ตำราวิชาการ งานวิจัย และเอกสารที่เกี่ยวข้อง (Documentary search)

๒. นำข้อมูลที่ได้รับจากการสัมภาษณ์มาวิเคราะห์ตามแนวทางวิพากษ์วิธี

๓. นำข้อมูลจากข้อ ๑ และ ๒ เปรียบเทียบกับหลักการและเหตุผล นำไปสู่การบูรณาการเพื่อผลการวิจัยและข้อยุติที่เป็นรูปธรรมสามารถนำไปปฏิบัติได้ รวมทั้งข้อคิดเห็นและข้อเสนอแนะที่เป็นประโยชน์

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทราบแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ

๒. สามารถกำหนดหน้าที่และขีดความสามารถข่าวกรองไซเบอร์ที่จำเป็นของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร

๓. ได้ตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต ที่สอดคล้องกับแนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

คำจำกัดความ

ไซเบอร์	หมายถึง	กิจกรรมที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ การสื่อสารข้อมูลคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์
ความมั่นคงปลอดภัยไซเบอร์	หมายถึง	มาตรการและการดำเนินการเพื่อปกป้อง ป้องกัน การส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ
ข่าวกรองไซเบอร์	หมายถึง	ข่าวสารต่างๆ ที่ได้รับความสนใจและมีความเกี่ยวข้องกับระบบเครือข่าย ระบบสารสนเทศ ที่ผ่านการตรวจสอบ วิเคราะห์ หรือได้รับพิสูจน์ว่าเป็นข่าวที่เชื่อถือได้ สามารถนำไปเป็นหลักฐานอ้างอิงได้
ภัยคุกคามไซเบอร์	หมายถึง	การกระทำใด ๆ ที่มุ่งต่อระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมโยงติดกันรวมทั้งฐานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ระบบดังกล่าวไม่สามารถปฏิบัติการได้ตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกจารกรรมหรือถูกทำลาย รวมทั้งการแสวงใช้ประโยชน์เครือข่ายคอมพิวเตอร์เพื่อก่ออาชญากรรมหรือใช้ในทางประสงค์ไม่ดี
การจารกรรมทางไซเบอร์	หมายถึง	การจารกรรมข้อมูลบนเครือข่ายคอมพิวเตอร์หรือผ่านทางอินเทอร์เน็ต โดยใช้วิธีการค้นหาช่องโหว่ที่มีอยู่ในระบบและทำการแสวงประโยชน์จากช่องโหว่ที่ตรวจพบ ด้วยการเจาะเข้าผ่านทางช่องโหว่นั้น
การโจมตีทางไซเบอร์	หมายถึง	การกระทำหรือการดำเนินกิจกรรมใดผ่านมิติทางไซเบอร์โดยรัฐ องค์กร กลุ่ม หรือบุคคล ที่มุ่งหวังให้ระบบเครือข่ายคอมพิวเตอร์ ระบบข้อมูลข่าวสาร และระบบโครงสร้างพื้นฐานของฝ่ายตรงข้ามถูกขัดขวาง ทำลาย ควบคุม เปลี่ยนแปลง และไม่สามารถดำเนินการได้เป็นปกติ
นักเจาะระบบคอมพิวเตอร์	หมายถึง	ผู้ซึ่งใช้วิธีการต่าง ๆ เพื่อให้ได้มาซึ่งสิทธิในการใช้งานระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
พื้นที่ปฏิบัติการบนไซเบอร์	หมายถึง	สมรภูมิรบทางไซเบอร์ ซึ่งประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์และหลักการด้านรังสีแม่เหล็กไฟฟ้า ในการจัดเก็บแก้ไขหรือแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายหรือโครงสร้างพื้นฐานทางกายภาพ (Physical Infrastructures)

บทที่ ๒
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การวิจัยครั้งนี้ ผู้วิจัยได้ศึกษาแนวคิด นโยบาย และขีดความสามารถที่ต้องการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กระบวนการข่าวกรองที่สนับสนุนการปฏิบัติการไซเบอร์ตามหลักวิชาการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ รวมถึงบทบาทและหน้าที่ของงานข่าวในการรับมือกับภัยคุกคามทางไซเบอร์ของต่างประเทศจากวรรณกรรมที่เกี่ยวข้องดังต่อไปนี้

๑. การประเมินภัยคุกคามทางไซเบอร์ในระยะ ๕ ปี คณะที่ปรึกษาการข่าว สำนักนายกรัฐมนตรี

๒. กรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยในปัจจุบัน

๓. ร่างกรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (พ.ศ.๒๕๖๐ – ๒๕๗๙)

๔. นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔

๕. ยุทธศาสตร์ข่าวกรองแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔

๖. ยุทธศาสตร์ป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๗๙

๗. กรอบงานความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework) และงานข่าวกรองที่เกี่ยวข้อง

๘. กระบวนการข่าวกรองที่สนับสนุนการปฏิบัติการไซเบอร์ตามหลักวิชา

๙. การดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ

๑๐. บทบาทหน้าที่ของงานข่าวกรองไซเบอร์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ

๑๑. ผลงานวิจัยที่เกี่ยวข้อง

การประเมินภัยคุกคามทางไซเบอร์ในระยะ ๕ ปี คณะที่ปรึกษาการข่าว สำนักนายกรัฐมนตรี

คณะที่ปรึกษาด้านการข่าว สำนักนายกรัฐมนตรี ได้ศึกษาสถานการณ์ภัยคุกคามทางไซเบอร์ของไทยและต่างประเทศในห้วงระยะ พ.ศ.๒๕๕๒ – ๒๕๕๘ ทำให้สามารถประเมินลักษณะภัยคุกคามดังกล่าวในระยะ ๕ ปีข้างหน้าได้ว่า การโจมตีไซเบอร์ส่วนใหญ่จะเป็นในลักษณะการจารกรรมข้อมูลโดยผู้กระทำที่ไม่ใช่รัฐ (Non-State Actor) และผู้กระทำที่มีรัฐเป็นผู้ให้การสนับสนุน (State-Sponsors Actor)

ซึ่งทำให้ภัยคุกคามดังกล่าวมีความซับซ้อนมากขึ้น ขณะที่การแสวงประโยชน์จากไซเบอร์ อาทิ การโฆษณาชวนเชื่อ การบ่มเพาะแนวคิดนิยมความรุนแรง ฯลฯ จะมีแนวโน้มเพิ่มสูงขึ้นเช่นกัน ในส่วนของรัฐบาลและเอกชนจะถูกโจมตีทางเว็บไซต์ของตนเป็นระยะ โดยมีวัตถุประสงค์เพื่อก่อกวน หรือแสดงการประท้วงเชิงสัญลักษณ์

อย่างไรก็ตาม สงครามไซเบอร์ขนาดใหญ่ในลักษณะรัฐต่อรัฐ ยังคงไม่เกิดขึ้นในอนาคตอันใกล้ เนื่องจากไทยไม่มีประเทศที่เป็นศัตรูโดยตรง รวมทั้งยังมีความสัมพันธ์อันดีกับต่างประเทศ

มุมมองส่วนตัวของผู้วิจัยมองว่า แม้ไทยจะไม่ได้เป็นศัตรูกับประเทศใด แต่การโจมตีทางไซเบอร์จากประเทศอื่นหรือรัฐอื่นมีโอกาสเป็นไปได้ เนื่องจากบางครั้งการทำสงครามระหว่างกันอาจไม่จำเป็นต้องมีความขัดแย้งเสมอไป แต่หากวันใดก็ตามเกิดกรณีที่ประเทศหนึ่งจำเป็นต้องรักษาผลประโยชน์ของตนเอง รวมถึงไม่ต้องการให้อีกฝ่ายได้ประโยชน์ หรือในกรณีที่ผลประโยชน์ของประเทศหนึ่งสร้างผลกระทบให้กับอีกฝ่าย อาทิ การค้าระหว่างประเทศ การแข่งขันทางการค้า เป็นต้น การใช้การโจมตีไซเบอร์จะกลายเป็นหนึ่งในเครื่องมือที่เหมาะสมที่ช่วยให้ประเทศนั้นบรรลุผลลัพธ์สุดท้ายที่ต้องการ โดยไม่สร้างความเสียหายต่อโครงสร้างพื้นฐานของประเทศที่ถูกโจมตี ขณะเดียวกันก็ยากต่อการพิสูจน์ทราบว่าประเทศใดเป็นผู้กระทำ เนื่องจากประเทศที่ทำการโจมตีย่อมไม่ทิ้งร่องรอยของตนเองไว้เป็นหลักฐาน อีกทั้งพื้นที่ปฏิบัติการทางไซเบอร์ไม่มีอาณาเขตดินแดนเหมือนกับรัฐหรือประเทศ ดังนั้น สภาพของความเป็นรัฐหรือประเทศจึงไม่มีตัวตนในโลกไซเบอร์ ส่งผลให้แนวคิดในการป้องกันภัยคุกคามในรูปแบบเดิม รวมถึงการใช้กระบวนการทางการทูต อาจไม่เหมาะสมต่อการรับมือกับภัยคุกคามรูปแบบใหม่อย่างภัยคุกคามทางไซเบอร์

การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยในปัจจุบัน

ปัจจุบันประเทศไทยมีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ๒ แห่ง คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Thailand Computer Emergency Response Team : ThaiCERT) ในการกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ซึ่งมีภาระหน้าที่หลักในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้การสนับสนุนที่จำเป็น และให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต และศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต) (Government Computer Emergency And Readiness Team : G-Cert)

ในการกำกับดูแลของ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ รวมทั้งการสร้างเครือข่ายพันธมิตรเพื่อให้เกิดความมั่นคงปลอดภัยและช่วยลดความเสี่ยงต่อการเกิดอาชญากรรมทางคอมพิวเตอร์

นอกจากนี้ยังมีการปรับปรุงกลไกการบังคับใช้กฎหมาย ให้สามารถลดภัยคุกคามที่มีต่อความมั่นคงทางไซเบอร์ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ ๒ พ.ศ.๒๕๖๐ และเสนอร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดให้มีหน่วยงานหลักในการรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และทำการบูรณาการประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องเรียกว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Committee : NCSC) เรียกโดยย่อว่า “กปช.” (ปัจจุบันอยู่ระหว่างการรับฟังความคิดเห็นร่าง พ.ร.บ.ฯ) ทั้งนี้คณะรัฐมนตรีได้เห็นชอบในหลักการให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จัดทำระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ (ประกาศใช้เมื่อวันที่ ๑๘ ตุลาคม ๒๕๖๐) สำหรับใช้บังคับในระหว่างการจัดทำร่าง พ.ร.บ.ฯ มีวัตถุประสงค์เพื่อใช้ระเบียบนี้เป็นเครื่องมือสำคัญอย่างหนึ่งที่จะช่วยในการปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ของประเทศไทย ทำให้ประชาชนและประเทศไทยมีความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีดิจิทัล โดยในระเบียบฯ ดังกล่าวได้กำหนดให้มีคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีอำนาจหน้าที่สำคัญในการจัดทำนโยบายและแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนการเตรียมการจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการเตรียมการไซเบอร์แห่งชาติได้จัดประชุมคณะเตรียมการด้านการรักษาความปลอดภัยมั่นคงไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๑ เมื่อวันที่ ๙ พฤษภาคม ๒๕๖๑ เวลา ๑๔.๐๐ น. ณ ตึกภักดีบดินทร์ ทำเนียบรัฐบาล โดยมี พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานฯ ซึ่งการจัดประชุมครั้งนี้ที่ประชุมเสนอเรื่องเพื่อพิจารณา ๔ เรื่อง คือ

๑. กรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อปกป้อง รับมือ ป้องกัน ลดความเสี่ยงและความสอดคล้องไปในทิศทางเดียวกัน

๒. แนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศ และแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure : SOP)

๓. แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน

๔. แนวทางการจัดตั้ง Cybersecurity Agency (CSA) ทำหน้าที่หน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความปลอดภัยมั่นคงไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

สาระสำคัญของการประชุม

๑. ยกระดับ Ranking ด้านความมั่นคงปลอดภัยไซเบอร์ ให้ติด ๑ ใน ๒๐

สำหรับดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เมื่อเปรียบเทียบกับต่างประเทศในปี ๒๕๖๐ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ทำการสำรวจระดับความเอาจริงเอาจัง (Commitment) ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงานและนโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity Building) และด้านความร่วมมือ (Cooperation) พบว่า Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ ขณะเดียวกันเมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ ๓ รองจากประเทศสิงคโปร์และประเทศมาเลเซีย ซึ่งกระทรวงและหน่วยงานที่เกี่ยวข้องจะช่วยกันขับเคลื่อนให้ไทยติดใน ๒๐ อันดับแรกของประเทศที่มีความพร้อม

๒. แผนเร่งด่วนขับเคลื่อนความเข้มแข็งไซเบอร์

ส่วนเรื่องของยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศถือว่าเป็นสิ่งสำคัญมากในการขับเคลื่อนประเทศ โดยคณะกรรมการชุดนี้ได้กำหนดแผนงานระยะเร่งด่วน ๖ เดือน ๑ ปี และ ๒ ปี ที่หน่วยงานจะร่วมกันทำต่อไปใน ๘ ด้าน ที่สอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ – ๒๕๖๔ คือ

๒.๑ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection : CIIP)

๒.๒ การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness)

๒.๓ การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance)

๒.๔ การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public - Private Partnership)

๒.๕ การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building)

๒.๖ การพัฒนากฎหมาย ระเบียบและมาตรฐานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Law Regulation and Standard)

๒.๗ การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ (International Cooperation)

๒.๘ การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ (Research & Development)

๓. จัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ๖ กลุ่ม

มติที่ประชุมได้เห็นชอบการจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure : CII) ๖ กลุ่มแรก ได้แก่

๓.๑ กลุ่มความมั่นคงและบริการภาครัฐ

๓.๒ กลุ่มการเงิน

๓.๓ กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม

๓.๔ กลุ่มการขนส่งและโลจิสติกส์

๓.๕ กลุ่มพลังงานและสาธารณูปโภค

๓.๖ กลุ่มสาธารณสุข

พร้อมยกระดับแผนการทำงานร่วมกัน เช่น ซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมถึงจัดทำแผนปฏิบัติการรับมือไซเบอร์ (National Incident Handling Flow)

๔. เพิ่มกำลังคนไซเบอร์

ดร.พิเชฐ ฯ กล่าวเพิ่มเติมว่า เรื่องการจัดตั้งศูนย์ความร่วมมืออาเซียน - ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ หรือ ASEAN - Japan Cybersecurity Capacity Building Centre ตามมติที่ประชุม Telmin - Japan หรือการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่นที่ประเทศกัมพูชาเมื่อปลายปีที่ผ่านมา โดยประเทศไทยได้รับเลือกให้เป็นเจ้าภาพจัดตั้งศูนย์ฯ ขณะนี้ได้มีความพร้อมเป็นอย่างมาก โดยจะเปิดตัวอย่างเป็นทางการประมาณเดือนมิถุนายน ๒๕๖๑ ที่จะถึงนี้ ซึ่งกระทรวงดีอีได้มอบหมายให้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) เป็นเจ้าภาพหลักในการดำเนินงาน เนื่องจากเป็นหน่วยงานที่มีประสบการณ์ในการพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ของประเทศมาอย่างต่อเนื่อง โดยศูนย์ฯ นี้ได้รับการสนับสนุนจากประเทศญี่ปุ่นทั้งด้านงบประมาณและองค์ความรู้ต่าง ๆ ทำให้สามารถดำเนินการฝึกอบรมให้แก่ประเทศสมาชิกอาเซียนได้อย่างมีประสิทธิภาพ ซึ่งนับเป็นโอกาสสำคัญในการรับถ่ายทอดความรู้และประสบการณ์จากประเทศชั้นนำด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะผนึกกำลังสำคัญในการยกระดับขีดความสามารถของบุคลากร อันจะส่งผลดีต่อการประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในเวทีสากล รวมถึงการปรับปรุงอันดับ ITU และ GCI ให้ขึ้นสู่ ๒๐ อันดับต้นของโลก

นอกจากนี้ยังมีความจำเป็นในการดำเนินโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์กว่า ๑,๐๐๐ คน ที่ผ่านการรับรองจากหน่วยงาน (CII) ภาครัฐ - เอกชน และสถาบันการศึกษา

๕. เตรียมพร้อมหน่วยงานประสานงานกลาง

มอบหมายให้ ETDA ทำหน้าที่หน่วยประสานงานกลางเป็นการชั่วคราวระหว่างจัดตั้ง Cybersecurity Agency (CSA) เพื่อรับมือภัยคุกคามทางไซเบอร์และทำงานร่วมกับหน่วยงานที่เกี่ยวข้องลดความเสี่ยงจากการถูกโจมตี

ร่างกรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (พ.ศ.๒๕๖๐ – ๒๕๗๙)

ยุทธศาสตร์ที่ ๑ ยุทธศาสตร์ด้านความมั่นคง ตามร่างกรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (พ.ศ.๒๕๖๐ – ๒๕๗๙) มีเนื้อหามุ่งเน้นการพัฒนาศักยภาพในการป้องกันประเทศพร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่น ๆ ทั้งจากการสร้างขีดความสามารถภายในและการสร้างความร่วมมือกับประเทศเพื่อนบ้านและมิตรประเทศ นอกจากนี้การบูรณาการความร่วมมือกับต่างประเทศที่เอื้อให้เกิดความมั่นคงในทุกด้านและป้องกันภัยคุกคามจากอาชญากรรมข้ามชาติในทุกรูปแบบก็เป็นแนวทางที่มีความสำคัญมากขึ้นภายใต้ภูมิทัศน์โลกไร้พรมแดนและการเปลี่ยนแปลงด้านภูมิรัฐศาสตร์ที่เป็นเครือข่ายซับซ้อนขึ้นมาก โดยเฉพาะอย่างยิ่งในการวางระบบบริหารจัดการความเสี่ยงจากการโจมตีทางไซเบอร์และการบริหารจัดการภัยพิบัติและภัยในรูปแบบใหม่ที่ต้องบูรณาการความร่วมมือให้เกิดผล โดยมีแนวทางและประเด็นการพัฒนาที่เกี่ยวข้องกับการข่าวกรองและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

ประเด็นที่ ๑.๒ การพัฒนาศักยภาพในการป้องกันประเทศ พร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่น ๆ เสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่องให้สามารถประเมินสถานการณ์ในระยะยาวได้อย่างแม่นยำ พัฒนาความเป็นหุ้นส่วนทางการข่าวกรองกับทุกภาคส่วน รวมถึงพัฒนาศักยภาพของบุคลากรและเทคโนโลยีที่เกี่ยวข้อง ตลอดจนพัฒนาระบบฐานข้อมูลด้านความมั่นคงให้มีความทันสมัยครอบคลุมความต้องการการใช้งานอย่างครบถ้วน

ประเด็นที่ ๑.๓ บูรณาการความร่วมมือกับต่างประเทศที่เอื้อให้เกิดความมั่นคง ความมั่งคั่งทางเศรษฐกิจ ป้องกันภัยคุกคามข้ามชาติ และคุณภาพชีวิตของคนในชาติ เสริมสร้างความมั่นคงและปกป้องโครงสร้างพื้นฐานและสาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ ให้ปลอดภัยจากการโจมตี รวมถึงส่งเสริมวัฒนธรรมสร้างความตระหนักรู้ในการใช้ไซเบอร์ในทางที่เหมาะสมตลอดจนพัฒนาเพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ทั้งยามปกติ ยามเกิดเหตุ การฟื้นตัวและฟื้นฟูหลังเกิดเหตุและการเยียวยาแก้ไขผลกระทบ

นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔

นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔ ได้กล่าวถึงบริบทการเปลี่ยนแปลงที่นำไปสู่ภัยคุกคามรูปแบบใหม่ไว้ว่า กระแสโลกาภิวัตน์ทำให้การเชื่อมโยงในมิติต่าง ๆ เป็นไปอย่างรวดเร็ว ส่งผลให้ความมั่นคงที่เกี่ยวกับเทคโนโลยีสารสนเทศและเครือข่ายมีแนวโน้มจะเป็นประเด็นที่มีความเสี่ยงจากการถูกโจมตีและการจารกรรมทางไซเบอร์ เนื่องจากการกำหนดมาตรการป้องกันทำได้ยากและไม่ทันต่อความก้าวหน้าทางเทคโนโลยี ทั้งนี้ประเทศกำลังพัฒนาจะตกเป็นเป้าหมายการโจมตีมากขึ้น เพราะมีความล้าหลังทางเทคโนโลยีและขาดความรู้ในการกำหนดมาตรการป้องกันที่ต้องใช้ผู้ที่มีความชำนาญเฉพาะทาง นอกจากนี้อิทธิพลของสื่อประเภทเครือข่ายสังคมเป็นเครื่องมือสำคัญของประชาชนในการรวมตัวดำเนินกิจกรรมทางสาธารณะ และการเคลื่อนไหวกิจกรรมทางการเมือง ทำให้สื่อดังกล่าวมีโอกาสถูกนำมาใช้ในทางที่ผิดเพื่อโจมตี บ่อนทำลาย หรือบิดเบือนข้อเท็จจริง

รวมถึงการแพร่กระจายถ้อยคำที่สร้างความเกลียดชังที่มีฐานมาจากอคติและการเลือกปฏิบัติ ซึ่งอาจทำให้เกิดความเกลียดชังและปัญหาความแตกแยกภายในประเทศรวมถึงส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ ในกรณีที่มีการใช้สื่อประเภทนี้โจมตีหรือบ่อนทำลายประเทศอื่น

ดังนั้นนโยบายความมั่นคงแห่งชาติฉบับนี้ จึงได้กำหนดนโยบายความมั่นคงไว้รองรับในส่วนที่ ๒ นโยบายความมั่นคงแห่งชาติทั่วไป นโยบายที่ ๑๐ เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ดังนี้

ข้อ ๑๐.๑ ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยการบูรณาการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากรองค์กรและผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกัน การโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ การกู้คืนข้อมูลระบบและเครือข่าย และการพัฒนามาตรฐานด้านความปลอดภัยในทุกด้าน

ข้อ ๑๐.๒ พัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคล ข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปของการทำธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูลสารสนเทศ การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิด ตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

ข้อ ๑๐.๓ พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยส่งเสริมการวิจัย พัฒนา และจดสิทธิบัตรเทคโนโลยีสารสนเทศที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบรัฐบาลอิเล็กทรอนิกส์ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) ตลอดจนการพัฒนาบุคลากรภาครัฐ องค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านระบบเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัยและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงปริมาณและคุณภาพอย่างต่อเนื่อง

นอกจากนี้นโยบายความมั่นคงแห่งชาติ ฯ ส่วนที่ ๒ นโยบายความมั่นคงแห่งชาติทั่วไป ยังได้กำหนดนโยบายด้านการพัฒนางานข่าวกรองไว้ในนโยบายที่ ๑๕ พัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ ดังนี้

ข้อ ๑๕.๑ ดำเนินงานข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพทั้งภัยคุกคามต่อความมั่นคงแห่งชาติ และความเคลื่อนไหวที่สนับสนุนการเสริมสร้างความมั่นคงและผลประโยชน์แห่งชาติ

ข้อ ๑๕.๒ เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วยงานภาครัฐ รวมทั้งหน่วยงานข่าวกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนและประชาชน

ข้อ ๑๕.๓ เสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่อง โดยพัฒนาบุคลากรและเพิ่มศักยภาพของเทคโนโลยี ระบบฐานข้อมูลและองค์กรด้านการข่าว

ยุทธศาสตร์ข่าวกรองแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔

ยุทธศาสตร์ข่าวกรองแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔ ได้ประเมินสถานการณ์ภัยคุกคามความมั่นคงและสถานการณ์ที่เป็นโอกาสในการเสริมสร้างความมั่นคงในระยะ ๗ ปี (พ.ศ.๒๕๕๘ – ๒๕๖๔) ระบุว่าสถานการณ์ภายในประเทศยังคงมีความรุนแรงและมีแนวโน้มที่จะขยายตัว โดยหนึ่งในประเด็นที่สำคัญ คือ ภัยคุกคามใหม่และความมั่นคงทางเทคโนโลยีสารสนเทศ

ดังนั้นยุทธศาสตร์ข่าวกรองแห่งชาติฉบับนี้ จึงมีวัตถุประสงค์เพื่อให้มีงานข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยคุกคามได้อย่างมีประสิทธิภาพรวมทั้งสนับสนุนโอกาสและผลประโยชน์ในการแข่งขันของไทย และให้เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรองทั้งในประเทศและต่างประเทศ รวมถึงเครือข่ายภาคเอกชนและประชาชน อีกทั้งเสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรอง ทั้งนี้ในยุทธศาสตร์ที่ ๒ ยุทธศาสตร์ข่าวกรองเพื่อป้องกันและแก้ไขภัยคุกคามทั่วไปและเสริมสร้างโอกาสด้านความมั่นคง ได้กำหนดกลยุทธ์ที่ ๒ ป้องกันและแก้ไขภัยคุกคามระบบสารสนเทศไว้รองรับประเด็นยุทธศาสตร์

ยุทธศาสตร์ป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๗๙

ยุทธศาสตร์ป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๗๙ บทที่ ๔ แนวความคิดและประเด็นยุทธศาสตร์ ได้กำหนดมาตรการและขีดความสามารถที่ต้องการด้านการข่าวกรองและการปฏิบัติการด้านไซเบอร์ ในประเด็นยุทธศาสตร์ที่ ๖ การปฏิบัติการทางทหารเพื่อรักษาอธิปไตยและผลประโยชน์แห่งชาติ ดังนี้

ด้านการข่าวกรอง

ระยะที่ ๑ (พ.ศ.๒๕๖๐ - ๒๕๖๔) พัฒนาระบบข่าวกรองด้วยเทคโนโลยีที่ทันสมัยให้สามารถแจ้งเตือนภัยคุกคามทางทหารได้อย่างมีประสิทธิภาพ รวมทั้งสามารถใช้ประโยชน์ในการแจ้งเตือนภัยคุกคามที่ไม่ใช่ทางทหาร และความท้าทายด้านความมั่นคงที่เกี่ยวข้องกับกระทรวงกลาโหมได้ด้วย โดยต้องมีระบบฐานข้อมูลข่าวกรองร่วม สามารถหาข่าวและแจ้งเตือนภัยคุกคามในพื้นที่ชายแดน พื้นที่ระวังป้องกันและพื้นที่สนใจอื่น ๆ มีความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรองหน่วยงานภาครัฐและหน่วยงานข่าวกรองต่างประเทศ มีเครือข่ายข้อมูลข่าวสารกับภาคเอกชนและประชาชน รวมทั้งมีขีดความสามารถในการประเมินสภาวะแวดล้อมด้านความมั่นคงทั่วทุกภูมิภาคของโลกที่มีผลกระทบต่อไทย

ระยะที่ ๒ (พ.ศ.๒๕๖๕ - ๒๕๖๙) ระยะที่ ๓ (พ.ศ.๒๕๗๐ - ๒๕๗๔) จนถึง ระยะที่ ๔ (พ.ศ.๒๕๗๕ - ๒๕๗๙) นั้น ตัวยุทธศาสตร์ได้กำหนดทิศทางใน ๓ ระยะนี้เป็นไปในทิศทางเดียวกัน คือ พัฒนาระบบข่าวกรองอย่างต่อเนื่องให้สามารถแจ้งเตือนภัยคุกคามทางทหารได้อย่างมีประสิทธิภาพ รวมทั้งสามารถใช้ประโยชน์ในการแจ้งเตือนภัยคุกคามที่ไม่ใช่ทางทหาร และความท้าทายด้านความมั่นคงที่เกี่ยวข้องกับกระทรวงกลาโหมได้ด้วย โดยให้ความสำคัญกับระบบฐานข้อมูลข่าวกรองร่วม ขีดความสามารถในการหาข่าวและแจ้งเตือนภัยคุกคามในพื้นที่ชายแดน พื้นที่ระวังป้องกันและพื้นที่สนใจอื่น ๆ ความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง หน่วยงานภาครัฐและหน่วยงานข่าวกรองต่างประเทศ เครือข่ายข้อมูลข่าวสารกับภาคเอกชนและประชาชน รวมทั้งมีขีดความสามารถในการประเมินสภาวะแวดล้อมด้านความมั่นคง

ด้านการปฏิบัติการด้านไซเบอร์

ระยะที่ ๑ (พ.ศ.๒๕๖๐ - ๒๕๖๔) พัฒนากำลังพล โครงสร้างพื้นฐาน และเทคโนโลยีให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ สร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วนและสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ

ระยะที่ ๒ (พ.ศ.๒๕๖๕ - ๒๕๖๙) และ ระยะที่ ๓ (พ.ศ.๒๕๗๐ - ๒๕๗๔) พัฒนาศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ เพื่อให้มีพลังอำนาจทางไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง

ระยะที่ ๔ (พ.ศ.๒๕๗๕ - ๒๕๗๙) เพิ่มศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ให้อยู่ในแนวหน้าและเป็นที่ยอมรับในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้

กรอบงานความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework) และงานข่าวกรองที่เกี่ยวข้อง

๑. บทความเรื่อง “Standard และ Framework ที่น่าสนใจในยุค Thailand 4.0 โดย Acinfotec ได้แนะนำมาตรฐานด้านความมั่นคงปลอดภัยที่น่าสนใจสำหรับประเทศไทยโดยระบุว่า วิวัฒนาการด้านระบบ IT ในประเทศไทยที่เห็นชัดเจนที่สุดในตอนนี้คือ การนำระบบ Cloud เข้ามาใช้งาน

ในองค์กรไม่ว่าจะเป็นการย้าย Data Center ไปยังระบบ Cloud การใช้ระบบ Cloud เป็น DR Site หรือให้บริการเซอร์วิสผ่านระบบ Cloud ทำให้ข้อมูลของพนักงานและข้อมูลของลูกค้ามีการเคลื่อนย้ายไปยังระบบ Cloud ดังนั้น มาตรฐานและกรอบการดำเนินงานด้านความมั่นคงปลอดภัยสมัยใหม่ที่ควรพิจารณาถึงตอนนี้ ประกอบด้วย

๑.๑ ISO/IEC 27001:2013 มาตรฐานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) เรียกได้ว่าเป็นมาตรฐานยอดนิยมขององค์กรในประเทศไทยที่มีการดำเนินงานหรือบริการเกี่ยวกับสารสนเทศ จากสถิติทั่วโลกพบว่าปี ๒๐๑๕ มีองค์กรที่ได้รับการรับรองมาตรฐานดังกล่าวเพิ่มขึ้นจากปี ๒๐๑๔ ถึง ๒๐% รวมเป็น ๒๓,๐๐๕ แห่ง

๑.๒ ISO/IEC 27002:2013 ข้อปฏิบัติสำหรับสนับสนุน ISO 27001 ซึ่งระบุแนวทางปฏิบัติที่ดีที่สุด (Best Practice) สำหรับการเริ่มต้นการพัฒนาและการบำรุงรักษา ISMS

๑.๓ ISO/IEC 20000 - 1:2011 มาตรฐานด้านการบริหารจัดการการให้บริการ (SMS) ซึ่งเป็นข้อปฏิบัติสำหรับ Service Provider ในการวางแผน เริ่มต้น พัฒนา ดำเนินการ ติดตาม ทบทวน บำรุงรักษา และปรับปรุง SMS อย่างต่อเนื่อง

๑.๔ ISO 22301:2012 มาตรฐานด้านการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) เป็นมาตรฐานที่ช่วยให้แต่ละองค์กรสามารถวางแผนรับมือกับภัยพิบัติรูปแบบต่าง ๆ ได้อย่างเป็นระบบโดยเฉพาะอย่างยิ่งการโจมตีไซเบอร์

๑.๕ ISO/IEC 27032:2012 ส่วนขยายของ ISO 27001 ซึ่งเน้นโฟกัสที่การธำรงไว้ซึ่ง Confidentiality Integrity และ Availability ใน Cyberspace หรือก็คือความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บริการ รวมไปถึงสิ่งที่จับต้องไม่ได้ (Virtual Assets) เช่น ชื่อเสียง แบรนด์ เป็นต้น

๑.๖ ISO 31000:2009 มาตรฐานด้านการบริหารจัดการความเสี่ยงระดับองค์กร เป็นแกนหลักสำคัญของทุกมาตรฐาน ISO

๑.๗ ISO/IEC 27017:2015 ส่วนขยายของ ISO 27001 ที่มีขอบเขตครอบคลุมบริการบนระบบ Cloud โดยมีการขยายความข้อปฏิบัติบน ISO 27002 เช่น สิทธิในการลบข้อมูลบนระบบ Cloud เมื่อเปลี่ยนไปใช้ Cloud Provider เจ้าใหม่ เป็นต้น โดยมาตรฐานนี้ครอบคลุมมาตรการควบคุมสำหรับผู้ให้บริการและผู้ใช้บริการ

๑.๘ ISO/IEC 27018:2014 เช่นเดียวกับ ISO 27017 มาตรฐานนี้เป็นข้อปฏิบัติสำหรับการปกป้องข้อมูลส่วนบุคคล (PII) บนระบบ Cloud สาธารณะ โดยมีการขยายความเพิ่มเติมจาก ISO 27002 และเพิ่มมาตรการควบคุมจาก ISO 29100 เข้าไป

๑.๙ CSA - STAR มาตรฐานด้านความมั่นคงปลอดภัยในการให้บริการระบบ Cloud โดยผู้ที่ขอใบรับรองจำเป็นต้องได้รับการรับรองมาตรฐาน ISO 27001 แบ่งออกเป็น ๓ ระดับ คือ

๑.๙.๑ Self - Assessment – Cloud Provider ประเมินตนเองตาม Cloud Control Matrix

๑.๙.๒ Third Party Assessment - based Certification มี Auditor ภายนอกเป็นผู้ตรวจในประเทศไทยมี Cloud Provider ที่ได้รับการรับรองแล้ว ๓ ราย

๑.๙.๓ Continuous Monitoring - based Certification กำลังพัฒนาอยู่ โดยมีจุดประสงค์เพื่อให้มีความมั่นคงปลอดภัยอย่างต่อเนื่อง

๑.๑๐ NIST Cyber Security Framework กรอบการดำเนินด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ๕ องค์ประกอบหลัก คือ Identity Protect Detect Response Recovery

๒. รายงานเรื่อง Cybersecurity Strategy A Guildline and Recommendations September 2015 โดย พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ ประธานกรรมการกิจการโทรคมนาคม และรองประธาน กสทช. จัดทำขึ้นเพื่อเป็นแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) โดยผลของรายงานฉบับนี้ได้มาจากการศึกษา วิจัย และวิเคราะห์แนวทางการพัฒนายุทธศาสตร์จากประเทศต่าง ๆ ทั่วโลก ระบุว่า “เนื่องจากปัจจุบันระบบสารสนเทศขององค์กรต่าง ๆ มีขนาดใหญ่ขึ้นการบริหารจัดการจึงเป็นสิ่งสำคัญ องค์กรจำเป็นต้องมีการกำหนดนโยบายและมาตรการควบคุมเพื่อให้ระบบสารสนเทศทั้งหมดที่อยู่ภายใต้การกำกับดูแลมีแนวปฏิบัติด้านความมั่นคงปลอดภัยเดียวกันและเป็นไปตามที่องค์กรกำหนด ซึ่งมาตรฐานด้านความมั่นคงปลอดภัยที่ทั่วโลกนิยมใช้ ได้แก่ ISO ของสหภาพยุโรป และ NIST ของประเทศสหรัฐอเมริกา โดยผู้วิจัยได้ศึกษากรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework) ที่ได้รับการยอมรับจากนานาประเทศรวมถึงองค์กรต่าง ๆ ในประเทศไทย คือ กรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework) ที่ร่างโดยสถาบันมาตรฐานและเทคโนโลยี (NIST) กระทรวงพาณิชย์สหรัฐอเมริกา เพื่อเป็นแนวทางให้ภาครัฐและเอกชนใช้ในการดำเนินการเกี่ยวกับการดูแลและปกป้องค์กรจากภัยในโลกไซเบอร์ ซึ่งกรอบการดำเนินงานดังกล่าวเป็นการกำหนดนโยบายเกี่ยวกับความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญ แต่ไม่ได้เป็นการเพิ่มมาตรฐานหรือแนวคิดใหม่ ในทางตรงข้ามกลับเป็นการผลักดันและผสมผสานแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมชั้นนำที่ได้รับการพัฒนาจากองค์กรต่าง ๆ เช่น NIST และองค์การระหว่างประเทศว่าด้วยเรื่องมาตรฐาน (ISO)

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นผลมาจากคำสั่ง Executive Order ของประธานาธิบดีสหรัฐอเมริกา ในเดือนกุมภาพันธ์ พ.ศ.๒๕๕๖ ที่ชื่อว่า “Improving Critical Infrastructure Cybersecurity” หรือ “การพัฒนาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญของประเทศ” ระยะเวลา ๑๐ เดือนที่มีการปรึกษาหารือร่วมกันจากผู้เชี่ยวชาญด้านความปลอดภัยมากกว่า ๓,๐๐๐ คน รวมถึงการรวบรวมแนวทางความเสี่ยงที่อาจเกิดขึ้นจะสามารถช่วยองค์กรต่าง ๆ ในการระบุจัดเตรียม และพัฒนาแนวปฏิบัติสำหรับความมั่นคงปลอดภัยไซเบอร์ให้สำเร็จ และยังสร้างภาษากลางสำหรับการสื่อสารกันทั้งภายในและระหว่างองค์กรเกี่ยวกับประเด็นความมั่นคงปลอดภัยไซเบอร์อีกด้วย

กรอบการดำเนินงานนี้เป็นกระบวนการแบบวนซ้ำ ซึ่งถูกออกแบบมาเพื่อพัฒนาแบบค่อยเป็นค่อยไปพร้อมกับการเปลี่ยนแปลงรูปแบบภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ กระบวนการและเทคโนโลยี ซึ่งจะมีการปรับปรุงเป็นระยะจากบทเรียนต่าง ๆ ที่ได้รับและผลตอบรับจากภาคอุตสาหกรรม โดยที่กรอบการดำเนินงานนี้มองความมั่นคงปลอดภัยไซเบอร์ที่มีการพัฒนาอย่างมีประสิทธิภาพ จะต้องมีการพัฒนาปรับปรุงยุทธศาสตร์และกลยุทธ์ในลักษณะวงจรพลวัตแบบต่อเนื่องที่มีการรับมือจากภัยคุมคามและมีแนวทางการแก้ปัญหา

โครงสร้างหลักของกรอบดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เป็นตัวกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ ผลลัพธ์ที่เกิดขึ้นและเป็นกรอบอ้างอิงที่สามารถนำไปใช้งานและมีกิจกรรมพื้นฐานที่ต่อเนื่องกันสามารถแบ่งย่อยได้ ๕ กิจกรรมหลัก ได้แก่ การกำหนด การป้องกัน การตรวจจับ การรับมือ และการคืนสภาพ โดยโครงสร้างหลักของกรอบการดำเนินงานอธิบายวงจรต่อเนื่องของกระบวนการทางธุรกิจ ซึ่งทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

๓. บทความเรื่อง “ทำความรู้จักกับ NIST Cybersecurity Framework” โดยบริษัท กสท. โทรคมนาคม จำกัด (มหาชน) ระบุว่า

NIST Cybersecurity Framework เป็นหนึ่งในกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบันไม่เพียงแค่องค์กรในสหรัฐฯ เท่านั้น Framework ดังกล่าวยังเป็นที่แพร่หลายไปยังทุกภูมิภาคทั่วโลกรวมไปถึงประเทศไทย ซึ่งหลายองค์กรเริ่มนำ Framework นี้มาประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์

Framework นี้นำเสนอหลักการและแนวทางปฏิบัติที่ดีที่สุดของการบริหารจัดการความเสี่ยงเพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทุกระดับ รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกันตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ในขณะที่ธุรกิจยังคงดำเนินต่อไปได้อย่างต่อเนื่อง โดยหัวใจสำคัญของ Framework แบ่งออกเป็น ๕ ฟังก์ชั่นหลัก คือ

๑. Identify การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง

๒. Protect การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

๓. Detect การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

๔. Respond การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

๕. Recovery การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

ซึ่งแต่ละฟังก์ชั่นหลักจะแบ่งออกเป็นฟังก์ชันย่อยพร้อมระบุเอกสารอ้างอิง เช่น ISO/IEC 27001:2013 COBIT 5 NIST SP800 - 53 เพื่อให้ผู้อ่านนำกระบวนหรือแนวทางปฏิบัติจากเอกสารเหล่านั้นมาใช้เพื่อดำเนินการตามฟังก์ชั่นย่อยเหล่านี้ได้ทันที

แผนภาพที่ ๒ - ๑ กรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework

ที่มา : N. Hanacek/NIST, Online, 2013

๔. ข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence : CTI) เป็นรูปแบบของข่าวกรองที่แพร่หลายและเป็นที่รู้จักกันดีในกลุ่มองค์กรหรือหน่วยงานต่าง ๆ ทั่วโลก ที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่ง CTI เป็นการนำข้อมูลที่รวบรวมได้จากเครือข่ายมาวิเคราะห์ร่วมกับฐานข้อมูลของการโจมตีเพื่อให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ โดยเว็บไซต์วิกิพีเดียได้อธิบายความหมายของข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence : CTI) ว่า “เป็นกระบวนการที่ประกอบด้วยการคัดเลือกผู้เชี่ยวชาญด้านการรักษาความปลอดภัยสารสนเทศและการระดมทรัพยากรทางเทคนิค เพื่อป้องกันโครงสร้างพื้นฐานวิกฤติและทรัพย์สินทางปัญญาขององค์กร โดยใช้พื้นฐานของงานข่าวกรองในการรวบรวมผ่านข่าวกรองจากแหล่งข่าวเปิด (OSINT) ข่าวกรองสื่อสังคมออนไลน์ (SOCMINT) ข่าวกรองบุคคล (HUMINT) ข่าวกรองเทคนิค (TECHINT) หรือข่าวกรองเชิงลึกจากเว็บไซต์ลับ โดย CTI มีภารกิจหลักคือการวิจัยและวิเคราะห์แนวโน้ม และการพัฒนาด้านเทคนิคใน ๓ มิติ ได้แก่ อาชญากรรมไซเบอร์ นักเจาะระบบ และการจารกรรมไซเบอร์ ซึ่งการสะสมฐานข้อมูลการวิจัยและวิเคราะห์เหล่านี้จะถูกพัฒนาเป็นมาตรการป้องกันการโจมตีทางไซเบอร์ ข้อพิจารณาเกี่ยวกับผลกระทบจากภัยคุกคามไซเบอร์ ซึ่ง CTI จะช่วยพัฒนาประสิทธิภาพในการแก้ไขปัญหาและรักษาความมั่นคงปลอดภัยในระดับชาติ”

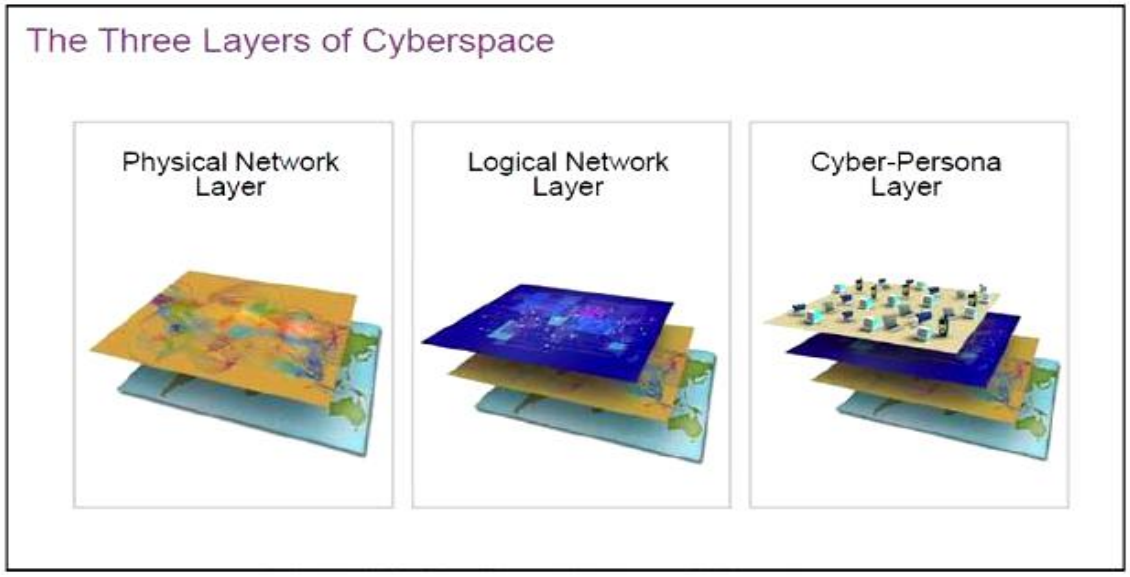
กระบวนการข่าวกรองที่สนับสนุนการปฏิบัติการไซเบอร์ตามหลักวิชา

Joint Publication 3 - 12(R) Cyberspace Operations (5 Feb 2013) ได้กล่าวถึงกระบวนงานข่าวกรองไซเบอร์ ซึ่งมีส่วนสำคัญในการสนับสนุนการปฏิบัติการทางไซเบอร์ทั้งเชิงรับและเชิงรุก และเป็นการดำเนินการร่วมกันทั้งหน่วยข่าวในระดับกลาโหมและหน่วยข่าวระดับชาติทั้งภาครัฐและเอกชน เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรวดเร็วกว่าภัยคุกคามทางทหารซึ่งเป็นภัยคุกคามในรูปแบบเดิม ดังนั้นข่าวกรองที่ได้รับจากหลายภาคส่วนจะช่วยในการวิเคราะห์ ระบุสิ่งบอกเหตุ เพื่อทำให้ทราบถึงหนทางการปฏิบัติทางไซเบอร์ของฝ่ายตรงข้าม

สำหรับการปฏิบัติการด้านการข่าวในมิติของไซเบอร์นั้น เป็นการดำเนินตามวงรอบข่าวกรองเช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ ซึ่งจะดำเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ รวมทั้งการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการทางไซเบอร์เพื่อใช้ในการวางแผนสำหรับการปฏิบัติการไซเบอร์ สำหรับการปฏิบัติการข่าวในมิติทางไซเบอร์จะดำเนินการในทุกระดับชั้นของมิติทางไซเบอร์ ประกอบด้วย

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

แผนภาพที่ ๒ - ๒ การแบ่งระดับชั้นต่าง ๆ ในมิติไซเบอร์



ที่มา : Joint Publication 3-12 Cyberspace Operations, Online, 2018

กระบวนการวงรอบข่าวกรองในการปฏิบัติการไซเบอร์ ประกอบด้วย

๑. การวางแผนรวบรวมข่าวสาร

๒. การรวบรวมข่าวสาร รวมทั้งการปฏิบัติการเฝ้าตรวจและการลาดตระเวน

๓. กระบวนการประมวลผลข้อมูลและแสวงหาประโยชน์

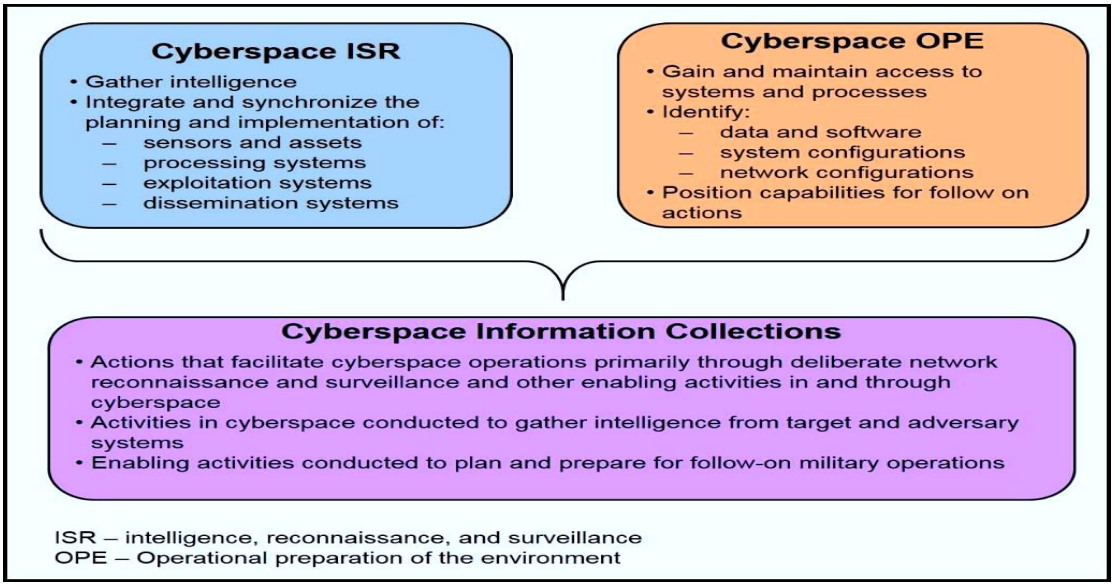
๔. การวิเคราะห์ข้อมูลและดำเนินกรรมวิธีผลิตข่าวกรอง

๕. การกระจายข่าวกรอง

๖. การประเมินผลคุณภาพและประสิทธิภาพของข่าวกรอง

United States Army War College ได้กล่าวถึง งานด้านข่าวกรองไซเบอร์ไว้ใน Strategic Cyberspace Operations Guide (1 June 2016) ซึ่งมีส่วนสำคัญในการช่วยให้เกิดการรับรู้สถานการณ์ในสภาพแวดล้อมทางไซเบอร์ของผู้บังคับบัญชาและกำลังฝ่ายเดียวกัน ช่วยให้เห็นภาพในเรื่องของภัยคุกคามและจุดอ่อนทางไซเบอร์ ขีดความสามารถทางไซเบอร์ หลักคิด หลักนิยม ยุทธวิธี และหนทางปฏิบัติของฝ่ายตรงข้าม โดยการรวบรวมข่าวสารในมิติไซเบอร์นั้นมีบทบาทสำคัญต่อการปฏิบัติการทางไซเบอร์ สำหรับการรวบรวมข่าวสารในมิติไซเบอร์ (Cyberspace Information Collections) แยกออกเป็น ๒ ส่วน คือ การข่าวกรอง การเฝ้าตรวจและลาดตระเวนทางไซเบอร์ (Cyberspace ISR) การดำเนินการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการทางไซเบอร์ (Cyberspace OPE)

แผนภาพที่ ๒ - ๓ ความสัมพันธ์ของการรวบรวมข่าวสารทางไซเบอร์กับการข่าวกรอง การเฝ้าตรวจ การลาดตระเวน และการเตรียมสภาพแวดล้อมพื้นที่ปฏิบัติการ



ที่มา : US ARMY FM 3-38, Online, 2014

Steven P. Winterfeld (December 2001) ได้กล่าวถึง กระบวนการจัดเตรียมข่าวกรองพื้นที่การรบทางไซเบอร์ (Cyber IPB) เพื่อใช้ในการปฏิบัติภารกิจของ ทบ.สหรัฐฯ ซึ่งใช้ ๔ ขั้นตอน เหมือนกับการจัดเตรียมข่าวกรองพื้นที่การรบของสงครามตามแบบ สำหรับกระบวนการจัดเตรียมข่าวกรองพื้นที่การรบทางไซเบอร์ ประกอบด้วยขั้นตอนดังนี้

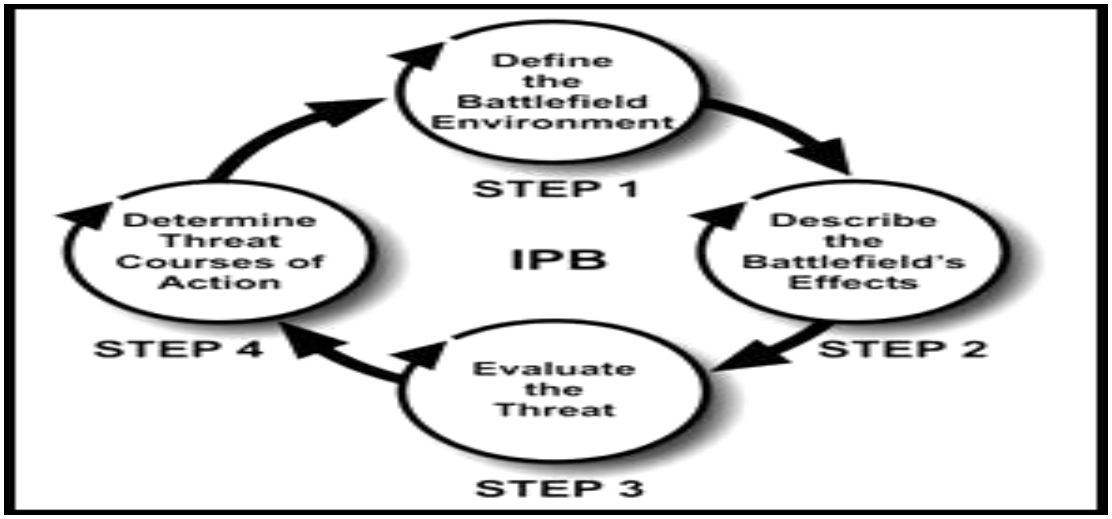
๑. การระบุสภาพแวดล้อมพื้นที่การรบทางไซเบอร์ ซึ่งมุ่งเน้นในเรื่องชนิดของเครือข่ายที่ใช้ ระบบฐานข้อมูล ระบบปฏิบัติการคอมพิวเตอร์ การเชื่อมต่อ ขีดจำกัดของระบบ และการเชื่อมต่อต่าง ๆ ช่องโหว่ของระบบฝ่ายตรงข้าม

๒. การระบุผลกระทบของพื้นที่การรบทางไซเบอร์ เป็นการวิเคราะห์ฝ่ายข้าศึกในด้านของการป้องกัน การตรวจจับ การตอบสนอง ตลอดจนการเก็บรักษาข้อมูล การให้บริการ และระบบเครือข่าย รวมทั้งมาตรการการรักษาความปลอดภัย ขั้นตอนการตรวจประเมินและการสำรองระบบ

๓. การประเมินภัยคุกคามทางไซเบอร์ เป็นการระบุที่ตั้งทางกายภาพของอุปกรณ์ทางไซเบอร์ของข้าศึก ทักษะในการออกแบบระบบ นโยบายและการรักษาความปลอดภัย กิจกรรม พื้นฐาน จุดอ่อน และขีดความสามารถในการปฏิบัติการทางไซเบอร์ของข้าศึก

๔. ระบุหนทางปฏิบัติทางไซเบอร์ของฝ่ายข้าศึก เป็นการระบุเป้าหมายและผลลัพธ์สุดท้ายที่ต้องการของฝ่ายข้าศึก โดยวิเคราะห์ออกมาเป็นหนทางที่ปฏิบัติเป็นไปได้มากที่สุดกับหนทางปฏิบัติที่อันตรายที่สุด โดยจำเป็นต้องมีการปรับปรุงตามข้อมูลที่เปลี่ยนแปลงอยู่ตลอดเวลา

แผนภาพที่ ๒ - ๔ วงรอบการจัดทำข่าวกรองพื้นที่การรบ



ที่มา : US ARMY FM 3-06, Online, 2006

การดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ

นับตั้งแต่ภัยคุกคามทางไซเบอร์ถูกประเมินให้เป็นหนึ่งในภัยคุกคามรูปใหม่ที่มีความอันตรายมากที่สุด ส่งผลให้หลายประเทศเริ่มพัฒนายุทธศาสตร์ หลักนิยม หรือแนวคิดในการรักษาความมั่นคงปลอดภัยไซเบอร์ของตนเองขึ้น ซึ่งมีประเทศที่มีการจัดทำเป็นรูปธรรมและเหมาะสมแก่การศึกษาค้นคว้า ได้แก่ สหรัฐฯ รัสเซีย เยอรมนี และสิงคโปร์ เป็นต้น

โดยสหรัฐฯ มี กห.สหรัฐฯ เป็นผู้รับผิดชอบในการพัฒนายุทธศาสตร์ด้านไซเบอร์ (Cyber Strategy) มีเป้าหมายคือสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศในทุกระดับผ่านเป้าหมายทางยุทธศาสตร์ ๕ เป้าหมาย[๑] ได้แก่

๑. การเสริมสร้างและดำรงขีดความสามารถและความพร้อมให้แก่กองทัพในการปฏิบัติการไซเบอร์

๒. การป้องกันเครือข่ายและรักษาความปลอดภัยข้อมูลต่าง ๆ ของ กห.สหรัฐฯ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นกับภารกิจ

๓. การเตรียมความพร้อมในการป้องกันมาตุภูมิ และผลประโยชน์สำคัญของสหรัฐฯ จากการถูกโจมตีทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายร้ายแรงตามมา

๔. การเสริมสร้างและดำรงขีดความสามารถทางไซเบอร์ ให้เป็นหนึ่งในทางเลือกของผู้กำหนดนโยบายหรือผู้บังคับบัญชาใช้ในการวางแผนโดยใช้ตัวเลือกดังกล่าวควบคุมสถานการณ์ความขัดแย้งและสร้างสภาวะที่ฝ่ายเราต้องการในทุกระดับ อาทิ การใช้ปฏิบัติการไซเบอร์หรือการโจมตีทางไซเบอร์ ลดขีดความสามารถของฝ่ายตรงข้ามเพื่อยับยั้งไม่ให้สถานการณ์ความขัดแย้งการปะทะหรือสงครามที่มีอยู่ขยายตัวเพิ่มมากขึ้น

๕. การเสริมสร้างและดำรงความสัมพันธ์กับประเทศพันธมิตรและประเทศหุ้นส่วนในการยับยั้งภัยคุกคามทางไซเบอร์รวมถึงเสริมสร้างความมั่นคงและเสถียรภาพระหว่างประเทศเพิ่มมากขึ้น

สำหรับรัสเซียจะแตกต่างจากประเทศอื่น ๆ โดยเรียกการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศตนเองว่า “การรักษาความมั่นคงปลอดภัยทางข้อมูลข่าวสาร (Information Security)”[๒] ซึ่งหลักนิยมในเรื่องดังกล่าวมีเนื้อหาสำคัญคือ ปกป้องผลประโยชน์ของรัสเซียในพื้นที่

---

[๑] US DOD. “The Department of Defense Cyber Strategy”. (Online). Available : http : //archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, 2015.

[๒] “Doctrine of Information Security of the Russian Federation”. (Online). Available : http : //www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, 2016.

ข้อมูลข่าวสาร (Information Sphere) ซึ่งพื้นที่ดังกล่าวรวมถึงพื้นที่ปฏิบัติการทางไซเบอร์ อินเทอร์เน็ต และระบบเครือข่ายสื่อสาร โดยใช้มาตรการต่าง ๆ เป็นเครื่องมือในการป้องกัน อาทิ หลักกฎหมาย การข่าวกรอง การต่อต้านข่าวกรอง การวิเคราะห์ข้อมูลข่าวสาร การใช้ความรู้ด้านวิทยาศาสตร์และเทคโนโลยี ฯลฯ เป็นต้น

ขณะที่การรักษาความมั่นคงปลอดภัยไซเบอร์ของเยอรมนี มีกองทัพเยอรมนี (The Bundeswehr)[๓] เป็นหน่วยงานหลักที่ดำเนินการในด้านดังกล่าว โดยมีวัตถุประสงค์คือการเสริมสร้างขีดความสามารถในการป้องกันภัยคุกคามทางไซเบอร์และดำเนินการตอบโต้เชิงรุกต่อภัยคุกคามดังกล่าวได้อย่างมีประสิทธิภาพ ผ่านการพัฒนาในองค์ประกอบหลัก ๓ ด้าน คือ

๑. ด้านบุคลากร ทำการคัดสรรบุคลากรที่มีความเชี่ยวชาญและขีดความสามารถด้านไซเบอร์เข้ามาบรรจุในหน่วยงาน และกำหนดเส้นทางการเจริญเติบโตของสายงานดังกล่าวโดยชัดเจน

๒. ด้านอุปกรณ์และเทคโนโลยี ทำการเสริมสร้างความแข็งแกร่งของระบบรักษาความปลอดภัยในเครือข่ายเทคโนโลยีสารสนเทศในทุกหน่วยของกองทัพเยอรมนี

๓. ด้านการดำเนินความสัมพันธ์ ทำการเสริมสร้างความสัมพันธ์กับสถาบันวิจัยและหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับด้านไซเบอร์ รวมถึงมิตรประเทศเพื่อแบ่งปันความรู้และสร้างพันธมิตรในการป้องกันภัยคุกคามทางไซเบอร์ร่วมกัน

ในส่วนของภูมิภาคเอเชีย ตอ./ต. สิงคโปร์นับว่าเป็นประเทศแรกที่ให้ความสำคัญในเรื่องการรักษาความมั่นคงปอดภัยไซเบอร์ โดยมีการกำหนดยุทธศาสตร์ในด้านนี้อย่างชัดเจนแบ่งเป็น ๔ เสาหลัก[๔] ได้แก่

๑. การสร้างโครงสร้างพื้นฐานด้านไซเบอร์ที่มีความยืดหยุ่น และมีความเหมาะสมสามารถรองรับการรักษาความมั่นคงปลอดภัยระบบเครือข่ายของภาครัฐและภาคประชาชนได้

๒. การสร้างพื้นที่ทางไซเบอร์ที่มีความปลอดภัย ด้วยการเฝ้าระวังและต่อสู้กับอาชญากรรมและการโจมตีทางไซเบอร์

๓. การพัฒนาระบบนิเวศด้านความมั่นคงปลอดภัยไซเบอร์ที่ดี ด้วยการร่วมมือกับสถาบันการศึกษาและบริษัทเอกชนภายในประเทศที่มีความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์มาให้การอบรมและความรู้แก่บุคลากรที่ทำงานหรือเกี่ยวข้องกับไซเบอร์ รวมถึงสนับสนุนให้บริษัทที่มีขีดความสามารถในด้านนี้พัฒนาตนเองให้เป็นหนึ่งในผู้ให้บริการในระดับโลก

๔. การกระชับความสัมพันธ์กับต่างประเทศ เนื่องจากภัยคุกคามทางไซเบอร์เป็นภัยคุกคามที่ไม่มีเส้นเขตแดน และผู้ก่อเหตุโจมตีทางไซเบอร์ได้ใช้ช่องโหว่นี้ในการแสวงประโยชน์ ดังนั้นแต่ละประเทศจึงจำเป็นต้องร่วมมือกันสร้างเสถียรภาพและความมั่นคงปลอดภัยทางไซเบอร์

---

[๓]The Federal Government of Germany. “White Paper 2016 on German Security Policy and the Future of the Bundeswehr”.(Online). Available : https://www.bundeswehr.de/resource/.../2016%20White%20Paper.pdf, 2016.

[๔]Singapore Prime Minister’s Office. “Singapore’s Cyber Security Strategy”. (Online). Available : https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf, 2016.

จากการค้นคว้าและทบทวนการดำเนินการของแต่ละประเทศที่กล่าวมาข้างต้น ผู้วิจัยเห็นว่ากลุ่มประเทศที่ทำการศึกษาจะเน้นในเรื่องการสร้างสภาวะแวดล้อมที่เกื้อกูลต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีจุดร่วมที่เหมือนกันใน ๒ ประเด็น คือ

๑. การสร้างขีดความสามารถในการเฝ้าระวังและป้องกันพื้นที่ปฏิบัติการหรือมิติทางไซเบอร์ของตนเองจากภัยคุกคามและการโจมตีทางไซเบอร์ เนื่องจากพื้นที่หรือมิติดังกล่าวเปรียบเสมือนอธิปไตยของแต่ละประเทศไม่แตกต่างไปจากพื้นที่ทางภาคพื้น พื้นที่ห้วงอากาศ และพื้นที่ทางทะเลที่ทุกประเทศสามารถใช้และแสวงประโยชน์ทั้งด้านเศรษฐกิจและความมั่นคงรวมไปถึงประโยชน์ในด้านอื่น ๆ จึงจำเป็นต้องมีการป้องกันดูแลรักษาผลประโยชน์ของชาติตนเอง

๒. การดำเนินความสัมพันธ์และขอความร่วมมือกับต่างประเทศ เนื่องจากพื้นที่ปฏิบัติการหรือห้วงมิติทางไซเบอร์ไม่มีเส้นเขตแดน ทำให้การป้องกันพื้นที่ที่เป็นผลประโยชน์ของประเทศตนเองโดยเพียงลำพังอย่างมีประสิทธิภาพเป็นไปได้ยาก ดังนั้นการแสวงหาความร่วมมือในการป้องกันภัยคุกคามด้านดังกล่าวร่วมกัน รวมถึงการแบ่งปันและแลกเปลี่ยนข้อมูลข่าวสารในเรื่องไซเบอร์ เป็นหนึ่งในแนวทางที่เหมาะสมในการรับมือกับภัยคุกคามทางไซเบอร์ ซึ่งมีลักษณะแตกต่างจากภัยคุกคามในรูปแบบเดิม

เมื่อพิจารณาจากจุดร่วมทั้ง ๒ ประเด็นแล้วยิ่งเป็นการช่วยสนับสนุนให้เห็นว่าการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต้องมีงานข่าวกรองที่เข้มแข็ง เนื่องจากทั้งการเฝ้าระวังและป้องกันภัยคุกคาม รวมถึงการดำเนินนโยบายด้านความสัมพันธ์ และการแลกเปลี่ยนข้อมูลข่าวสารและข่าวกรองกับต่างประเทศ เป็นหน้าที่และความรับผิดชอบของส่วนข่าวที่จะต้องดำเนินการ

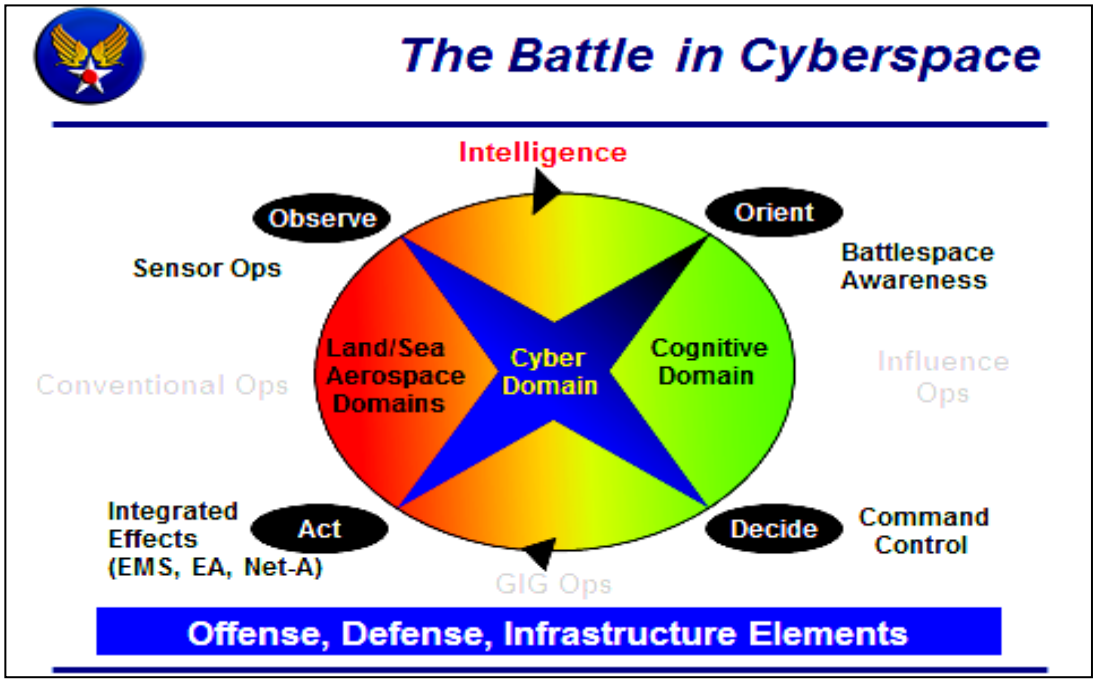
บทบาทและหน้าที่ของงานข่าวในการรับมือกับภัยคุกคามทางไซเบอร์ของต่างประเทศเพื่อนำแนวคิดมาพัฒนาเป็นตัวแบบของไทย

พล.อ.ท.โรเบิร์ต เจ เอลเดอร์ (บ็อบ เอลเดอร์) อดีต ผบ.กองทัพอากาศที่ ๘ (8th Air Force) ของสหรัฐฯ เคยบรรยายสรุปถึงบทบาทและหน้าที่ของงานข่าวกรองทางทหารในภารกิจไซเบอร์ยามทำการรบ โดยนำวงรอบ OODA LOOP[๕] ของ น.อ.จอห์น บอยด์ มาประกอบการอธิบายว่าบทบาทและหน้าที่สำคัญของงานข่าวกรองในพื้นที่ปฏิบัติการทางไซเบอร์ (Cyberspace Domain) คือการมองเห็นหรือการสังเกต (Observe) โดยใช้ระบบตรวจจับในการเฝ้าตรวจ (Sensor Ops) และการรู้ (Oriented) จากการวิเคราะห์ในสิ่งที่เห็น เพื่อสร้างการตระหนักรู้สถานการณ์ในพื้นที่การรบให้กับฝ่ายเรา (Battlespace Awareness) และผลักดันให้งานด้านยุทธการเข้าสู่การวางแผนตัดสินใจ (Decide) และลงมือปฏิบัติ (Act) ต่อไป

---

[๕] จอห์น บอยด์, นาวาอากาศเอก. “OODA LOOP (Observes Orients Decides Acts)”. เอกสารประกอบการบรรยายหลักสูตร รร.สธ.ทอ.รุ่นที่ ๖๐ บทที่ ๓ การทหาร. พ.ศ.๒๕๖๐.

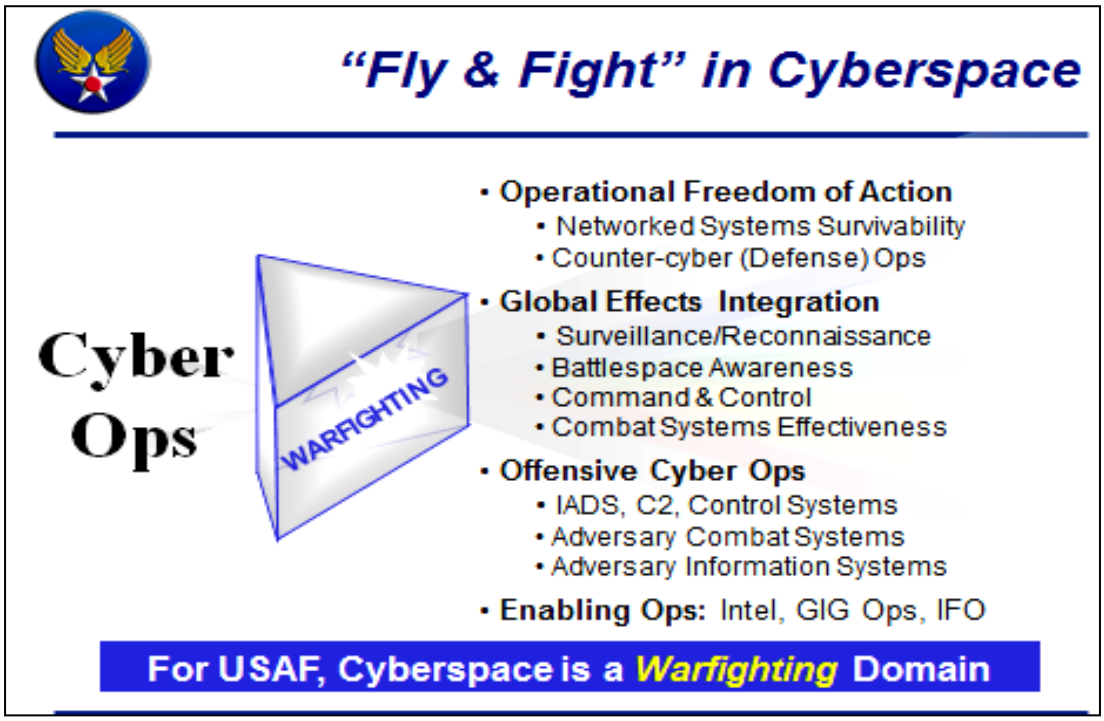
แผนภาพที่ ๒ – ๕ อธิบายถึงบทบาทและหน้าที่ของงานข่าวกรองในการทำสงครามบนพื้นที่ปฏิบัติการทางไซเบอร์



ที่มา : U.S. Air Force, Briefing Slide Presentation of the U.S.Air Force, 2007 : P.9

นอกจากนี้ งานข่าวกรองยังเป็นส่วนสำคัญที่ทำให้การปฏิบัติการไซเบอร์ของฝ่ายเรามีอิสระในการปฏิบัติ เนื่องจากช่วยให้ระบบเครือข่ายมีขีดความสามารถในการอยู่รอดเพิ่มขึ้น และด้วยขีดความสามารถในการดำเนินภารกิจการข่าวกรอง การเฝ้าตรวจและการลาดตระเวน (Intelligence Surveillance and Reconnaissance : ISR) ทั้งในพื้นที่ห้วงอากาศและพื้นที่ปฏิบัติการทางไซเบอร์จะทำให้ฝ่ายเรามีความตระหนักรู้สถานการณ์ทราบถึงภัยคุกคามที่จะเกิดขึ้นโดยเฉพาะในห้วงมิติไซเบอร์นั้น เหตุที่เกิดขึ้นจากอีกจุดหนึ่งของโลกจะส่งผลกระทบไปยังส่วนอื่น ๆ ของโลกอย่างรวดเร็ว ขณะที่การปฏิบัติการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามด้วยการโจมตีไซเบอร์นั้น งานข่าวกรองมีบทบาทสำคัญในการค้นคว้าข้อมูลและวิเคราะห์เกี่ยวกับจุดล่อแหลมของฝ่ายตรงข้าม (Critical Vulnerabilities : CV) เพื่อให้ส่วนยุทธการดำเนินการวางแผนโจมตีต่อจุดล่อแหลมดังกล่าวต่อไป

แผนภาพที่ ๒ - ๖ อธิบายให้เห็นถึงภารกิจต่าง ๆ ในพื้นที่ปฏิบัติการทางไซเบอร์ โดยงานข่าวกรองถือเป็นหนึ่งในขีดความสามารถที่สนับสนุนและเกื้อกูลให้ภารกิจต่าง ๆ ประสบความสำเร็จ

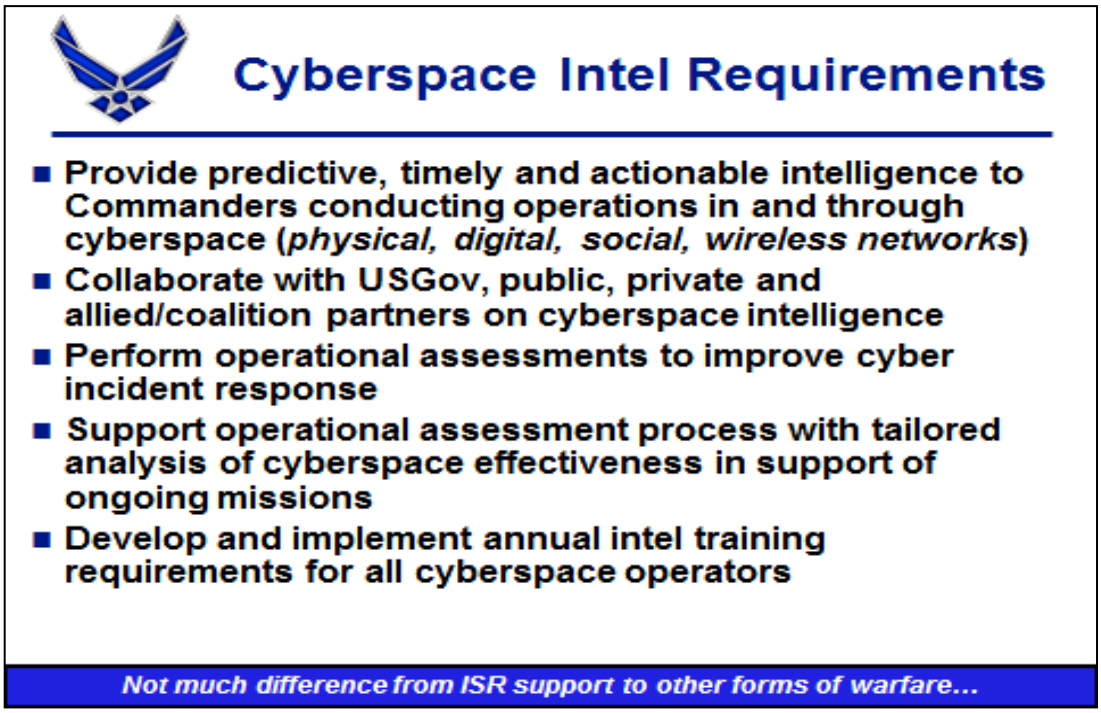


ที่มา : U.S. Air Force, Briefing Slide Presentation of the U.S.Air Force, 2007 : P.10

ด้าน น.อ.มาร์ค ครอสส์ ผบ.หน่วย 26th Network Operations Group ของ ทอ.สหรัฐฯ ได้บรรยายและให้แนวคิดงานข่าวกรองในภารกิจป้องกันเครือข่ายและการปฏิบัติการอื่น ๆ บนพื้นที่ปฏิบัติการทางไซเบอร์ ว่างานข่าวกรองและภารกิจ ISR ในพื้นที่ปฏิบัติการทางไซเบอร์ ไม่ได้มีความแตกต่างไปจากพื้นที่ปฏิบัติการอื่น ๆ โดยยังมีหน้าที่ในการให้ข้อมูลข่าวกรอง รวมถึงวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามแก่ ผบช.ในการตัดสินตกลงใจในการดำเนินภารกิจหรือการปฏิบัติการใด ๆ ได้อย่างทันเวลา รวมถึงทำการประเมินผลการโจมตีของฝ่ายเราต่อข้าศึก เพื่อสนับสนุนให้การดำเนินภารกิจเป็นไปอย่างต่อเนื่อง และสามารถตอบสนองต่อสถานการณ์ที่เกิดขึ้นได้อย่างรวดเร็ว

ทั้งนี้ ผู้วิจัยเห็นว่าแนวคิดงานข่าวกรองจากผู้ชำนาญการทางด้านไซเบอร์ทั้ง ๒ คน ของ ทอ.สหรัฐฯ ตั้งอยู่บนพื้นฐานของบทบาทและหน้าที่ของส่วนข่าว หรือ ฝสธ.๒ ที่ดำเนินการในพื้นที่ปฏิบัติการปกติอยู่แล้ว อาทิ การสร้างการตระหนักรู้สถานการณ์ การแจ้งเตือน การวิเคราะห์หนทางปฏิบัติของข้าศึก การสนับสนุนข้อมูลที่ส่วนยุทธการและ ผบช.ต้องการเพื่อนำไปใช้ประกอบการตัดสินตกลงใจ ฯลฯ แต่สิ่งหนึ่งที่แตกต่างจากการปฏิบัติการในพื้นที่อื่น ๆ คือพื้นที่ปฏิบัติทางไซเบอร์มีสภาพแวดล้อมและอาณาเขตแดนที่ไม่ชัดเจน

แผนภาพที่ ๒ - ๗ อธิบายให้เห็นถึงความต้องการงานด้านข่าวกรองในพื้นที่ปฏิบัติการทางไซเบอร์



ที่มา : Colonel Mark Kross, Briefing Slide Presentation of the U.S.Air Force, 2007 : P.20

ขณะที่การตอบโต้เชิงรับและการตอบโต้เชิงรุกนั้นจะต้องเฝ้าระวังฝ่ายตรงข้าม และดำเนินการโจมตีฝ่ายตรงข้ามด้วยอาวุธที่ไม่มีความร้ายแรงหรือจำพวกเครื่องกระสุน (Non-Lethal Weapon) ที่จำเป็นต้องใช้บุคลากรที่มีความเชี่ยวชาญและความเข้าใจเฉพาะด้านมาปฏิบัติงานด้านการข่าว ซึ่งในส่วนของ สหรัฐฯ มีขีดความสามารถที่จะคัดเลือกและพัฒนากำลังพลให้สามารถดำเนินงานข่าวกรองไซเบอร์ได้เพียงพอต่อการดำเนินภารกิจ ขณะที่ไทยยังคงมีความจำเป็นเป็นอย่างยิ่งที่จะต้องหาองค์ความรู้ในเรื่องดังกล่าว นำมาพัฒนาบุคลากรให้มีขีดความสามารถเสียก่อน

เอกสารวิชาการเรื่อง "Intelligence Preparation of the Cyber Environment" ของนาย Rob Dartnall ผอ.ข่าวกรองไซเบอร์ของสถาบัน SANS ซึ่งเป็นสถาบันการศึกษาและวิจัยด้านความมั่นคงปลอดภัยระดับโลก ได้ระบุข้อเสนอแนะเกี่ยวกับความจำเป็น หน้าที่และขีดความสามารถของงานข่าวกรองไซเบอร์ที่ชัดเจน โดยนำรูปแบบของงานข่าวกรองตามรูปแบบปกติ (Conventional Intelligence) มาใช้ในกระบวนการกำหนดหารูปแบบข่าวกรองที่เหมาะสมต่อการปฏิบัติในพื้นที่ปฏิบัติการทางไซเบอร์ ได้แก่

๑. การเข้าใจหลักและพื้นฐานของงานด้านการข่าว รวมถึงศึกษาหลักพิชัยสงครามของ ซุนวู (“รู้เขา รู้เรา รบร้อยครั้ง ชนะร้อยครั้ง”)

๒. การวิเคราะห์สภาพแวดล้อมพื้นฐานที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (PESTLE-M : การเมือง เศรษฐกิจ สังคมจิตวิทยา เทคโนโลยี ตัวบทกฎหมาย สภาพแวดล้อมทางกายภาพ และการทหาร)

๓. กระบวนการวิเคราะห์อย่างเป็นเหตุเป็นผล เพื่อลดอคติ (BIAS) ในการวิเคราะห์ข่าวกรอง

๔. เครื่องมือและวิธีการที่ช่วยในการวิเคราะห์ เพื่อวิเคราะห์หนทางปฏิบัติของข้าศึก อาทิ เทคนิคการวิเคราะห์เครือข่าย (Network Analysis) เทคนิคการวิเคราะห์รูปแบบการปฏิบัติการของภัยคุกคาม (Pattern Analysis) และเทคนิคการวิเคราะห์ห้วงเวลาในการดำเนินการของภัยคุกคาม (Timeline Analysis)

๕. การจำลองสถานการณ์สมมติด้านการข่าว เพื่อฝึกและทำความเข้าใจเกี่ยวกับข้าศึกและตัวภัยคุกคาม

พร้อมกับระบุว่าหน้าที่หลักของงานข่าวกรอง คือ การแจ้งเตือนภัยล่วงหน้า การวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้าม และผลผลิตหลักที่เป็นหัวใจสำคัญ คือ การเตรียมข่าวกรองของสนามรบ (Intelligence Preparation of Battlefield : IPB) ซึ่งเป็นการศึกษาและทำความเข้าใจกับสภาพแวดล้อมของสนามรบหรือพื้นที่ปฏิบัติการ การรู้ขีดความสามารถของฝ่ายเราและฝ่ายตรงข้าม แต่ในพื้นที่ปฏิบัติการทางไซเบอร์จะมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ คือไม่มีพื้นที่อาณาเขตชัดเจน รูปแบบของภัยคุกคามที่อาจไม่ได้มาจากข้าศึกโดยตรง เป็นต้น ดังนั้น นาย Rob Dartnall จึงพัฒนาการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) ขึ้น โดยใช้แนวทางเดียวกับการพัฒนา IPB แต่แตกต่างกันในบริบทของสภาพแวดล้อม คือ

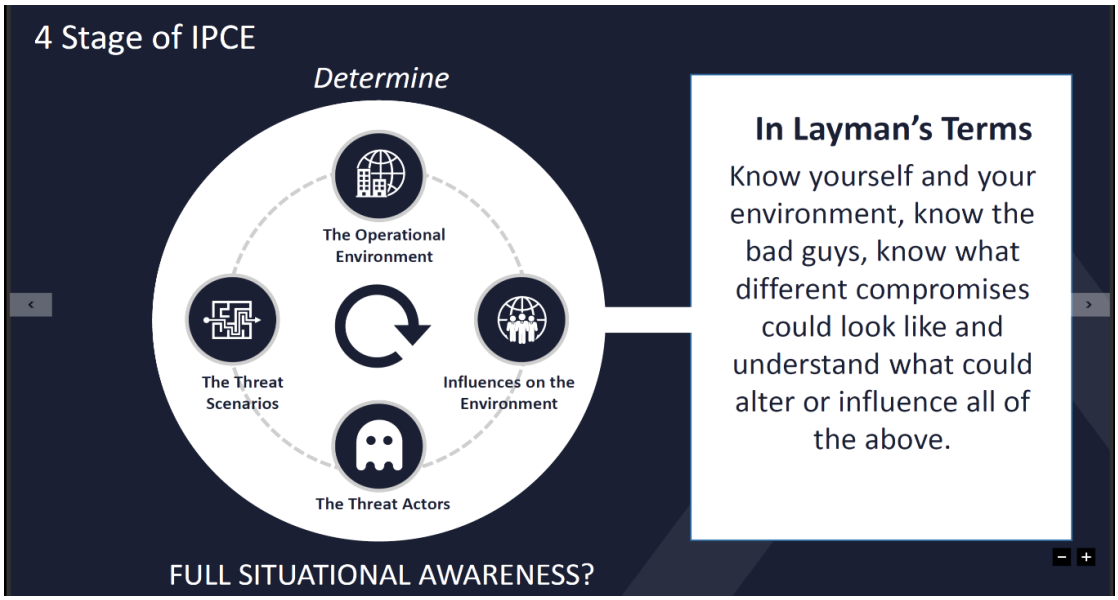
๑. การระบุสภาพแวดล้อมของการปฏิบัติการ (Determine The Operational Environment) คือ รู้สภาพแวดล้อมและพื้นที่ปฏิบัติการภายในเครือข่ายของฝ่ายเรา และสภาพแวดล้อมเครือข่ายภายนอกที่มีความเกี่ยวข้องกับเครือข่ายของฝ่ายเรา

๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ (Determine Influences on the Environment) คือ การนำหลัก PMESII-PT และ PESTLE-M มาวิเคราะห์สิ่งที่จะเป็นผลกระทบต่อการปฏิบัติของฝ่ายเรา

๓. การระบุตัวภัยคุกคาม (Determine the Threat Actors) คือ การระบุได้ว่าภัยคุกคามคือใคร ภัยคุกคามนั้นได้รับการสนับสนุนจากใคร มีกระบวนการการโจมตีหรือคุกคามอย่างไร มีวัตถุประสงค์ในการกระทำเพื่ออะไร และจะปฏิบัติการอีกเมื่อไหร่ เป็นต้น

๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม (Determine the Threat Scenarios) คือ การเข้าใจถึงหลักนิยม เทคนิค กลยุทธ์ และกระบวนการโจมตีของภัยคุกคาม และสามารถวิเคราะห์ได้ถึงหนทางปฏิบัติที่ภัยคุกคามอาจโจมตีฝ่ายเราได้

แผนภาพที่ ๒ - ๘ อธิบายถึงวงรอบการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ ๔ ขั้นตอน (4 Stage of Intelligence Preparation of the Cyber Environment)



ที่มา : Rob Dartnall Director, Briefing Slide Presentation of the Cyber Intelligence of Bank of England, 2017

ทั้งนี้งานข่าวกรองไม่ว่าจะอยู่บนพื้นฐานของมิติหรือพื้นที่ปฏิบัติการใด จะมีหน้าที่และความรับผิดชอบหลักคือ การแจ้งเตือนเพื่อสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเรา การวิเคราะห์หนทางปฏิบัติของภัยคุกคาม และผลผลิตพื้นฐานที่สำคัญคือ การเตรียมข่าวกรองของสภาพแวดล้อมปฏิบัติการในมิติต่าง ๆ ซึ่งช่วยสนับสนุนการวางแผนและงานยุทธการของฝ่ายเรา รวมถึงสนับสนุนการตัดสินตกลงใจของผู้บังคับบัญชาหรือผู้กำหนดนโยบาย ดังนั้น หน้าที่และความรับผิดชอบของข่าวกรองในห้วงมิติและพื้นที่ปฏิบัติการทางไซเบอร์ก็ไม่ได้แตกต่างไปจากแนวคิดดังกล่าวเช่นกัน

ผลงานวิจัยที่เกี่ยวข้อง

นาย Jay Mcallister[๖] ได้ทำการศึกษาเรื่องการประยุกต์กระบวนการคิดเชิงวิพากษ์ เพื่อนำมาใช้กับงานข่าวกรองไซเบอร์ สรุปว่านักวิเคราะห์ในทุกระดับควรอุทิศเวลาให้กับการพัฒนาวิธีการคิดโดยการลงลึกไปถึงกระบวนการทำงานของจิตใจมนุษย์ เพื่อปรับปรุงทักษะการวิเคราะห์ ซึ่งผู้วิจัยพบว่าหลักวิธีเช่นนี้ไม่ต่างกับการวิเคราะห์ข่าวกรองชนิดอื่น ๆ

นาย Robert M. Lee[๗] ทำการศึกษางานข่าวกรองไซเบอร์เพื่อบรรยายในหลักสูตรบัณฑิตศึกษาด้านความมั่นคงและปลอดภัยทางไซเบอร์ สรุปว่าขั้นตอนแรกในการเข้าใจงานข่าวกรองไซเบอร์ คือการเข้าใจวงรอบข่าวกรองทั้งในด้านยุทธวิธี เทคนิค และขั้นตอนการปฏิบัติ ซึ่งการดำเนินการข่าวกรองประเภทต่าง ๆ มีอยู่นานก่อนที่จะเกิดงานข่าวกรองไซเบอร์ โดยเฉพาะด้านการตัดสินตกลงใจทางทหารที่ผู้บังคับบัญชา ต้องการทราบเจตนารมณ์ของฝ่ายตรงข้ามเพื่อเลือกยุทธศาสตร์ที่ดีกว่าในสนามรบหรือเตรียมตัวให้พร้อมสำหรับการโจมตี รวมถึงการป้องกันอย่างเหมาะสม เพราะฉะนั้นการเริ่มศึกษาข่าวกรองไซเบอร์สามารถเริ่มได้จากการศึกษาแนวทางข่าวกรองทหาร

เครือข่าย Intelligence and National Security Alliance ระบุว่า ข่าวกรองไซเบอร์คือการประเมินขีดความสามารถ เจตนารมณ์ และกิจกรรมของข้าศึก ในห้วงมิติทางไซเบอร์ (Cyber Domain) เพื่อสนับสนุนการแจ้งเตือน การโจมตี และการป้องกันภัยคุกคาม ซึ่งเป็นผลผลิตที่ได้จากการดำเนินวงรอบข่าวกรองโดยมีขีดความสามารถที่จำเป็น ได้แก่

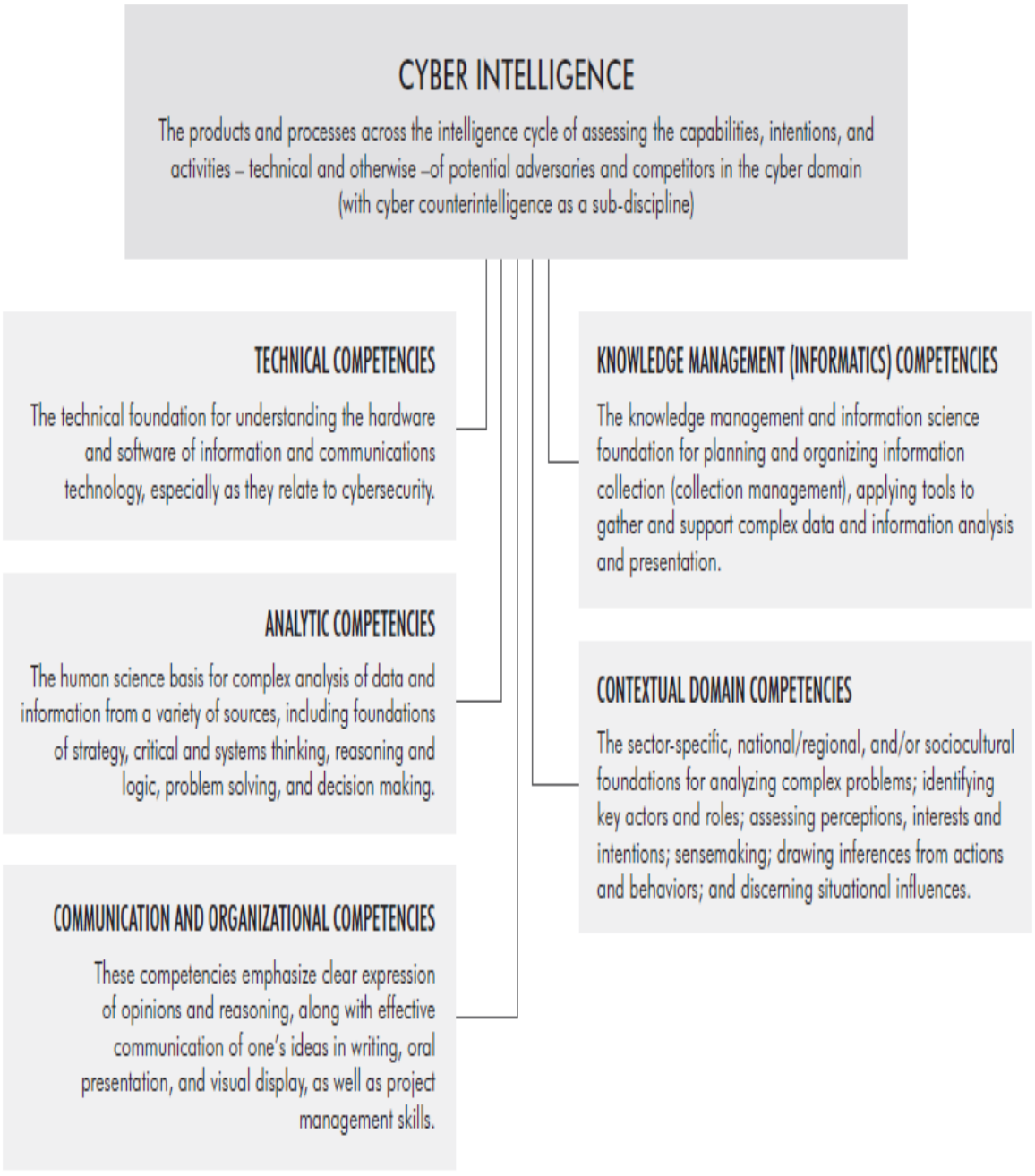
๑. ความเข้าใจในเรื่องของระบบฮาร์ดแวร์ ซอฟท์แวร์ ระบบสารสนเทศและการสื่อสาร
๒. ทักษะการคิดวิเคราะห์
๓. การนำเสนอ รายงาน ให้ความเห็นที่เป็นเหตุเป็นผล
๔. การบริหารจัดการวางแผนรวบรวมข้อมูลข่าวกรอง
๕. ความเข้าใจในภารกิจ และบริบทของหน่วยงาน เช่น ผู้แสดงหลัก กลุ่มผลประโยชน์

---

[๖]Jay McAllister. Senior Analyst. “Emerging Technology Center”. (Online). Available. : Https : //www.Insights.Sei.Cmu.Edu/Sei_Blog/2016/02/Cyber-Intelligence-And-Critical-Thinking. Html, 2016.

[๗]Robert M. Lee. Adjunct Lecturer. “Utica College”. (Online). Available. : https : //www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/, 2014.

แผนภาพที่ ๒ - ๙ ขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์



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

แผนภาพที่ ๒ - ๑๐ บทบาทหน้าที่ของข่าวกรองไซเบอร์ในระดับต่าง ๆ

STRATEGIC CYBER INTELLIGENCE

- Produced for senior executive leadership; C-Suite and equivalent in both private and public sectors.
- Used to inform organizational/national strategy and policy development that will direct enterprise over the long term (3+ years).
- Collected broadly within sector to which organization belongs and likely includes complementary sectors.
- Focused broadly on threat vectors and adversaries and on contextual political, economic, and social trends. Includes understanding of state and non-state threat actors' interests, policies, doctrines, and concepts of operations.
- Generally nontechnical in nature, focused on trend analysis across and between sectors, stated and unstated objectives of state and non-state actors, and other strategic indicators.

OPERATIONAL CYBER INTELLIGENCE

- Produced for executive managers in IT and security such as the CIO and CISO, as well as other management team members (e.g., public affairs, human resources, legal)
- Used to inform risk-based decisions about resource allocation and activity to maintain business continuity and prevent disruption.
- Collected with an emphasis on enterprises' operations, to include partners, suppliers, competitors, customers and other trusted relationships.
- Focus on targeted, opportunistic, and persistent threat vectors that pose greatest risk to business continuity.
- Blends technical and nontechnical collection to explore and prioritize threats, the mechanisms and signatures of potential attacks, and organizational vulnerabilities.

TACTICAL CYBER INTELLIGENCE

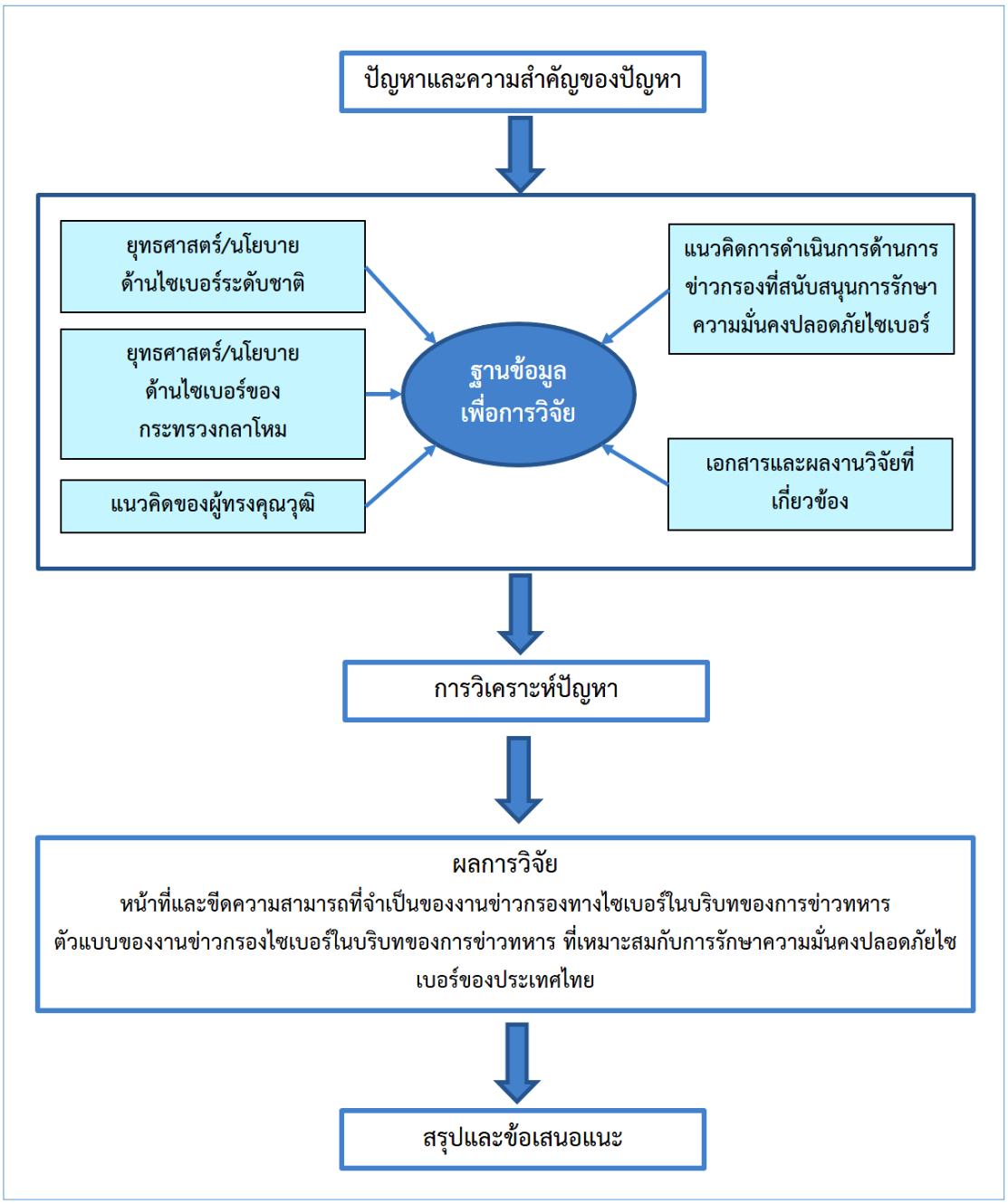
- Produced for incident response teams.
- Used to restore operations quickly and collect cyber forensic evidence following a cyber attack or intrusion.
- Collected with internal emphasis on organization, including personnel, assets and networks.
- Focused on understanding and analyzing an adversary's use of technical/logical tactics, techniques and procedures (TTP) to target the organization.
- Generally more technical in nature (e.g., exploits and malware, delivery mechanisms, technical/logical artifacts of an attack)

ที่มา : SANS Institute, Online, 2017

แผนภาพที่ ๒ – ๑๑ ขีดความสามารถและทักษะที่จำเป็นของนักวิเคราะห์ข่าวกรองทางไซเบอร์

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

กรอบแนวคิดของการวิจัย



สรุป

จากการศึกษา ค้นคว้า และทบทวนวรรณกรรมที่เกี่ยวข้องกับการวิจัย ทั้งของประเทศไทยและต่างประเทศในบทที่ ๒ ทำให้ผู้วิจัยเข้าใจภาพขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ประเทศไทยต้องการ และเห็นร่างตัวแบบข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหารในการป้องกันและรับมือกับภัยคุกคามดังกล่าว โดยสิ่งที่กรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี และนโยบายด้านความมั่นคงแห่งชาติกำหนดความต้องการในการป้องกันและรับมือกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ คือ การสร้างขีดความสามารถในการเฝ้าระวังและป้องกันพื้นที่ปฏิบัติการหรือมิติดังกล่าว ไม่ให้ถูกคุกคามหรือถูกโจมตี ซึ่งหน้าที่ในการเฝ้าระวังและสร้างความตระหนักรู้สถานการณ์ ถือเป็นงานในบริบทของข่าวในทุกพื้นที่ปฏิบัติการหรือทุกมิติอยู่แล้ว

ทั้งนี้ การที่งานด้านการข่าวจะสามารถทำการเฝ้าระวัง และสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเราทราบก่อนที่ภัยคุกคามต่าง ๆ จะทำการโจมตีนั้น จำเป็นต้องทราบและสามารถระบุสภาพแวดล้อมของการปฏิบัติการให้ได้ก่อน และเมื่อทราบถึงคุณลักษณะสำคัญและผลกระทบของสภาพแวดล้อมการปฏิบัติการที่มีต่อฝ่ายเราแล้ว งานด้านการข่าวจะทราบว่าภัยคุกคามหรือศัตรูของฝ่ายเรานั้นคือใคร มีจุดมุ่งหมายอะไร มีขีดความสามารถ และมีหนทางปฏิบัติอย่างไร ดังนั้น การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) นับเป็นตัวแบบที่เหมาะสมต่อการศึกษา ที่จะช่วยให้การพัฒนาข่าวกรองไซเบอร์ในบริบทของการข่าวทหารเกิดความสมบูรณ์ในขั้นต่อไป ประกอบด้วย

๑. เรื่องของภัยคุกคาม (Threat) สามารถระบุ และตรวจสอบได้ว่าภัยคุกคามคือใคร ทราบถึงขีดความและหนทางปฏิบัติของภัยคุกคาม

๒. การรวบรวมข่าวสาร (Collection) เมื่อเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (IPCE) แล้ว จะทำให้ทราบว่ายังขาดข้อมูลข่าวสาร/ข่าวกรองใด ที่กระทบต่อการวิเคราะห์ภัยคุกคาม และทำให้สามารถรวบรวมข้อมูลข่าวสาร/ข่าวกรองในพื้นที่ปฏิบัติการได้อย่างเหมาะสม

๓. การกำหนดเป้าหมาย (Targeting) เมื่อทราบถึงคุณลักษณะสำคัญของสภาพแวดล้อมการปฏิบัติการและภัยคุกคามแล้ว จะทำให้การกำหนดเป้าหมายเพื่อตอบโต้ภัยคุกคามที่ทำการโจมตีฝ่ายเรานั้น ทำได้ง่ายขึ้น และตรงตามเจตนารมณ์ของผู้บังคับบัญชา

บทที่ ๓
การวิเคราะห์ข้อมูล

จากการเก็บรวบรวมข้อมูลทั้งจากแหล่งข้อมูลปฐมภูมิ โดยการสัมภาษณ์ และข้อมูลทุติยภูมิที่รวบรวมได้จากบทความ ตำราวิชาการ งานวิจัย และเอกสารที่เกี่ยวข้อง ในบทนี้ผู้วิจัยจะนำข้อมูลดังกล่าวมาวิเคราะห์โดยใช้หลักการของเหตุผลในเชิงตรรกวิทยาตามกรอบแนวคิด ดังประเด็นต่อไปนี้

ศึกษาแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ และบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน

๑. แนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ

จากการศึกษาเอกสารและตำราทางวิชาการ ประกอบกับการติดตามข่าวสารเกี่ยวกับแนวทางการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามยุทธศาสตร์และนโยบายระดับชาติ พบว่า ยุทธศาสตร์และนโยบายระดับชาติมีเนื้อหามุ่งเน้นการพัฒนาศักยภาพในการป้องกันประเทศให้พร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่น ๆ โดยให้ความสำคัญกับการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ เพื่อปกป้องโครงสร้างพื้นฐานหรือสาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ให้ปลอดภัยจากการโจมตี ทั้งนี้ ยุทธศาสตร์ป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๗๙ ซึ่งเป็นกรอบแนวทางการดำเนินงานด้านการป้องกันประเทศให้สอดรับกับยุทธศาสตร์และนโยบายระดับชาติ ได้กำหนดประเด็นยุทธศาสตร์การปฏิบัติการทางทหารเพื่อรักษาอธิปไตยและผลประโยชน์แห่งชาติที่มุ่งเน้นการเสริมสร้างศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ ด้วยการพัฒนากำลังพล โครงสร้างพื้นฐาน และเทคโนโลยีให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ สร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วนและสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ

ปัจจุบันประเทศไทยมีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ๒ แห่ง คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Thailand Computer Emergency Response Team : ThaiCERT) ในการกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ซึ่งมีภาระหน้าที่หลักในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้การสนับสนุนที่จำเป็น

และให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต และศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต) (Government Computer Emergency And Readiness Team : G-CERT) ในการกำกับดูแลของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ รวมทั้งการสร้างเครือข่ายพันธมิตรเพื่อให้เกิดความมั่นคงปลอดภัยและช่วยลดความเสี่ยงต่อการเกิดอาชญากรรมทางคอมพิวเตอร์ นอกจากนี้ยังมีการปรับปรุงกลไกการบังคับใช้กฎหมายให้สามารถลดภัยคุกคาม ที่มีต่อความมั่นคงทางไซเบอร์ อาทิ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ ๒ พ.ศ.๒๕๖๐ และเสนอร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดให้มีหน่วยงานหลักในการรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และทำการบูรณาการและประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องเรียกว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Committee : NCSC) เรียกโดยย่อว่า “กปช.” (ปัจจุบันอยู่ระหว่างการรับฟังความคิดเห็นร่าง พ.ร.บ.ฯ)

คณะรัฐมนตรีได้เห็นชอบในหลักการให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จัดทำระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ ประกาศใช้เมื่อวันที่ ๑๘ ตุลาคม ๒๕๖๐ สำหรับใช้บังคับในระหว่างการจัดทำร่าง พ.ร.บ.ฯ มีวัตถุประสงค์เพื่อใช้ระเบียบนี้เป็นเครื่องมือสำคัญอย่างหนึ่งที่จะช่วยในการปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ของประเทศไทย ทำให้ประชาชนและประเทศไทยมีความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีดิจิทัล โดยในระเบียบฯ ดังกล่าว ได้กำหนดให้มีคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีอำนาจหน้าที่สำคัญในการจัดทำนโยบายและแผนระดับชาติ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนการเตรียมการจัดตั้ง สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งคณะกรรมการเตรียมการไซเบอร์แห่งชาติ ได้จัดประชุมคณะเตรียมการด้านการรักษาความปลอดภัยมั่นคงไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๑ เมื่อวันที่ ๙ พฤษภาคม ๒๕๖๑ เวลา ๑๔.๐๐ น. ณ ตึกภักดีบดินทร์ ทำเนียบรัฐบาล โดยมี พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานฯ ซึ่งการจัดประชุมครั้งนี้มีสาระสำคัญของการประชุม ซึ่งถือเป็นทิศทางและกรอบแนวทางในการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยใน ๔ ประเด็น คือ

๑. การกำหนดกรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงและความสอดคล้องไปในทิศทางเดียวกัน

๒. วางแนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศ และแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure : SOP)

๓. แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน

๔. แนวทางการจัดตั้ง Cybersecurity Agency (CSA) ทำหน้าที่หน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความปลอดภัยมั่นคงไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

ด้านการแปลงนโยบายสู่การปฏิบัติ ปัจจุบันกระทรวงกลาโหมได้ขับเคลื่อนปฏิรูปกองทัพด้านไซเบอร์ต่อเนื่องตลอด ๓ ปีที่ผ่านมา ให้สอดรับกับยุทธศาสตร์ชาติ (ด้านความมั่นคง) และยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม โดยได้จัดทำแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม (ปี ๒๕๖๐ – ๒๕๖๔) และกำหนดให้ไซเบอร์เป็นมิติหนึ่งของสงครามที่ต้องจัดเตรียมกำลังและใช้กำลัง เช่นเดียวกับมิติของการสงครามอื่น ๆ มีการนำนโยบายมาสู่การปฏิบัติโดยการจัดตั้งศูนย์ไซเบอร์กระทรวงกลาโหม และหน่วยไซเบอร์ระดับปฏิบัติการของแต่ละเหล่าทัพ ซึ่งอยู่ระหว่างการเสริมสร้างศักยภาพและขีดความสามารถการปฏิบัติทั้งด้านนโยบายและ แผน ด้านกำลังพล ด้านการปฏิบัติการ ด้านเทคโนโลยีและการวิจัยพัฒนา รวมทั้งโครงสร้างพื้นฐานและเทคโนโลยีให้พร้อมในการปฏิบัติ ขณะเดียวกันก็ได้ให้ความสำคัญกับการผนึกกำลังด้านไซเบอร์โดยระยะแรกได้มุ่งเน้นการพัฒนาขีดความสามารถเชิงรับ เช่น ด้านการป้องกันโครงสร้างพื้นฐานและด้านการเฝ้าระวัง ซึ่งแต่ละเหล่าทัพได้จัดตั้งโรงเรียนและเปิดสอนผู้ปฏิบัติงานไซเบอร์ระดับต่าง ๆ ควบคู่กับการฝึกปฏิบัติการ สำหรับการผนึกกำลังด้านไซเบอร์ได้กำหนดเป้าหมายให้มีกำลังพลสำรองไซเบอร์ พร้อมทั้งขยายความร่วมมือและผนึกกำลังกับหน่วยงานทั้งภายในประเทศและต่างประเทศ เช่น การฝึกไซเบอร์ในการฝึกร่วมหรือผสมทางทหาร โดยการปฏิรูปกองทัพด้านไซเบอร์จะเป็นส่วนสำคัญให้กองทัพมีความพร้อมและมีขีดความสามารถในการรับมือกับการโจมตีและการคุกคามทางไซเบอร์ ซึ่งสามารถพัฒนาไปสู่การทำสงครามไซเบอร์ได้ในอนาคต ซึ่งหากขาดการผนึกกำลังด้านไซเบอร์ร่วมกันโดยกองทัพไม่เตรียมความพร้อมและภาคประชาชนไม่ตระหนักรู้และตื่นตัวในทิศทางเดียวกัน สงครามไซเบอร์จะกระทบต่อความมั่นคงและผลประโยชน์ชาติอย่างใหญ่หลวง

สรุปทิศทางการพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามกรอบยุทธศาสตร์ชาติและยุทธศาสตร์ป้องกันประเทศ จะมุ่งประเด็นไปที่การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ เพื่อปกป้องโครงสร้างพื้นฐานหรือสาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ให้ปลอดภัยจากการโจมตี และมุ่งเน้นการเสริมสร้างศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ด้วยการพัฒนากำลังพล โครงสร้างพื้นฐาน และเทคโนโลยีให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ สร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ ส่วนทิศทางการขับเคลื่อนยุทธศาสตร์และนโยบายของภาครัฐคือ การกำหนดนโยบายและแผนระดับชาติสู่การปฏิบัติที่มีความสอดคล้องในทุกภาคส่วนเป็นไปในทิศทางเดียวกัน การสร้างความเข้มแข็ง

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ CII การพัฒนากำลังคนเพื่อรับมือภัยคุกคามไซเบอร์อย่างพอเพียงทั้งหน่วยงานภาครัฐและเอกชน และการจัดตั้งหน่วยงานกลาง Cyber Security Agency เพื่อเป็นหน่วยเผชิญเหตุและรับมือภัยคุกคามไซเบอร์ทุกรูปแบบ ทั้งนี้การวิเคราะห์การดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการทหารตามยุทธศาสตร์และนโยบายระดับชาติ พบว่า กระทรวงกลาโหม กองทัพไทย และเหล่าทัพยังอยู่ในช่วงของการเสริมสร้างและพัฒนาขีดความสามารถในการปฏิบัติการด้านไซเบอร์ โดยการจัดตั้งศูนย์ไซเบอร์กระทรวงกลาโหม และหน่วยไซเบอร์ระดับปฏิบัติการของแต่ละเหล่าทัพที่มุ่งเน้นการผนึกกำลังป้องกันภัยคุกคามทางไซเบอร์ร่วมกันในอนาคต

๒. สำหรับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน ผู้วิจัยได้รวบรวมข้อมูลโดยการสัมภาษณ์กลุ่มประชากร ดังนี้

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
๑.	ผู้อำนวยการศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและ อวกาศ กระทรวงกลาโหม (พล.ต.เสรี คณธมาลัย)	กระทรวงกลาโหม มีบทบาทสำคัญในการให้การสนับสนุนการดำเนินการตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ - ๒๕๖๔ ซึ่งกำหนดบทบาทหน้าที่ให้กองทัพดูแลรับผิดชอบการป้องกันประเทศในมิติทางไซเบอร์ และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับมอบหมายจากรัฐบาล โดยเฉพาะเมื่อเกิดสถานการณ์วิกฤตทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์ สำหรับศูนย์ไซเบอร์ฯ สำนักงานปลัดกระทรวงกลาโหม เป็นหน่วยงานที่ดำเนินการในเชิงนโยบาย ซึ่งจะกำหนดยุทธศาสตร์เพื่อใช้เป็นแนวทางงานด้านไซเบอร์ของกระทรวงกลาโหมให้กับหน่วยงานภายในกระทรวงกลาโหม โดยในห้วงที่ผ่านมาได้มีการดำเนินการด้านไซเบอร์ที่สำคัญของ กห. อาทิ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์ เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๘ แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ - ๒๕๖๔ มีการจัดตั้งหน่วยงานในลักษณะศูนย์ไซเบอร์ เพื่อเป็นหน่วยรับผิดชอบหลักด้านไซเบอร์ ซึ่งในส่วนของศูนย์ไซเบอร์ของกลาโหมนั้น จะมีหน้าที่ดูแลความปลอดภัยและเฝ้าระวังเครือข่ายของกลาโหมและในส่วนที่มี

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหาร ที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		การเชื่อมต่อไปยัง บก.ทท.และเหล่าทัพ นอกจากนั้นแล้วยังมีความร่วมมือด้านไซเบอร์กับหน่วยงานที่เกี่ยวข้องทั้งในประเทศและกระทรวงกลาโหมมิตรประเทศ นอกจากนี้ ยังมีการดำเนินงานในรูปของคณะกรรมการ ซึ่งมีเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศ กระทรวงกลาโหม เป็นประธานคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม ซึ่งมีหน้าที่ในการขับเคลื่อนงานด้านไซเบอร์ในระดับกระทรวง และเป็นส่วนหนึ่งของ คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม สำหรับงานข่าวกรองไซเบอร์ ปัจจุบันศูนย์ไซเบอร์กระทรวงกลาโหมมุ่งเน้นการพัฒนางานข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) โดยนำมาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคคล/กลุ่มบุคคลที่เฝ้าระวังทั้งภายในและภายนอกประเทศ และส่งเสริมให้เกิดการเชื่อมโยงระบบกับกองทัพไทย และเหล่าทัพ เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามและระวังป้องกันภัยร่วมกัน
๒.	ผู้อำนวยการศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย (พล.ต.ชาติชาย ชัยเกษม)	การปฏิบัติการในมิติไซเบอร์ของกองทัพไทย ถือเป็นการปฏิบัติการทางทหารอย่างหนึ่งเพื่อรับมือกับภัยคุกคามรูปแบบใหม่ ซึ่งมีความสอดคล้องกับหน้าที่ของกองทัพไทย ในการเตรียมกำลังการป้องกันราชอาณาจักรและการดำเนินการเกี่ยวกับการใช้กำลังทางทหาร โดยปัจจุบันกองบัญชาการกองทัพไทยได้จัดตั้งศูนย์ไซเบอร์ทหารขึ้น เพื่อรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพไทย โดยมีเป้าหมายที่จะเชื่อมโยงการทำงานระหว่างหน่วยไซเบอร์ในภาพรวมไม่ว่าจะเป็น กห. บก.ทท.และเหล่าทัพ ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง โดยกองทัพต้องผลักดันให้มี Cyber Command เมื่อเกิดเหตุการณ์ทางไซเบอร์ขึ้น (Cyber War) โดยตั้งฝ่ายบัญชาการรบแล้วแยกการปฏิบัติไปยังหน่วยต่าง ๆ เพื่อความเป็นเอกภาพในการบังคับบัญชา ปัจจุบันหน่วยงานด้านไซเบอร์ของกองทัพไทย ต่างมีความเข้าใจใน NIST Cybersecurity Framework ซึ่งเป็น

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		กรอบทำงาน ด้านความมั่นคงปลอดภัยไซเบอร์ที่แพร่หลายไปยังทุกภูมิภาคทั่วโลกรวมถึงประเทศไทย และมีการนำ Framework ดังกล่าว มาประยุกต์ใช้เพื่อรับมือกับภัยคุกคามไซเบอร์ของหน่วย โดยหัวใจสำคัญของ Framework แบ่งออกเป็น ๕ ฟังก์ชั่นหลัก คือ ๑. การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง (Identify) ๒. การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วย (Protect) ๓. การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ (Detect) ๔. การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น (Respond) ๕. การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้หน่วยสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม (Recovery) ทั้งนี้ งานข่าวกรองไซเบอร์ (Cyber Intelligence) ถือเป็นกลไกหลักที่มีบทบาทสำคัญของ Framework ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วย ซึ่งแนวความคิดในการปฏิบัติด้านการข่าวในมิติของไซเบอร์นั้น เป็นการดำเนินวงรอบข่าวกรองเช่นเดียวกันกับการปฏิบัติการด้านการข่าวในมิติอื่น ๆ โดยจะต้องดำเนินการทั้งในระดับยุทธวิธี ระดับยุทธการ และระดับยุทธศาสตร์ และจะต้องคัดสรรกำลังพลที่มีความรู้ทั้งในด้านการข่าวและการปฏิบัติการไซเบอร์มาปฏิบัติภารกิจดังกล่าว ซึ่งถือเป็นเรื่องที่ยากลำบาก การดำเนินงานด้านข่าวกรองไซเบอร์ของกองบัญชาการกองทัพไทย ในปัจจุบันจะเป็นการประสานความร่วมมือระหว่างกรมข่าวทหาร และศูนย์ไซเบอร์ทหาร โดยกรมข่าวทหารมีหน้าที่ติดตามสถานการณ์ภัยคุกคามไซเบอร์ในระดับยุทธศาสตร์ และส่งข้อมูลให้ศูนย์ไซเบอร์ทหารดำเนินการข่าวกรองไซเบอร์

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		ในระดับยุทธการ ซึ่งเป็นการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence : CTI) ระหว่างกันภายในกองบัญชาการกองทัพไทยและเหล่าทัพ และนำไปขยายผลในระดับยุทธวิธีเพื่อระบุได้ว่าฝ่ายตรงข้ามใช้เทคนิค ยุทธวิธี หรือรูปแบบการปฏิบัติการอย่างไร
๓.	ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก (พล.ต.มานพ สัมมาขันธ์)	ปัจจุบันภัยคุกคามความมั่นคงมีขอบเขตที่กว้างขวาง มีความเชื่อมโยงต่อบริบทโลกและสังคมไทยในมิติต่าง ๆ ทั้งมิติด้านเศรษฐกิจ สังคม และการเมือง ซึ่งมีความซับซ้อน และส่งผลกระทบต่อประชาชนโดยตรงมากขึ้น โดยเฉพาะความมั่นคงที่เกี่ยวกับเทคโนโลยีสารสนเทศและเครือข่าย ที่มีแนวโน้มเป็นประเด็นที่มีความเสี่ยงต่อการถูกการโจมตีและการจารกรรมทางไซเบอร์ เนื่องจากการกำหนดมาตรการป้องกันทำได้ยากและไม่ทันต่อความก้าวหน้าทางเทคโนโลยี ทั้งนี้ประเทศกำลังพัฒนาจะตกเป็นเป้าหมายการโจมตีมากขึ้น เนื่องจากมีความล้าหลังทางเทคโนโลยี และขาดความรู้ในการกำหนดมาตรการป้องกันที่ต้องใช้ผู้ที่มีความชำนาญเฉพาะทาง ขณะที่อิทธิพลของสื่อประเภทเครือข่ายสังคมออนไลน์กลายเป็นเครื่องมือสำคัญของประชาชนในการรวมตัวดำเนินกิจกรรมทางสาธารณะและการเคลื่อนไหวกิจกรรมทางการเมือง ซึ่งสื่อดังกล่าวมีโอกาสถูกนำมาใช้ในทางที่ผิดเพื่อโจมตี บ่อนทำลาย หรือบิดเบือนข้อเท็จจริง รวมถึงการแพร่กระจายถ้อยคำที่สร้างความเกลียดชัง ที่มีฐานมาจากอคติและการเลือกปฏิบัติ ซึ่งอาจทำให้เกิดความเกลียดชังและปัญหาความแตกแยกภายในประเทศ รวมถึงส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศในกรณีที่มีการใช้สื่อประเภทนี้โจมตีหรือบ่อนทำลายประเทศอื่น ทั้งนี้ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เป็นกระบวนการที่เหมาะสมที่สุด ในการป้องกันและตอบโต้ภัยคุกคามดังกล่าว และกระบวนการนี้จำเป็นต้องมีข่าวกรองไซเบอร์เป็นกลไกสำคัญสนับสนุนให้การป้องกันพื้นที่ปฏิบัติการทางไซเบอร์ สามารถดำเนินการ

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหาร ที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		ได้อย่างมีประสิทธิภาพสามารถตอบสนองและป้องกันภัยคุกคามได้อย่างทันท่วงที ในปัจจุบัน การดำเนินงานด้านการข่าวกรองไซเบอร์ของกองทัพบก จะเป็นรูปแบบการประสานความร่วมมือระหว่างกรมข่าวทหารบกกับศูนย์ไซเบอร์กองทัพบก โดยกรมข่าวทหารบกสนับสนุนข้อมูลข่าวกรองไซเบอร์ระดับยุทธศาสตร์ (Strategic) สำหรับการหาตัวผู้ที่อยู่เบื้องหลังการโจมตีเรา ซึ่งต้องอาศัยข่าวกรองยุทธศาสตร์มาหาข้อมูลความเคลื่อนไหวของตัวแปรต่าง ๆ ประกอบการวิเคราะห์ให้เห็นภาพภัยคุกคามในเชิงกว้าง ส่วนข่าวกรองไซเบอร์ระดับยุทธวิธี (Tactical) จะเป็นหน้าที่ของศูนย์ไซเบอร์กองทัพบกรับผิดชอบดำเนินการ
๔.	ผู้อำนวยการกองข่าวเทคนิค กรมข่าวทหาร (พ.อ.ปิยะ ศรีพลอย)	ภัยคุกคามทางไซเบอร์ หมายถึง เหตุการณ์ที่ก่อให้เกิดอันตรายต่อระบบหรือข้อมูลสารสนเทศของหน่วยงาน และบุคคลในเชิงของการสูญเสีย ความลับ ความครบถ้วนถูกต้อง และสภาพความพร้อมใช้งาน ซึ่งอาจส่งผลกระทบต่อความมั่นคงของกองทัพและประเทศ ความมั่นคงทางเศรษฐกิจและโครงสร้างสาธารณูปโภคต่าง ๆ ถือเป็นภัยคุกคามรูปแบบใหม่ที่ไม่ต้องการฝึกทางทหารทั่วไป ไม่ต้องคำนึงถึงสัดส่วนกำลังพล เงินทุนหรือการสนับสนุนไม่จำเป็นต้องอาศัยพาหนะ และไม่มีข้อจำกัดเกี่ยวกับระยะทางหรือสภาพแวดล้อมทางกายภาพ ผู้ก่อการร้ายที่มีความมุ่งหมายจะคุกคามบุคคลหรือกลุ่มบุคคลหรือประเทศในอีกซีกโลกหนึ่งสามารถทำได้ทันทีที่สามารถเชื่อมต่อกับเครือข่ายสารสนเทศได้ ฝ่ายตรงข้ามอาจเป็นได้ทั้งประเทศปรปักษ์ที่มุ่งทำลายประเทศของเราด้วยวิถีทางต่าง ๆ อยู่แล้ว กลุ่มทุนข้ามชาติที่ใช้เทคโนโลยีไซเบอร์เล่นงานประเทศหรือองค์กรเศรษฐกิจเพื่อหวังผลกำไรมหาศาล อาชญากรเศรษฐกิจที่ทั้งเป็นเครือข่ายองค์กรลับและปัจเจกที่มีพฤติกรรมไม่ต่างจากกลุ่มทุนฯ คนรักชาติของประเทศข้าศึกปฏิบัติการเป็นอิสระเพื่อโจมตีจุดศูนย์ดุลของประเทศเรา คนต่อต้านนโยบายรัฐภายในประเทศไม่ว่าจะเป็นเรื่องการเมือง

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหาร ที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		หรือมีวัตถุประสงค์ก็สามารถกระทำได้ กลุ่มผู้ที่ต้องการแสดงฝีมือให้ประจักษ์ ผู้ก่อการร้ายสากลที่อาศัยช่องทางนี้เพิ่มความได้เปรียบในสงครามไร้สมมาตร ไปจนถึงในอนาคตอาจจะใช้หุ่นยนต์โรบอทกระทำเองตามสมองกลของมัน ดังนั้นการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) จึงเป็นกระบวนการที่เหมาะสมที่สุดในการป้องกันและตอบโต้ภัยคุกคามดังกล่าว และกระบวนการนี้จำเป็นต้องมีข่าวกรองไซเบอร์เป็นกลไกสำคัญ ข่าวกรองไซเบอร์ คือ ข่าวสารต่าง ๆ ที่ได้รับความสนใจและมีความเกี่ยวข้องกับระบบเครือข่าย ระบบสารสนเทศ ที่ผ่านการตรวจสอบ วิเคราะห์ หรือได้รับพิสูจน์ว่าเป็นข่าวที่เชื่อถือได้ สามารถนำไปเป็นหลักฐานอ้างอิงได้ ซึ่งในปัจจุบันการปฏิบัติการไซเบอร์ในระดับกองบัญชาการกองทัพไทย จะเป็นหน้าที่รับผิดชอบของศูนย์ไซเบอร์ทหาร ซึ่งการดำเนินงานข่าวกรองไซเบอร์ในกระบวนการ จะเป็นการประสานการปฏิบัติร่วมกับหน่วยงานที่เกี่ยวข้อง โดยกรมข่าวทหารจะมีบทบาทในการสนับสนุนข้อมูลข่าวกรองเพื่อแจ้งเตือนภัยคุกคาม การดำเนินการข่าวกรองในระดับยุทธศาสตร์ สนับสนุนข้อมูลมาประกอบ เพื่อวิเคราะห์หาถึงตัวผู้กระทำที่อยู่เบื้องหลัง หรือโอกาสที่ผู้อยู่เบื้องหลังนั้นจะมาโจมตีเรา ส่วนข่าวกรองในระดับปฏิบัติการส่วนมากจะดำเนินการโดยศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย อย่างไรก็ตาม กรมข่าวทหาร ได้จัดทำระเบียบปฏิบัติประจำข่าวกรองทางไซเบอร์ กองบัญชาการกองทัพไทย พ.ศ.๒๕๖๐ ขึ้น เพื่อกำหนดแนวทางการปฏิบัติให้กับส่วนราชการที่มีหน้าที่ความรับผิดชอบเกี่ยวกับการปฏิบัติงานด้านการข่าว ในการดำเนินการด้านการข่าวกรองทางไซเบอร์ ให้เป็นไปในแนวทางเดียวกันและมีขั้นตอนที่ชัดเจนในการรายงานการปฏิบัติในสถานการณ์วิกฤติ

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหาร ที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
๕.	ผู้อำนวยการกองสารสนเทศ สำนักนโยบายและแผน กรมข่าวทหารบก (พ.อ.พงษ์พิสิทธิ์ มีสูงเนิน)	การดำเนินงานด้านข่าวกรองไซเบอร์นั้น มีวงรอบการทำงานคล้ายกับข่าวกรองทั่วไป คือ เริ่มจากการวางแผนและกำหนดทิศทาง (Planning and Direction) ไม่ว่าจะเป็นการรับคำสั่งหรือคำร้องขอจากหน่วยเหนือหรือทางหน่วยกำหนด หขส.ขึ้นเอง โดยต้องมีเป้าหมายและวัตถุประสงค์ที่ต้องการจะบรรลุผลชัดเจน หลังจากนั้นจึงเข้าสู่ขั้นตอนรวบรวมข้อมูลข่าวสาร (Collection) จากแหล่งต่าง ๆ อาทิ การเจาะระบบข้อมูลหรือการหาข้อมูลจากแหล่งเปิด (Open Sources) เมื่อได้ข้อมูลที่รวบรวมมาแล้วจึงนำข้อมูลที่ได้รับมานั้นเข้าสู่การดำเนินกรรมวิธี (Processing) ซึ่งขั้นตอนส่วนใหญ่จะเป็นการตีความข้อมูลที่รวบรวมมาได้ คืออะไร เนื่องจากข้อมูลที่ได้มามักจะมีการเข้ารหัสต้องใช้เครื่องมือระดับสูงและ จนท.ที่เชี่ยวชาญทำการถอดรหัสหรือแปลความ และเมื่อได้ข้อมูลที่ตอบคำสั่งหรือคำร้องขอจากหน่วยเหนือแล้ว จึงกระจาย (Disseminate) ข้อมูลดังกล่าว ไปยังผู้บังคับบัญชาและหน่วยอื่นต่อไปให้ทราบเพื่อให้ผู้มีหน้าที่ต่าง ๆ นำข้อมูลที่ได้รับไปดำเนินการให้บรรลุภารกิจต่อไป ปัจจุบัน กรมข่าวทหารบกมีหน้าที่สนับสนุนข้อมูลข่าวกรองยุทธศาสตร์ (Strategic) ให้กับศูนย์ไซเบอร์กองทัพบก เพื่อติดตามประเมินสถานการณ์ ระบุถึงภัยคุกคาม ความเคลื่อนไหวของผู้ที่อยู่เบื้องหลังการโจมตีทางไซเบอร์ (Cyber Attack) หรือโอกาสที่ผู้อยู่เบื้องหลังจะมาโจมตีฝ่ายเรา และแจ้งเตือนให้ฝ่ายเราทราบ (การสร้างความตระหนักรู้สถานการณ์ (Situation Awareness : SA)) ส่วนการดำเนินงานข่าวกรองไซเบอร์ระดับยุทธการ (Operation) และระดับยุทธวิธี (Tactical) จะเป็นหน้าที่ของศูนย์ไซเบอร์กองทัพบกรับผิดชอบ

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหาร ที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
๖.	ผู้อำนวยการกองข่าว สำนักข่าวกรอง กรมข่าวทหารเรือ (น.อ.ปณิธิ ทองเจือ ร.น.)	กรมข่าวทหารเรือไม่ได้รับผิดชอบดำเนินงานด้านข่าวกรองไซเบอร์ แต่สามารถส่งข้อมูลข่าวกรองยุทธศาสตร์สนับสนุนการปฏิบัติการไซเบอร์ให้กับกองไซเบอร์ สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ เมื่อได้รับการร้องขอ โดยงานข่าวกรองไซเบอร์ของกองทัพเรือในปัจจุบันจะอยู่ในกระบวนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพเรือ ที่มีกรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือเป็นผู้รับผิดชอบดำเนินการ ทั้งนี้ กรมข่าวทหารเรือยังไม่มีนโยบายที่จะพัฒนาการดำเนินงานด้านข่าวกรองไซเบอร์ที่เป็นรูปธรรม
๗.	ผู้อำนวยการกองสงครามไซเบอร์ สำนักบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศทหารอากาศ (น.อ.อมร ชมเชย)	ข่าวกรองไซเบอร์เป็นสิ่งที่จำเป็นและมีความสำคัญมากต่อการรับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน มีความเกี่ยวข้องกับการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงป้องกัน โดยการปฏิบัติการเชิงรุกจะมุ่งเน้นการรวบรวมข่าวสารด้วยวิธีจารกรรมข้อมูล (Hack) ที่จัดเก็บด้วยระบบ ICT ของฝ่ายตรงข้าม เช่น ข้อมูลภัยคุกคามไซเบอร์ (Cyber threat) รวมทั้งขีดความสามารถ (Capabilitiy) โดยนำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์ (Cyber Threat Target Folder) เพื่อเตรียมการปฏิบัติการไซเบอร์เชิงรุก ส่วนการปฏิบัติการเชิงรับจะให้ความสนใจกับภัยคุกคามไซเบอร์ (Cyber Threat) เพื่อเตรียมการระวังป้องกัน เนื่องจากภัยคุกคามไซเบอร์ (Cyber Threat) ซึ่งไม่มีขอบเขตทางภูมิศาสตร์ ผู้กระทำ (Actor) จะเป็นใครก็ได้ทั่วทุกมุมโลก ไม่จำเป็นต้องมีประเด็นขัดแย้งหรือมีพรมแดนติดกับประเทศไทย เช่น กรณีการปล่อยมัลแวร์เรียกค่าไถ่ Wanna Cry โดยเกาหลีเหนือ ประเทศไทยก็ได้รับผลกระทบ ทั้งที่ไม่ใช่ประเทศเป้าหมายที่เกาหลีเหนือจะโจมตี ดังนั้น การป้องกันภัยคุกคามที่เกิดขึ้น

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		เราจึงเริ่มต้นจากการหาข่าวผู้กระทำภัยคุกคามไซเบอร์ Cyber Threat Actors ทั่วโลก ทั้งที่มีรัฐชาติสนับสนุนหรือกลุ่มองค์กรอิสระ โดยติดตามข่าวสารจาก APT Groups (Advanced Persistent Threat Groups) ที่วิเคราะห์โดยบริษัทด้านการป้องกันภัยคุกคามทางไซเบอร์ขั้นสูง FireEye โดยนำข่าวสารที่ได้มาวิเคราะห์และพิสูจน์ทราบเจตนารมณ์ ขีดความสามารถ รูปแบบการโจมตีของ Cyber Threat Actors กลุ่มต่าง ๆ พร้อมกับการสำรวจตนเอง (Self Assessment) เพื่อป้องกันช่องโหว่ของระบบที่อาจถูกโจมตีหรือได้รับผลกระทบจากการโจมตีเหล่านั้น ปัจจุบัน กองทัพอากาศได้จัดทำแนวความคิดในการปฏิบัติการไซเบอร์ (Cyber Conops) โดยอ้างอิงจากกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework นำมาประยุกต์ให้สอดคล้องกับบริบทของกองทัพ โดยงานข่าวกรองไซเบอร์ (Cyber Intelligence) ถือเป็นกลไกสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตาม Cyber Conops เพราะมีส่วนในการสนับสนุนการประเมินความเสี่ยง (Risk) ที่จะเกิดภัยคุกคามไซเบอร์ และการกำหนดมาตรการในการระวังป้องกัน ทั้งยังสนับสนุนการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ ดังนั้นจึงกล่าวได้ว่าข่าวกรองไซเบอร์มีความสำคัญและจำเป็นอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ อย่างไรก็ตาม งานข่าวกรองไซเบอร์ในทุกระดับทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี หน่วยรับผิดชอบงานด้านการข่าวควรมีบทบาทนำในการปฏิบัติ โดยมีหน้าที่ติดตามประเมินสถานการณ์ ระบุถึงภัยคุกคาม และแจ้งเตือนฝ่ายให้เราทราบ (การสร้างความตระหนักรู้สถานการณ์ (Situation Awareness : SA)) เพราะหน่วยข่าวเป็นศูนย์กลางในการบูรณาการข้อมูลเพื่อผลิตเป็นข่าวกรองสนับสนุนงานยุทธการ ส่วนหน่วยงานด้านไซเบอร์ควรมีบทบาทในการเป็นเครื่องมือสนับสนุนการรวบรวมข่าวสารมากกว่า

ตารางที่ ๓ – ๑ สรุปผลการรวบรวมข้อมูลเกี่ยวกับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		แม้ว่าการฝึกคนข่าวให้มีขีดความสามารถด้านไซเบอร์จะเป็นงานที่ยากลำบาก แต่ถ้ามองถึงความจำเป็นทางยุทธการ และความเหมาะสมตามหน้าที่รับผิดชอบแล้ว กรมข่าวทหารอากาศ ควรเป็นหน่วยงานหลักที่รับผิดชอบงานข่าวกรองไซเบอร์ โดยมีการจัดตั้งทีมที่ประกอบกำลังกับกองสงครามไซเบอร์ ของกรมเทคโนโลยีสารสนเทศทหารอากาศ และกองยุทธการข่าวสาร ของกรมยุทธการทหารอากาศ ส่วนภารกิจการลาดตระเวนทางไซเบอร์เพื่อตรวจจับและค้นหาภัยคุกคามที่จะกระทำต่อระบบเครือข่ายของกองทัพอากาศ ควรมีการจัดทำแผนรวบรวมข่าวสารจากการลาดตระเวนทางไซเบอร์ หรือส่งหัวข้อข่าวสารสำคัญ (หขส.) ให้หน่วยไซเบอร์นำไปปฏิบัติการ โดยในขั้นการวางแผนจะต้องมีการประชุมหารือร่วมกันเพื่อกำหนดขีดความสามารถและข้อจำกัดในการปฏิบัติ ด้านการปฏิบัติการร่วมในระดับกองทัพไทย ควรทำในลักษณะ automate และรวมการ โดยมีศูนย์ไซเบอร์ทหารเป็นศูนย์กลางในการรวบรวมข้อมูลที่ได้รับรายงาน Cyber Threat Intelligence จากหน่วยไซเบอร์ของกองทัพไทยและเหล่าทัพ ซึ่งจะทำให้เกิดการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามร่วมกัน

การวิเคราะห์ข้อมูลจากการสัมภาษณ์พบว่า ปัจจุบันหน่วยงานด้านไซเบอร์ของกองทัพไทยต่างให้ความสำคัญในการเตรียมกำลังด้านการปฏิบัติการในมิติไซเบอร์ โดยจัดตั้งศูนย์ไซเบอร์กระทรวงกลาโหม และหน่วยไซเบอร์ระดับปฏิบัติการของแต่ละเหล่าทัพขึ้น เพื่อดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายในส่วนงานของตน แต่การดำเนินงานในภาพรวมยังขาดความเป็นเอกภาพและความเป็นมาตรฐาน เนื่องจากแยกกันปฏิบัติไม่มีสายการบังคับบัญชาที่เชื่อมโยงกัน และยังไม่มีหลักนิยมแนวความคิดในการปฏิบัติหรือกรอบการทำงานที่เป็นมาตรฐานกลาง โดยที่ผ่านมาหน่วยต่าง ๆ จะดำเนินงานตามแนวความคิดในการปฏิบัติหรือกรอบการทำงานที่หน่วยพัฒนาขึ้นใช้เองตามธรรมชาติการปฏิบัติการของเหล่าทัพตนเท่านั้น

สำหรับบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ ในปัจจุบันผู้ตอบส่วนใหญ่มีความเห็นตรงกันว่าการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เป็นกระบวนการที่เหมาะสมที่สุดในการป้องกันและตอบโต้ภัยคุกคามไซเบอร์ และกระบวนการนี้จำเป็นต้องมีข่าวกรองไซเบอร์ (Cyber Intelligence) เป็นกลไกสำคัญ โดยงานข่าวกรองไซเบอร์แบ่งออกเป็น ๓ ระดับ คือ ข่าวกรองยุทธศาสตร์ ข่าวกรองยุทธการ และข่าวกรองยุทธวิธี และต้องใช้บุคลากรที่เชี่ยวชาญทั้งในด้านงานข่าวกรองและด้านการปฏิบัติการไซเบอร์ ทั้งนี้การดำเนินงานข่าวกรองไซเบอร์ของกองทัพไทยในปัจจุบันยังไม่มีหลักนิยมหรือแนวความคิดในการปฏิบัติที่ชัดเจน การดำเนินงานจึงเป็นลักษณะของการประสานความร่วมมือ แลกเปลี่ยน หรือสนับสนุนข้อมูลระหว่างหน่วยงานด้านการข่าวกับหน่วยไซเบอร์เป็นหลัก โดยหน่วยข่าวส่วนใหญ่จะสนับสนุนข้อมูลข่าวกรองยุทธศาสตร์เพื่อแจ้งเตือนให้ทราบถึงสถานการณ์หรือเบื้องหลังเหตุการณ์การโจมตีทางไซเบอร์ ส่วนหน่วยไซเบอร์จะเป็นผู้ดำเนินการข่าวกรองยุทธการและข่าวกรองยุทธวิธีเอง เนื่องจากมีความเชี่ยวชาญด้านเทคโนโลยีที่ใช้ในการรวบรวมข่าวสารและการวิเคราะห์ภัยคุกคามไซเบอร์

เปรียบเทียบรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ

ตารางที่ ๓ – ๒ สรุปผลการรวบรวมข้อมูลเกี่ยวกับรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ

หัวข้อ	หัวข้อเปรียบเทียบ	ผลการเปรียบเทียบข้อมูล
๑.	สิ่งที่เหมือนกัน	รูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านไซเบอร์ของกองทัพไทย และเหล่าทัพต่าง ๆ ในปัจจุบัน ได้นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์ มาประยุกต์ใช้กับหน่วยงานของตนเอง โดยมีกระบวนการการทำงานหลัก คือ Identify Protect Detect Respond and Recovery ที่เป็นกรอบแนวคิดในการปฏิบัติที่เป็นที่ยอมรับและนำไปใช้อย่างแพร่หลายทั่วโลก ขณะที่งานข่าวจะเน้นในเชิงป้องกันมากกว่าเชิงรุก ด้วยการดำเนินการด้านข่าวกรองด้านภัยคุกคามไซเบอร์ (Cyber Threat Intelligence) ที่เน้นในการศึกษาว่าภัยคุกคามคือใคร มีเทคนิคและวิธีการโจมตีอย่างไร ได้รับการสนับสนุนจากใคร มีหนทางปฏิบัติต่อผู้ที่เป็นเป้าหมายอย่างไร นอกจากนี้ แนวคิดในการพัฒนาขีดความสามารถในด้านไซเบอร์ของไทยยังมีรูปแบบเดียวกันกับอีกหลายประเทศ อาทิ เยอรมนี สิงคโปร์ เป็นต้น โดยมุ่งเน้นในการพัฒนาองค์ประกอบหลัก ๓ ด้าน คือ ด้านบุคลการ (People) ให้มีขีดความสามารถและความพร้อม ในการปฏิบัติงานด้านไซเบอร์ ด้านอุปกรณ์และเทคโนโลยี (Technology) ให้มีขีดความสามารถในการป้องกันภัยคุกคามไซเบอร์ และการเสริมสร้างความสัมพันธ์กับต่างประเทศ (Enhance Relationship) ในการแบ่งปันองค์ความรู้และสร้างพันธมิตร ในการป้องกันภัยทางไซเบอร์ร่วมกัน

ตารางที่ ๓ – ๒ สรุปผลการรวบรวมข้อมูลเกี่ยวกับรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ (ต่อ)

หัวข้อ	หัวข้อเปรียบเทียบ	ผลการเปรียบเทียบข้อมูล
๒.	สิ่งที่แตกต่างกัน	มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศโดยเฉพาะประเทศที่มีความเชี่ยวชาญในงานด้านดังกล่าว อาทิ อิสราเอล สหรัฐฯ เยอรมนี ฯลฯ นั้น งานข่าวกรองไซเบอร์ (Cyber Intelligence) จะเป็นหน้าที่และความรับผิดชอบของหน่วยงานด้านการข่าวโดยชัดเจน โดยจะทำงานและบูรณาการข้อมูลกับหน่วยที่ปฏิบัติการด้านไซเบอร์หรือหน่วยงานด้านยุทธการอย่างใกล้ชิด เนื่องจากงานข่าวกรองเป็นงานที่ใช้ความรู้และความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องใช้ประสบการณ์จากการปฏิบัติงานมาเป็นระยะเวลาหนึ่ง จึงจะสามารถวิเคราะห์สถานการณ์ที่อาจจะเกิดขึ้นในอนาคตได้ ขณะที่ประเทศไทยงานทุกด้านที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ (Cyber Operations) และสงครามไซเบอร์ (Cyber Warfare) จะเป็นหน้าที่และความรับผิดชอบศูนย์ไซเบอร์ของหน่วยงานนั้นทั้งหมด ไม่ว่าจะเป็นขั้นตอนการระบุภัยคุกคาม การป้องกันและการแจ้งเตือน ไม่ได้มีการแบ่งหน้าที่งานด้านการข่าวในพื้นที่ปฏิบัติการไซเบอร์ให้กับหน่วยงานด้านการข่าวของหน่วย นอกจากนี้ การบูรณาการข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่มีหลักการปฏิบัติและการดำเนินการที่ชัดเจนเหมือนกับของต่างประเทศ

จากการเก็บรวบรวมข้อมูลโดยการสัมภาษณ์ และการศึกษาตำราวิชาการรวมถึงทบทวนวรรณกรรมที่เกี่ยวข้องพบว่า รูปแบบและลักษณะมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศมีข้อแตกต่างที่สำคัญคือ การกำหนดหน้าที่และความรับผิดชอบของหน่วยงานด้านไซเบอร์ โดยในประเทศไทยงานทุกงานที่เป็นการปฏิบัติการบนพื้นที่ไซเบอร์ จะอยู่ภายใต้ความรับผิดชอบของศูนย์ไซเบอร์หรือหน่วยไซเบอร์ขององค์กรหรือหน่วยงานนั้นทั้งหมด ไม่ได้มีการแบ่งหน้าที่ให้กับหน่วยงานอื่นที่เป็นหัวหน้าสายวิทยาการในงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ขณะที่ต่างประเทศจะมีหลักนิยม และแนวคิดการปฏิบัติที่ชัดเจนในการแบ่งหน้าที่และความรับผิดชอบที่เหมาะสมต่อกิจของงาน โดยมอบหมายให้แก่หัวหน้าสายวิทยาการในสายงานนั้นเป็นผู้รับผิดชอบ อาทิ หน่วยงานด้านการข่าวมีหน้าที่รับผิดชอบงานข่าวกรองไซเบอร์ ตัวอย่างคือ กองทัพอากาศสหรัฐฯ ภาคแปซิฟิก (PACAF) มอบหมายให้กรมข่าว (A2) รับผิดชอบงานข่าวกรองไซเบอร์ โดยสนับสนุนข้อมูลสำคัญให้แก่กรมสื่อสาร (A6) นำไปใช้ในการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ

วิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์

ตารางที่ ๓ – ๓ สรุปผลการรวบรวมข้อมูลเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
๑.	ผู้อำนวยการศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศ กระทรวงกลาโหม (พล.ต.เสรี คณธมาลัย)	ด้านขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์นั้น ปัจจุบันศูนย์ไซเบอร์กระทรวงกลาโหมมุ่งเน้นการดำเนินงานข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) ซึ่งเจ้าหน้าที่ปฏิบัติจำเป็นที่จะต้องมีทักษะทางไซเบอร์เป็นอย่างดี มีขีดความสามารถในการวิเคราะห์ข้อมูลข่าวสารที่รวบรวมมาได้ พร้อมจัดทำเป็นข่าวกรองภัยคุกคามไซเบอร์ที่สามารถแจ้งเตือนและระวังป้องกันภัยคุกคามล่วงหน้าได้อย่างมีประสิทธิภาพ ที่สำคัญข้อมูลข่าวกรองภัยคุกคามไซเบอร์ ต้องสามารถเชื่อมโยงและแลกเปลี่ยนกันระหว่างกองบัญชาการกองทัพไทยและเหล่าทัพ เพื่อสร้างความตระหนักรู้ล่วงหน้าและการระวังป้องกันภัยร่วมกัน
๒.	ผู้อำนวยการศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย (พล.ต.ชาติชาย ชัยเกษม)	งานข่าวกรองไซเบอร์ที่ศูนย์ไซเบอร์ฯ ถือปฏิบัติจะดำเนินการตามแนวคิดกระบวนการจัดเตรียมข่าวกรองพื้นที่การรบทางไซเบอร์(Cyber IPB) โดยในลำดับแรกเราจะต้องทำความเข้าใจกับข้าศึก (Enemy) ว่าเป็นใคร ทำอะไรได้บ้าง (Use Cases) มีหนทางปฏิบัติอย่างไร (Enemy COA) และพื้นที่ปฏิบัติการอยู่ที่ไหน (Area of Operations : AO) มีสภาพแวดล้อมและสิ่งที่ส่งผลกระทบอย่างไร (Operational Environment : OE) เพื่อกำหนดมาตรการในการรับมือกับภัยคุกคาม อย่างไรก็ตามงานข่าวกรองที่ดีจะต้องมีเอกภาพและกระทำในลักษณะเครือข่ายประชาคมข่าวที่มีมาตรฐานเดียวกัน มีความเข้าใจที่ตรงกัน แต่ในปัจจุบันการปฏิบัติการไซเบอร์ของกองทัพไทยและเหล่าทัพ ต่างยังดำเนินการแยกกัน และไม่ได้ใช้เทคโนโลยี หรือเครื่องมือที่มีมาตรฐานเดียวกัน กระบวนการแลกเปลี่ยนข้อมูลจึงยังขาดประสิทธิภาพ

ตารางที่ ๓ – ๓ สรุปผลการรวบรวมข้อมูลเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
๓.	ผู้อำนวยการศูนย์ไซเบอร์ กองทัพบก (พล.ต.มานพ สัมมาขันธ์)	ขีดความสามารถของงานข่าวกรองไซเบอร์ที่เหมาะสมกับบริบทความมั่นคงของไทย คือ สามารถเฝ้าระวังและแจ้งเตือนภัยล่วงหน้าให้แก่ส่วนความมั่นคงของรัฐได้ก่อนที่ภัยคุกคามต่าง ๆ จะเข้ามาโจมตีหรือบ่อนทำลายประเทศ สามารถระบุได้ว่าภัยคุกคามคืออะไร ใครคือผู้ประสงค์ร้าย และสามารถวิเคราะห์หนทางปฏิบัติของภัยคุกคามและฝ่ายตรงข้ามได้ อาทิ การป้องกันไม่ให้เกิดการโจมตีทางไซเบอร์จากโปรแกรมประสงค์ร้าย (Malware) ซึ่งการถูกโจมตีเพียงครั้งเดียวก็สามารถเข้าไปหยุดการทำงานของกระบวนการสำคัญของโครงสร้างพื้นฐานประเทศได้ และอาจส่งผลให้ทั้งระบบล้มพังลง รวมถึงสามารถสนับสนุนงานยุทธการของฝ่ายความมั่นคงที่สำคัญ คือ การสงครามข้อมูลข่าวสาร เพื่อยับยั้งและตอบโต้การบ่อนทำลายประเทศ และการสร้างความแตกแยกให้กับคนในชาติ
๔.	ผู้อำนวยการกองข่าวเทคนิค กรมข่าวทหาร (พ.อ.ปิยะ ศรีพลอย)	เมื่อพูดถึงขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ คนส่วนใหญ่จะเล็งเห็นความจำเป็นเฉพาะเรื่องของเทคนิคและเครื่องมือทางอิเล็กทรอนิกส์ในการหาข่าวว่าเป็นสิ่งที่สำคัญที่สุด แต่ในความเป็นจริง ข่าวกรองไซเบอร์นั้นแบ่งออกเป็นหลายระดับ ทั้งข่าวกรองยุทธศาสตร์ (Strategic) ยุทธการ (Operation) ยุทธวิธี (Tactical) และเทคนิค (Technical) โดยข่าวกรองยุทธศาสตร์จะมีขีดความสามารถในการหาถึงตัวผู้กระทำ เจตนารมณ์ที่มุ่งกระทำ หรือโอกาสที่ผู้อยู่เบื้องหลังนั้นจะมาทำการโจมตีระบบ โดยจะต้องนำข่าวกรองทางยุทธศาสตร์อื่น ๆ มาประกอบการวิเคราะห์ ซึ่งการหาข้อมูลความเคลื่อนไหวของตัวแปรต่าง ๆ ในเชิงวิชาการนั้นก็เป็นข่าวกรองประเภทนี้ด้วย ส่วนข่าวกรองยุทธการนั้นใช้ในกรณีเตรียมเปิดศึกกับศัตรู โดยมีขีดความสามารถในการพิสูจน์ทราบว่าศัตรูเฉพาะนั้น ๆ มีขีดความสามารถในการโจมตีและ

ตารางที่ ๓ – ๓ สรุปผลการรวบรวมข้อมูลเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ (ต่อ)

ลำดับ	ประชากร	ผลการรวบรวมข้อมูล
		ขีดความสามารถในการสนับสนุนอย่างไร รวมทั้งมีหนทางปฏิบัติอย่างไรบ้าง สำหรับข่าวกรองยุทธวิธีจะมีขีดความสามารถในการพิสูจน์ทราบว่าศัตรูใช้เครื่องมืออะไรในการโจมตี มีรูปแบบการปฏิบัติอย่างไร ซึ่งโดยมากจะเป็นข่าวที่ได้มาหลังจากถูกโจมตีแล้ว สำหรับการที่อาวุธนั้นได้ถูกใช้อย่างไร จะเป็นข่าวกรองเทคนิค
๕	ผู้อำนวยการ กองสารสนเทศ สำนักนโยบายและแผน กรมข่าวทหารบก (พ.อ.พงษ์พิสิทธิ์ มีสูงเนิน)	ขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ คือ การพิสูจน์ทราบให้ได้ว่าศัตรูคือใคร โจมตีเราอย่างไร ฝ่ายต่อต้านข่าวกรองจะป้องกันอย่างไร ฝ่ายยุทธการจะโจมตีกลับอย่างไร การวิเคราะห์โครงสร้างและระบบเครือข่ายข้อมูลของฝ่ายตรงข้าม เพื่อหาจุดล่อแหลม (Vulnerability) หรือช่องโหว่ในระบบของฝ่ายตรงข้าม และสามารถหาข้อมูลเกี่ยวกับจุดอ่อนของเครื่องมือที่ฝ่ายตรงข้ามใช้โจมตี เช่น โปรแกรมประสงค์ร้าย (Malware) เพื่อหาวิธีการป้องกันได้อย่างมีประสิทธิภาพ
๖.	ผู้อำนวยการ กองสงครามไซเบอร์ สำนักบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศทหารอากาศ (น.อ.อมร ชมเชย)	งานข่าวกรองไซเบอร์จะต้องสามารถสนับสนุนการกำหนดมาตรการในการระวังป้องกัน ทั้งยังสนับสนุนการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ โดยเชิงรุกจะมุ่งเน้นการรวบรวมและวิเคราะห์ข้อมูลเกี่ยวกับข้าศึก นำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์เพื่อเตรียมการโจมตี ทั้งนี้หน้าที่และขีดความสามารถที่จำเป็นสำหรับงานข่าวกรองทางไซเบอร์ คือการระบุภัยคุกคามหนทางปฏิบัติและโอกาสในการโจมตี เพื่อแจ้งเตือนหน่วยไซเบอร์ในการรับมือกับภัยคุกคามนั้น

การวิเคราะห์ข้อมูลจากการสัมภาษณ์พบว่า ผู้ตอบมีแนวความคิดที่สอดคล้องกันเกี่ยวกับขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ โดยสรุปคือ ขีดความสามารถในการการระบุตัวข้าศึกหรือภัยคุกคาม (Enemy/Threat) หนทางปฏิบัติของข้าศึกหรือภัยคุกคาม (Enemy COA) พื้นที่ปฏิบัติการ (Area of Operations : AO) รวมถึงสภาพแวดล้อมในการปฏิบัติการ (Operational Environment : OE) ซึ่งมีความสอดคล้องกับแนวคิดการเตรียมข่าวกรองในพื้นที่ปฏิบัติการรบในมิติอื่น ๆ

ความเห็นเพิ่มเติมเกี่ยวกับขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ คือ ข้อมูลข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence : CTI) ต้องสามารถเชื่อมโยงและแลกเปลี่ยนกันระหว่างกองบัญชาการกองทัพไทยและเหล่าทัพ เพื่อสร้างความตระหนักรู้ล่วงหน้าและการระวังป้องกันภัยร่วมกัน อีกทั้งการทำงานข่าวกรองไซเบอร์ควรจำแนกขีดความสามารถของงานข่าวกรองไซเบอร์ในแต่ละระดับ ซึ่งนอกจากขีดความสามารถในการวิเคราะห์ข้าศึกหรือภัยคุกคาม หนทางปฏิบัติ พื้นที่ปฏิบัติการและสภาพแวดล้อมที่ส่งผลกระทบแล้ว ข่าวกรองไซเบอร์ต้องมีขีดความสามารถในการระบุให้ได้ถึงเครื่องมือ รูปแบบและวิธีการที่ข้าศึกนำมาใช้ในการโจมตี (ข่าวกรองไซเบอร์ระดับยุทธวิธี) นอกจากนี้ผู้ตอบบางท่านยังมีความคิดเห็นเพิ่มเติมว่า ข่าวกรองไซเบอร์ต้องมีขีดความสามารถในการสนับสนุนการปฏิบัติการทั้งเชิงรุกและเชิงรับ โดยเชิงรุกจะมุ่งเน้นการรวบรวมและวิเคราะห์ข้อมูลเกี่ยวกับข้าศึกนำมาจัดทำเป็นแฟ้มเป้าหมายทางไซเบอร์เพื่อเตรียมการโจมตี

สรุป

จากการวิเคราะห์ข้อมูลในบทที่ ๓ ที่ได้มาจากทั้งการสัมภาษณ์ และการรวบรวมมาจากบทความ ตำราวิชาการ งานวิจัย และเอกสารที่เกี่ยวข้อง ทำให้ผู้วิจัยได้มาซึ่งแนวคิดสำคัญที่ระบุตัวแบบงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่กองทัพไทยและเหล่าทัพต่าง ๆ ต้องการสนับสนุนในการป้องกันและรับมือกับภัยคุกคามไซเบอร์

โดยจากการวิเคราะห์ข้อมูลที่ได้รับจากการสัมภาษณ์นั้น แสดงให้เห็นว่า หน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับกองทัพไทยและเหล่าทัพนั้น นำมาตรฐาน NIST Cybersecurity Framework และ ISO 20071 ซึ่งเป็นกรอบการทำงานตามมาตรฐานสากลในด้านความมั่นคงปลอดภัยไซเบอร์ มาประยุกต์ใช้กับหน่วยงาน และต้องการสนับสนุนจากงานด้านการข่าวในการสร้างสภาวะความตระหนักรู้สถานการณ์ให้แก่ผู้ปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ในการเฝ้าระวัง และแจ้งเตือนภัยล่วงหน้าได้ รวมถึงการเห็นภาพของสภาพแวดล้อมในการปฏิบัติการ สามารถระบุตัวตน ขีดความสามารถ กลยุทธ์และหนทางปฏิบัติของข้าศึก จนไปถึงการระบุและให้ข้อมูลเกี่ยวกับเป้าหมายได้เมื่อต้องดำเนินการตอบโต้ ซึ่งถือเป็นหน้าที่และความรับผิดชอบของงานด้านการข่าวในสภาพแวดล้อมและพื้นที่ปฏิบัติการปกติอยู่แล้ว นอกจากนี้ การจัดทำฐานข้อมูลและการแลกเปลี่ยนข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) ถือเป็นแนวคิดสำคัญ เนื่องจากห้วงมิติไซเบอร์ไม่มีการแบ่งพรมแดนและอาณาเขตชัดเจน บางครั้งภัยคุกคามไซเบอร์ที่ต้องการจะโจมตีเป้าหมายหนึ่ง อาจส่งผลกระทบต่อบุคคลหรือรัฐที่ไม่ใช่เป้าหมายของการโจมตีนั้นได้เช่นกัน ดังนั้นการจัดทำฐานข้อมูลและการแลกเปลี่ยน CTI ร่วมกันในทุก ๆ หน่วยงานจึงถือว่ามีความจำเป็น อย่างไรก็ตาม ปัจจุบันการปฏิบัติการไซเบอร์ของกองทัพไทยและเหล่าทัพต่าง ๆ อยู่ภายใต้ความรับผิดชอบของศูนย์ไซเบอร์หรือหน่วยไซเบอร์ขององค์กรหรือหน่วยงานนั้นทั้งหมด ยังไม่มีการแบ่งหน้าที่ให้กับหน่วยงานอื่นที่เป็นหัวหน้าสายวิทยาการในงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนั้นเมื่อเกิดกรณีที่ต้องการข้อมูลข่าวสาร/ข่าวกรอง จึงมีเพียงแต่การส่งคำสั่งคำขอข้อมูลและประสานไปยังหน่วยข่าว ให้การสนับสนุนข้อมูลตามที่ศูนย์ไซเบอร์หรือหน่วยไซเบอร์ต้องการเท่านั้น

บทที่ ๔
ผลการวิจัย

จากการศึกษาแนวทางการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามยุทธศาสตร์และนโยบายระดับชาติ และบทบาทด้านการข่าวกรองในบริบทการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ในปัจจุบัน ประกอบกับการเปรียบเทียบรูปแบบและลักษณะของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ รวมถึงการวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ จากข้อมูลที่เก็บรวบรวมได้จากการสัมภาษณ์กลุ่มผู้บริหารและผู้เชี่ยวชาญทั้งในด้านการข่าวกรองและด้านการปฏิบัติการไซเบอร์ และข้อมูลที่เก็บรวบรวมได้จากบทความ ตำราวิชาการ งานวิจัย และเอกสารที่เกี่ยวข้อง โดยใช้หลักการของเหตุผลในเชิงตรรกวิทยาตามกรอบแนวคิดการวิจัย ผู้วิจัยได้สรุปผลการวิจัยตามวัตถุประสงค์การวิจัย ดังนี้

ศึกษาแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ

ผลการวิจัย พบว่า แนวทางตามยุทธศาสตร์และนโยบายระดับชาติของไทย ที่เกี่ยวกับการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ จะมุ่งประเด็นไปที่การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ เพื่อปกป้องโครงสร้างพื้นฐานหรือสาธารณูปโภคที่บริหารจัดการด้วยไซเบอร์ให้ปลอดภัยจากการโจมตี ด้วยการเสริมสร้างศักยภาพและขีดความสามารถของกำลังพล โครงสร้างพื้นฐานและเทคโนโลยีให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ การสร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ สำหรับนโยบายภาครัฐเกี่ยวกับการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในปัจจุบัน คือ การพัฒนาไปสู่การบริหารจัดการที่มีความเป็นเอกภาพโดยจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) ทำหน้าที่เป็นหน่วยงานหลักในการกำหนดนโยบายด้านไซเบอร์ในระดับประเทศ และทำการบูรณาการและประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง พร้อมกำหนดนโยบายและแผนระดับชาติสู่การปฏิบัติที่มีความสอดคล้องในทุกภาคส่วนเป็นไปในทิศทางเดียวกัน มุ่งเน้นการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection : CIIP) โดยกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ การพัฒนากำลังคนทั้งหน่วยงานภาครัฐและเอกชนให้เพียงพอต่อการรับมือภัยคุกคามไซเบอร์ และการจัดตั้งหน่วยงานกลาง

Cyber Security Agency (CSA) เพื่อเป็นหน่วยเผชิญเหตุและรับมือภัยคุกคามไซเบอร์ทุกรูปแบบ ทั้งนี้ รัฐบาลมีความมุ่งหวังที่จะยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระดับมาตรฐานสากล

สำหรับการขับเคลื่อนยุทธศาสตร์และนโยบายของภาครัฐด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการทหาร ก็มีการทำงานที่สอดคล้องกับยุทธศาสตร์และนโยบายระดับชาติ โดยดำเนินการตามกรอบยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม ที่แบ่งการพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์ ออกเป็น ๔ ระยะ (ระยะละ ๕ ปี) เริ่มต้นจากการพัฒนากำลังพล โครงสร้างพื้นฐาน และเทคโนโลยี ให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ สร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ ในระยะที่ ๑ นำไปสู่การพัฒนาศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ เพื่อให้มีพลังอำนาจทางไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง ในระยะที่ ๒ และ ๓ และเพิ่มศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ให้อยู่ในแนวหน้า และเป็นที่ยอมรับในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้ในระยะที่ ๔

หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร

ผลการวิจัยพบว่า งานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร มีหลักการเหมือนกันกับงานข่าวกรองในพื้นที่ปฏิบัติการในมิติอื่น ๆ ที่มุ่งสนใจข้อมูลเกี่ยวกับข้าศึกหรือภัยคุกคาม (Enemy/Threat) หนทางปฏิบัติของข้าศึกหรือภัยคุกคาม (Enemy COA) พื้นที่ปฏิบัติการ (Area of Operations : AO) รวมถึงผลกระทบของสภาพแวดล้อมในการปฏิบัติการ (Operational Environment : OE) เพียงแต่คุณลักษณะทางกายภาพของสิ่งที่สนใจจะมีบริบทที่แตกต่างกัน โดยเฉพาะพื้นที่ปฏิบัติการในมิติไซเบอร์มีสภาพแวดล้อมและอาณาเขตที่ไม่ชัดเจน จึงมีความแตกต่างจากพื้นที่ปฏิบัติการในมิติอื่น ๆ ผู้วิจัยจึงสรุปได้ว่า งานข่าวกรองไม่ว่าจะอยู่บนพื้นฐานของมิติหรือพื้นที่ปฏิบัติการใดจะมีหน้าที่และความรับผิดชอบหลัก ๆ คือ การแจ้งเตือนเพื่อสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเรา การวิเคราะห์หนทางปฏิบัติของภัยคุกคาม ดังนั้น หน้าที่และความรับผิดชอบของข่าวกรองในห้วงมิติและพื้นที่ปฏิบัติการทางไซเบอร์จึงไม่ได้แตกต่างไปจากแนวคิดดังกล่าว ในการนี้ผู้วิจัยได้นำรูปแบบของงานข่าวกรองตามรูปแบบปกติมาประยุกต์ใช้ในการกำหนดหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร คือ

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

๒. รวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำมาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคคลหรือกลุ่มบุคคลที่เฝ้าระวังทั้งภายในและภายนอกประเทศ

๓. จัดเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation Of The Cyber Environment : IPCE) และการวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคาม เพื่อใช้สำหรับการวางแผนการปฏิบัติการไซเบอร์

๔. จัดทำเป้าหมายทางไซเบอร์ เมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม

ตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร ที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

ด้วยผลผลิตข่าวกรองหลักที่เป็นหัวใจสำคัญในการสนับสนุนการวางแผนการยุทธ คือ การเตรียมข่าวกรองของสนามรบ (Intelligence Preparation of Battlefield : IPB) ซึ่งเป็นการศึกษาและทำความเข้าใจกับสภาพแวดล้อมของสนามรบหรือพื้นที่ปฏิบัติการ การรู้ขีดความสามารถของฝ่ายเราและฝ่ายตรงข้าม โดย IPB เป็นตัวแบบการเตรียมข่าวกรองของสนามรบที่เหมาะสมและสอดคล้องกับกระบวนการแสวงข้อตกลงใจทางทหาร (MDMP Process) ที่กองทัพไทยยึดถือปฏิบัติและใช้เป็นเครื่องมือในการประมาณสถานการณ์ข่าวกรองสนับสนุนการวางแผนการยุทธ์ ดังนั้น จึงควรนำ IPB มาประยุกต์ใช้ในการเตรียมข่าวกรองของสนามรบในมิติไซเบอร์ (Cyber IPB) และใช้เป็นตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร อย่างไรก็ตามพื้นที่ปฏิบัติการในมิติไซเบอร์ก็มีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ คือ ไม่มีพื้นที่อาณาเขตชัดเจนและรูปแบบของภัยคุกคามที่อาจไม่ได้มาจากข้าศึกโดยตรง

จากการรวบรวมและวิเคราะห์ข้อมูลจากเอกสารตำราทางวิชาการ และการสัมภาษณ์ผู้เชี่ยวชาญ ผู้วิจัยพบว่า การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) ของนาย Rob Dartnall ผู้อำนวยการข่าวกรองไซเบอร์ของสถาบัน SANS ซึ่งเป็นสถาบันการศึกษาและวิจัยด้านความมั่นคงปลอดภัยระดับโลก มีความสอดคล้องกับแนวคิดและหลักนิยมในการปฏิบัติการทางทหารของกองทัพไทย ทั้งยังสอดคล้องกับแนวความคิดของกลุ่มประชากรที่ได้ดำเนินการสัมภาษณ์อีกด้วยจึงนำเสนอ “การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE)” เป็นตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

IPCE เป็นกระบวนการวิเคราะห์ที่ต่อเนื่องและเป็นระบบ มุ่งเน้นศึกษาและทำความเข้าใจกับสภาพแวดล้อมของสนามรบหรือพื้นที่ปฏิบัติการในมิติทางไซเบอร์ การล่วงรู้ถึงขีดความสามารถของฝ่ายเราและฝ่ายตรงข้าม โดยมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ และรูปแบบของภัยคุกคามที่อาจไม่ได้มาจากข้าศึกโดยตรง ซึ่งตัวแบบ IPCE เป็นการนำการเตรียมข่าวกรองของสนามรบ (Intelligence Preparation of Battlefield : IPB) มาประยุกต์ใช้บนพื้นฐานหลักการเดียวกันแต่แตกต่างกันในบริบทของสภาพแวดล้อม มีขั้นตอนการปฏิบัติ ๔ ขั้นตอน ดังนี้

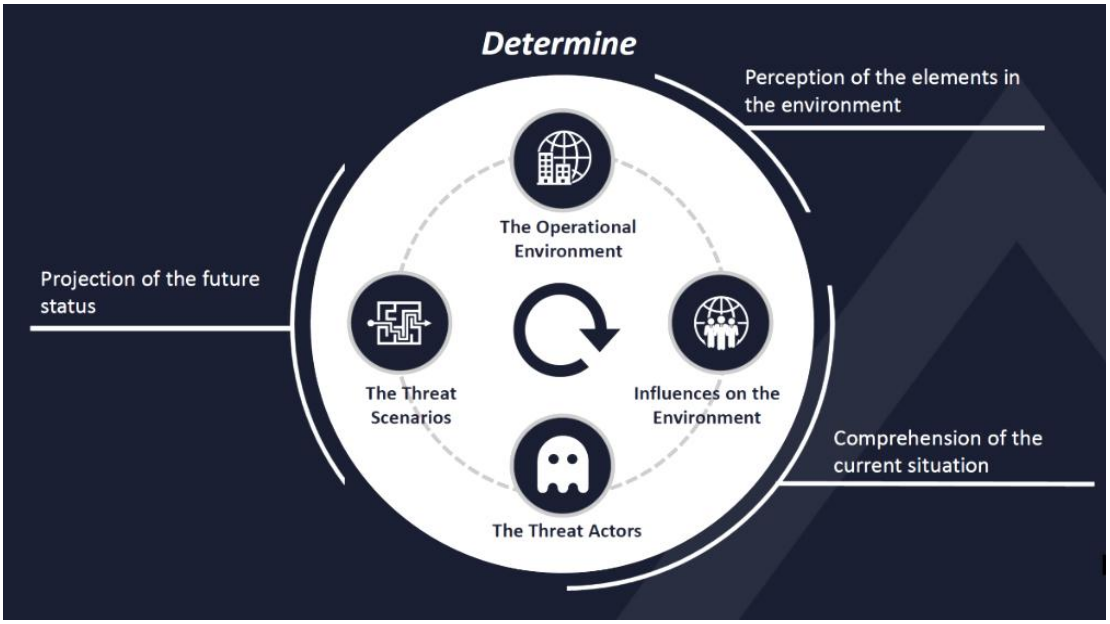
๑. การระบุสภาพแวดล้อมของการปฏิบัติการ (Determine The Operational Environment) คือ รู้สภาพแวดล้อมและพื้นที่ปฏิบัติการภายในเครือข่ายของฝ่ายเรา และสภาพแวดล้อมเครือข่ายภายนอกที่มีความเกี่ยวข้องกับเครือข่ายของฝ่ายเรา

๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ (Determine Influences On The Environment) คือ การนำสิ่งที่มีอิทธิพลต่อพื้นที่การรบในมิติต่าง ๆ ทั้งในทางการเมือง ทางทหาร ทางเศรษฐกิจ สังคม ข่าวสาร และโครงสร้างพื้นฐาน มาวิเคราะห์สิ่งที่จะเป็นผลกระทบต่อการปฏิบัติของฝ่ายเราตามหลัก PMESII-PT และ PESTLE-M

๓. การระบุตัวภัยคุกคาม (Determine the Threat Actors) คือ การระบุได้ว่าภัยคุกคามคือใคร ภัยคุกคามนั้นได้รับการสนับสนุนจากใคร มีกระบวนการการโจมตีหรือคุกคามอย่างไร มีวัตถุประสงค์ในการกระทำอย่างนั้นไปเพื่ออะไร และจะปฏิบัติการอีกเมื่อไหร่ เป็นต้น

๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม (Determine the Threat Scenarios) คือ การเข้าใจถึงหลักนิยม เทคนิค กลยุทธ์ และกระบวนการโจมตีของภัยคุกคาม และสามารถวิเคราะห์ได้ถึงหนทางปฏิบัติที่ภัยคุกคามอาจโจมตีฝ่ายเราได้

ภาพที่ ๔ - ๑ อธิบายถึงวงรอบการเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ ๔ ขั้นตอน
(4 Stage Of Intelligence Preparation Of The Cyber Environment)



ที่มา : Rob Dartnall Director of Cyber Intelligence of Bank of England, Online, 2017

สรุป

ผลการวิจัย พบว่า แนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ตามยุทธศาสตร์และนโยบายระดับชาติของไทย จะมุ่งประเด็นไปที่การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์เพื่อปกป้องโครงสร้างพื้นฐานหรือสาธารณูปโภคที่บริหารจัดการด้วยระบบไซเบอร์ให้ปลอดภัยจากการโจมตีเป็นหลัก ด้วยการเสริมสร้างศักยภาพและขีดความสามารถของกำลังพล โครงสร้างพื้นฐานและเทคโนโลยีให้มีความพร้อมในการปฏิบัติการในมิติไซเบอร์ การสร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ

เมื่อลงมายังหน่วยงานในระดับกองทัพไทยและเหล่าทัพ จะมีงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร ที่มีบทบาทและหน้าที่ในการติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคามและแจ้งเตือนฝ่ายให้เราทราบ ด้วยการจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีรายละเอียดเกี่ยวกับภัยคุกคามต่าง ๆ ทางไซเบอร์ รวมถึงกลุ่มบุคคลที่ต้องเฝ้าระวังทั้งภายในและภายนอกประเทศ และเมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม สามารถให้ข้อมูลสนับสนุนการจัดทำเป้าหมายทางไซเบอร์ได้

ซึ่งตัวแบบที่เหมาะสมต่อการรองรับบทบาทและหน้าที่ดังกล่าว คือ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) ที่เป็นกระบวนการวิเคราะห์อย่างต่อเนื่องและเป็นระบบ มุ่งเน้นการศึกษาและทำความเข้าใจกับสภาพแวดล้อมของพื้นที่ปฏิบัติการในมิติทางไซเบอร์ ระบุถึงขีดความสามารถและหนทางปฏิบัติของฝ่ายตรงข้าม โดยมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ นอกจากนี้การรวบรวมข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ หรือการรวบรวมและแบ่งปันข่าวกรองภัยคุกคามไซเบอร์ (Cyber Threat Intelligence : CTI) ถือเป็นอีกกระบวนการหนึ่งที่จะทำให้การจัดทำฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ประสบผลสำเร็จ

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การวิจัยครั้งนี้ ผู้วิจัยใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ โดยอาศัยข้อมูลปฐมภูมิจากการสัมภาษณ์ (Interview) เพื่อรวบรวมข้อมูลเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารและการพัฒนาตัวแบบของงานข่าวกรองไซเบอร์เชิงแนวคิด (Conceptual) ควบคู่กับการรวบรวมข้อมูลทุติยภูมิ ที่ได้จากบทความตำราวิชาการ งานวิจัยและเอกสารที่เกี่ยวข้อง (Documentary Search) เกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ตามยุทธศาสตร์และนโยบายระดับชาติ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์และบทบาทของงานข่าวกรองไซเบอร์ ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศเปรียบเทียบกับมาตรการของไทย (กองทัพไทย) ในปัจจุบัน

ผลการวิจัยในครั้งนี้ สามารถอภิปรายผลในเรื่องของแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ การวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร จนนำมาสู่การนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติได้ตรงตามวัตถุประสงค์การวิจัย กล่าวคือ หน่วยงานด้านการทหารมีบทบาทสำคัญในการขับเคลื่อนปฏิรูปกองทัพด้านไซเบอร์ต่อเนื่องตลอดหลายปีที่ผ่านมา ให้สอดรับกับยุทธศาสตร์ชาติ (ด้านความมั่นคง) และยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม ยุทธศาสตร์และนโยบายของภาครัฐด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นการเสริมสร้างขีดความสามารถและความพร้อมในการปฏิบัติในมิติไซเบอร์ มุ่งเน้นการพัฒนาองค์ประกอบที่สำคัญทั้งการพัฒนากำลังพล โครงสร้างพื้นฐานและเทคโนโลยี ตลอดจนการสร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ จนนำไปสู่การพัฒนาศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์เพื่อให้มีพลังอำนาจทางไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง จนสามารถอยู่ในระดับแนวหน้าและเป็นที่ยอมรับในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้

งานข่าวกรองทางไซเบอร์ถือเป็นกลไกหลักสำคัญ และเป็นกุญแจแห่งความสำเร็จในการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกภาคส่วน เมื่อวิเคราะห์ถึงงานข่าวกรองไซเบอร์ในบริบทการข่าวทหาร ผลการวิจัยพบว่า หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหารไม่แตกต่างจากงานข่าวกรองในพื้นที่ปฏิบัติการอื่น ๆ ได้แก่ การติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคามและแจ้งเตือนฝ่ายให้เราทราบ การรวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อนำมาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ การจัดเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ และการวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคาม เพื่อใช้สำหรับการวางแผน

การปฏิบัติการไซเบอร์และการจัดทำเป้าหมายทางไซเบอร์เมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม

อย่างไรก็ตาม แม้ว่างานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหารจะมีหน้าที่และขีดความสามารถที่จำเป็นไม่แตกต่างจากงานข่าวกรองในพื้นที่ปฏิบัติการอื่น ๆ แต่ในมิติไซเบอร์นั้นเป็นการปฏิบัติการบนระบบเครือข่ายคอมพิวเตอร์ที่ไม่มีขอบเขตที่ชัดเจนเหมือนกับพื้นที่ทางบก ทางทะเลและอากาศ รวมทั้งทักษะที่จำเป็นต้องใช้ในการปฏิบัติการนั้นไม่ได้ใช้ความสามารถและประสบการณ์ทางด้านการข่าวกรองเพียงอย่างเดียว แต่ต้องอาศัยทักษะทางด้านระบบเครือข่ายคอมพิวเตอร์ซึ่งต้องมีความรู้ความเข้าใจ และประสบการณ์งานด้านไซเบอร์ตลอดจนเครื่องมืออุปกรณ์ Software ต่าง ๆ ที่ใช้สำหรับงานด้านไซเบอร์ โดยขีดความสามารถที่จำเป็นสำหรับงานข่าวกรองทางไซเบอร์สามารถแบ่งออกเป็นขีดความสามารถทางด้านการข่าวกรอง และขีดความสามารถทางด้านไซเบอร์ ซึ่งปัจจุบันบุคลากรภายในกระทรวงกลาโหมที่ปฏิบัติงานในส่วนของงานด้านการข่าวและไซเบอร์จะมีทักษะและขีดความสามารถเฉพาะในด้านนั้น ๆ จึงเป็นอุปสรรคต่อการพัฒนางานข่าวกรองไซเบอร์ในปัจจุบัน

การวิจัยครั้งนี้ ได้นำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ คือ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation Of The Cyber Environment : IPCE) ซึ่งประกอบด้วย ๔ ขั้นตอน คือ

๑. การระบุสภาพแวดล้อมของการปฏิบัติการ (Determine The Operational Environment)

๒. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ (Determine Influences On The Environment)

๓. การระบุตัวภัยคุกคาม (Determine The Threat Actors)

๔. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม (Determine The Threat Scenarios)

สำหรับตัวแบบการเตรียมข่าวกรองสภาพแวดล้อมทางไซเบอร์ (IPCE) ที่ได้ มีพื้นฐานมาจากการจัดเตรียมข่าวกรองของสนามรบ (Intelligence Preparation Of Battlefield: IPB) ซึ่งเป็นตัวแบบการเตรียมข่าวกรองของสนามรบทางกายภาพที่เหมาะสมและสอดคล้องกับกระบวนการแสวงข้อตกลงใจทางทหาร (MDMP Process) ที่กองทัพไทยยึดถือปฏิบัติและใช้เป็นเครื่องมือในการประมาณสถานการณ์ข่าวกรองสนับสนุนการวางแผนการยุทธ์ จึงสามารถนำ IPCE มาประยุกต์ใช้ในงานข่าวกรองที่สนับสนุนการปฏิบัติการไซเบอร์เพื่อป้องกันประเทศได้อย่างเหมาะสม ทั้งนี้งานข่าวกรองไซเบอร์ในบริบทการข่าวทหารจะมุ่งเน้นการป้องกันภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบเครือข่ายในการควบคุมบัญชาการและควบคุมการรับส่งข้อมูลของฝ่ายตรงข้าม รวมทั้งสนับสนุนมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของรัฐบาลตามที่ได้รับมอบหมายโดยเป็นงานในเชิงรับ และการจัดทำเป้าหมายทางไซเบอร์ซึ่งเป็นงานในเชิงรุกในการปฏิบัติการทางทหาร

ข้อเสนอแนะ

๑. ผู้บังคับบัญชาของหน่วยในทุกระดับชั้นควรให้ความสำคัญในการพัฒนาบุคลากร ระบบเครือข่าย และอุปกรณ์ให้มีความพร้อมในการรองรับการปฏิบัติงานด้านการข่าวกรองไซเบอร์

๒. ควรมีการผนึกกำลังระหว่างหน่วยข่าวกรองไซเบอร์ภายในกระทรวงกลาโหมและหน่วยงานภายนอก รวมทั้งมิตรประเทศ

๓. ข่าวกรองไซเบอร์ในทุกระดับทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี หน่วยรับผิดชอบงานด้านการข่าวควรมีบทบาทนำในการปฏิบัติ เพราะเป็นศูนย์กลางในการบูรณาการข้อมูลเพื่อผลิตเป็นข่าวกรองสนับสนุนงานยุทธการ ทั้งนี้กองทัพควรปรับโครงสร้างหน่วยข่าวเพื่อให้สามารถรองรับการปฏิบัติการด้านข่าวกรองไซเบอร์ และพัฒนาขีดความสามารถของผู้ที่จะปฏิบัติงานด้านการข่าวกรองไซเบอร์ในระดับยุทธการและยุทธวิธี ให้มีทักษะทั้งด้านการข่าวกรองและการปฏิบัติการไซเบอร์ควบคู่กัน

๔. ระบบเครือข่ายของแต่ละหน่วยงานภายในกระทรวงกลาโหมควรกำหนดให้มีการเชื่อมโยงข้อมูลบนมาตรฐานเดียวกันเพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลข่าวสารทางไซเบอร์ที่รวดเร็วและทั่วถึง ซึ่งในเบื้องต้นหน่วยที่มีขีดความสามารถทางด้านไซเบอร์สูง ควรให้การสนับสนุนหน่วยที่กำลังเริ่มต้นหรือมีขีดความสามารถน้อยกว่า เพื่อให้เกิดการบูรณาการข้อมูลและการป้องกันภัยคุกคามทางไซเบอร์ร่วมกัน นอกจากนี้ควรมีการเชื่อมโยงระบบกับเครือข่ายทางไซเบอร์ในทุกภาคส่วนให้สามารถแลกเปลี่ยนข้อมูลข่าวสารและช่วยเหลือซึ่งกันและกันในกรณีที่เกิดสถานการณ์วิกฤตทางไซเบอร์ได้

๕. สำหรับข้อเสนอแนะในการวิจัยครั้งต่อไป ผู้วิจัยเห็นว่าควรนำตัวแบบของงานข่าวกรองไซเบอร์เชิงแนวคิดจากเอกสารวิจัยฉบับนี้ไปขยายผลต่อในการจัดทำแนวคิดในการปฏิบัติการข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร เพื่อให้เกิดผลอย่างเป็นรูปธรรม และสามารถให้ข่าวกรองไซเบอร์สามารถสนับสนุนงานยุทธการและการปฏิบัติการไซเบอร์ในระดับกองทัพและเหล่าทัพต่าง ๆ ได้ อย่างไรก็ตาม ผู้วิจัยมีข้อเสนอแนะเพิ่มเติมว่า การนำข้อมูลในเอกสารวิจัยฉบับนี้ไปเป็นแนวความคิดในการทำวิจัยในประเด็นอื่นต่อไป ควรจะตรวจสอบและศึกษาถึงสภาพแวดล้อมของการปฏิบัติการ ณ เวลานั้นด้วย เนื่องจากพื้นที่ปฏิบัติการหรือมิติทางไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่ตลอดเวลา จึงอาจทำให้ต้องมีการปรับปรุงเปลี่ยนแปลงแนวคิดของการจัดทำตัวแบบของงานข่าวกรองไซเบอร์ให้เหมาะสม

บรรณานุกรม

ภาษาไทย

กองทัพอากาศ. “นโยบายผู้บัญชาการทหารอากาศ ประจำปีพุทธศักราช ๒๕๖๐ – ๒๕๖๑”. “ยุทธศาสตร์ ทอ. ๒๐ ปี ประจำปีพุทธศักราช ๒๕๖๐ – ๒๕๗๙”. (ออนไลน์). เข้าถึงได้จาก : http : // www.rtaf.mi.th, ๒๕๖๑.

จอห์น บอยด์. นาวาอากาศเอก. “OODA LOOP (Observes Orients Decides Acts)”. เอกสารประกอบการบรรยายหลักสูตร รร.สธ.ทอ.รุ่นที่ ๖๐ บทที่ ๓ การทหาร. พ.ศ.๒๕๖๐.

ไทยเซิร์ต. “สถิติภัยคุกคาม”. (ออนไลน์). เข้าถึงได้จาก : Https : // www.Thaicert.Or.Th/Statistics/Statistics. Html, ๒๕๖๐.

ภาษาต่างประเทศ

Colonel Mark Kross. "Operationalizing Network Defense/Cyberspace Intel Requirements". (Briefing Slide Presentation of the U.S.Air Force. 2007). P.20.

Daniel R Coats. “Worldwide Threat Assessment of the Us Intelligence Community” Statement for the Record Senate Select Committee on Intelligence. 11 May 2017.

Decree of the President of the Russian Federation No.646 of December 5, 2016. “Doctrine of Information Security of the Russian Federation”. (Online). Available : http : //www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, 2016.

ENISA. CTI Analyst Skillset. “CTI –EU | Bonding EU Cyber Threat Intelligence ENISA”. (Online). Available : https : //www.enisa.europa.eu/events/cti-eu-event, 2017.

Jay McAllister. Senior Analyst. “Emerging Technology Center”. (Online). Available. : Https : //www.Insights.Sei.Cmu.Edu/Sei_Blog/2016/02/Cyber-Intelligence-And-Critical-Thinking. Html, 2016.

“Joint Publication 3-12 Cyberspace Operations”. (Online). Available : https : //www.Publicintelligence.net/jcs-cyberspace-operations, 2018.

N. Hanacek/NIST. (Online). Available : https : //www.nist.gov/Cyberframework, 2013.

Rob Dartnall Director. “Cyber Intelligence of Bank of England”. Briefing Slide Presentation of the Cyber Intelligence of Bank of England. 2017.

Robert M. Lee. Adjunct Lecturer. “Utica College”. (Online). Available. : https : //www.tripwire.co4m/state-of-security/security-data-protection/introduction-cyber-intelligence/, 2014.

"SANS Institute". (Online). Available : https : //www.twitter.com/sansawareness, 2017.

Singapore Prime Minister's Office. "Singapore's Cyber Security Strategy". (Online). Available : https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf, 2016.

The Federal Government of Germany. "White Paper 2016 on German Security Policy and the Future of the Bundeswehr".(Online). Available : https://www.bundeswehr.de/resource/.../2016%20White%20Paper.pdf, 2016.

U.S. Air Force . "U.S. Air Force Cyber Operations Command". Briefing Slide Presentation of the U.S.Air Force. 2007. P.9. – 10.

US ARMY FM 3-06. (Online). Available : https : //www.fas.org/irp/doddir/army/fm3-06.pdf, 2006.

US ARMY FM 3-38. (Online). Available : https : //www.fas.org/irp/doddir/army/fm3-12.pdf, 2014.

US DOD. "The Department of Defense Cyber Strategy". (Online). Available : http : //archive.defense.gov/home/features/2015/0415_cyber- strategy/final_2015_dod_cyber_strategy_for_web.pdf, 2015.

World Economic Forum. "The Global Risks Report 2017 12Th Edition". (Online). Available : http : //www3.weforum.org/docs/GRR17_Report_web.pdf, 2017.

ประวัติย่อผู้วิจัย

ชื่อ	พลอากาศตรี พงษ์สวัสดิ์ จันทสาร		
วัน เดือน ปีเกิด	๖ มกราคม ๒๕๐๗		
การศึกษา	โรงเรียนอยุธยาวิทยาลัย	มัธยมศึกษาปีที่ ๓	ปี ๒๕๒๓
	โรงเรียนเตรียมทหาร	รุ่นที่ ๒๓	ปี ๒๕๒๕
	โรงเรียนนายเรืออากาศ	รุ่นที่ ๓๐	
	นายทหารชั้นผู้บังคับฝูง	รุ่นที่ ๗๗	ปี ๒๕๓๖
	โรงเรียนเสนาธิการทหารอากาศ	รุ่นที่ ๔๒	ปี ๒๕๕๑
	วิทยาลัยการทัพอากาศ	รุ่นที่ ๔๔	ปี ๒๕๕๓

ประวัติการทำงานโดยย่อ

ผู้บังคับฝูงบิน ๒๓๑ กองบิน ๒๓
ผู้บังคับการกรมนักเรียนนายเรืออากาศรักษาพระองค์ โรงเรียนนายเรืออากาศ
ผู้บังคับการ กองบิน ๔
ผู้ช่วยทูตฝ่ายทหารอากาศไทย ประจำสถานเอกอัครราชทูต ณ กรุงเบอร์ลิน
ผู้อำนวยการสำนักนโยบายและแผน กรมข่าวทหารอากาศ

ตำแหน่งปัจจุบัน รองเจ้ากรมข่าวทหารอากาศ

สรุปย่อ

ลักษณะวิชา การทหาร

เรื่อง การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร

ผู้วิจัย พลอากาศตรี พงษ์สวัสดิ์ จันทสาร **หลักสูตร** วปอ. **รุ่นที่** 60

ตำแหน่ง ผู้อำนวยการสำนักนโยบายและแผน

ความเป็นมาและความสำคัญของปัญหา

ภัยคุกคามทางไซเบอร์ (Cyber Threat) เป็นภัยคุกคามรูปแบบใหม่ที่เน้นกระทำต่อระบบอินเทอร์เน็ตและระบบเครือข่ายคอมพิวเตอร์ ซึ่งส่งผลกระทบต่อความมั่นคงในทุกระดับตั้งแต่ในระดับประชาคมโลก ภูมิภาค ประเทศชาติ และลงมาถึงประชาชน ทำให้ประชาคมโลกเริ่มตื่นตัวและตระหนักถึงภัยคุกคามดังกล่าวมากขึ้น ในห้วงที่ผ่านมาโดยผู้อำนวยการข่าวกรองแห่งชาติสหรัฐฯ (DNI) ได้เสนอประมาณการภัยคุกคามต่อวุฒิสภาสหรัฐฯ ในปี 60 โดยระบุให้ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามความมั่นคงอันดับ 1 เหนือการก่อการร้ายและอาวุธที่มีอานุภาพทำลายล้างสูง (WMD) และมีอัตราการขยายตัวของภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างต่อเนื่องและสร้างความเสียหายต่อสังคมโลกมากยิ่งขึ้น ด้วยเหตุนี้นานาประเทศจึงตระหนักถึงความจำเป็นในการหาวิธีการป้องกันและรับมือกับภัยคุกคามนี้อย่างจริงจัง ด้วยการดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) อาทิ การป้องกันโครงสร้างพื้นฐานระบบสารสนเทศที่สำคัญและสร้างสภาพแวดล้อมทางไซเบอร์ให้แข็งแกร่ง

ในส่วนของประเทศไทย ก็ได้ตระหนักถึงอันตรายจากภัยคุกคามทางไซเบอร์ และหาวิธีการรับมือกับภัยคุกคามนี้อย่างจริงจังเช่นกัน โดยปัจจุบัน มีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) 2 แห่ง คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) และศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (G-CERT) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ นอกจากนี้รัฐบาลยังได้จัดทำร่าง พ.ร.บ. ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดให้มีหน่วยงานหลักในการรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ และทำการบูรณาการและประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องเรียกว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC) เรียกโดยย่อว่า “กปช.” (ปัจจุบันอยู่ระหว่างการรับฟังความคิดเห็น และยังไม่มีผลบังคับใช้) อย่างไรก็ตาม ในระหว่างการจัดทำร่าง พ.ร.บ.ฯ รัฐบาลได้จัดตั้งคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อวันที่ 18 ตุลาคม 60 โดยมีอำนาจหน้าที่ในการจัดทำนโยบายแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งคณะกรรมการฯ มีแผนจะผลักดัน 4 เรื่อง คือ

1. การเพิ่มกำลังคนไซเบอร์ของหน่วยงานภาครัฐและเอกชนให้เพียงพอรับมือภัยคุกคามไซเบอร์
2. การจัดตั้ง Cybersecurity Agency (CSA) รับมือภัยคุกคามไซเบอร์ทุกรูปแบบ
3. การสร้างความเข้มแข็งโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)
4. ยกระดับ Ranking ด้านความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระดับต้นๆ ของโลก ซึ่งเป็นการเตรียมการระวังป้องกัน และแสดงให้เห็นถึงทิศทางการพัฒนาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของไทยในอนาคต

อย่างไรก็ตาม การป้องกันภัยคุกคามไซเบอร์มีความสำคัญและความจำเป็นไม่ต่างจากการป้องกันภัยคุกคามในมิติอื่นๆ และงานข่าวกรองถือเป็นเครื่องมือที่สำคัญในการป้องกันภัยคุกคาม ซึ่งจากการศึกษาค้นคว้าเกี่ยวกับมาตรฐานที่เป็นข้อกำหนดสำหรับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management System: ISMS) เช่น ISO ISO/IEC 27001 ของยุโรป และกรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework ของสหรัฐอเมริกา ที่นานาประเทศยึดถือเป็นมาตรฐานและกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พบว่างานข่าวกรองเป็นองค์ประกอบที่สำคัญในกระบวนการโดย “ข่าวกรองภัยคุกคามไซเบอร์ Cyber Threat Intelligence (CTI)” เป็นรูปแบบของข่าวกรองที่แพร่หลายและเป็นที่รู้จักกันดี ในกลุ่มองค์กรหรือหน่วยงานต่าง ๆ ทั่วโลก ที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่ง CTI เป็นการนำข้อมูลที่รวบรวมได้จากเครือข่ายมาวิเคราะห์ร่วมกับฐานข้อมูลของการโจมตีที่รู้จัก เพื่อให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ สิ่งนี้เป็นจุดเริ่มต้นที่จะนำเอาแนวคิดของข่าวกรองไซเบอร์จากภาคความมั่นคงเข้ามาใช้ในภาคอุตสาหกรรมมากขึ้น จึงเป็นเครื่องยืนยันถึงความจำเป็นและความสำคัญของงานข่าวกรองในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาค้นคว้าข้อมูลของผู้วิจัย ประกอบกับหน้าที่ในปัจจุบันที่มีความเกี่ยวข้องกับงานด้านการข่าวกรองโดยตรง มีความเห็นว่า การรักษาความมั่นคงทางไซเบอร์เป็นเรื่องที่มีความสำคัญอย่างยิ่งในยุคปัจจุบัน และถือเป็นเรื่องใหม่ที่ยังขาดแคลนผู้เชี่ยวชาญและองค์ความรู้โดยเฉพาะ “งานข่าวกรองไซเบอร์” ซึ่งเป็นกลไกสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงมีความสนใจที่จะศึกษาวิจัยเรื่อง “การพัฒนางานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร” เพื่อศึกษาวิเคราะห์ให้ทราบถึงหน้าที่และขีดความสามารถข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร และนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ โดยมุ่งหวังให้สามารถนำไปใช้เป็นตัวแบบในการจัดทำแนวความคิดในการปฏิบัติด้านข่าวกรองไซเบอร์ของหน่วยงาน หรือสถาบันศึกษาที่เกี่ยวข้องกับความมั่นคงหรือนำไปประยุกต์ใช้ในการศึกษาและปรับปรุงให้ตัวแบบมีความสมบูรณ์และเหมาะสมกับยุคสมัยต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ
2. เพื่อศึกษาวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร
3. เพื่อนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ

ขอบเขตของการวิจัย

3.1 ด้านเนื้อหา การวิจัยครั้งนี้มุ่งเน้นศึกษายุทธศาสตร์และนโยบายระดับชาติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนนิยามและขอบเขตข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่ใช้รับมือกับภัยคุกคามไซเบอร์ตามแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยเท่านั้น

3.2 ด้านประชากร การศึกษานี้มุ่งศึกษาความคิดเห็นของบุคลากรเฉพาะที่เกี่ยวข้องกับงานด้านการปฏิบัติการไซเบอร์และการข่าวทหารเท่านั้น โดยกลุ่มบุคลากรดังกล่าวประกอบด้วยกลุ่มผู้บริหารและผู้เชี่ยวชาญทั้งในด้านการปฏิบัติการไซเบอร์และด้านการข่าวกรองของกองทัพไทย จำนวน 7 คน

3.3 ด้านเวลา การศึกษานี้ผู้วิจัยได้ใช้ระยะเวลาในการดำเนินการวิจัยตั้งแต่เดือนมกราคมถึงพฤษภาคม 2560 รวมระยะเวลาทั้งสิ้น 5 เดือน

วิธีดำเนินการวิจัย

ผู้วิจัยได้กำหนดวิธีดำเนินการวิจัย ดังนี้

1. ใช้วิธีการรวบรวมข้อมูลในเชิงคุณภาพ โดยอาศัยข้อมูลปฐมภูมิจากการสัมภาษณ์ (Interview) โดยออกแบบสัมภาษณ์เพื่อรวบรวมข้อมูลเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร และการพัฒนาตัวแบบของงานข่าวกรองไซเบอร์เชิงแนวคิด (Conceptual) และรวบรวมข้อมูลทุติยภูมิที่ได้จากบทความตำราวิชาการงานวิจัยและเอกสารที่เกี่ยวข้อง (Documentary Search) เกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ตามยุทธศาสตร์และนโยบายระดับชาติ ข้อมูลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และบทบาทของงานข่าวกรองไซเบอร์ในกระบวนการข้อมูลเกี่ยวกับรูปแบบของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศเปรียบเทียบกับมาตรการของไทย (กองทัพไทย) ในปัจจุบัน
2. นำข้อมูลที่ได้รับจากการสัมภาษณ์มาวิเคราะห์ตามแนวทางวิพากษ์วิธี

3. นำข้อมูลจากข้อ 1 และ 2 มาเปรียบเทียบโดยใช้หลักการของเหตุผลในเชิงตรรกวิทยา ตามกรอบแนวคิดการวิจัยจนนำไปสู่การบูรณาการเพื่อสรุปผลการวิจัยและข้อยุติ เป็นคำตอบเกี่ยวกับหน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร และตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย รวมทั้งเสนอแนะข้อคิดเห็นที่เป็นประโยชน์

ผลการวิจัย

ผู้วิจัยได้สรุปผลการวิจัยตามวัตถุประสงค์ 3 ข้อ ดังนี้

1. เพื่อศึกษาแนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ

ผลการวิจัยพบว่า แนวทางการพัฒนาความมั่นคงไซเบอร์ของประเทศไทยจากยุทธศาสตร์และนโยบายระดับชาติ มีกรอบการดำเนินการ ดังนี้

1.1 พัฒนาไปสู่การบริหารจัดการที่มีความเป็นเอกภาพ โดยมีการจัดตั้งหน่วยงานกลาง (คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSC)) ทำหน้าที่เป็นหน่วยงานหลักในการกำหนดนโยบายการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และทำการบูรณาการและประสานการทำงานกับหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง

1.2 มีการกำหนดกรอบแนวคิด นโยบายและแผนระดับชาติ และแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure : SOP) ให้หน่วยงานภาครัฐและองค์กรเอกชน นำไปปฏิบัติให้เกิดความสอดคล้องและเป็นไปในทิศทางเดียวกัน

1.3 มุ่งเน้นการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection: CIIP) โดยกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ เช่น กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค และกลุ่มสาธารณสุข เพื่อป้องกันภัยคุกคามในภาพรวม

1.4 เสริมสร้างศักยภาพและขีดความสามารถการปฏิบัติการในมิติไซเบอร์ โดยเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐ เอกชน และสถาบันการศึกษา เพื่อให้มีกำลังคนเพียงพอในการรับมือกับภัยคุกคามไซเบอร์ในอนาคต

1.5 มีการจัดตั้ง Cybersecurity Agency (CSA) ทำหน้าที่หน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความปลอดภัยมั่นคงไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

1.6 ยกระดับ Ranking ด้านความมั่นคงปลอดภัยไซเบอร์ ให้อยู่ในระดับแนวหน้าของภูมิภาค โดยในปี 60 ดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทยอยู่ในอันดับที่ 22 จาก 194 ประเทศ โดยอยู่อันดับที่ 3 ของประเทศสมาชิกในกลุ่มอาเซียน รองจากสิงคโปร์ และมาเลเซีย

สำหรับกิจการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านการทหาร ก็มีการทำงานที่สอดคล้องกับนโยบายและกรอบแนวทางระดับชาติ โดยกรอบดำเนินการตามยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม ได้แบ่งการพัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์ออกเป็น 4 ระยะ (ระยะละ 5 ปี) เริ่มต้นจากการพัฒนากำลังพล โครงสร้างพื้นฐาน และเทคโนโลยีให้มีความพร้อมในการปฏิบัติในมิติไซเบอร์ สร้างความตระหนักรู้ทางไซเบอร์ให้กับทุกภาคส่วน และสร้างความร่วมมือทางไซเบอร์ทั้งในและต่างประเทศ ในระยะที่ 1 นำไปสู่การพัฒนาศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ เพื่อให้มีพลังอำนาจทางไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง ในระยะที่ 2 และ 3 และเพิ่มศักยภาพและขีดความสามารถในการปฏิบัติในมิติไซเบอร์ให้อยู่ในแนวหน้าและเป็นที่ยอมรับในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้ในระยะที่ 4

ทั้งนี้ จากการศึกษาวิจัย พบว่า กระทรวงกลาโหมได้ขับเคลื่อนปฏิรูปกองทัพด้านไซเบอร์อย่างต่อเนื่อง เพื่อให้สอดรับกับแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ยุทธศาสตร์ชาติ (ด้านความมั่นคง) และยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม โดยมีการจัดทำแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม (ปี 60-64) และกำหนดให้ไซเบอร์เป็นมิติหนึ่งของสงครามที่ต้องจัดเตรียมกำลังและใช้กำลัง เช่นเดียวกับมิติของการสงครามอื่น ๆ มีการแปลงนโยบายมาสู่การปฏิบัติด้วยการจัดตั้งหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นรูปธรรม ได้แก่ ศูนย์ไซเบอร์กระทรวงกลาโหม และหน่วยไซเบอร์ระดับปฏิบัติการของแต่ละเหล่าทัพ ซึ่งอยู่ระหว่างการเสริมสร้างศักยภาพและขีดความสามารถในด้านนโยบายและแผน ด้านกำลังพล ด้านการปฏิบัติการ ด้านเทคโนโลยีและการวิจัย พัฒนา รวมทั้งโครงสร้างพื้นฐานและเทคโนโลยีให้พร้อมในการปฏิบัติ ขณะเดียวกันก็ได้ให้ความสำคัญกับการผนึกกำลังด้านไซเบอร์ โดยส่งเสริมให้เกิดการเชื่อมโยงระบบกับกองทัพไทย และเหล่าทัพเพื่อแลกเปลี่ยนข้อมูลภัยคุกคามและระวังป้องกันภัยร่วมกัน ซึ่งในระยะแรกของการพัฒนากระทรวงกลาโหมได้มุ่งเน้นการพัฒนาขีดความสามารถเชิงรับ เช่น ด้านการป้องกันโครงสร้างพื้นฐาน และด้านการเฝ้าระวัง ซึ่งแต่ละเหล่าทัพได้จัดตั้งโรงเรียนและเปิดสอนผู้ปฏิบัติงานไซเบอร์ระดับต่างๆ ควบคู่กับการฝึกปฏิบัติการ สำหรับการผนึกกำลังด้านไซเบอร์ได้กำหนดเป้าหมายให้มีกำลังพลสำรองไซเบอร์ พร้อมทั้งขยายความร่วมมือและผนึกกำลังกับหน่วยงานทั้งภายในประเทศและต่างประเทศ เช่น การฝึกไซเบอร์ในการฝึกร่วม/ผสมทางทหาร โดยการปฏิรูปกองทัพด้านไซเบอร์จะเป็นส่วนสำคัญให้กองทัพมีความพร้อมและมีขีดความสามารถในการรับมือกับการโจมตีและการคุกคามทางไซเบอร์ ซึ่งสามารถพัฒนาไปสู่การทำสงครามไซเบอร์ได้ในอนาคต

2. เพื่อศึกษาวิเคราะห์หน้าที่และขีดความสามารถที่จำเป็นของงานข่าวกรองทางไซเบอร์ในบริบทของการข่าวทหาร

ผลการวิจัยสรุปว่า งานข่าวกรองไม่ว่าจะอยู่บนพื้นฐานของมิติหรือพื้นที่ปฏิบัติการใดจะมีหน้าที่และความรับผิดชอบหลัก ๆ คือ การแจ้งเตือนเพื่อสร้างความตระหนักรู้สถานการณ์ให้แก่ฝ่ายเรา การวิเคราะห์หนทางปฏิบัติของภัยคุกคาม ดังนั้น หน้าที่และความรับผิดชอบของข่าวกรองในห้วงมิติและพื้นที่ปฏิบัติการทางไซเบอร์จึงไม่ได้แตกต่างไปจากแนวคิดดังกล่าว ในการนี้ ผู้วิจัยได้นำรูปแบบของงานข่าวกรองตามรูปแบบปกติมาประยุกต์ใช้ในการกำหนดหน้าที่และขีดความสามารถที่จำเป็นของข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร คือ

2.1 ติดตาม ประเมินสถานการณ์ ระบุถึงภัยคุกคาม และแจ้งเตือนฝ่ายให้เราทราบ (การสร้างความตระหนักรู้สถานการณ์ (Situation Awareness : SA))

2.2 รวบรวมข้อมูลข่าวสารและเหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำมาจัดทำฐานข้อมูลทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงบุคคล/กลุ่มบุคคลที่เฝ้าระวังทั้งภายในและภายนอกประเทศ

2.3 จัดเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) และการวิเคราะห์หนทางปฏิบัติของฝ่ายตรงข้ามหรือภัยคุกคามเพื่อใช้สำหรับการวางแผนการปฏิบัติการไซเบอร์

2.4 จัดทำเป้าหมายทางไซเบอร์ เมื่อจำเป็นต้องใช้มาตรการตอบโต้เชิงรุกต่อฝ่ายตรงข้ามหรือภัยคุกคาม

3. เพื่อนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ ในบริบทของการข่าวทหารที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตและสอดรับกับยุทธศาสตร์และนโยบายระดับชาติ

ผู้วิจัยได้ศึกษาค้นคว้า และวิเคราะห์ตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยนำตัวแบบของงานข่าวกรองตามรูปแบบปกติ คือ การเตรียมข่าวกรองของสนามรบ (Intelligence Preparation of Battlefield : IPB) มาประยุกต์ใช้ในการกำหนดตัวแบบของงานข่าวกรองในมิติไซเบอร์ ผลการวิจัยพบว่า การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE) ของนาย Rob Dartnall ผู้อำนวยการข่าวกรองไซเบอร์ของสถาบัน SANS ซึ่งเป็นสถาบันการศึกษาและวิจัยด้านความมั่นคงปลอดภัยระดับโลก มีความสอดคล้องกับแนวคิดจากเอกสารทางวิชาการ รวมถึงแนวคิดและหลักนิยมในการปฏิบัติการทางทหารของกองทัพไทย นอกจากนี้ กระบวนการและผลผลิตในแต่ละขั้นตอนมีความสอดคล้องกับแนวความคิดของกลุ่มประชากรที่ได้ดำเนินการสัมภาษณ์ จึงนำเสนอตัวแบบของงานข่าวกรองไซเบอร์ในบริบทของการข่าวทหารที่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย คือ การเตรียมข่าวกรองของสภาพแวดล้อมทางไซเบอร์ (Intelligence Preparation of the Cyber Environment : IPCE)

โดย IPCE เป็นกระบวนการวิเคราะห์ที่ต่อเนื่องและเป็นระบบ มุ่งเน้นศึกษาและทำความเข้าใจกับสภาพแวดล้อมของสนามรบหรือพื้นที่ปฏิบัติการในมิติทางไซเบอร์ การล่วงรู้ถึงขีดความสามารถของฝ่ายเราและฝ่ายตรงข้าม โดยมีลักษณะสภาพแวดล้อมที่แตกต่างจากพื้นที่ปฏิบัติการอื่น ๆ และรูปแบบของภัยคุกคามที่อาจไม่ได้มาจากข้าศึกโดยตรง โดยเป็นการนำการเตรียมข่าวกรองของสนามรบ (Intelligence Preparation of Battlefield : IPB) มาประยุกต์ใช้บนพื้นฐานหลักการเดียวกัน แต่แตกต่างกันในบริบทของสภาพแวดล้อม และมีขั้นตอนการปฏิบัติ 4 ขั้นตอน คือ

1. การระบุสภาพแวดล้อมของการปฏิบัติการ (Determine The Operational Environment)

2. การระบุถึงสิ่งที่ส่งผลกระทบต่อสภาพแวดล้อมของการปฏิบัติการ (Determine Influences on the Environment)

3. การระบุตัวภัยคุกคาม (Determine the Threat Actors)

4. การระบุถึงแผนการหรือหนทางปฏิบัติของภัยคุกคาม (Determine the Threat Scenarios)

ข้อเสนอแนะ

1. ผู้บังคับบัญชาของหน่วยในทุกระดับชั้นควรให้ความสำคัญในการพัฒนาบุคลากร ระบบเครือข่าย และอุปกรณ์ให้มีความพร้อมในการรองรับการปฏิบัติงานด้านการข่าวกรองไซเบอร์

2. ควรมีการผนึกกำลังระหว่างหน่วยข่าวกรองไซเบอร์ภายในกระทรวงกลาโหม และหน่วยงานภายนอก รวมทั้งมิตรประเทศ

3. ข่าวกรองไซเบอร์ในทุกระดับทั้งระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี หน่วยรับผิดชอบงานด้านการข่าวควรมีบทบาทนำในการปฏิบัติ เพราะเป็นศูนย์กลางในการบูรณาการข้อมูล เพื่อผลิตเป็นข่าวกรองสนับสนุนงานยุทธการ ทั้งนี้ กองทัพควรปรับโครงสร้างหน่วยข่าวเพื่อให้สามารถรองรับการปฏิบัติการด้านข่าวกรองไซเบอร์ และพัฒนาขีดความสามารถของผู้ที่จะปฏิบัติงานด้านการข่าวกรองไซเบอร์ในระดับยุทธการและยุทธวิธี ให้มีทักษะทั้งด้านการข่าวกรองและการปฏิบัติการไซเบอร์ควบคู่กัน

4. ระบบเครือข่ายของแต่ละหน่วยงานภายในกระทรวงกลาโหมควรกำหนดให้มีการเชื่อมโยงข้อมูลบนมาตรฐานเดียวกันเพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลข่าวสารทางไซเบอร์ที่รวดเร็วและทั่วถึง ซึ่งในเบื้องต้นหน่วยที่มีขีดความสามารถทางด้านไซเบอร์สูง ควรให้การสนับสนุนหน่วยที่กำลังเริ่มต้นหรือมีขีดความสามารถน้อยกว่า เพื่อให้เกิดการบูรณาการข้อมูลและการป้องกันภัยคุกคามทางไซเบอร์ร่วมกัน นอกจากนี้ ควรมีการเชื่อมโยงระบบกับเครือข่ายทางไซเบอร์ในทุกภาคส่วนให้สามารถแลกเปลี่ยนข้อมูลข่าวสารและช่วยเหลือซึ่งกันและกันในกรณีที่เกิดสถานการณ์วิกฤตทางไซเบอร์ได้

5. สำหรับข้อเสนอแนะในการวิจัยครั้งต่อไป ผู้วิจัยเห็นว่าควรนำตัวแบบของงานข่าวกรองไซเบอร์เชิงแนวคิดจากเอกสารวิจัยฉบับนี้ไปขยายผลต่อในการจัดทำแนวคิดในการปฏิบัติการข่าวกรองไซเบอร์ในบริบทของการข่าวทหาร เพื่อให้เกิดผลอย่างเป็นรูปธรรม และสามารถให้ข่าวกรองไซเบอร์สามารถสนับสนุนงานยุทธการและการปฏิบัติการไซเบอร์ในระดับกองทัพและเหล่าทัพต่าง ๆ ได้ อย่างไรก็ตาม ผู้วิจัยมีข้อเสนอแนะเพิ่มเติมว่า การนำข้อมูลในเอกสารวิจัยฉบับนี้ไปเป็นแนวความคิดในการทำวิจัยในประเด็นอื่นต่อไป ควรจะตรวจสอบและศึกษาถึงสภาพแวดล้อมของการปฏิบัติการ ณ เวลานั้นด้วย เนื่องจากพื้นที่ปฏิบัติการหรือมิติทางไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วอยู่ตลอดเวลา จึงอาจทำให้ต้องมีการปรับปรุงเปลี่ยนแปลงแนวคิดของการจัดทำตัวแบบของงานข่าวกรองไซเบอร์ให้เหมาะสม