การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทย
รองรับยุทธศาสตร์ชาติด้านความมั่นคง

โดย

พลตรีมานพ สัมมาขันธ์
ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก
กองทัพบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 61
ประจำปีการศึกษา พุทธศักราช 2561– 2562

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคง”ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี ของ พลตรี มานพ สัมมาขันธ์ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักรรุ่นที่ 61 ประจำปีการศึกษา พุทธศักราช 2561 - 2562

พลโท

(ขจรฤทธิ์ นิลกำแหง)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคง

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย พลตรีมานพสัมมาขันธ์ **หลักสูตร** วปอ. **รุ่นที่** 61

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาและแนวทางในการพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยให้สามารถปฏิบัติหน้าที่ตามรัฐธรรมนูญและรองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคงในฐานะส่วนราชการที่เป็นเหล่าทัพหลักในกระทรวงกลาโหมการวิจัยนี้เป็นการวิจัยเชิงคุณภาพ ใช้การเก็บข้อมูลจากเอกสาร การสัมภาษณ์ผู้ให้ข้อมูลเชิงลึก และการสังเกตการณ์แบบมีส่วนร่วมของผู้วิจัยเอง โดยใช้ทฤษฎีด้านความมั่นคง ทฤษฎีองค์การและหลักการบริหารทรัพยากรบุคคลตลอดจนความรู้ด้านไซเบอร์มาใช้ในการอธิบายปรากฏการณ์ที่เกิดขึ้นและกำหนดแนวทางในการพัฒนาทั้งระบบ

ผลการวิจัยสรุปว่ากองทัพบกไทยจะต้องมีความพร้อมในการปฏิบัติการไซเบอร์ทั้งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยเบอร์ พ.ศ.2562 และการปฏิบัติการไซเบอร์เพื่อสนับสนุนการปฏิบัติทางทหาร แต่ในปัจจุบันกองทัพไทยยังขาดความชัดเจนในเรื่องบทบาทและหน้าที่ของหน่วยงานไซเบอร์ซึ่งยังคงเป็นกรมฝ่ายกิจการพิเศษ ไม่ได้ถูกจัดความสัมพันธ์กับงานที่คล้ายคลึงกัน เช่น งานสื่อสาร งานสารสนเทศ และการปฏิบัติการข่าวสารรวมทั้งไม่มีสายงานฝ่ายอำนวยการที่รับผิดชอบเป็นการเฉพาะเหมือนกับกองทัพมิตรประเทศจึงเป็นข้อจำกัดในการพัฒนาหน่วยงานด้านไซเบอร์ การวิจัยนี้เสนอให้กองทัพบกไทยแก้ไขปัญหาดังกล่าวและพัฒนาระบบงานที่เกี่ยวข้องได้แก่ ระบบอัตรากำลัง ระบบการบริหารงานบุคคล และระบบการฝึกและศึกษาเพื่อให้หน่วยงานไซเบอร์ของกองทัพบกไทยมีความพร้อมในการสนับสนุนกองทัพให้สามารถปฏิบัติภารกิจตามที่รัฐธรรมนูญกำหนดและรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้

คำสำคัญ:ไซเบอร์, การปฏิบัติการไซเบอร์, ความมั่นคงทางไซเบอร์

Keyword:cyber, cyber operations, cyber security

Abstract

Title A Development of Cyber Units in the Royal Thai Army for National Strategy on Security

Field Science and Technology

Name Major GeneralManopSummakhan **Course**NDC **Class**61

The objective of this research is to study problems and prospects for development of the cyber units in the Royal Thai Army, to perform duty according toThai Constitution and National Strategyon security, as a main service of the Ministry of Defense. This research is qualitative research, collected data from documents, in-depth interviews and participant observation by the researcher. The explanation of the phenomenon and prospects for development of training and military education system in the Royal Thai Army for the whole system was applied by international relations theories, organization theories, and human resource management principal.

The research concluded that the Royal Thai Army must has readiness to perform duty according to the Cyber Security Act of B.E. 2562 and conduct cyber operations to support military operations. However, the Thai Armed Forces lack of the precise of the role and function of cyber unitswhichstill be the Army Special Staff, the lack of proper function among signal corps, information units, and information operations.Furthermore, the Thai Armed Forces has not established the Cyber Coordination staff as the others Armed Forces. These result to the limitation of the development of cyber units. The research prospects thatthe Royal Thai Army should provide a clear definition of cyber role and staff function properly, like armed forces in others countries, including develop the force developmentsystem, human resource management system, and training and education system simultaneously. These will provide readiness to cyber unit, in order to support the Royal Thai Army to conduct security duty according to Thai Constitutions, and National Strategyonsecurity.

คำนำ

งานวิจัยฉบับนี้ เป็นส่วนหนึ่งของการศึกษาหลักสูตรการป้องกันราชอาณาจักร และศึกษาเกี่ยวกับปัญหาและแนวทางในการพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยให้สามารถรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างเป็นรูปธรรมโดยการพัฒนาระบบงานอื่นๆ ที่เกี่ยวข้องให้เห็นภารกิจความรับผิดชอบที่ชัดเจน ผู้วิจัยหวังเป็นอย่างยิ่งว่า การวิจัยครั้งนี้จะก่อให้เกิดประโยชน์ต่อกองทัพในภาพรวม

พลตรี

(มานพ สัมมาขันธ์)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ 61

ผู้วิจัย

กิตติกรรมประกาศ

งานวิจัยฉบับนี้สำเร็จได้ด้วยดีและสามารถนำกรอบแนวคิดที่ได้รับไปใช้ประโยชน์ในการพัฒนาหน่วยงานไซเบอร์ของกองทัพบกไทยรวมทั้งหน่วยงานไซเบอร์อื่นในกระทรวงกลาโหมให้สามารถปฏิบัติหน้าที่ตามแผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคงได้ ขอขอบคุณผู้บังคับบัญชาในกองทัพบกที่ได้กรุณาสนับสนุนให้ผู้วิจัยได้มีโอกาสปฏิบัติหน้าที่ในศูนย์ไซเบอร์กองทัพบกซึ่งเปิดโอกาสให้สามารถทำการสังเกตแบบมีส่วนร่วมและนำผลลัพธ์มาใช้ประกอบการวิจัยได้ ขอขอบคุณ พลตรี ดร.นพนันต์ ชั้นประดับ ผู้ซึ่งปฏิบัติงานในกรมยุทธการทหารบกมากว่า 20 ปี ได้อธิบายผลของการไม่มีกรมฝ่ายเสนาธิการรับผิดชอบงานไซเบอร์เป็นการเฉพาะเหมือนกองทัพมิตรประเทศเป็นอุปสรรคต่อการพัฒนาหน่วยงานไซเบอร์เนื่องจากมีความเร่งด่วนต่ำกว่างานยุทธการอื่น ขอขอบคุณพันเอก ดร.นพดล แก้วกำเนิด ที่ได้กรุณาให้ข้อมูลความสัมพันธ์ระหว่างระบบงานไซเบอร์การสื่อสาร และการปฏิบัติการข่าวสารจากประสบการณ์ที่ได้จากปฏิบัติงานในกรมยุทธการทหารบกมานาน และขอขอบคุณคณาจารย์ในวิทยาลัยป้องกันราชอาณาจักรทุกท่านที่ได้กรุณาให้ความรู้ในเรื่องยุทธศาสตร์ชาติด้านความมั่นคงตลอดจนแนวคิดทฤษฎีเรื่องที่เกี่ยวข้องจนกระทั่งผู้วิจัยสามารถนำมาเชื่อมโยงกับเรื่องที่ทำการวิจัยได้เป็นอย่างดีหากมีความผิดพลาดประการใดผู้วิจัยขออภัยไว้ ณ ที่นี้ด้วย

พลตรี
(มานพ สัมมาขันธ์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 61
ผู้วิจัย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

สารบัญแผนภาพ (ต่อ)

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ยุทธศาสตร์ชาติระยะ 20 ปี พ.ศ.2561-2580 ซึ่งจัดทำรองรับรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 ได้กำหนดวิสัยทัศน์ไว้ว่า “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” หรือเป็นคติพจน์ประจำชาติว่า “มั่นคง มั่งคั่ง ยั่งยืน” ทั้งนี้ วิสัยทัศน์ดังกล่าวจะต้องตอบสนองต่อผลประโยชน์แห่งชาติ ได้แก่ การมีเอกราชอธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ การดำรงอยู่อย่างมั่นคง ยั่งยืนของสถาบันหลักของชาติ การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ การอยู่ร่วมกันในชาติอย่างสันติสุขเป็นปึกแผ่น มีความมั่นคงทางสังคมท่ามกลางพหุสังคมและการมีเกียรติและศักดิ์ศรีของความเป็นมนุษย์ ความเจริญเติบโตของชาติ ความเป็นธรรมและความอยู่ดีมีสุขของประชาชน ความยั่งยืนของฐานทรัพยากรธรรมชาติสิ่งแวดล้อม ความมั่นคงทางพลังงานและอาหาร ความสามารถในการรักษาผลประโยชน์ของชาติภายใต้การเปลี่ยนแปลงของสภาวะแวดล้อมระหว่างประเทศและการอยู่ร่วมกันอย่างสันติประสานสอดคล้องกันด้านความมั่นคงในประชาคมอาเซียนและประชาคมโลกอย่างมีเกียรติและศักดิ์ศรี[1]โดยกองทัพเป็นเครื่องมือหนึ่งของรัฐที่จะทำให้บรรลุผลประโยชน์แห่งชาติดังกล่าวได้

ยุทธศาสตร์ชาติด้านความมั่นคง กำหนดให้มีการพัฒนาศักยภาพในการป้องกันประเทศพร้อมรับมือกับภัยคุกคามทั้งทางทหารและภัยคุกคามอื่นๆ ในส่วนที่เกี่ยวข้องกับการวิจัย ได้แก่ การพัฒนาเสริมสร้างศักยภาพการผนึกกำลังป้องกันประเทศและการรักษาความสงบเรียบร้อยภายในประเทศ การส่งเสริมการวิจัยพัฒนาวิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ ตลอดจนสร้างความร่วมมือกับประเทศเพื่อนบ้านและมิตรประเทศรวมถึงการรักษาสันติภาพในกรอบความร่วมมือที่เกี่ยวข้อง[2]ซึ่งกองทัพยังคงเป็นเครื่องมือหลักในการดำเนินการตามยุทธศาสตร์ด้านความมั่นคงดังกล่าว

ในด้านความมั่นคงไซเบอร์นั้น ยุทธศาสตร์ชาติ 20 ปี ได้กำหนดปัจจัยและแนวโน้มที่คาดว่าจะส่งผลต่อการพัฒนาประเทศความมั่นคงของประเทศอันเกิดจากภัยคุกคามและความเสี่ยง

---

[1]“ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ.2561-2580)”,ราชกิจจานุเบกษา.เล่มที่ 135, 13 ตุลาคม 2561, หน้า 5.

[2]เรื่องเดียวกัน, หน้า 16.

ด้านอื่นๆที่ซับซ้อนขึ้น[3] โดยเร่งเสริมสร้างความเข้มแข็งและความรักความสามัคคีปรองดองของคนในชาติตลอดถึงการปลุกจิตสำนึกด้านความมั่นคงให้เกิดขึ้นในประชาชนทุกระดับการพัฒนาระบบงานด้านการข่าวให้มุ่งเน้นการบูรณาการข้อมูลข่าวสารด้านความมั่นคงอย่างเป็นระบบ การพัฒนาปรับปรุงกลไกการขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคงและกลไกในการป้องกันและแก้ไขปัญหาความมั่นคงให้มีเอกภาพมีประสิทธิภาพและมีการบูรณาการการดำเนินงานอย่างแท้จริง โดยปัญหาด้านความมั่นคงที่จะต้องดำเนินการแก้ไขอย่างเร่งด่วนมีหลายด้าน ซึ่งหนึ่งในปัญหาเหล่านั้นคือ ปัญหาอาชญากรรมทางไซเบอร์[4]

ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง เป็นการเร่งรัดการแก้ไขปัญหาเดิมที่มีอยู่อย่างจริงจังจนยุติลงหรือไม่ส่งผลกระทบต่อประเทศชาติรวมทั้งบริหารและพัฒนาบ้านเมืองให้เดินหน้าไปได้อย่างต่อเนื่องและมีประสิทธิภาพโดยผลักดันการวิเคราะห์หาสาเหตุที่แท้จริงของปัญหาของทุกภาคส่วนในทุกประเด็นอย่างเป็นระบบส่งเสริมการหารือวางแผนและยกระดับวิธีการแก้ไขปัญหาที่อาศัยการผนึกกำลังคนและทรัพยากรให้มีส่วนร่วมแบบบูรณาการอย่างแท้จริงเสริมสร้างความร่วมมือระหว่างหน่วยงานหลักและรองในการป้องกันแก้ไขปัญหาและช่วยเหลือประชาชนทั้งจากภัยคุกคามและปัญหาต่างๆ ที่ส่งผลกระทบต่อความมั่นคงของชาติเช่นการก่อการร้ายการค้ามนุษย์ การฟอกเงิน รวมถึงอาชญากรรมทางไซเบอร์[5]

ยุทธศาสตร์ยังได้กำหนดการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงรวมทั้งการติดตามและประเมินผลอย่างมีประสิทธิภาพในทุกขั้นตอนเสริมสร้างพลังของประชาชนและชุมชนให้ร่วมกับกำลังตำรวจทหารและหน่วยงานด้านความมั่นคงอื่นๆในการเฝ้าระวังป้องกันและแก้ไขปัญหาสำคัญต่างๆอาทิภัยคุกคามทางไซเบอร์การก่อการร้ายและอาชญากรรมข้ามชาติการแผ่อิทธิพลทางเศรษฐกิจของมหาอำนาจและการย้ายถิ่นของทุนข้ามชาติที่อาจกระทบต่อความมั่นคงไปจนถึงติดตามตรวจสอบการปฏิบัติงานของส่วนราชการต่างๆให้ดำเนินการไปตามเป้าหมายการบริหารจัดการและพัฒนาประเทศที่กำหนดอย่างราบรื่น[6]โดยกองทัพบกเป็นส่วนราชการหนึ่งที่มีหน้าที่ด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ (Cyber Security) เช่นเดียวกับทุกส่วนราชการในขณะเดียวกันก็มีหน้าที่สนับสนุนการปฏิบัติการทางไซเบอร์(Cyber Operations) ให้กับทั้งทางพลเรือนและทางทหารเช่นเดียวกับกองทัพของทุกประเทศในโลกปัจจุบัน

ต่อมาคณะรัฐมนตรีได้พิจารณาให้ความเห็นชอบแผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2561 – 2580) ในส่วนแผนแม่บทประเด็นความมั่นคงได้กำหนดแผนย่อยการป้องกันและแก้ไข

---

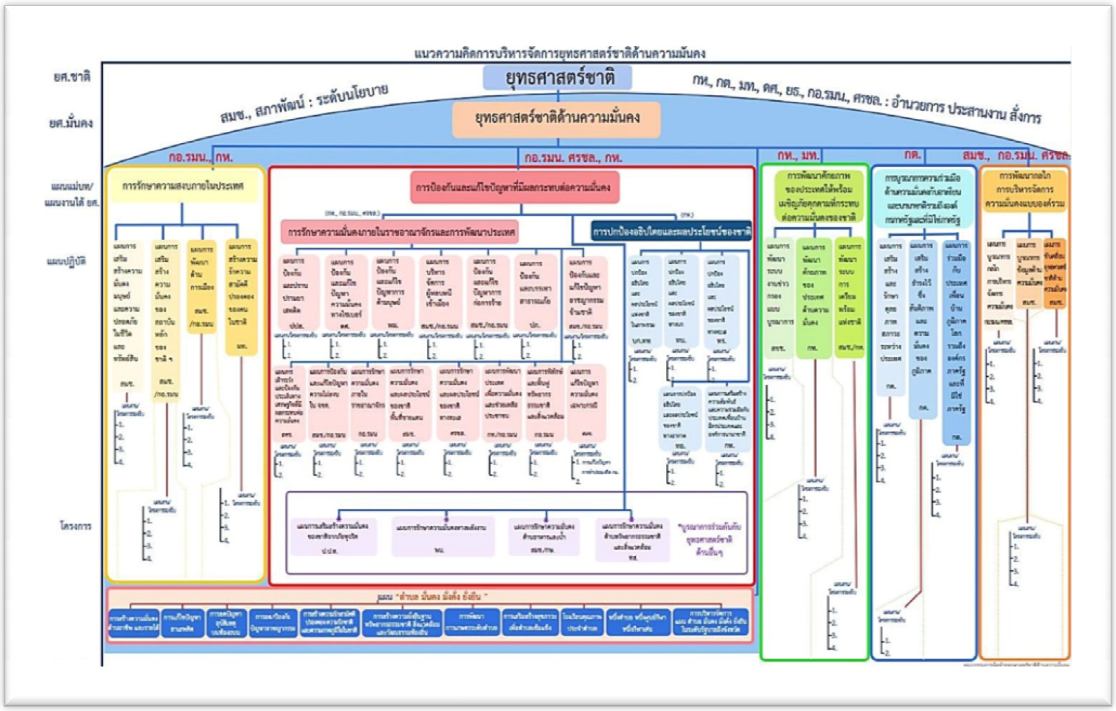
[3] เรื่องเดียวกัน,หน้า 3.

[4] เรื่องเดียวกัน,หน้า 12.

[5] เรื่องเดียวกัน,หน้า 14.

[6] เรื่องเดียวกัน,หน้า 15.

ปัญหาที่มีผลกระทบต่อความมั่นคง รวมทั้งแนวทางการพัฒนา เป้าหมายและตัวชี้วัดไว้ชัดเจน ประกอบด้วยแผนย่อยจำนวน 5 แผนย่อย ได้แก่ (1) การรักษาความสงบภายในประเทศ (2) การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง (3) การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ (4) การบูรณาการความร่วมมือด้านความมั่นคงกับอาเซียนและนานาชาติรวมทั้งองค์กรภาครัฐและมิใช่ภาครัฐ และ (5) การพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม ซึ่งแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคงนี้ได้ครอบคลุมทั้ง5แผนย่อยที่มีความสัมพันธ์เกี่ยวเนื่องเชื่อมโยงและส่งเสริมสนับสนุนซึ่งกันและกันถือเป็นปัจจัยแห่งความสำเร็จที่สำคัญของยุทธศาสตร์ชาติด้านความมั่นคงเนื่องด้วยถึงแม้จะมียุทธศาสตร์ที่ครบถ้วนสมบูรณ์แต่หากมิได้มีการนำไปสู่การปฏิบัติหรือนำไปปฏิบัติอย่างไม่ถูกต้องหรือไม่ครบถ้วนทั้ง5แผนย่อยแล้วก็จะทำให้การดำเนินการไม่สามารถบรรลุผลสำเร็จตามเป้าหมายที่กำหนดเอาไว้ได้ โดยแนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง ซึ่งแสดงได้ตามแผนภาพที่ 1 - 1



แผนภาพที่ 1 - 1 แนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง

ที่มา: สำนักนายกรัฐมนตรี, ประกาศ,2562

สำหรับแผนการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงโดยมีแนวทางการพัฒนาที่สำคัญแบ่งออกเป็น 2 ส่วนคือส่วนการรักษาความมั่นคงภายในราชอาณาจักรและการพัฒนา

ประเทศและส่วนการปกป้องอธิปไตยและผลประโยชน์ของชาติโดยส่วนการรักษาความมั่นคงภายในราชอาณาจักรและการพัฒนาประเทศมีแนวทางการพัฒนาที่สำคัญรวมทั้งสิ้น 15 แนวทาง ประกอบด้วย (1) การป้องกันและปราบปรามยาเสพติด (2) การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ (3) การป้องกันและแก้ไขปัญหาการค้ามนุษย์ (4) การบริหารจัดการผู้หลบหนีเข้าเมือง(5) การป้องกันและแก้ไขปัญหาการก่อการร้าย (6) การป้องกันและบรรเทาสาธารณภัย(7) การป้องกันและแก้ไขปัญหาอาชญากรรมข้ามชาติ (8) การเฝ้าระวังและป้องกันประเด็นทางเศรษฐกิจที่มีผลกระทบต่อความมั่นคง (9) การป้องกันและแก้ไขปัญหาความไม่สงบในจังหวัดชายแดนภาคใต้ (10) การรักษาความมั่นคงภายในราชอาณาจักร (11) การรักษาความมั่นคงและผลประโยชน์ของชาติพื้นที่ชายแดน (12) การรักษาความมั่นคงและผลประโยชน์ของชาติทางทะเล (13) การพัฒนาประเทศเพื่อความมั่นคงและช่วยเหลือประชาชน (14) การพิทักษ์และฟื้นฟูทรัพยากรธรรมชาติและสิ่งแวดล้อมและ (15) การแก้ไขปัญหาความมั่นคงเฉพาะ

ในส่วนการปกป้องอธิปไตยและผลประโยชน์ของชาติมีแนวทางการพัฒนาที่สำคัญรวม5 แนวทางประกอบด้วย (1) การปกป้องอธิปไตยและผลประโยชน์ของชาติในภาพรวม (2) การปกป้องอธิปไตยและผลประโยชน์ของชาติทางบก (3) การปกป้องอธิปไตยและผลประโยชน์ของชาติทางทะเล (4) การปกป้องอธิปไตยและผลประโยชน์ของชาติทางอากาศและ (5) การเสริมสร้างความสัมพันธ์และความร่วมมือกับประเทศเพื่อนบ้านมิตรประเทศและองค์การนานาชาติ

จากที่กล่าวมาการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์จัดอยู่ในส่วนการรักษาความมั่นคงภายในราชอาณาจักรและการพัฒนาประเทศ ซึ่งอยู่ในแผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงในแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ดังนั้นสามารถสรุปได้ว่าภัยคุกคามความมั่นคงด้านไซเบอร์เป็นประเด็นความมั่นคงหลักที่กำหนดไว้ในยุทธศาสตร์ชาติไว้อย่างชัดเจน

เรื่องความมั่นคงปลอดภัยทางไซเบอร์ นอกจากจะถูกกำหนดไว้ในแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคงแล้ว ยังมีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งมีผลบังคับใช้กับทุกส่วนราชการโดยกำหนดนิยามของคำว่า “ไซเบอร์ หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป”[7] นอกจากนี้ยังได้กำหนดนิยามของ “โครงสร้างพื้นฐานสำคัญทางสารสนเทศหมายความว่าคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐ

[7]“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562”, ราชกิจจานุเบกษา. เล่ม 136, 27 พฤษภาคม 2562, หน้า 21.

หรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐความปลอดภัยสาธารณะความมั่นคงทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ”[8]ซึ่งมีความเกี่ยวข้องกับงานด้านไซเบอร์ ส่งผลให้หน่วยงานเหล่านี้อยู่ในความหมายของ “ไซเบอร์” และกองทัพไทยก็ต้องพัฒนาระบบงานไซเบอร์เพื่อรองรับพระราชบัญญัติฯ ดังกล่าวด้วย

หลังจากการจัดตั้งหน่วยงานด้านไซเบอร์ขึ้นในสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย และทุกเหล่าทัพแล้ว ดูเหมือนว่างานไซเบอร์ของกองทัพไทยจะดำเนินไปด้วยความเรียบร้อย แต่จากการปฏิบัติงานไปได้ระยะหนึ่งพบว่าความก้าวหน้าของงานไซเบอร์ยังไม่ดีเท่าที่ควรโดยยังมีข้อจำกัดอีกหลายด้านที่ยังไม่ได้ดำเนินการพัฒนาไปพร้อมการจัดตั้งหน่วยงานไซเบอร์

สาเหตุขั้นต้นคาดว่าน่าจะเกิดจากงานไซเบอร์ได้ถูกแยกมาจากงานด้านการสื่อสารด้วยวิธีการแยกหน่วยรองมาจัดตั้งเป็นหน่วยใหม่เพื่อรองรับงานไซเบอร์ ในขณะที่ระบบงานสื่อสารเดิมก็ยังไม่ได้รับการปรับบทบาทหรือกำหนดขอบเขตหน้าที่ความรับผิดชอบงานให้ชัดเจน จึงทำให้เกิดปัญหาความซ้ำซ้อนและความไม่ชัดเจนในการเชื่อมโยงระบบงานตั้งแต่ภารกิจ ขอบเขตหน้าที่และความรับผิดชอบที่สำคัญในอัตรา ซึ่งส่งผลกระทบถึงการจัดโครงสร้างอัตรากำลัง และการบริหารงานบุคคล รวมถึงการปฏิบัติภารกิจต่างๆ

สาเหตุที่น่าจะเป็นไปได้ประการต่อมาคือ การจัดฝ่ายอำนวยการรับผิดชอบงานไซเบอร์ในระดับเหล่าทัพขึ้นไปยังขาดความชัดเจนเนื่องจากระบบงานกรมฝ่ายเสนาธิการของกองทัพไทยยังคงยึดถือตามระบบเดิมที่แบ่งออกเป็น 6 สายงาน ได้แก่ สายงานกำลังพล สายงานข่าว สายงานยุทธการ สายงานส่งกำลังบำรุง สายงานกิจการพลเรือน และสายงานปลัดบัญชี ส่งผลทำให้งานด้านไซเบอร์ งานด้านการสื่อสาร และงานด้านสารสนเทศยังคงรวมอยู่ในความรับผิดชอบของสายงานยุทธการหรือกรมยุทธการของเหล่าทัพและกองบัญชากองทัพไทยซึ่งมีภาระหน้าที่เร่งด่วนจำนวนมากทำให้ความเร่งด่วนในการพัฒนาหน่วยงานไซเบอร์ถูกจัดอยู่ในลำดับความสำคัญลำดับท้ายๆ

สาเหตุที่น่าจะเป็นไปได้ประการสุดท้ายคือ กองทัพบกก็เป็นส่วนราชการหนึ่งที่จะต้องปฏิบัติตามกฎหมาย ระเบียบ ที่กำหนดให้ทุกส่วนราชการปฏิบัติ แต่ในความเป็นจริงแล้วกองทัพมีความมุ่งหมายในการจัดตั้งที่แตกต่างไปจากพลเรือนโดยเฉพาะต้องปฏิบัติตามหลักนิยมเพื่อสนับสนุนการปฏิบัติการทางทหารซึ่งแบ่งออกเป็นการปฏิบัติการไซเบอร์เชิงรุก (Offensive Cyber Operations) และการปฏิบัติการไซเบอร์เชิงรับ (Defensive Cyber Operations) ในขณะที่กฎหมายของฝ่ายพลเรือนมีเพียงเฉพาะการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เท่านั้น จึงทำให้ฝ่าย

---

[8]เรื่องเดียวกัน, หน้า 22.

พลเรือนขาดมุมมองในการพัฒนาหน่วยงานไซเบอร์เพื่อสนับสนุนการปฏิบัติภารกิจทางทหารซึ่งรวมถึงการจัดสรรงบประมาณและบุคลากรให้กับกองทัพ

จากสาเหตุที่น่าจะเป็นไปได้สามประการดังกล่าวน่าจะส่งผลทำให้กองทัพขาดความชัดเจนในเรื่องโครงสร้างการจัดอัตรากำลังหน่วยงานไซเบอร์ และเมื่อพิจารณาระบบงานปฏิบัติการข่าวสาร รวมทั้งการพัฒนาระบบงานการข่าวซึ่งขยายขอบเขตเข้าไปในระบบงานสารสนเทศมากขึ้น ยิ่งทำให้เกิดความไม่ชัดเจนของระบบงานไซเบอร์ทั้งในด้านโครงสร้างการจัด อัตรากำลัง รวมถึงระบบการบริหารงานบุคคล ซึ่งอาจจะกล่าวสรุปได้ในภาพรวมว่ากองทัพไทยมุ่งไปที่การจัดตั้งหน่วยไซเบอร์เพื่อรองรับงาน แต่ไม่ได้ปรับปรุงระบบงานอื่นๆ ให้สอดคล้องกันไปด้วย จึงจำเป็นต้องศึกษาวิจัยการพัฒนาหน่วยงานด้านไซเบอร์ เพื่อให้รองรับงานตามยุทธศาสตร์ชาติได้ชัดเจน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาหน่วยงานด้านไซเบอร์ของกองทัพบกไทย ในด้านความเหมาะสม ความเพียงพอที่จะสามารถรองรับภัยคุกคามด้านไซเบอร์ตามยุทธศาสตร์ชาติด้านความมั่นคง

2. เพื่อศึกษาความเชื่อมโยงระหว่างระบบไซเบอร์กับระบบที่เกี่ยวข้องซึ่งขยายมาจากกลุ่มงานของกองทัพบกเดิม ได้แก่ ระบบสื่อสาร ระบบสารสนเทศ ระบบปฏิบัติการข้อมูลข่าวสาร และระบบควบคุมบังคับบัญชา

3. เพื่อศึกษาการพัฒนากำลังพลในหน่วยงานไซเบอร์ของกองทัพบกไทยให้สามารถรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้

ขอบเขตของการวิจัย

การวิจัยนี้จะจำกัดขอบเขตระดับในการวิเคราะห์ (Level of Analysis) และหน่วยในการวิเคราะห์(Unit of Analysis) ที่ระดับกองทัพบกไทย เพื่อให้เหมาะสมกับข้อจำกัดด้านเวลาและระดับของเอกสารวิจัยในหลักสูตรวิทยาลัยป้องกันราชอาณาจักร โดยการจำกัดขอบเขตที่กองทัพบกดังกล่าวไม่ได้ส่งผลกระทบต่อการวิจัยข้ามระดับในการเชื่อมโยงถึงระดับยุทธศาสตร์ชาติด้านความมั่นคง เนื่องจากกองทัพบกไทยเป็นหน่วยปฏิบัติหลักด้านความมั่นคงของรัฐที่กำหนดในแผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคงด้วย และปัญหาของระบบงานไซเบอร์ของทุกส่วนราชการในกระทรวงกลาโหมจะคล้ายกัน ซึ่งการวิจัยจะได้อธิบายความเชื่อมโยงระหว่างระดับกระทรวงกลาโหม

กองบัญชาการกองทัพไทย และเหล่าทัพอื่นด้วยแล้วจึงสามารถนำผลการวิจัยที่ค้นพบไปอธิบายปรากฏการณ์ที่เกิดขึ้นกับส่วนราชการอื่นในกระทรวงกลาโหมได้

วิธีดำเนินการวิจัย

การวิจัยในครั้งนี้มุ่งเน้นไปที่โครงสร้างการจัดและระบบงานด้านไซเบอร์ ซึ่งจัดอยู่ในสาขาสังคมศาสตร์ที่เป็นปฏิสัมพันธ์ระหว่างคน โดยเป็นการวิจัยเพื่อหาข้อสรุปเชิงนโยบาย ดังนั้น จึงใช้ระเบียบวิธีวิจัยเชิงคุณภาพซึ่งมีความเหมาะสมกับวัตถุประสงค์ในการวิจัย โดยใช้การเก็บข้อมูลจากเอกสารที่เกี่ยวข้อง การสัมภาษณ์ผู้ให้ข้อมูลสำคัญที่มีประสบการณ์ในการปฏิบัติงาน และการสังเกตการณ์แบบมีส่วนร่วมของผู้วิจัย ร่วมกับการเก็บข้อมูลระบบงานไซเบอร์ของกองทัพไทยและส่วนราชการขึ้นตรง ระบบไซเบอร์ของประเทศไทย และประเทศอื่น รวมทั้งความเชื่อมโยงในด้านต่างๆ ที่เกี่ยวข้อง ได้แก่ การฝึกและศึกษาทางทหาร ระบบอัตรากำลัง และระบบการบริหารงานบุคคล แล้วนำข้อมูลที่ได้มาจัดระเบียบ ตีความ และสรุปผลออกมาเป็นข้อสรุปและข้อเสนอของการวิจัย

ประโยชน์ที่ได้รับจากการวิจัย

1. ผลการวิจัยสามารถใช้เป็นข้อเสนอเชิงนโยบายในการพัฒนาระบบงานไซเบอร์ของกองทัพไทย เพื่อให้สามารถนำไปกำหนดเป็นนโยบายในการเตรียมบุคลากรให้มีความพร้อม สามารถรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้

2. หน่วยงานของกระทรวงกลาโหมสามารถนำผลการวิจัยไปเป็นแนวทางในการพัฒนาระบบไซเบอร์ให้มีความเชื่อมโยงกับระบบไซเบอร์ระดับประเทศ

3. หน่วยงานต่างๆ สามารถนำแบบจำลองหน่วยงานทางไซเบอร์ที่ได้จากผลการวิจัย ไปพัฒนาต่อยอดให้เหมาะสมกับสภาพแวดล้อมและสถานการณ์ทางไซเบอร์ได้

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคงจะเกี่ยวข้องกับความรู้ด้านความมั่นคง ทฤษฎีองค์การ และการบริหารงานบุคคล โดยทฤษฎีด้านความมั่นคงจะได้อธิบายถึงความสำคัญของกองทัพในฐานะที่เป็นเครื่องมือของรัฐในการรักษาความมั่นคงของรัฐทั้งต่อภัยคุกคามระหว่างรัฐและภัยคุกคามรูปแบบใหม่ซึ่งรวมถึงความมั่นคงด้านไซเบอร์ (Cyber Security) ด้วย ส่วนแนวคิดทฤษฎีองค์การ ซึ่งอธิบายถึงการที่เราจะเตรียมความพร้อมหน่วยงานปฏิบัติการไซเบอร์เพื่อให้สามารถปฏิบัติหน้าที่รักษาความมั่นคงดังกล่าวได้นั้น ต้องมีโครงสร้างการจัดของกองทัพที่มีความเชื่อมโยงกับระบบเดิมอย่างไร โดยกองทัพเป็นองค์การภาครัฐองค์การหนึ่งซึ่งยึดถือหลักเช่นเดียวกับทุกองค์การทั้งภาครัฐและภาคเอกชน สำหรับทฤษฎีการบริหารงานบุคคลนั้น จะได้อธิบายรายละเอียดการพัฒนาบุคลากรด้านไซเบอร์ โดยทุกขั้นตอนมีความสัมพันธ์เชื่อมโยงกันอย่างเป็นระบบ ดังนั้น จึงมีความจำเป็นที่จะต้องศึกษาให้ครบทุกขั้นตอนในทั้งสามระบบดังกล่าว รวมถึงการทบทวนวรรณกรรมและหลักการที่เกี่ยวข้องด้านการฝึกและศึกษาทางทหารซึ่งกองทัพไทยและกองทัพต่างประเทศได้กำหนดขึ้นไว้ด้วยเพื่อกำหนดเป็นกรอบแนวทางในการดำเนินการศึกษาและรวบรวมข้อมูลในบทต่อไป

พัฒนาการแนวคิดและทฤษฎีกองทัพกับความมั่นคงรูปแบบใหม่

หลังจากสงคราม 30 ปี ระหว่างปี ค.ศ.1618-1648 ได้มีการลงนามสนธิสัญญาเวสต์ฟาเลียส่งผลทำให้เกิดรัฐอธิปไตยในยุโรปขึ้นโดยรัฐมีอำนาจที่จะจัดการกิจการภายในและภายนอกได้โดยปราศจากการแทรกแซงจากภายนอกโดยเฉพาะอิทธิพลของศาสนาจักร ดังนั้นกำลังทหารซึ่งเดิมเป็นทหารของขุนนางหรือทหารรับจ้างก็จำเป็นต้องรวบรวมเป็นหน่วยสำหรับเป็นเครื่องมือของรัฐเพื่อให้สามารถใช้อำนาจอธิปไตยดังกล่าวได้ กองทัพที่มีการจัดเป็นหน่วยถาวรเหมือนในปัจจุบันเกิดขึ้นมาพร้อมกับรัฐอธิไตยเพื่อเป็นเครื่องมือของรัฐในการดำเนินนโยบายการเมืองระหว่างประเทศ แนวคิดรัฐอธิปไตยดังกล่าวได้เผยแพร่เข้ามาในภูมิภาคเอเชียตะวันออกเฉียงใต้ในยุคการล่าอาณานิคมช่วงปลายศตวรรษที่ 19หรือสมัยพระบาทสมเด็จพระปิยะมหาราช รัชกาลที่ 5 ส่งผลทำให้สยามจำเป็นต้องกำหนดเขตแดนรัฐที่ชัดเจนรวมทั้งปฏิรูปการปกครองที่เดิมเป็นหัวเมืองต่างๆ มาเป็นการ

รวมศูนย์อำนาจไว้ที่เมืองหลวง พร้อมกับปฏิรูปกิจการทหารสมัยใหม่ให้เป็นทหารของรัฐ โดยเป็นอาชีพที่ชัดเจน มีการฝึกและศึกษา มีค่ายที่พักเหมือนกับกองทัพในรัฐตะวันตก

1.กองทัพไทยกับความมั่นคงของรัฐ

การปฏิรูปกองทัพสยามในสมัยรัชกาลที่ 5 ไม่ได้จัดตั้งขึ้นเพื่อทำสงครามระหว่างรัฐตามแนวคิดของรัฐตะวันตกเนื่องจากสยามและทุกรัฐในเอเชียตะวันออกในขณะนั้นล้วนแล้วแต่ยังไม่มีขีดความสามารถในการทำสงครามกับชาติตะวันตกได้อังกฤษและฝรั่งเศสต่างก็มีขีดความสามารถทางทหารสูงและครอบครองดินแดนประเทศเพื่อนบ้านเสียทั้งหมด ทำให้สยามต้องยอมเสียดินแดนรอบประเทศจำนวนมากเพื่อแลกกับเอกราช กองทัพไทยในช่วงแรกมีบทบาทด้านการรักษาความมั่นคงภายในรัฐทั้งการปฏิบัติหน้าที่แทนตำรวจซึ่งยังไม่ได้มีการจัดตั้ง ตลอดจนการช่วยเหลือในการรักษาความปลอดภัยในการเก็บภาษี กองทหารซึ่งส่งออกไปประจำการตามหัวเมืองชั้นนอกและชั้นในสมัยตอนต้นรัชกาลที่ 5 มีหน้าที่ปราบปรามโจรผู้ร้ายและช่วยเหลือการเก็บภาษีอากร ตามข้อบังคับกรมทหารบก พ.ศ.2430[9] ต่อมาเมื่อปีพ.ศ.2440 สยามได้จัดตั้งกรมตำรวจภูธรเพื่อทำหน้าที่รักษาความปลอดภัยปราบปรามโจรผู้ร้าย แต่ในช่วงแรกก็ยังคงใช้กำลังทหารในการปฏิบัติงาน ต่อมาในปี พ.ศ.2453 พระบาทสมเด็จพระจุลจอมเกล้าเจ้าอยู่หัวทรงพระกรุณาโปรดเกล้าให้กรมยุทธนาธิการหรือกระทรวงกลาโหมปัจจุบัน ส่งสัญญาบัตรทหารกรมตำรวจภูธรไปพระราชทานแก่ข้าราชการซึ่งรับราชการอยู่ ณ หัวเมืองต่างๆ[10] หรืออาจจะกล่าวได้ว่ากองทัพไทยมีหน้าที่ในการรักษาความมั่นคงภายในราชอาณาจักรและการรักษาความสงบเรียบร้อยมานานแล้ว

หลังจากนั้นสยามได้ขยายโครงสร้างกำลังกองทัพไทยมากขึ้นตามแผนโครงสร้างกองทัพบกสยาม พ.ศ.2451 ซึ่งกำหนดให้กองทัพบกมี 10 กองพลต่อมาในปี พ.ศ.2452 กรมหมื่นนครไชยศรีสุรเดช กราบบังคมทูลขอพระราชทานพระบรมราชานุญาตจัดและขนามนามกรมทหารเป็น 10 กองพล ตามเป้าหมาย รัชกาลที่ 5 ทรงพระดำริให้จัดตั้งแบบหลวมๆ ไปก่อนเมื่อมีเงินน้อยจัดกำลังกรมทหารในกองพลให้น้อยลง และเมื่อได้รับเงินจำนวนมากก็เพิ่ม[11] โดยวางกำลังหน่วยกระจายไปตามพื้นที่ทั่วประเทศตามการแบ่งการปกครองเป็นมณฑลและข้อจำกัดด้านเส้นทางคมนาคม ซึ่งรูปแบบการวางกำลังทหารกระจายทั่วประเทศดังกล่าวได้สืบทอดมาจนถึงปัจจุบัน หรืออาจสรุปได้ว่าโครงสร้างกองทัพไทยในปัจจุบันเป็นผลสืบทอดมาจากอดีตที่มีการจัดวางกำลังที่ตั้งหน่วยทหารเสร็จแล้วตั้งแต่การปกครองตามระบอบสมบูรณาญาสิทธิราชย์เพียงแต่ขยายเพิ่มจำนวนให้ครบตามแนวคิด

---

[9]ศาลายุทธนาธิการ ข้อบังคับกรมทหารบก คำสั่งที่ 2 ว่าด้วยน่าที่ของออฟฟิศเซอบังคับทหารรักษาราชการตามหัวเมือง จุลศักราช 1249.

[10]ราชกิจจานุเบกษา เล่มที่ 26 น่า 1103 วันที่ 22 สิงหาคม ร.ศ.128.

[11]ก.จ.ช. เอกสาร ร.5 ก.13.2/37 สำเนา ที่ 31/17914 กรมหมื่นนครไชยศรีสุรเดช กราบบังคมทูลพระบาทสมเด็จพระเจ้าอยู่หัว ลง วันที่ 4 กุมภาพันธ์ ร.ศ.126 (พ.ศ.2452).

เดิมและจัดหายุทโธปกรณ์ให้ทันสมัยตามยุคสมัย แต่อย่างไรก็ตาม ยังไม่ได้มีบทบาทในการรักษาอธิปไตยของรัฐตามแนวคิดการมีกองทัพเป็นเครื่องมือทางการเมืองระหว่างประเทศแต่อย่างใด

ในสมัยรัชกาลที่ 5 กองทัพไทยมีการพัฒนาให้มีความเข้มแข็งอย่างต่อเนื่องโดยมีการจัดตั้งกระทรวงยุทธนาธิการและทำการปฏิรูปกองทัพจนสามารถทำการรบชนะฝรั่งเศสในสงครามมหาเอเชียบูรพาในปี พ.ศ.2483 และการประกาศเข้าร่วมสงครามโลกครั้งที่2 ในปี พ.ศ.2484 จึงนับว่าไทยได้ใช้กำลังทหารเป็นเครื่องมือในการดำเนินการเมืองระหว่างประเทศต่อเนื่องถึงช่วงสงครามโลกครั้งที่ 2 ยุติลง จนถึงช่วงสงครามเย็น ไทยได้จัดส่งกำลังทหารไปช่วยรบในสงครามเกาหลีเมื่อปี พ.ศ.2493เพื่อป้องกันไม่ให้ลัทธิคอมมิวนิสต์ขยายแผ่มาถึงลาวและเวียดนาม ทำให้ไทยต้องร่วมมือกับสหรัฐอเมริกาโดยการส่งกำลังทหารเข้าร่วมสงครามในลาวและเวียดนามจนกระทั่งสงครามเย็นยุติลง ดังนั้น ในช่วงตั้งแต่สงครามโลกครั้งที่2 จนถึงสงครามเย็นยุติ ไทยได้ใช้กำลังทหารในการดำเนินการทางการเมืองระหว่างประเทศอย่างแท้จริง ส่งผลทำให้การเสริมสร้างความพร้อมรบของกองทัพไทยในช่วงดังกล่าวมุ่งเน้นไปที่การใช้กองทัพเป็นเครื่องมือในการทำสงครามระหว่างรัฐ ในขณะเดียวกันกองทัพไทยได้รับการพัฒนาจากกองทัพสหรัฐอเมริกาทั้งในด้านการจัด อาวุธยุทโธปกรณ์ งบประมาณ ตลอดจนการฝึกและศึกษา ส่งผลให้กองทัพไทยมีความคล้ายคลึงกับกองทัพสหรัฐอเมริกาตั้งแต่นั้นเป็นต้นมา ในขณะที่ปัจจุบันกองทัพสหรัฐอเมริกาได้มีการพัฒนาไปไกลเพื่อรองรับการปฏิบัติการไซเบอร์ตลอดจนย่านคลื่นความถี่แม่เหล็กไฟฟ้าและอวกาศ

หลังสงครามเย็นยุติลง กองทัพทั่วโลกได้ลดบทบาทในการใช้กองทัพเป็นเครื่องมือทางการเมืองระหว่างรัฐพร้อมกับการกำหนดแนวคิดความมั่นคงของมนุษย์โดยสหประชาชาติในปี ค.ศ.1994 ที่นับว่าเป็นความมั่นคงรูปแบบใหม่ ประกอบกับรัฐในประเทศที่กำลังพัฒนาได้เริ่มการต่อสู้เพื่อแย่งอำนาจทางการเมืองภายในรัฐ ดังนั้น ความขัดแย้งระหว่างรัฐได้กลายมาเป็นความขัดแย้งภายในรัฐ ทำให้กองทัพของรัฐต่างๆ พยายามปรับบทบาทในการใช้กำลังทหารเพื่อปฏิบัติภารกิจทางทหารที่นอกเหนือจากสงคราม (Military Operations Other Than Wars: MOOTW)ซึ่งรวมถึงการปฏิบัติการไซเบอร์ด้วยโดยกองทัพไทยได้มีบทบาทใหม่ในการรักษาความมั่นคงภายในรัฐและภัยคุกคามรูปแบบใหม่มากขึ้น ส่งผลทำให้กองทัพไทยต้องเสริมสร้างกองทัพใหม่ให้มีความพร้อมปฏิบัติภารกิจตลอดทุกย่านของความขัดแย้งรวมถึงภัยคุกคามรูปแบบใหม่ซึ่งมีการเปลี่ยนแปลงตลอดเวลาเพื่อตอบสนองต่อความก้าวหน้าทางเทคโนโลยีในด้านต่างๆ โดยเฉพาะเทคโนโลยีสารสนเทศจึงนับได้ว่ากองทัพไทยมีพัฒนาการอย่างมากในช่วงสองทศวรรษที่ผ่านมา

2. แนวคิดและทฤษฎีกองทัพกับความมั่นคงของรัฐ

จากการที่การเมืองระหว่างประเทศอยู่ในสภาวะอนาธิปไตยซึ่งไม่มีรัฐบาลกลางมาควบคุมส่งผลทำให้พลังอำนาจทางทหารยังคงมีความจำเป็นต่อรัฐพลังอำนาจทางทหารจึงรวมเข้ากับการเมืองโดยไม่สามารถแยกออกจากนโยบายต่างประเทศได้และกำลังทหารสามารถใช้ในภารกิจที่

หลากหลายทั้งวัตถุประสงค์ทางทหารและไม่ใช่ทางทหาร[12]หลังจากสงครามเย็นยุติลงในต้นทศวรรษ 1990 ความขัดแย้งจนถึงระดับการใช้กำลังทหารทำสงครามระหว่างรัฐ (Interstate War) ลดน้อยลงเหลือเพียงความขัดแย้งระดับต่ำ (Low Intensity Conflict) ทำให้มีแนวคิดในการนำกำลังทหารมาใช้ภายในรัฐมากขึ้นโดยเฉพาะหลังจากเหตุการณ์ 9/11 ได้ทำให้ประชาคมระหว่างประเทศเพิ่มบทบาทกองทัพต่อภัยคุกคามรูปแบบใหม่ (Non-traditional Threat) มากขึ้น โดยมีลักษณะของภัยคุกคามที่ข้ามพรหมแดนเข้ามาภายในรัฐ

ถึงแม้ว่ารัฐจะมีอำนาจอธิปไตยภายในรัฐ แต่การใช้กำลังทหารภายในรัฐไม่ใช่สิ่งที่อ้างว่าเป็นอธิปไตยภายในที่รัฐจะสามารถใช้กำลังทหารอย่างไรก็ได้ โดยเฉพาะผลกระทบต่อประชาชนภายในรัฐเองแต่เป็นประเด็นสากลที่เกี่ยวข้องกับกฎหมายสิทธิมนุษยชนตามพันธะกรณีที่ทุกรัฐได้เป็นสมาชิกองค์การระหว่างประเทศโดยเฉพาะหลังจากเหตุการณ์ 9/11 รัฐต่างๆได้นำกองทัพเข้ามาปฏิบัติภารกิจในการบังคับใช้กฎหมายภายในรัฐมากขึ้น กองทัพบกสหรัฐอเมริกาได้กำหนดวิสัยทัศน์ในยุทธศาสตร์ 2028 ให้มีความพร้อมในการวางกำลัง การต่อสู้ และเอาชนะทุกฝ่ายตรงข้ามทุกเวลา และทุกสถานที่ ในการปฏิบัติการร่วม/ผสม ในทุกขอบเขต ในความขัดแย้งระดับสูงในขณะเดียวกันก็พร้อมที่จะดำรงขีดความสามารถในการปฏิบัติการสงครามที่ไม่เป็นตามแบบ ซึ่งกองทัพทำได้โดยการวางกำลังยานรบและอากาศยานทั้งที่มีคนขับและไม่มีคนขับ บนพื้นฐานของหลักนิยมการรบสมัยใหม่ บนศูนย์กลางของผู้นำชั้นยอดและทหารที่มีขีดความสามารถในการทำลายล้างสูง สำหรับการรบแบบ Multi-domain นั้น กองทัพบกไม่เพียงแต่จะรบบนพื้นดิน ทะเล และอากาศเท่านั้น แต่ยังมีขีดความสามารถในทุกขอบเขตรวมทั้งไซเบอร์ อวกาศ และย่านความถี่แม่เหล็กไฟฟ้าอีกด้วย[13] ซึ่งจะทำให้ขอบเขตบทบาทของกองทัพกับความมั่นคงของรัฐในด้านภัยคุกคามรูปแบบใหม่เปลี่ยนแปลงไปจากเดิมอย่างมาก ตามตัวอย่างภารกิจในการบังคับใช้กฎหมายของรัฐต่างๆรวมถึงการปฏิบัติการไซเบอร์ (Cyber Operations)

ผลกระทบจากแนวคิดในการใช้กำลังทหารในภารกิจที่นอกเหนือสงครามซึ่งรวมถึงการปฏิบัติการไซเบอร์ดังกล่าว ทำให้รัฐต่างๆจำเป็นต้องพัฒนาการจัดและการพัฒนาบุคคลให้สอดคล้องตามไปด้วย เพื่อให้สามารถใช้กำลังกองทัพได้อย่างมีประสิทธิภาพและไม่เกิดผลกระทบต่อประชาชนของรัฐ จึงทำให้รูปแบบโครงสร้างการจัดที่กองทัพไทยได้นำมาจากกองทัพสหรัฐในอดีตจำเป็นต้องได้รับการปรับปรุงให้ทันสมัยในขณะที่โครงสร้างพื้นฐานกองทัพไทยตั้งแต่ระบบอัตรากำลังระบบการบริหารงานบุคคลยังคงไม่เปลี่ยนแปลง

---

[12]Robert J. Art and Robert Jervis. "The fungibility of force",inInternational politics: Enduring concepts and contemporary issues. (New York : Pearson, 2009). p.205.

[13]The U.S. Army."The Army Strategy". (Headquarters, Deputy Chief of Staff, G-3-5-7. 2018). p.1.

การปฏิบัติการไซเบอร์กับความพร้อมรบของกองทัพ

ในปัจจุบันนี้ยังไม่มีหลักการแนวคิด และทฤษฎีที่สามารถนำมาใช้ในการกำหนดโครงสร้างการจัดกำลังกองทัพให้มีความพร้อมรบให้เป็นที่ยอมรับของประชาชนในรัฐโดยไม่มีข้อโต้แย้งเกิดขึ้น เพราะความพร้อมรบของกองทัพเป็นเรื่องที่ขึ้นอยู่กับการรับรู้ (Perception) ของรัฐและประชาชนภายในรัฐว่ามีความพร้อมหรือไม่ ทั้งภัยคุกคามรูปแบบเดิมและภัยคุกคามรูปแบบใหม่ ปัญหาสำคัญที่สุดในการกำหนดโครงสร้างการจัดอัตรากำลัง หรือองค์ประกอบของความพร้อมรบของกองทัพนั้น อยู่ที่ข้อจำกัดด้านงบประมาณ ถ้ารัฐไม่มีข้อจำกัดด้านงบประมาณก็ย่อมสามารถจัดกำลังอย่างใดก็ได้ แต่โดยปกติแล้วทุกรัฐล้วนมีข้อจำกัดด้านงบประมาณการทหารทั้งสิ้นมากน้อยแตกต่างกันออกไป ความพร้อมรบของกองทัพไม่ได้ขึ้นอยู่กับฝ่ายเราแต่เพียงลำพัง แต่ขึ้นอยู่กับฝ่ายตรงข้ามด้วย ดังนั้น ถ้าการประมาณการภัยคุกคามผิดพลาดไปก็จะส่งผลให้รัฐต้องจัดสรรงบประมาณจำนวนมากไปใช้ในการจัดเตรียมกำลังกองทัพ ซึ่งจะกระทบต่องบประมาณของรัฐที่ต้องนำไปใช้ในกิจการอื่นโดยเฉพาะสภาวะแวดล้อมในปัจจุบันทั้งการเข้าสู่ประชาคมอาเซียนและการพัฒนากฎหมายระหว่างประเทศด้านสิทธิมนุษยชน

สำหรับกองทัพไทยนั้น ได้กำหนดความพร้อมรบของกองทัพประกอบด้วย 4 ด้าน ได้แก่ กำลังพล ยุทโธปกรณ์ การฝึกและศึกษาและแผนปฏิบัติ[14]ซึ่งการปฏิบัติการไซเบอร์เป็นแผนปฏิบัติการหนึ่งในการที่จะทำให้กองทัพมีความพร้อมรบดังนั้นปัจจุบันทุกกองทัพจึงให้ความสำคัญกับการปฏิบัติการไซเบอร์มาก เพื่อปฏิบัติตามแผนให้บรรลุตามหน้าที่ที่กำหนดไว้ในกฎหมายได้อย่างมีประสิทธิภาพควบคู่ไปกับความพร้อมรบด้านอื่น

นอกจากการปฏิบัติการไซเบอร์จะเกี่ยวข้องในด้านแผนปฏิบัติแล้ว ยังมีความเกี่ยวข้องกับความพร้อมรบด้านกำลังพลซึ่งจะเกิดขึ้นได้ต่อเมื่อมีการบริหารจัดการที่เหมาะสมกองทัพก็เป็นองค์การภาครัฐหนึ่งเหมือนองค์การทั่วไปซึ่งจำเป็นต้องมีระบบการบริหารจัดการเช่นเดียวกัน แตกต่างกันตรงที่กองทัพมีหน้าที่ในการใช้อำนาจของรัฐและมีสิทธิในการครอบครองอาวุธร้ายแรง ส่วนในเรื่องอื่นโดยทั่วไปแล้วไม่มีความแตกต่างกันมากนัก โดยเฉพาะระบบโครงสร้างอัตรากำลัง ระบบการบริหารงานบุคคล และระบบงบประมาณ ซึ่งมีขั้นตอนในการพิจารณาในฐานะเป็นส่วนราชการหนึ่งของรัฐ สำหรับในหัวข้อนี้จะมุ่งเน้นที่ทฤษฎีการบริหารทรัพยากรบุคคลซึ่งประกอบด้วยขั้นตอนต่างๆ จำนวน 7 ขั้นตอนอย่างเป็นระบบ ได้แก่ การจัดองค์การ การพัฒนาตำแหน่ง การรับสมัคร การสัมภาษณ์และคัดเลือก การฝึกอบรม การประเมินผล และการตอบแทน[15] ตามแผนภาพที่ 2 - 1

---

[14]กองทัพบก. “แผนพัฒนากองทัพบก ปี 2560 – 2564”.

[15]Gary Dessler.Human Resource Management, 12th ed., (New Jersey: Pearson, 2011). p.332.

แผนภาพที่ 2 - 1 ขั้นตอนการบริหารทรัพยากรบุคคล

ที่มา : Gary Dessler, 2011 : 332

ทฤษฎีองค์การกับการพัฒนาหน่วยงานไซเบอร์ของกองทัพบก

กองทัพบกไทยมีพื้นที่ฐานโครงสร้างการจัดมาจากกองทัพบกสหรัฐอเมริกา เนื่องจากสหรัฐให้ความช่วยเหลือไม่ให้ไทยเป็นฝ่ายแพ้สงครามโลกครั้งที่ 2 พร้อมญี่ปุ่น โดยความสัมพันธ์ไทย - สหรัฐ เริ่มใกล้ชิดมากขึ้นในปี พ.ศ.2493 เมื่อสหรัฐวิตกกังวลเรื่องการขยายอิทธิพลของลัทธิคอมมิวนิสต์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งสหรัฐเห็นความสำคัญทางยุทธศาสตร์ของไทยในการต่อต้านคอมมิวนิสต์ ในขณะเดียวกันรัฐบาลไทยภายใต้การนำของจอมพล ป.พิบูลสงคราม หวั่นเกรงภัยคุกคามต่อความมั่นคงจากลัทธิคอมมิวนิสต์โดยเฉพาะจากจีน ไทยและสหรัฐจึงมีผลประโยชน์ร่วมกันและกลายมาเป็นพันธมิตรร่วมกันในหลายด้าน จนนำไปสู่การลงนามในความตกลง 3 ฉบับในปีเดียวกัน ซึ่งเกี่ยวกับการแลกเปลี่ยนการศึกษาและวัฒนธรรม ความร่วมมือทางเศรษฐกิจและวิทยาการ และความช่วยเหลือด้านการป้องกันประเทศ[16] ผลที่ตามมาคือกองทัพไทยได้รับรูปแบบโครงสร้างการจัดมาจากสหรัฐแทบทุกด้านและแทบไม่ได้มีการเปลี่ยนแปลงไปจากเดิม

ในขณะที่กองทัพบกสหรัฐได้มีการปรับปรุงโครงสร้างการจัดกองทัพตามยุทธศาสตร์กองทัพบก ค.ศ.2028 โดยทุกหน่วยระดับกองพลน้อยจนถึงกองทัพน้อยจะต้องมีขีดความสามารถในการปฏิบัติการภาคพื้นดิน ทางอากาศ การเฝ้าตรวจ การลาดตระเวน สงครามอิเล็กทรอนิกส์ และการปฏิบัติการไซเบอร์เพื่อให้สามารถดำรงการควบคุมสนามรบได้อย่างต่อเนื่อง[17]ซึ่งกองทัพเป็นองค์การภาครัฐองค์การหนึ่งเหมือนกับทุกองค์การภาครัฐ ซึ่งทุกองค์การจะเป็นไปตามทฤษฎีองค์การตั้งแต่การกำหนดวัตถุประสงค์ของการจัดตั้งองค์การ การออกแบบโครงสร้างองค์การ โดยรายละเอียดจะมีความแตกต่างกันบ้างเล็กน้อยเพื่อให้สอดคล้องกับลักษณะขององค์การทั้ง 5 แบบ ทั้งฝ่ายทหารและฝ่ายพลเรือน แต่ในภาพรวมแล้วทุกองค์การทั้งภาครัฐและภาคเอกชนจะเป็นไปตามทฤษฎี

---

[16]จุลชีพ ชินวรรโณ.“สหรัฐอเมริกากับประเทศไทยในบริบทของความมั่นคงร่วมกันในเอเชียอาคเนย์”, ใน เส้นทางมหาอำนาจ: เอกสารด้านนโยบายต่างประเทศอเมริกาต่อเอเชีย.(กรุงเทพ: โครงการจัดพิมพ์คบไฟ, 2544).หน้า 271.

[17]The U.S. Army.“The Army Strategy”. (Headquarters, Deputy Chief of Staff, G-3-5-7. 2018). p.8.

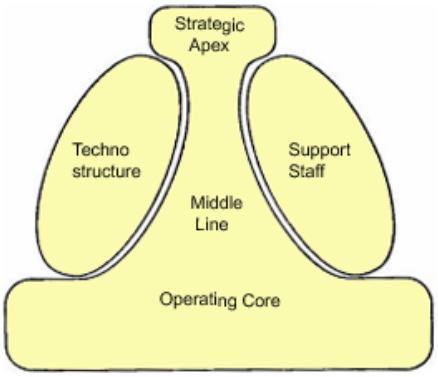
องค์การ โดยในส่วนของกองทัพอาจจะมีความหลากหลายมากกว่าองค์การอื่นเนื่องจากประกอบด้วยองค์การหลากหลายรูปแบบและมีความซับซ้อน

1. หลักทฤษฎีองค์การ

หลักการจัดองค์การระบบราชการของ แมกซ์ เวเบอร์ (Max Weber) ได้อธิบายคุณลักษณะของระบบราชการประการหนึ่งคือ การมีหลักปฏิบัติคงที่และมีขอบเขตอำนาจอย่างเป็นทางการ ซึ่งปกติแล้วจะเป็นการทำตามกฎหมายหรือระเบียบการบริหารจัดการ[18]กองทัพก็เป็นส่วนราชการของไทยซึ่งไม่แตกต่างจากทุกองค์การภาครัฐอื่นที่มีกฎหมายรองรับโดยการกำหนดหน้าที่และผู้รับผิดชอบของส่วนราชการไว้ชัดเจนแล้วจนถึงระดับบุคคล ขึ้นอยู่กับระดับของส่วนราชการ ซึ่งอาจจะกำหนดไว้ในระดับต่างๆ ได้แก่ พระราชบัญญัติ พระราชกฤษฎีกา หรือกฎกระทรวง รวมถึงอัตราการจัดที่จะแจกแจงจนถึงรายตำแหน่ง

เฮนรี มินท์ซเบอร์ก (Henry Mintzberg) ได้อธิบายองค์ประกอบขององค์การ ซึ่งแบ่งออกเป็น 5 ส่วนที่มีความเป็นอิสระต่อกัน ได้แก่ นักบริหารระดับสูง (Strategic Apex) นักบริหารระดับกลาง (Middle Line) ฝ่ายปฏิบัติงานหลัก (Operating Core) ฝ่ายเสนาธิการ (Support Staff) และฝ่ายสนับสนุน (Technostructure) ตามแผนภาพที่ 2 - 2

แผนภาพที่ 2 - 2องค์ประกอบของรูปแบบองค์การ



ที่มา : Machine Bureaucracy Wiki

โดยรูปแบบองค์การสามารถกำหนดได้โดยนำคุณลักษณะขององค์ประกอบทั้ง 5 ส่วนนี้มาผสมกันในที่แตกต่างกัน ทำให้เกิดรูปแบบองค์การในอุดมคติ 5 รูปแบบ แต่รูปแบบขององค์การในความเป็นจริงจะเป็นการผสมของรูปแบบทั้ง 5 อย่างสลับซับซ้อน ขึ้นอยู่กับประสบการณ์ที่จะนำไป

[18]Max Weber. “Bureaucracy”, in Classics of Organization Theory. J. M. Shafritz and others. (California: Thomson/Wadsworth, 2005). p.73-74.

ออกแบบให้เป็นไปตามความต้องการ[19] ซึ่งทำให้มีความอ่อนตัวรองรับกับทุกหน้าที่มินท์ซเบอร์ก ได้นำคุณลักษณะขององค์ประกอบทั้ง 5 ส่วนนี้ มาผสมกันในที่แตกต่างกัน ทำให้เกิดรูปแบบองค์การในอุดมคติ 5 รูปแบบ ได้แก่

1. องค์การแบบเรียบง่าย (TheSimple Structure) มีคุณลักษณะสำคัญคือมีการประกอบกันของส่วนนักบริหารระดับสูงและฝ่ายปฏิบัติงาน โดยนักบริหารจะนำองค์การ ควบคุมและประสานงานกับฝ่ายปฏิบัติงานหลัก ตัวอย่างเช่น กิจการร้านค้า ร้านอาหาร

2. องค์การระบบราชการแบบเครื่องจักรกล(TheMachine Bureaucracy) เป็นแบบระบบราชการโดยมีคุณลักษณะสำคัญคือมีระบบงานส่วนต่างๆ ขององค์การค่อนข้างสมบูรณ์ มีการรวมอำนาจการตัดสินใจ มีฝ่ายปฏิบัติขนาดใหญ่ มีความเป็นทางการสูงการติดต่อภายในเป็นไปตามกฎระเบียบ มีการแยกหน้าที่ตามความชำนาญอย่างมาก ตัวอย่างเช่น กองทัพ โรงงานประกอบรถยนต์ขนาดใหญ่

3. องค์การระบบราชการแบบวิชาชีพ (TheProfessional Bureaucracy) เป็นแบบระบบราชการโดยมีคุณลักษณะสำคัญซึ่งแตกต่างจากระบบราชการแบบเครื่องจักรกลตรงที่มีการกระจายอำนาจให้ผู้ปฏิบัติที่มีความเชี่ยวชาญสูงเฉพาะเรื่อง ตัวอย่างเช่น โรงพยาบาล มหาวิทยาลัย ซึ่งงานไซเบอร์เป็นงานที่มีความเชี่ยวชาญเฉพาะด้านสูง จึงควรใช้รูปแบบการจัดองค์การแบบนี้มากกว่าการจัดแบบเครื่องจักรกล

4. องค์การแบบสาขา (TheDivisionalizedForm) เป็นองค์การที่แบ่งแยกโครงสร้างระดับกลางออกเป็นองค์การย่อยแยกต่างหากจากสำนักงานใหญ่เพื่อบริการลูกค้าในพื้นที่ต่างๆ ตัวอย่างเช่นธนาคาร บริษัทข้ามชาติ ทั้งนี้ องค์การแบบสาขาบางแห่งพัฒนามาจากองค์การระบบราชการแบบเครื่องจักรกล

5. องค์การแบบโครงการ (TheAdhocracy, The Project Structure) เป็นองค์การที่มีสภาพแวดล้อมที่ซับซ้อนและเปลี่ยนแปลงมาก มีวัตถุประสงค์คิดค้นความรู้และสิ่งประดิษฐ์ใหม่ซึ่งต้องการผู้เชี่ยวชาญหลายด้านมาร่วมกันในลักษณะชั่วคราว

การจัดกระทรวงกลาโหมไทย เป็นการจัดองค์การแบบระบบราชการเครื่องจักรกลที่มีขนาดใหญ่ที่สุดในประเทศ โดยภายในมีองค์การทั้ง 5 รูปแบบ ซ้อนกันอยู่ทั้งทางกว้างตามช่วงการควบคุม (Span of Control) และทางดิ่งตามสายการบังคับบัญชา (Chain of Command) โดยกำหนดไว้ในอัตราการจัด ตัวอย่างเช่น กองทัพบกมีแบบองค์การซึ่งจัดไว้ปฏิบัติงานรวมจำนวนประมาณ 500 แบบ ซึ่งมีตั้งแต่หน่วยที่มีการจัดแบบระบบราชการอย่างแท้จริง เช่น กองทัพภาค โรงงานประกอบรถยนต์ขนาดใหญ่หน่วยที่มีการจัดแบบองค์การระบบราชการแบบวิชาชีพ เช่น

---

[19]Henry Mintzberg. Structure in Fives: Designing Effective Organizations. (New Jersey: Prentice-Hall, 1983). p.283-284.

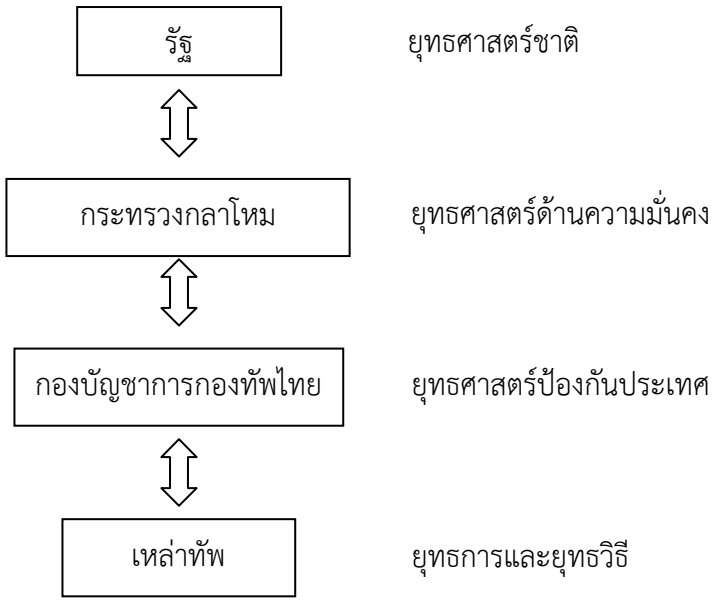
โรงพยาบาล สถานศึกษา ดังนั้นการพัฒนาหน่วยงานไซเบอร์ในด้านโครงสร้างการจัดจึงควรกำหนดรูปแบบองค์การให้เหมาะสมกับงานไซเบอร์ที่ต้องใช้ความเชี่ยวชาญทางเทคนิคสูง

นอกจากความซับซ้อนของการจัดองค์การ ซึ่งประกอบขึ้นจากรูปแบบที่มีความหลากหลายซ้อนกันอยู่ทั้งสายการบังคับบัญชาและช่วงการควบคุม ความแตกต่างของการจัดองค์การทางทหารกับองค์การสาธารณะอีกประการหนึ่ง คือ ความสัมพันธ์ระหว่างขอบเขตงานทางทหารกับรัฐบาลพลเรือน หรือเรียกศัพท์เฉพาะทางรัฐศาสตร์ว่าการจัดความสัมพันธ์พลเรือน-ทหาร (Civil-Military Relations) ซึ่งเป็นความสัมพันธ์ระหว่างทหารกับรัฐบาลพลเรือนที่มาจากการเลือกตั้งตามระบอบประชาธิปไตย ทั้งในยามปกติและยามสงคราม สำหรับความสัมพันธ์ในยามปกติสามารถอธิบายได้ตามสาขาวิชาการบริหารงานภาครัฐ ส่วนความสัมพันธ์ยามสงครามได้อธิบายไว้ในสาขาวิชาความสัมพันธ์ระหว่างประเทศเพื่อใช้องค์การทางทหารบรรลุวัตถุประสงค์ทางการเมือง ซึ่งทำให้ระบบการฝึกและศึกษาทางทหาร เป็นระบบที่ออกแบบมาสำหรับวัตถุประสงค์ดังกล่าวโดยเฉพาะ ไม่ใช่การฝึกและศึกษาทั่วไป

ความสัมพันธ์ระดับยุทธศาสตร์ (Strategy Level) เป็นการเชื่อมต่อระหว่างอำนาจทางทหารกับวัตถุประสงค์ทางการเมืองซึ่งเป็นผู้สร้างยุทธศาสตร์ โดยฝ่ายทหารเป็นผู้นำยุทธศาสตร์ไปปฏิบัติในยามสงคราม[20] แบ่งออกเป็นระดับยุทธศาสตร์ชาติ (National Strategy) และยุทธศาสตร์ทหาร(Military Strategy) สำหรับระดับยุทธการ (Operational Level) เป็นการแปลงยุทธศาสตร์ทหารให้กลายมาเป็นแผนการทัพให้หน่วยระดับยุทธวิธี (Tactical Level) วางแผนการใช้กำลังทหารเพื่อการรบซึ่งในหน่วยระดับยุทธวิธีนี้จะเป็นแกนหลัก (Core Function) ที่ใช้งานมุ่งเน้นไปในการใช้กำลังเข้าทำการรบเพื่อให้บรรลุผลตามภารกิจทั้งการปฏิบัติการในสภาวะสงครามและการปฏิบัติการในสภาวะที่ไม่ใช่สงครามซึ่งกระบวนการในระดับนี้จะมีระบบทางทหารเข้ามาเป็นมาตรฐานสากลและมีตัวชี้วัดทางทหารโดยเฉพาะ ไม่ได้มีหน้าที่งานทางด้านพลเรือน จึงทำให้กองทัพมิตรประเทศไม่นำระบบการฝึกและศึกษาทางพลเรือนมาใช้ในหน่วยระดับล่าง และการจัดการฝึกและศึกษาทางทหารของหน่วยทั้งสามระดับจึงมีความแตกต่างกันตามแผนภาพที่2 - 3

[20]Colin S. Gray.Modern Strategy.(New York: Oxford University press, 1999).p.17, 58.

แผนภาพที่ 2 - 3 ความสัมพันธ์ทางดิ่งภายในกระทรวงกลาโหม



ที่มา : 1. ยุทธศาสตร์ชาติ 20 ปี

2. พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551

ความสัมพันธ์ดังกล่าวต่อมาได้กำหนดไว้ในพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551มาตรา29กำหนดให้โครงสร้างองค์กรการฝึกและการศึกษาของทหารและข้าราชการพลเรือนกลาโหมให้เป็นไปตามนโยบายที่กระทรวงกลาโหมกำหนดโดยให้กองบัญชาการกองทัพไทยรับผิดชอบการฝึกและศึกษาในระดับยุทธศาสตร์การปฏิบัติการร่วมของกองทัพไทยและการปฏิบัติการของกองบัญชาการกองทัพไทยและให้กองทัพบกกองทัพเรือและกองทัพอากาศรับผิดชอบในระดับปฏิบัติการและระดับยุทธวิธี[21]ซึ่งนำมาสู่ปัญหาในการบริหารจัดการ

[21]"พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. 2551". ราชกิจจานุเบกษา. เล่ม 125, 1 กุมภาพันธ์ 2551, หน้า 43.

ระบบต่างๆ ภายในกระทรวงกลาโหมเนื่องจากต้องการให้ทุกส่วนราชการที่กล่าวมามีการบริหารจัดการที่เหมือนกัน

ปัญหาที่เกิดขึ้นในกระทรวงกลาโหมอีกประการหนึ่ง คือการนำระบบพลเรือนเข้ามาใช้ในระบบทางทหารแบบเหมารวม ทำให้เกิดปัญหาความขัดแย้งระหว่างระบบในองค์การเดิมซึ่งได้ขยายระบบแผ่ปกคลุมไปทั่วกองทัพ กับระบบที่นำเข้ามาใหม่ซึ่งรวมถึงอำนาจใหม่ในการควบคุม กำกับดูแล ตรวจสอบประเมินผล การต่อสู้ระหว่างสองระบบดังกล่าวทำให้เกิดความขัดแย้ง เมื่อไม่สามารถแก้ไขความขัดแย้งก็อาจลุกลามจนเป็นการต่อต้าน ยกตัวอย่างเช่นการนำระบบการพัฒนาราชการเข้ามาใช้ในกองทัพผลจากการที่กองทัพได้นำระบบของพลเรือนเข้ามาใช้ในกองทัพทำให้เกิดแนวคิดแบ่งออกเป็นสองฝ่ายขึ้นอยู่กับว่าแต่ละฝ่ายมีลักษณะงานที่เป็นงานทหารหรืองานพลเรือนทำให้เกิดปัญหาการต่อสู้กันไปมาในเรื่องแนวคิดในการพัฒนาหน่วยงานทั้งสองแบบ เนื่องจากแนวคิดวิธีการ แต่ละแบบมีความแตกต่างกัน เมื่อนำมาใช้กับอีกฝ่ายหนึ่งจะกระทบถึงเทคโนโลยีหลักในการผลิตบุคลากรตามหลักทฤษฎีองค์การ

การต่อสู้กันไปมาในเรื่องแนวคิดในการจัดหน่วยที่มีการจัดทางทหารและพลเรือนทั้งสองแบบดังกล่าวเป็นไปตามที่ เจมส์ ธอมป์สัน (James D. Thompson) ได้เสนอแนวทางการศึกษาองค์การที่นำไปสู่การปรับปรุงประสิทธิภาพจากยุทธศาสตร์ระบบเปิด (Open-system Strategy) ซึ่งจะต้องพบกับสิ่งที่ไม่แน่นอนเป็นการมุ่งเน้นความอยู่รอดมากกว่าเป้าหมายและเป็นการรักษาความสมดุลภายใต้ความเป็นเหตุผลองค์การจะมองหาวิธีป้องกันตัวเองออกจากอิทธิพลของสิ่งแวดล้อมที่อยู่รอบเทคโนโลยีหลัก รวมถึงส่วนประกอบที่เป็นปัจจัยนำเข้าและปัจจัยส่งออก[22]ซึ่งแนวทางดังกล่าวสามารถนำมาใช้อธิบายการต่อต้านการนำระบบงานพลเรือนที่เข้ามาใช้ภายในกองทัพได้ เช่น การพัฒนาระบบราชการ การจัดการศึกษา และการประเมินค่าการปฏิบัติงานแบบรอบตัว และอาจรวมถึงการปฏิบัติการไซเบอร์ในกรณีที่ระบบดังกล่าวส่งผลกระทบต่อกองทัพโดยเฉพาะ Core Technology ที่จำเป็นสำหรับหน้าที่ขององค์การ ก็อาจจะมีการต่อต้านจากกองทัพเนื่องจากวิธีการแบบเหมารวมดังกล่าวได้ส่งผลกระทบต่อเทคโนโลยีหลักในการดำรงไว้ซึ่งขีดความสามารถในการป้องกันประเทศ

2.ความเชื่อมโยงระหว่างหน่วยงานแบบภารกิจ (Mission) และหน่วยงานแบบพันธกิจ (Function)

การที่จะพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยให้สามารถปฏิบัติงานรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างมีประสิทธิภาพได้นั้น จำเป็นต้องกำหนดหน้าที่

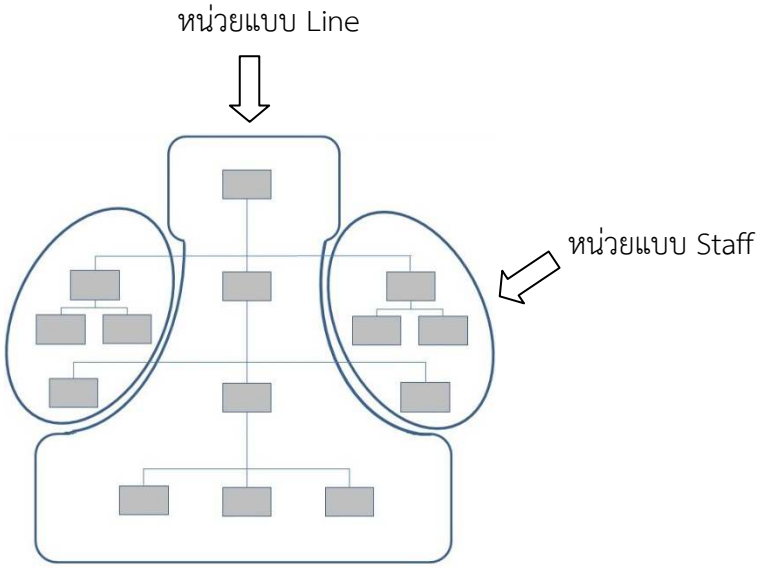
---

[22]James D. Thompson. “Organizations in Action”,inClassics of Organization Theory. J. M. Shafritz; and others. (California: Thomson/Wadsworth, 2005), p.499-450.

ความรับผิดชอบงานด้านไซเบอร์ของกองทัพบกไทยให้มีความชัดเจนก่อนว่าจะยังคงมีบทบาทเป็นฝ่ายกิจการพิเศษ (Special Staff) ซึ่งมุ่งเน้นไปที่มีความชำนาญทางด้านเทคนิคเฉพาะด้านไซเบอร์ โดยมีบทบาทจำกัดเฉพาะงานที่เกี่ยวข้องในการปฏิบัติหรือให้การสนับสนุนหน่วยอื่นเท่านั้น หรือจะยกระดับเป็นการปฏิบัติการทางทหาร (Cyber Operations) ในลักษณะเดียวกับการปฏิบัติการข่าวสาร (Information Operations) ซึ่งจำเป็นต้องเกี่ยวข้องกับทุกหน่วยโดยผ่านกระบวนการวางแผนทางทหารเหมือนกับการปฏิบัติการทางทหารอื่น

กองทัพสหรัฐอเมริกาได้นำมาหลักทฤษฎีองค์การมาพัฒนาเป็นหลักในการแบ่งหน่วยแบบ Line และ Staffมาพัฒนาเป็นหน่วยปฏิบัติงานทางทหารหลักซึ่งมีการจัดและยุทโธปกรณ์คงที่และหน่วยที่เป็นฝ่ายเสนาธิการหรือหน่วยสนับสนุนที่มีการจัดและสิ่งอุปกรณ์เปลี่ยนแปลงได้ตามแผนภาพที่ 2 - 4

แผนภาพที่ 2 - 4 โครงสร้างการจัดตามทฤษฎีองค์การแบ่งหน่วยแบบ Line และ Staff ซึ่ง ทบ.สหรัฐฯ ได้พัฒนามาเป็นหน่วยแบบ อจย. และ อฉก.



ที่มา : U.S. Army Center of Military History

- ส่วนที่เป็นหน่วยปฏิบัติหลัก (Line)ซึ่งต่อมา ทบ.สหรัฐ ได้พัฒนามาเป็นอัตราการจัดและยุทโธปกรณ์ หรือ อจย. (Table of Organization: TOE)

- ส่วนที่เป็นฝ่ายเสนาธิการ (Staff)ต่อมา ทบ.สหรัฐ ได้พัฒนามาเป็นอัตราการจัดเฉพาะกิจ หรือ อฉก. (Table of Distribution: TD)

จากหลักทฤษฎีองค์การแบ่งหน่วยแบบ Line และ Staff ซึ่งเกี่ยวข้องโดยตรงกับพัฒนาโครงสร้างการจัดหน่วยงานด้านไซเบอร์ที่กล่าวมาแล้ว จะเห็นความแตกต่างระหว่างหน่วยแบบ Staff ซึ่งมี ชกท. เฉพาะหน้าที่ และหน่วยแบบ Line ที่ประกอบจากหน้าที่ย่อย โดยหน่วยที่มีการจัดแบบ Lineซึ่งออกแบบมาเพื่อการปฏิบัติการทางทหารจะมีความเกี่ยวข้องกับทุกหน่วย ในขณะที่หน่วยที่มีการจัดแบบ Staff ซึ่งออกแบบมาเป็นฝ่ายเสนาธิการหรือฝ่ายกิจการพิเศษ จะมีความชัดเจนในสายงานเฉพาะของตนเอง ตามแผนภาพที่ 2 - 5

แผนภาพที่ 2 - 5 แสดงความแตกต่างระหว่างหน่วยแบบ Staff ซึ่งมี ชกท. เฉพาะหน้าที่และหน่วยแบบ line ที่ประกอบจากหน้าที่ย่อย

หน่วยที่มีการจัดแบบ อฉก. (หรือ Staff ตามหลักทฤษฎีองค์การ)
จะมีหน้าที่เฉพาะสายงาน

หน่วยที่มีการจัดแบบ อจย. (หรือ Line ตามหลักทฤษฎีองค์การ)เป็นการนำอัตรา ย่อยมาประกอบกันเพื่อปฏิบัติภารกิจ จึงมีหลาย

	กพ.	ขว.	ยก.	กบ.	กร.	สปช.		ไซเบอร์
	2260	9301	2162	2625	8104	6000		
ทบ.								
ทภ.								
กองพล								
กรม								
กองพัน								

หลักการดังกล่าว กองทัพบกได้นำมาพัฒนาระบบอัตราของกองทัพบก โดยมีคำสั่งรองรับ

- คำสั่ง กองทัพบก (คำชี้แจง) ที่ 315/22837 ลง 9 พ.ย.99 เรื่อง ให้ใช้ระบบหมายเลขความชำนาญการทางทหารสำหรับนายทหารชั้นประทวนและพลทหาร

- คำสั่ง กองทัพบก (เฉพาะ) ที่ 266 ลง 26 มิ.ย.02 เรื่อง การทำอัตราของกองทัพบก

- คำสั่ง กองทัพบก (คำสั่งชี้แจง) ที่ 38/23480 ลง 16 ต.ค.02 เรื่อง ระบบหมายเลขความชำนาญการทางทหารสำหรับนายทหารสัญญาบัตร

- คำสั่ง กองทัพบก (เฉพาะ) ที่ 289 ลง 11 ต.ค.06 เรื่อง การทำอัตราของกองทัพบก

- คำสั่ง กองทัพบก ที่ 566/2514 ลง 16 ธ.ค.14 เรื่อง ให้ใช้ระบบหมายเลขความชำนาญการทางทหาร (สำหรับนายทหารสัญญาบัตร)

การที่จะพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกให้มีประสิทธิภาพนั้น จะต้องเริ่มจากการพิจารณาให้ชัดเจนว่างานด้านไซเบอร์เป็นงานที่เป็นแบบพันธกิจ (Function) หรือเป็นแบบภารกิจ (Mission) ซึ่งในกองทัพมิตรประเทศได้จัดการปฏิบัติการไซเบอร์ (Cyber Operations) เป็นแบบเดียวกับการปฏิบัติการข่าวสาร (Information Operations) และอยู่ในความรับผิดชอบของสายงานยุทธการ (Operation Staff) หรืออาจจะแยกเป็นสายงานเฉพาะ ในขณะที่กองทัพไทยยังเป็นแบบฝ่ายกิจการพิเศษหรือแบบพันธกิจซึ่งมีส่วนประกอบที่เป็นฝ่ายเสนาธิการจะมีงานเฉพาะหน้าที่ทำให้การกำหนดหมายเลข ชกท. และคุณสมบัติเฉพาะตำแหน่ง รองรับเฉพาะหน่วยนั้นๆ ไม่สามารถนำไปใช้กับหน่วยอื่นได้ ทำให้ความชัดเจนในการพัฒนาหน่วยงานในด้านต่างๆ เป็นไปได้น้อยลง

3.ความเชื่อมโยงระหว่างทฤษฎีองค์การและการบริหารทรัพยากรมนุษย์

หากพิจารณาความเชื่อมโยงระหว่างความรู้ด้านทฤษฎีองค์การ และการบริหารทรัพยากรมนุษย์ของส่วนราชการภายในกระทรวงกลาโหมแล้วจะเหมือนกันโดยในที่นี้ขอนำเสนอตัวอย่างกองทัพบกเริ่มจากพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551ซึ่งกำหนดหน้าที่ของกองทัพบก ถัดลงมาจะเป็นกฎหมายในระดับพระราชกฤษฎีกาแบ่งส่วนราชการและจัดระเบียบส่วนราชการกองทัพบก พ.ศ.2552 ซึ่งจะกำหนดหน้าที่ของส่วนราชการต่างๆ ในกองทัพบก ดังนั้น จะเห็นได้ว่าหากนำระบบการบริหารงานใดมาใช้ในกระทรวงกลาโหม จำเป็นต้องพิจารณา

ความเชื่อมโยงให้สอดคล้องกันกับหน้าที่ที่กำหนดไว้ในกฎหมายของแต่ละส่วนราชการเพื่อตอบสนองความต้องการของส่วนราชการนั้นๆ มากกว่าที่จะมุ่งไปที่ทำให้ทุกส่วนราชการมีความเหมือนกัน

ในระดับถัดลงมาจากพระราชกฤษฎีกาฯ แต่ละส่วนราชการก็จะจัดทำโครงสร้างการจัดองค์การให้สอดคล้องตามหน้าที่ โดยมีการจัดองค์ประกอบ 5 รูปแบบที่แตกต่างกันออกไป เกิดเป็นองค์การรูปแบบต่างๆ ได้แก่ องค์การแบบเรียบง่าย องค์การระบบราชการแบบเครื่องจักรกลองค์การระบบราชการแบบวิชาชีพ องค์การแบบสาขา และองค์การแบบโครงการ ตามที่ได้กล่าวมาแล้วข้างต้น อย่างไรก็ตามรูปแบบองค์การจริงจะมีความซับซ้อนหลายชั้น ในปัจจุบันกองทัพบกมีจำนวนรูปแบบ 500 แบบ ซึ่งนำไปใช้กับหน่วยงานต่างๆ จำนวนมากตามแผนภาพที่ 2 - 6

แผนภาพที่ 2 - 6ความเชื่อมโยงหน้าที่ทางกฎหมายของส่วนราชการในกระทรวงกลาโหม

เมื่อได้โครงสร้างรูปแบบหน่วยงานในขั้นต้นเพื่อสามารถตอบสนองวัตถุประสงค์ในการจัดตั้งองค์การได้แล้ว หลังจากนี้จะเป็นส่วนของการบริหารทรัพยากรมนุษย์ โดยการนำรูปแบบองค์การมาขยายให้กลายเป็นกรอบอัตรากำลัง ตำแหน่ง ชั้นยศ หมายเลขความชำนาญการทหารซึ่ง

อธิบายหน้าที่โดยทั่วไปและหน้าที่เฉพาะหรือที่เรียกว่า “คำบรรยายลักษณะงาน (Job Description)” รวมทั้งเชื่อมโยงไปถึง “คุณสมบัติเฉพาะตำแหน่ง (Job Specification)” เพื่อให้มีบุคคลในจำนวนที่เพียงพอ มีคุณวุฒิที่เหมาะสมสามารถปฏิบัติงานในสาขาต่างๆ ขององค์การได้ ซึ่งตามปกติแล้วจะกำหนดออกมาในรูปแบบของกฎหมายที่ชัดเจน และใช้เป็นพื้นฐานในการดำเนินการบริหารทรัพยากรมนุษย์ในขั้นต่อไป ได้แก่ การวางแผนความต้องการกำลัง การสรรหา การบรรจุ การฝึก การประเมินค่าและการตอบแทน

แผนภาพที่2 - 7 ความเชื่อมโยงตามกฎหมายระหว่างการจัดองค์การ กับการบริหารทรัพยากรมนุษย์

จากแผนภาพที่ 2 - 7แสดงความเชื่อมโยงระหว่างการจัดองค์การกับการบริหารทรัพยากรมนุษย์ ซึ่งยังไม่มีความชัดเจนในทางปฏิบัติ ทุกกองทัพจึงต้องจัดทำโครงสร้างอัตราการจัดเพื่อให้มีผลบังคับใช้ตามกฎหมาย เช่นเดียวกับทุกส่วนราชการ แต่อาจจะมีความแตกต่างกันบ้าง อย่างเช่น ชื่อและรายละเอียด สำหรับกองทัพไทยได้ดัดแปลงมาจากกองทัพสหรัฐ โดยกำหนดเป็นอัตราการจัดและยุทโธปกรณ์ (อจย.) และอัตราการจัดเฉพาะกิจ (อฉก.) เชื่อมโยงจากหน้าที่ของแต่ละส่วนราชการจนถึงระดับรายตำแหน่ง โดยหน้าที่แต่ละตำแหน่งจะกำหนดไว้ในความชำนาญทางทหารหรือที่เรียกว่า คำบรรยายหน้าที่ (Job Description) และแต่ละหน้าที่กำหนด “คุณสมบัติเฉพาะตำแหน่ง (Job Specification)” ซึ่งจะมีความสัมพันธ์กับการพัฒนาหน่วยงานด้านไซเบอร์ต่อไปโดยปรากฏในอัตราการจัดที่ใช้ในทางทหาร ทั้งแบบอัตราการจัดและยุทโธปกรณ์ (อจย.) และอัตราการจัดเฉพาะกิจ (อฉก.) ตามตารางที่ 2 - 1

ตารางที่ 2 - 1รายละเอียดของอัตราการจัดและยุทโธปกรณ์ (อจย.) และอัตราการจัดเฉพาะกิจ (อฉก.)

	อจย.	**อฉก.**
ตอนที่ 1	กล่าวทั่วไป	กล่าวทั่วไป
	ภารกิจ, การแบ่งมอบ, ขีดความสามารถ, รายละเอียดและคำชี้แจงเกี่ยวกับยุทโธปกรณ์, ตอนเพิ่มเติมประกอบอัตรา	ภารกิจ, การแบ่งมอบ, ขอบเขตความรับผิดชอบและหน้าที่ที่สำคัญ, การแบ่งส่วนราชการและหน้าที่, ตอนเพิ่มเติมประกอบอัตรา
ตอนที่ 2	ผังการจัด	ผังการจัด
ตอนที่ 3	อัตรากำลังพล	อัตรากำลังพล
ตอนที่ 4	อัตรายุทโธปกรณ์	คำชี้แจง

จากตารางที่ 2 - 1 เมื่อนำหน้าที่แต่ละส่วนราชการมาจัดทำเป็นอัตราการจัดเพื่อให้มีผลบังคับใช้ทางกฎหมายต่อจากพระราชกฤษฎีกา จะเห็นว่าในแต่ละอัตราจะแบ่งออกเป็นตอนต่างๆ โดยตอนที่ 1 กล่าวทั่วไป จะอธิบายถึงภารกิจ การแบ่งมอบขีดความสามารถหรือหน้าที่ที่สำคัญ ตอนที่ 2 จะเป็นโครงสร้างการจัดที่ขยายรายละเอียดลงมาเพื่อให้สามารถปฏิบัติหน้าที่ที่กำหนดไว้ในพระราชกฤษฎีกาได้ และตอนที่ 3 จะเป็นอัตรากำลังพล โดยจะกำหนดรายละเอียดแต่ละตำแหน่งให้ชัดเจนว่ามีตำแหน่ง ชั้นยศ และจำนวนเท่าไร ซึ่งทุกตอนจะมีความสำคัญต่อการพัฒนาหน่วยงานด้าน

ไซเบอร์ของกองทัพบก เนื่องจากเป็นตัวกำหนดที่สำคัญในการนำกำลังพลในตำแหน่งมาทำการฝึกและศึกษาทางทหาร

ขั้นตอนที่กล่าวมาตั้งแต่รัฐธรรมนูญจนถึงอัตรากำลัง โดยทั่วไปแล้วไม่แตกต่างไปจากส่วนราชการอื่นแต่ส่วนราชการพลเรือนจะกำหนดจากพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ.2534 และพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545 ถัดลงมาจะเป็นกฎกระทรวงในลักษณะเดียวกับอัตรา อฉก. และ อจย. ของกระทรวงกลาโหม แต่เนื่องจากกระทรวงกลาโหมเป็นองค์การที่มีวิชาชีพเฉพาะทางทหาร ในขณะเดียวกันต้องการบุคคลที่มีความรู้สายงานพลเรือนเข้ามาทำงานให้รวมถึงงานไซเบอร์ แต่ในปัจจุบันกองทัพไทยยังไม่ได้แยกงานพลเรือนออกจากงานทหารให้ชัดเจนเหมือนกับกองทัพบกมิตรประเทศ ทุกตำแหน่งจึงเป็นทหาร ทำให้คุณวุฒิในบางตำแหน่งไม่ค่อยจำเป็นหรือกว้างมากเกินไปไม่เกี่ยวข้องกับคุณวุฒิในการสรรหาครั้งแรก ยกเว้นตำแหน่งวิชาชีพเฉพาะ เช่น อาจารย์ แพทย์ วิศวกร คอมพิวเตอร์ เป็นต้น

ทฤษฎีการบริหารงานบุคคลกับการพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทย

จากที่กล่าวมา เป็นหลักการทั่วไปซึ่งใช้ได้ทั้งการบริหารบุคคลภาครัฐและภาคเอกชน อย่างไรก็ตาม สำหรับขั้นตอนการบริหารงานบุคคลภาครัฐไทยนั้น ตามมิติของขั้นตอนการทำงานนั้นประกอบด้วยขั้นตอนสำคัญ 6 ขั้นตอน คือ การวางแผนทรัพยากรบุคคล การได้มาซึ่งบุคคล การโอนย้ายและการแต่งตั้ง การพัฒนาบุคคล การใช้ประโยชน์จากบุคคล การประเมินผลการปฏิบัติงานและการพ้นสภาพการเป็นบุคคล[23]ในปัจจุบันมีการรวมในขั้นการพัฒนาตำแหน่ง การรับสมัคร และการสัมภาษณ์และคัดเลือกนั้น เป็นการศึกษาเรียกว่าการสรรหา ซึ่งจะกล่าวเป็นภาพรวมเฉพาะการสรรหาโดยเป็นขั้นตอนที่เกี่ยวข้องกับการฝึกและศึกษาทางทหารของกองทัพ

การบริหารทรัพยากรมนุษย์ (Human Resource Management)ประกอบด้วยขั้นตอนการสรรหา การคัดเลือก การฝึกอบรม การประเมินผลการปฏิบัติงาน การจ่ายค่าตอบแทน และการจัดการพนักงานสัมพันธ์ การสรรหาบุคคลขององค์การส่วนใหญ่จะมีความคล้ายกันประกอบด้วย ขั้นการกำหนดทิศทางขององค์การ การคาดการณ์อุปสงค์กำลังคน การคาดการณ์อุปทานกำลังคน การกำหนดความต้องการกำลังคน และการจัดทำแผนทรัพยากรบุคคล โดยในขั้นแรกคือการกำหนดทิศทางองค์การนั้น ไม่ว่าภาครัฐภาคเอกชน รัฐวิสาหกิจและองค์การสาธารณะ

---

[23]ศุภชัย เยาวะประภาษ.การบริหารงานบุคคลภาครัฐไทย; กระแสใหม่และสิ่งท้าทาย. พิมพ์ครั้งที่ 2,(กรุงเทพ: จุดทอง, 2548). หน้า 119-120.

ต่างๆ มักกำหนดวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และแผนงาน โครงการ หรือเรียกรวมว่า “แผนกลยุทธขององค์การ”[24] ซึ่งก่อนหน้านั้น ภาครัฐไทยยังไม่มีการนำระบบดังกล่าวมาใช้

สำหรับการสรรหาบุคคลภาครัฐของไทย หากแบ่งตามแหล่งทรัพยากรแล้วโดยทั่วไปแบ่งได้ 2 ประเภทคือ การสรรหาจากภายใน (Recruitment from Inside) เมื่อตำแหน่งว่างลงก็จะดำเนินการสอบโดยประกาศรับสมัครจากบุคคลที่ทำงานอยู่แล้วเพื่อแข่งขันเลื่อนขั้นขึ้นมาซึ่งควรเรียกว่า การเลื่อนขั้น (Promotion) มากกว่าและการสรรหาจากภายนอก (Recruitment from Outside) โดยชักจูงบุคคลเพื่อสอบแข่งขันเข้าดำรงตำแหน่งตามความต้องการขององค์การด้วยการแสวงหาแหล่งกำลังคน การประกาศรับสมัคร การสรรหาบุคคลประกอบด้วยการวิเคราะห์งานการวางแผนกำลังคนและการคาดการณ์กำลังคน การสรรหาผู้สมัครงานรายละเอียดดังนี้

1.การวิเคราะห์งาน (JobAnalysis)

เพื่อให้รู้ว่ามีกิจกรรมใดในงานนั้น และต้องใช้บุคคลแบบใดมีรายละเอียดได้แก่ วัตถุประสงค์หลักที่แท้จริงและเป้าหมายของงาน ตำแหน่ง หน้าที่หลักซึ่งจะต้องจำแนกออกมาเป็นงานย่อยที่ต้องทำ จำนวนบุคคลที่ต้องการซึ่งคำนวณจากงานทั้งหมด และสภาวะแวดล้อมในการทำงาน[25]

หลังจากวิเคราะห์งานแล้วจึงจัดทำ “คำบรรยายลักษณะงาน (Job Description)” ซึ่งจะอธิบายหน้าที่และความรับผิดชอบของงานในแต่ละตำแหน่ง และอาจจะต้องนำมาใช้ตลอดขั้นตอนที่เหลือในการบริหารทรัพยากรบุคคล ตั้งแต่ขั้นการชักชวนให้เข้ามาทำงาน การฝึกอบรม การประเมินและการดำเนินการด้านวินัย รวมทั้งการประเมินงานและโครงสร้างค่าตอบแทน โดยทั่วไปแล้วโครงร่างของคำบรรยายลักษณะงานจะมีแตกต่างกันออกไปอาจจะประกอบด้วยหัวข้อ ได้แก่ ชื่องาน มีความรับผิดชอบต่อใคร และรับผิดชอบบุคคลใดบ้างที่อยู่ภายใต้การควบคุมบังคับบัญชา วัตถุประสงค์ในภาพรวมของงาน หน้าที่ที่สำคัญ ความรับผิดชอบในงาน[26]

หลังจากที่กำหนดคำบรรยายลักษณะงานแล้ว ในขั้นต่อไปจึงจะกำหนดว่าผู้ที่จะเข้ามาปฏิบัติงานในตำแหน่งดังกล่าวมีคุณสมบัติอย่างไรหรือที่เรียกว่า “คุณลักษณะเฉพาะของงาน (Job Specification)” ซึ่งประกอบด้วยคุณลักษณะทางร่างกายด้านต่างๆ ความรอบรู้ ความสามารถพิเศษ เป็นต้น[27] เพื่อใช้ในการนำไปคัดเลือกผู้สมัครให้ตรงตามความต้องการของงานในตำแหน่งนั้น

2.การวางแผนกำลังคนและการคาดการณ์กำลังคน

---

[24]เรื่องเดียวกัน, หน้า 27.

[25]Iain Maitland, How to recruit. (England: Gower, 1991), p. 3-5.

[26]Ibid., p. 5-11.

[27]Ibid., p. 5-11.

สำหรับองค์การที่จัดตั้งใหม่ย่อมแน่นอนว่าในช่วงแรกไม่มีกำลังคน แต่ถ้าหากเป็นองค์การที่จัดตั้งนานแล้ว จะมีการวางแผนกำลังคนและคาดการณ์กำลังคนอย่างต่อเนื่องเพื่อชดเชยกับการสูญเสียกำลังคน ตั้งแต่การลาออก การย้าย การเสียชีวิต รวมทั้งการเลื่อนตำแหน่งสูงขึ้น เพื่อนำข้อมูลที่ได้มาวางแผนบริหารทรัพยากร โดยมีการสะสมสถิติข้อมูลที่สามารถคาดการณ์ได้เพื่อไม่ให้เกิดภาวะชะงักงันซึ่งมีวิธี ได้แก่ การวิเคราะห์แนวโน้มตามห้วงระยะเวลา การวิเคราะห์อัตราส่วนกำลังคนต่องานที่จะต้องทำ และการกระจายทางสถิติเพื่อดูความสัมพันธ์ระหว่างงานกับจำนวนคนที่ใช้[28] เพื่อให้สามารถวางแผนคาดการณ์กำลังคนได้

กองทัพบกวางแผนความต้องการบุคคลทุกวงรอบ 5 ปี โดยมีพื้นฐานมาจากโครงสร้างอัตรากำลังของส่วนราชการต่างๆ ในกองทัพบกตามที่กล่าวมาแล้ว เมื่อนำมาพิจารณาสถานภาพการบรรจุ การสูญเสียเนื่องจากกรณีต่างๆ ได้แก่ การเกษียณ การลาออก การเสียชีวิต การดำรงตำแหน่งสูงขึ้น หลังจากพิจารณายุทธศาสตร์ของกระทรวงกลาโหม และสถานภาพงบประมาณแล้ว จึงนำมากำหนดการประมาณการบุคคลจะกำหนดในรูปแผนความต้องการกำลังพลวงรอบ 5 ปี ซึ่งเริ่มเกี่ยวข้องกับการฝึกและศึกษาของกองทัพโดยตรงเนื่องจากกำลังพลที่บรรจุในกองทัพส่วนใหญ่จะผลิตเอง

3.การสรรหาบุคคล

เช่นเดียวกับทุกส่วนราชการกองทัพบกจำเป็นต้องวางแผนงบประมาณที่ต้องใช้ในการจ้างบุคคลมาทำงาน เมื่อทราบความต้องการล่วงหน้าแล้วจึงนำมาเสนอของบประมาณล่วงหน้าแล้วจึงนำมาดำเนินการสรรหาตามขั้นตอนต่อไปทั้งจากแหล่งภายในและแหล่งภายนอก

-การสรรหาบุคคลจากแหล่งภายนอก กองทัพบกมีการสรรหาบุคคลจากแหล่งภายนอกและใช้เป็นวิธีการหลัก ได้แก่ นักเรียนนายร้อย นักเรียนแพทย์ทหาร นักเรียนพยาบาล นักเรียนนายสิบ ศิษย์การบินทหารบก นักเรียนดุริยางค์ทหารบก โดยการสอบคัดเลือกจากคณะกรรมการของหน่วยงานนั้นอย่างไรก็ตาม การสรรหาจากภายนอกดังกล่าวยังไม่ได้นำมาใช้ปฏิบัติงานทันที แต่จะต้องนำมาเข้ารับการศึกษาหลักสูตรก่อน ซึ่งแตกต่างจากระบบของสำนักงาน ก.พ. ที่ส่วนใหญ่สรรหาจากผู้ที่มีคุณวุฒิตามที่ต้องการ แล้วนำมาฝึกอบรมระยะสั้นให้สอดคล้องเฉพาะหน้าที่ ซึ่งกรณีดังกล่าวกองทัพบกก็มีการสอบบรรจุนายทหารสัญญาบัตรคุณวุฒิพลเรือน แล้วอบรมระยะสั้นแต่จะมีจำนวนไม่มาก สำหรับการสรรหาพนักงานราชการ และพลทหารที่มีทั้งการสมัครและการเกณฑ์นั้น ไม่ใช่ตำแหน่งถาวรจึงไม่นำมากล่าวถึง นอกจากนี้ ยังมีการโอนจากส่วนราชการอื่นซึ่งกำหนดอายุสูงสุดในแต่ละชั้นยศไว้ สำหรับการสรรหาจากแหล่งภายนอกเกี่ยวข้องกับระบบการฝึกและศึกษาทางทหารในขั้นแรกคือการอบรมหลักสูตรที่จำเป็นก่อนหรือหลังการบรรจุเข้ารับราชการ

---

[28] Gary Dessler.Human Resource Management, 12th ed., (New Jersey: Pearson, 2011). p.179-180.

-การสรรหาบุคคลจากแหล่งภายในเป็นการสรรหาจากสถานศึกษาภายในกองทัพเอง หลักสูตรการผลิตกำลังพลที่สำคัญได้แก่ นักเรียนายร้อย นักเรียนแพทย์ทหาร นักเรียนพยาบาล นักเรียนายสิบ และยังรวมถึงการสอบเลื่อนฐานะนายทหารประทวนคุณวุฒิปริญญาตรี การเลื่อนฐานะนายทหารชั้นประทวนเป็นนายทหารสัญญาบัตรหรือการปรับย้ายจากส่วนราชการอื่นภายในกระทรวงกลาโหมและนอกกระทรวงกลาโหม ซึ่งการสรรหาจากแหล่งภายในจะเกี่ยวข้องกับระบบการฝึกและศึกษาทางทหารของกองทัพโดยตรง

นอกจากนี้ยังมีบางตำแหน่งที่รับทั้งแหล่งภายนอกและแหล่งภายในพร้อมกัน เช่น การรับผู้ที่จะเป็นนักบิน จะเปิดรับการสอบจากบุคคลพลเรือนที่สำเร็จปริญญาตรีและนายทหารสัญญาบัตรในกองทัพบกที่มีอายุไม่เกินทำการสอบคัดเลือกเพื่อเข้ารับการศึกษาหลักสูตรการบินเป็นการคัดเลือกผู้สมัครที่เหมาะสมที่สุดกับงานจำเป็นต้องมีการทดสอบและการคัดเลือกเพื่อให้เกิดประสิทธิภาพเนื่องจากการจ้างเป็นต้นทุนขององค์การ จึงจำเป็นต้องมีวิธีทดสอบและคัดเลือกให้เที่ยงตรงและเชื่อถือได้โดยมีวิธีการต่างๆ จำนวนมาก การทดสอบความสามารถทางสติปัญญา ความฉลาด ด้านความสามารถ ด้านบุคลิกภาพ และการทดสอบความถนัด หลังจากนั้นจำเป็นต้องมีการสัมภาษณ์เพื่อให้เกิดความมั่นใจในข้อมูลที่ได้จากการทดสอบว่ามีความถูกต้องเหมาะสมที่จะมาปฏิบัติงานในตำแหน่งที่กำหนดตามวิธีการสัมภาษณ์ที่เหมาะสม[29]

จากที่กล่าวมาจะเห็นได้ว่าการฝึกและศึกษาทางทหารมีความสัมพันธ์อย่างใกล้ชิดกับการสรรหา ทั้งในขั้นการบรรจุเริ่มแรกในกรณีที่สรรหาจากแหล่งภายใน หรือการฝึกและศึกษาทางทหารเพิ่มเติมภายหลังการบรรจุแล้วสำหรับในส่วนของกองทัพแล้ว อัตราการจัดในตอนที่ 3 จะเป็นสิ่งสำคัญในการบรรจุและคัดไปทำการฝึกและศึกษาทางทหาร

ระบบการประเมินผลการปฏิบัติงานบุคคลกองทัพบกไทย

การบริหารงานภาครัฐของไทยในปัจจุบันกำหนดให้มีการประเมินผลการปฏิบัติงานบุคคล ซึ่งเป็นสิ่งที่จำเป็นเพื่อให้มั่นใจว่าการปฏิบัติงานของบุคคลตรงตามเป้าหมายขององค์การ มีความเหมาะสมกับงบประมาณที่รัฐต้องจ่ายค่าตอบแทน กองทัพบกไทยเป็นส่วนราชการที่มีการนำระบบการประเมินผลการปฏิบัติงานมานานตั้งแต่ พ.ศ.2530 โดยการนำแนวคิดมาจากกองทัพบกต่างประเทศซึ่งในขณะนั้นส่วนราชการไทยยังไม่แพร่หลาย แต่จากการที่ใช้มาเป็นระยะเวลานาน

[29] Ibid.,p.218-231, 256-263.

ดังกล่าวกลับปรากฏว่าระบบการประเมินผลการปฏิบัติงานของส่วนราชการอื่นซึ่งมีมาไม่นาน กลับมีความก้าวหน้าและประสบผลนำมาบริหารจัดการทรัพยากรมนุษย์อย่างเป็นรูปธรรม รายงานนี้จะตรวจสอบและเปรียบเทียบการประเมินผลการปฏิบัติงานบุคคลกองทัพบกไทยว่าสอดคล้องตามหลักการบริหารทรัพยากรมนุษย์หรือไม่ และปัจจัยที่ทำให้เกิดปัญหาและแนวทางแก้ไข

กองทัพบกไทยเป็นส่วนราชการตามพระราชบัญญัติจัดระเบียบกระทรวงกลาโหม พ.ศ.2551 ข้าราชการกองทัพบกมีจำนวน 3.8 แสนอัตรา บรรจุจริง 2.4 แสนคน ประกอบด้วยนายทหารชั้นสัญญาบัตรจำนวน 2.5 หมื่นคน นายทหารต่ำกว่าชั้นสัญญาบัตรและพลทหารประเภทละประมาณ1 แสนคน จึงนับได้ว่าเป็นส่วนราชการที่มีบุคคลมากที่สุดของภาครัฐไทย ภายในกองทัพบกยังแบ่งออกส่วนราชการต่างๆ จำนวนมาก ในแต่ละส่วนราชการมีหน้าที่ความรับผิดชอบที่แตกต่างกันออกไป ทั้งในส่วนกำลังรบ และส่วนสนับสนุนการรบ แต่เนื่องจากกองทัพไทยยังไม่ได้มีการแยกระบบงานพลเรือนในกองทัพออกจากงานทหารเช่นเดียวกับกองทัพมิตรประเทศ ทำให้บุคคลในส่วนนี้จำเป็นต้องเข้ารับการบรรจุในอัตราทหารและต้องเข้ารับการฝึกอบรมในหลักสูตรทหาร ในขณะที่เนื้องานไม่ได้มีส่วนเกี่ยวข้องกับการปฏิบัติการทางทหาร จึงส่งกระทบต่อการประเมินผลการปฏิบัติงานอย่างหลีกเลี่ยงไม่ได้จากการใช้ระบบการประเมินผลการปฏิบัติงานทางทหารและงานทางพลเรือนแบบเดียวกัน

จากการที่กองทัพบกมีบุคลากรจำนวนมากดังกล่าว และมีความหลากหลายในสาขาความรู้ที่นำมาใช้ในการปฏิบัติงานทางทหารรวมทั้งการสนับสนุน ตัวอย่างเช่น แพทย์ วิศวกร อาจารย์ นักกฎหมาย ตลอดจนลูกจ้าง พนักงานราชการ ทำให้มีความแตกต่างด้านตำแหน่งงานจำนวนมาก นอกจากนี้การแบ่งประเภทกำลังพลฝ่ายทหาร ยังแบ่งออกเป็นผู้บังคับบัญชา ฝ่ายอำนวยการ และเจ้าหน้าที่ปฏิบัติไม่แตกต่างไปจากส่วนราชการพลเรือน จึงทำให้มิติในการประเมินผลการปฏิบัติงานมีความซับซ้อนมากขึ้น จึงมีความจำเป็นต้องมีการแยกการประเมินผลการปฏิบัติงานให้มีความเฉพาะในงานแต่ละด้าน เพื่อให้สามารถนำมาใช้ในการบริหารทรัพยากรมนุษย์ได้อย่างเหมาะสม อย่างไรก็ตามการประเมินให้ได้ประสิทธิภาพนั้น ไม่ได้ขึ้นอยู่กับบุคลากรในกองทัพบกเพียงอย่างเดียว แต่ยังขึ้นอยู่กับวัฒนธรรมทางด้านประชาธิปไตยทั้งผู้ประเมินและผู้รับการประเมินด้วย

1.หลักการประเมินผลการปฏิบัติงานการบริหารทรัพยากรมนุษย์

การประเมินผลการปฏิบัติงาน (Performance Appraisal) หมายถึง การประเมินผลการปฏิบัติงานปัจจุบันหรือในอดีตโดยเปรียบเทียบกับมาตรฐานผลการปฏิบัติงานซึ่งถูกกำหนดไว้ โดยการเข้าถึงผลการประเมินอย่างแท้จริง และให้ผลสะท้อนกลับแก่ผู้รับการประเมินเพื่อช่วยลดข้อบกพร่องหรือรักษามาตรฐานการปฏิบัติงานไว้[30] ซึ่งนำไปบูรณาการกับการฝึกอบรม การให้รางวัล

[30] Gary Dessler.Human Resource Management, 12th ed., (New Jersey: Pearson, 2011). p.332.

ตอบแทนอย่างบูรณการหรือที่เรียกว่า การจัดการผลการปฏิบัติงาน (Performance Management) ซึ่งหมายถึง กระบวนการอย่างต่อเนื่องของการพิสูจน์ทราบ การวัด และการพัฒนาสมรรถภาพของแต่ละบุคคลหรือกลุ่ม และปรับสมรรถนะของพวกเขาเหล่านั้นให้ตรงตามเป้าหมายขององค์การ[31]

การประเมินผลการปฏิบัติงาน และการจัดการผลการปฏิบัติงาน มีความแตกต่างกันอย่างชัดเจนตรงที่ว่าการประเมินผลการปฏิบัติงานนั้นเป็นเหตุการณ์ที่เกิดขึ้นหนึ่งหรือสองครั้งต่อปีเมื่อสิ้นสุดวงรอบการปฏิบัติ ส่วนการจัดการผลการปฏิบัติงานเป็นกระบวนการที่เกิดขึ้นตั้งแต่ต้นปีมีการวางแผนและบูรณาการเข้ากับการจัดการบุคคลตลอดทั้งปีเกิดขึ้นทุกวัน ทุกสัปดาห์ ตอบโต้และป้อนกลับเพื่อให้แน่ใจว่ามีการปรับปรุงอย่างต่อเนื่องโดยเชื่อมโยงเข้ากับเป้าหมายทางยุทธศาสตร์ขององค์การ แล้วนำมาสู่การปรับปรุงการทำงาน การฝึกเพิ่มเติม การเปลี่ยนขบวนการทำงาน แผนการจูงใจ เป็นต้น[32]

- วงรอบการจัดการประเมิน มีวงรอบแบ่งออกเป็น 4 ขั้น[33] ดังนี้

ขั้นตอนที่ 1 การวางแผน : เพื่อตกลงเกี่ยวกับความรับผิดชอบหลักของแต่ละบุคคล พัฒนาความเข้าใจร่วมกันของเป้าหมายและวัตถุประสงค์ที่จำเป็นต้องบรรลุ กำหนดสมรรถนะสำคัญที่แต่ละคนต้องแสดงในงาน รวมทั้งสร้างแผนการพัฒนาที่เหมาะสมแต่ละคน

ขั้นตอนที่ 2 การดำเนินการ : มีความรับผิดชอบหลัก 2 ประการคือ การสร้างสภาวะที่กระตุ้น และเผชิญหน้าและแก้ไขทุกปัญหาของการประเมิน ซึ่งรวมถึงการทบทวนกลางปีเพื่อแน่ใจว่าการประเมินยังคงเป็นไปตามกำหนด

ขั้นตอนที่ 3 การประเมินค่า : เป็นการตัดสินว่าแต่ละคนทำงานได้ดีหรือไม่ และเติมลงไปในแบบประเมิน

ขั้นตอนที่ 4 การทบทวน : เป็นขั้นตอนสุดท้ายเกี่ยวกับการอภิปรายผลที่ได้จากการประเมิน โดยการทบทวนผลการประเมินปีที่ผ่านมาและความสำเร็จที่เกิดขึ้นจากการประเมิน หลังจากนั้นทั้งผู้ประเมินและผู้รับการประเมินจะสร้างเป้าหมาย วัตถุประสงค์ และพัฒนาแผนสำหรับปีต่อไป

- เครื่องมือและวิธีการประเมินผลการปฏิบัติงานเครื่องมือและวิธีการประเมินผลการปฏิบัติงานมีหลายแบบ ซึ่งอาจจะใช้หลายวิธีผสมกัน ได้แก่

1)แบบ Ranking :เป็นการประเมินแบบจัดลำดับซึ่งเป็นการเปรียบเทียบแบบง่ายๆ หรือเปรียบเทียบเฉพาะปัจจัย เพื่อจัดลำดับว่าแต่ละบุคคลอยู่ลำดับใด

---

[31] Ibid., p357.

[32] Ibid., p357-358.

[33] Dick Grote.The performance appraisal question and answer book: A survival guide for managers, (New York: American Management Association, 2002)

2)แบบ Rating :เป็นการประเมินตามแนวทางพฤติกรรมศาสตร์เพื่อแสดงออกมาเป็นตัวเลขโดยใช้แบบ Likert scale ใช้ปัจจัยต่างๆ ข้อดีคือสามารถใช้ได้กับทุกงานแต่มีข้อจำกัดคือค่าตัวเลขที่ประเมินไม่สามารถแสดงค่าจริงได้ โดยเกิดปัญหาการใช้ดุลยพินิจ เป็นการประเมินที่ได้รับความนิยมมาก

3)แบบ Checklist :เป็นการประเมินตามรายการว่ารายการใดได้ทำหรือไม่ ซึ่งทำให้ต้องมีรายละเอียดมาก และใช้ได้เฉพาะบางงาน

แบบการประเมินจะต้องออกแบบมาใช้เฉพาะกับองค์การ อย่างไรก็ตาม คำว่าองค์การตามทฤษฎีองค์การยังมีปัญหาเรื่องระดับในการวิเคราะห์ เนื่องจากองค์การขนาดใหญ่ประกอบด้วยองค์การขนาดเล็กหลายองค์การ องค์การแบบสาขาถึงแม้จะมีจำนวนมากแต่ก็มีความเหมือนกันจึงสามารถใช้แบบประเมินเดียวกัน เช่น โรงพยาบาลของกระทรวงสาธารณสุข แต่ถ้าองค์การรูปแบบราชการแบบเครื่องจักรกลจะประกอบด้วยองค์การเล็กหลายองค์การ โดยแต่ละองค์การมีความแตกต่างกันทั้งวัตถุประสงค์และวิธีการ จึงจำเป็นต้องใช้แบบประเมินที่แตกต่างกัน

รูปแบบองค์การที่ใช้ในกองทัพบกมีจำนวนประมาณ 500 รูปแบบ ซึ่งแต่ละรูปแบบได้นำไปใช้กับองค์การหลายหน่วย หากพิจารณารูปแบบองค์การ 5 รูปแบบตาม เฮนรี มินซ์เบอร์ก (Henry Mintzberg) แล้วภายในกองทัพบกจะมีรูปแบบองค์การแบบง่าย รูปแบบองค์การราชการแบบเครื่องจักรกล รูปแบบองค์การราชการแบบวิชาชีพ รูปแบบองค์การแบบสาขา และรูปแบบองค์การแบบโครงการ ถ้าหากพิจารณาแบ่งเป็นประเภท ได้แก่ หน่วยกำลังรบ โรงพยาบาล สถานศึกษา โรงงาน หน่วยงานวิจัย เป็นต้น ดังนั้น หากจะประเมินผลการปฏิบัติงานของกองทัพบกให้ได้ตามหลักการบริหารทรัพยากรมนุษย์ จึงจำเป็นต้องออกแบบประเมินมาเฉพาะกับรูปแบบหรือประเภทองค์การนั้นๆ

2.ปัญหาที่เกิดขึ้นในการประเมินผลการปฏิบัติงาน

การประเมินผลการปฏิบัติงานจะเกิดปัญหาต่างๆ ขึ้นเนื่องจากเป็นการดำเนินการโดยมนุษย์โดยมีผลกระทบต่อผู้ประเมินและผู้รับการประเมิน รวมทั้งแนวทางแก้ไขดังนี้[34]

- มาตรฐานไม่ชัดเจน (Unclear Standard) เกิดขึ้นกับการใช้วิธี Rating Scale โดยผู้ประเมินไม่ทราบว่า ดีเยี่ยม ดี พอใช้ ต่ำ ในแบบประเมินนั้น มีความหมายว่าอย่างไร หากใช้ผู้ประเมินหลายคน ก็จะทำให้ผู้รับการประเมินได้รับค่าแตกต่างกันไปด้วย

- ผลกระทบฮาโล (Halo effect) การประเมินในหัวข้อเดียวอาจจะส่งผลกระทบต่อการประเมินในหัวข้ออื่นด้วย เช่น การประเมินผู้ที่เข้ากับผู้อื่นไม่ได้ แล้วประเมินผลของงานของผู้นั้นต่ำไปด้วย แทนที่จะประเมินเฉพาะหัวข้อการเข้ากับผู้อื่นไม่ได้

---

[34]Gary Dessler.Human Resource Management, 12th ed., (New Jersey: Pearson, 2011).p.347-348.

- การให้คะแนนกลางทั้งหมด (Central Tendency) เกิดจากไม่อยากประเมินสูงหรือต่ำ ทำให้เกิดการให้คะแนนย่านกลางทั้งหมดซึ่งไม่สามารถนำผลมาใช้ในการจัดการได้ โดยจะเกิดกับการใช้วิธีประเมินแบบ Rating สามารถแก้ไขโดยใช้วิธีประเมินแบบ Ranking

- การให้คะแนนสูงหรือต่ำเกินไป (Leniency or Strictness) เป็นปัญหาที่ตรงข้ามกับการให้คะแนนกลางทั้งหมด เกิดจากผู้ประเมินใจดีหรือเข้มงวดมากเกินไป ทำให้ผลการประเมินสูงหรือต่ำเกินไป การแก้ไขปัญหาโดยการให้จัดลำดับผู้รับการประเมินทั้งหมด

- การมีอคติ (Bias) เป็นผลมาจากคุณลักษณะส่วนตัวของผู้ประเมินและผู้รับการประเมิน ทำให้ผลการประเมินแตกต่างไปจากความเป็นจริง

จากที่กล่าวมา จะเห็นได้ว่าการประเมินผลในการบริหารงานบุคคล นอกจากจะใช้ในขั้นตอนค่าตอบแทนแล้ว ยังต้องนำผลการประเมินไปใช้ในการพัฒนากำลังพลโดยจัดเข้ารับการฝึกและศึกษาทางทหารหลักสูตรต่าง ๆ เพื่อให้มีขีดความสามารถในการปฏิบัติงานแต่ละตำแหน่งในอัตราโครงสร้างการจัดได้อย่างมีประสิทธิภาพโดยเฉพาะหน่วยงานไซเบอร์ซึ่งมีคุณลักษณะที่ต้องใช้ความรู้ทางเทคนิคสูง

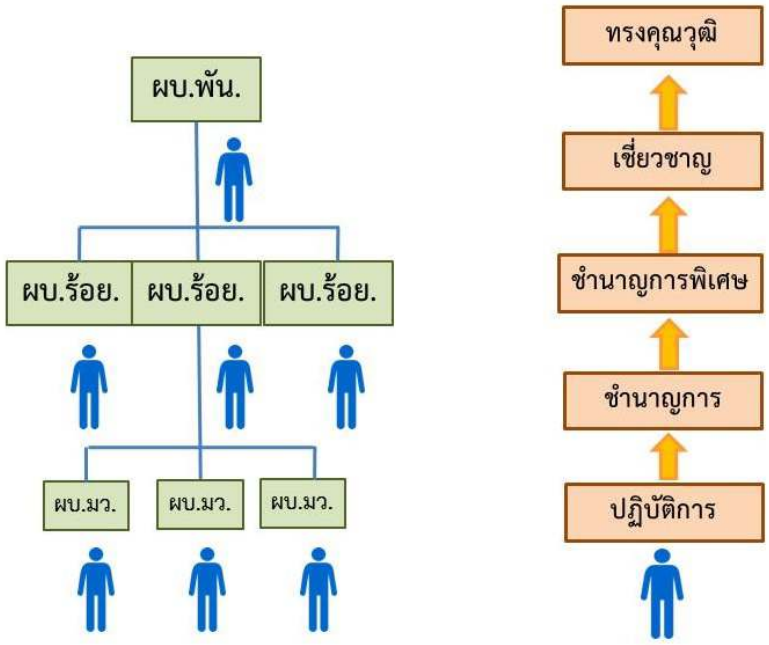
ทฤษฎีการจัดองค์การทางราบและการพัฒนาหน่วยงานด้านไซเบอร์

การจัดองค์การของกระทรวงกลาโหมไทยซึ่งยึดถือการจัดตามทฤษฎีองค์การระบบราชการแต่เดิมมายาวนานโดยมีลักษณะเป็นแบบสามเหลี่ยมทางดิ่งมาตั้งแต่สมัยรัชกาลที่ 5 ซึ่งในช่วงแรกกองทัพไทยได้มีข้าราชการพลเรือนทำงานในกระทรวงกลาโหม และต่อมาหลังการเปลี่ยนแปลงการปกครอง พ.ศ.2475 ประกอบกับยุคทหารนิยม (Militarism) ได้แผ่ขยายไปทั่วโลกก่อนสงครามโลกครั้งที่ 2 จึงทำให้เหลือเฉพาะอัตราทหารในกองทัพไทย โดยเฉพาะภายหลังจากการรับความช่วยเหลือจากสหรัฐอเมริกา พ.ศ.2495 ยิ่งทำให้โครงสร้างของทุกส่วนราชการในกระทรวงกลาโหมมีการจัดแบบโครงสร้างทางดิ่งเหมือนกับหน่วยกำลังรบที่มีอัตราส่วน 3:1 ตั้งแต่ระดับหมู่ปืนเล็ก จนถึงระดับกองทัพ ซึ่งโครงสร้างดังกล่าวมีข้อจำกัดคือแต่ละตำแหน่งมีการเปลี่ยนแปลงอยู่ตลอดเวลา ไม่เอื้ออำนวยต่อการปฏิบัติงานที่มีลักษณะเป็นงานเฉพาะ ดังนั้นพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551 จึงกำหนดให้มีข้าราชการกระทรวงกลาโหมขึ้นเพื่อปฏิบัติงานที่มีความชำนาญเฉพาะเหมือนกับทุกกองทัพมิตรประเทศ

การพัฒนาหน่วยงานด้านไซเบอร์กองทัพบกไทย จำเป็นต้องพิจารณาโครงสร้างแต่ละระดับที่เหมาะสมว่าจะเป็นองค์การทางดิ่ง องค์การทางราบ หรือเป็นแบบผสม ตามแผนภาพที่ 2 - 8เพื่อให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพซึ่งองค์การแต่ละรูปแบบมีพัฒนาความเป็นมาที่แตกต่างกัน โดยองค์การทางทหารจะมีรูปแบบเป็นสามเหลี่ยมทางดิ่ง มีข้อดีคือมีสายการบังคับบัญชาที่ชัดเจนและแน่นแฟ้นเนื่องจากช่วงการบังคับบัญชาไม่กว้างมากเกินไป แต่มีจุดอ่อนคือ

ตำแหน่งทุกตำแหน่งยึดติดกับชั้นยศทำให้มีการเปลี่ยนแปลงตัวบุคคลบ่อย ขาดความต่อเนื่อง จึงไม่เหมาะกับองค์การที่มีความชำนาญเฉพาะในปัจจุบันซึ่งมีลักษณะองค์การแห่งการเรียนรู้ (Knowledge-based Organization) ที่จำเป็นต้องจัดแบบทางราบโดยแต่ละตำแหน่งมีการเลื่อนไหลก้าวหน้าในตัวเองทำให้เหมาะสมกับองค์การที่มีความชำนาญเฉพาะด้าน แต่ทั้งนี้ขึ้นอยู่กับว่ากองทัพกำหนดบทบาทของหน่วยงานด้านไซเบอร์ไว้อย่างไร

แผนภาพที่ 2 - 8 การจัดองค์การทางดิ่ง (ทหาร) และทางราบ (พลเรือน)

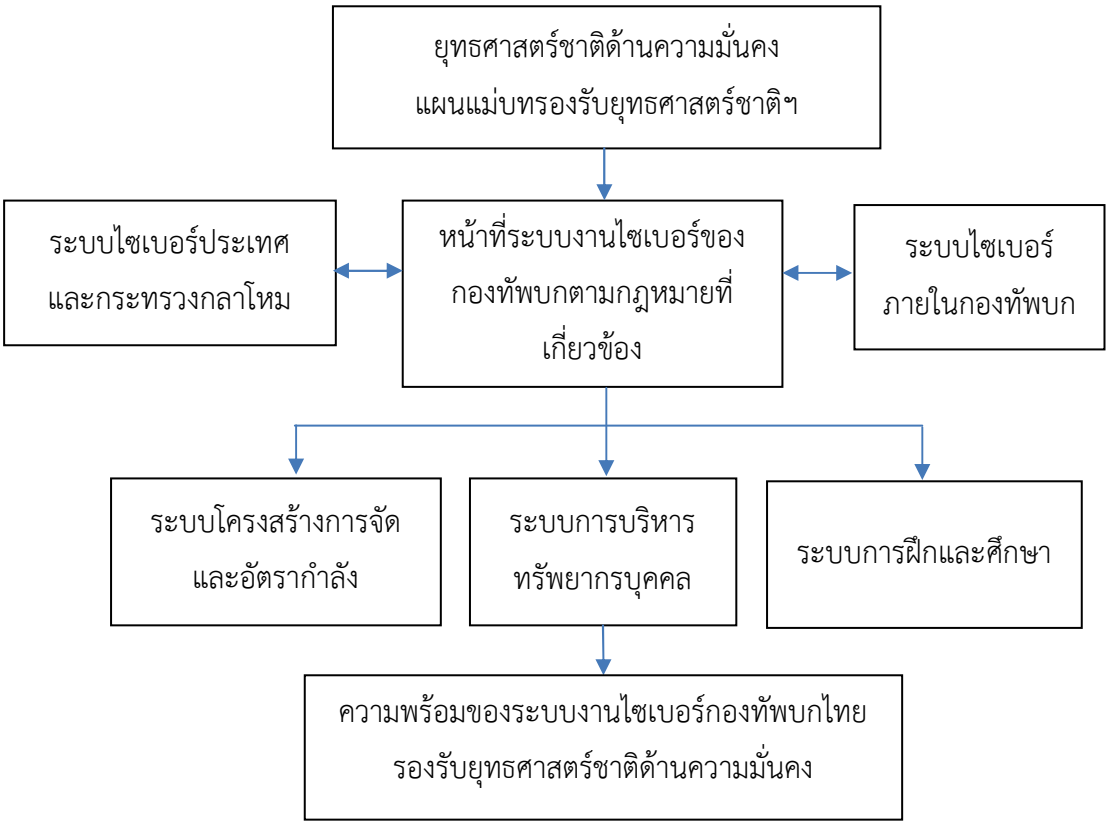


กรอบแนวคิดของการวิจัย

จากการทบทวนวรรณกรรม สามารถกำหนดแนวทางในการวิจัยซึ่งใช้ในการดำเนินการในบทต่อไปได้ว่า การที่จะพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยให้สามารถรองรับ

ยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างมีประสิทธิภาพนั้น จำเป็นต้องมีการกำหนดหน้าที่ของงานด้านไซเบอร์ให้มีความชัดเจนและเชื่อมโยงกับระบบการปฏิบัติการทางทหารอื่นๆ ให้มีความชัดเจน หลังจากนั้นจึงจะนำบทบาท อำนาจหน้าที่ดังกล่าวมาดำเนินการศึกษาว่าการที่หน่วยงานด้านไซเบอร์ของกองทัพบกไทยจะปฏิบัติงานดังกล่าวได้นั้น จะต้องพัฒนาในเรื่องใดบ้าง โดยกองทัพเป็นเครื่องมือหนึ่งของรัฐในการรักษาความมั่นคงของรัฐซึ่งได้มีการกำหนดหน้าที่ตามกฎหมายและขยายรายละเอียดลงมาจนถึงการจัดหน่วยทหารและระดับบุคคลตามหลักทฤษฎีองค์การ โดยทุกส่วนราชการในกองทัพบกไทยได้กำหนดหน้าที่ความรับผิดชอบไว้ตามกฎหมาย ซึ่งมีความเชื่อมโยงกับระบบงานของส่วนราชการอื่นในกระทรวงกลาโหมและประเทศไทยอย่างไทยเป็นระบบ โดยการวิจัยจะศึกษาความเชื่อมโยง และความซ้ำซ้อนของระบบงานไซเบอร์รวมทั้งการศึกษาเปรียบเทียบกับกองทัพมิตรประเทศ เมื่อได้ผลสรุปแล้วจึงจะนำมาศึกษาระบบโครงสร้าง การจัดอัตรากำลัง และการบริหารทรัพยากรบุคคล เพื่อให้ระบบงานไซเบอร์ของกองทัพบกไทยสามารถทำหน้าที่ตามที่กฎหมายกำหนด และรองรับยุทธศาสตร์ชาติด้านความมั่นคง แล้วสรุปในภาพรวมเป็นข้อสรุปและข้อเสนอในการวิจัยตามแผนภาพที่ 2 - 9

แผนภาพที่ 2 - 9 กรอบแนวคิดในการวิจัย



บทที่ 3
ผลการศึกษาข้อมูล

จากการทบทวนวรรณกรรมในบทที่ 2 ทำให้ทราบแนวคิดและทฤษฎีที่เกี่ยวข้องในการพัฒนาการระบบงานไซเบอร์ของกองทัพไทยและกองทัพมิตรประเทศ ซึ่งจะเริ่มเห็นแล้วว่าการที่จะพัฒนาระบบงานไซเบอร์ของกองทัพบกไทยให้มีความทันสมัยและมีประสิทธิภาพสามารถรองรับภัยคุกคามรูปแบบใหม่ที่กำหนดไว้ในยุทธศาสตร์ชาติด้านความมั่นคงได้อย่างมีประสิทธิภาพนั้น ไม่ใช่มุ่งไปที่เครื่องมือเทคโนโลยีชั้นสูงในการปฏิบัติงานเพียงอย่างเดียว แต่จำเป็นต้องพัฒนาหลายระบบไปพร้อมกันตั้งแต่แนวคิดการจัดหน่วยงานไซเบอร์ให้มีความสัมพันธ์กับระบบงานอื่นเพื่อให้สามารถสอดคล้องกับการปฏิบัติทางทหาร โครงสร้างการจัดหน่วยงานไซเบอร์ในระดับต่างๆ รวมถึงการบริหารงานบุคคล สำหรับในบทนี้จะได้สรุปผลการศึกษาข้อมูลซึ่งได้จากการศึกษาเอกสาร การสัมภาษณ์ผู้ให้ข้อมูลสำคัญ และการสังเกตการณ์แบบมีส่วนร่วมจากการปฏิบัติงานในหน่วยงานไซเบอร์

พัฒนาการระบบงานไซเบอร์ของกองทัพไทยและกองทัพมิตรประเทศ

ระบบงานไซเบอร์เป็นผลมาจากการเปลี่ยนแปลงเทคโนโลยีด้านการสื่อสารอย่างรวดเร็วเพียงแค่ในช่วงสองทศวรรษที่ผ่านมาเท่านั้น ซึ่งทำให้การติดต่อสื่อสารข้อมูลสามารถทำได้อย่างรวดเร็วจากการส่งเฉพาะคำพูดแบบอนาลอกในระบบ 1G มาเป็นการส่งเสียงและข้อมูลในระบบ 2G และการส่งภาพในระบบ 3 G จนกระทั่งในปัจจุบันกำลังก้าวไปสู่ระบบ 5G และยังไม่รู้ว่าจะยุติเมื่อใด การพัฒนาอย่างรวดเร็วดังกล่าวได้ก่อให้เกิดผลดีทั้งต่อรัฐในภาพรวมและประชาชนระดับบุคคล โดยนำข้อมูลข่าวสารทั้งหมดไปใส่ไว้ในระบบการสื่อสารที่มีความเร็วสูงและการเก็บข้อมูลขนาดใหญ่สามารถนำมาใช้งานได้อย่างสะดวก รวดเร็ว ในทุกสาขาวิชาชีพ ในขณะเดียวกัน ก็ได้ก่อให้เกิดผลเสียในการนำไปใช้งานทุกด้านด้วยเช่นกัน ทั้งการลักลอบนำข้อมูลมาใช้งาน และการขัดขวางในการติดต่อสื่อสารข้อมูล ซึ่งเกิดผลกระทบต่อความมั่นคงจนทำให้ในปัจจุบันความมั่นคงไซเบอร์ (Cyber Security) ถือว่าเป็นความมั่นคงของรัฐลำดับต้นในรัฐตะวันตก

1. พัฒนาการระบบงานไซเบอร์ของกองทัพไทย

การสื่อสารของกองทัพบกตั้งแต่ก่อนสมัยรัชกาลที่ 5 เป็นหน้าที่ของกรมทหารช่าง ต่อมาเมื่อการสื่อสารมีความสำคัญมากขึ้นและเทคโนโลยีการสื่อสารมีการพัฒนาอย่างมาก นายพลเอก พระเจ้าบรมวงศ์เธอ กรมพระกำแพงเพชรอัครโยธิน จึงแยกงานการสื่อสารออกจากงานทหารช่าง

และได้ก่อตั้งเหล่าทหารสื่อสารขึ้นเมื่อ 27 พฤษภาคม พ.ศ.2467[35] จากนั้นกองทัพเรือ กองทัพอากาศ และกองบัญชาการกองทัพไทย (กองบัญชาการทหารสูงสุดในสมัยนั้น) ได้จัดตั้งหน่วยทหารสื่อสารขึ้นตามลำดับ เพื่อรับผิดชอบงานด้านการสื่อสารและระบบสารสนเทศต่างๆ

ในช่วงทศวรรษ 2530 การติดต่อสื่อสารภาคพื้นในชีวิตประจำวันเป็นการส่งข้อมูลผ่านระบบคอมพิวเตอร์ยังคงเป็นการส่งข้อมูลที่เป็นตัวอักษร (Text) ผ่านระบบโมเด็มพื้นฐานแบบง่ายๆ ด้วยความ 1,200 BPS งานด้านไซเบอร์จึงยังไม่ปรากฏให้เห็นอย่างชัดเจนเนื่องมาจากข้อจำกัดของข้อมูลที่ติดต่อสื่อสารที่มีความเร็วช้าและปริมาณน้อย แต่ก็เริ่มมองให้เห็นการรักษาความปลอดภัยด้วยการเข้ารหัสในการส่งผ่านข้อมูลในหลายวิธี งานดังกล่าวจึงยังคงอยู่ในกิจการสื่อสารของทุกเหล่าทัพ โดยกองทัพบกได้จัดตั้งศูนย์สารสนเทศ ศูนย์ปฏิบัติการกองทัพบก ขึ้นในปี พ.ศ.2537 เพื่อนำเทคโนโลยีสารสนเทศมาเสริมการบริหารและการปฏิบัติงานของกองทัพบกให้มีประสิทธิภาพ[36]จะเห็นว่าเทคโนโลยีเป็นปัจจัยสำคัญที่ทำให้มีการปรับโครงสร้างกองทัพขึ้นมารองรับ

กองทัพบกได้จัดตั้งศูนย์เทคโนโลยีทางทหารกองทัพบกขึ้นในปี พ.ศ.2539 เพื่อให้มีหน่วยงานที่รับผิดชอบกิจการคอมพิวเตอร์ทั้งปวงของกองทัพบก รับผิดชอบและจัดการระบบฐานข้อมูลโดยใช้เทคโนโลยีที่ทันสมัย ทั้งเทคโนโลยีสารสนเทศ เทคโนโลยีภาพถ่ายดาวเทียม เทคโนโลยีคอมพิวเตอร์เพื่อให้เกิดประสิทธิภาพสูงสุดในการบริหารงานยามปกติและการควบคุมอำนวยการยุทธ์ทั้งในยามปกติและยามสงคราม โดยเป็นหน่วยขึ้นตรงกองทัพบกและเป็นหัวหน้าเหล่าสายวิทยาการด้านคอมพิวเตอร์ ต่อมาได้ปรับการบังคับบัญชาขึ้นตรงต่อกรมการทหารสื่อสาร ในปี พ.ศ.2548[37] การพัฒนาดังกล่าวแสดงให้เห็นว่าหน่วยงานด้านเทคโนโลยีรวมทั้งด้านไซเบอร์มีการเปลี่ยนแปลงอย่างรวดเร็วที่สุดเมื่อเปรียบเทียบกับหน่วยงานอื่นในกองทัพ ซึ่งเป็นผลมาจากการเปลี่ยนแปลงทางด้านเทคโนยีอย่างรวดเร็ว

ระบบการสื่อสารสารสนเทศได้พัฒนาอย่างรวดเร็วจนเข้าสู่ยุคไซเบอร์ เทคโนโลยีใหม่ๆ ที่ทันสมัยนำมาซึ่งภัยคุกคามรูปแบบใหม่ๆ และเริ่มทวีความรุนแรงขึ้นอย่างรวดเร็ว ทำให้งานดังกล่าวเริ่มมีความชัดเจนและแยกย่อยออกมาจากการติดต่อสื่อสารตามปกติ แต่ละเหล่าทัพเห็นถึงความจำเป็นในการรับมือและป้องกันความเสี่ยงที่อาจเกิดขึ้น จึงเริ่มจัดตั้งหน่วยไซเบอร์เพื่อรับผิดชอบด้านไซเบอร์โดยตรง ในส่วนของกองทัพบกได้แปรสภาพศูนย์เทคโนโลยีทางทหาร มาเป็นศูนย์ไซเบอร์ในปี พ.ศ.2559 เพื่อรับผิดชอบงานด้านไซเบอร์โดยเฉพาะ[38] จากการพัฒนาดังกล่าวจะเห็นได้ว่างานด้านไซเบอร์มีความเชื่อมโยงกับงานด้านสื่อสารและงานด้านคอมพิวเตอร์อย่างแนบแน่น จนทำให้ยาก

---

[35]กรมการทหารสื่อสาร. “กำเนิดกรมการทหารสื่อสาร”. (ออนไลน์). เข้าถึงได้จาก :http://signal.rta.mi.th/web/history.php, 2559.

[36]“ศูนย์ไซเบอร์กองทัพบก”. (ออนไลน์). เข้าถึงได้จาก :http://cyber.rta.mi.th, 2560.

[37]เรื่องเดียวกัน.

[38]เรื่องเดียวกัน.

ที่จะแยกออกจากกันอย่างชัดเจน ซึ่งปัญหาที่มีความเชื่อมโยงแต่ก็มีลักษณะงานที่สามารถแยกเฉพาะออกมาได้ดังกล่าวจึงเกิดแนวคิดในการจัดรวมเป็นกลุ่มงานเดียวกันในกองทัพมิตรประเทศ ในขณะที่กองทัพไทยยังไม่มีความชัดเจน

นอกจากหน่วยงานในกระทรวงกลาโหมแล้วในระดับรัฐยังได้มีการการรักษาความมั่นคงปลอดภัยไซเบอร์ตามเหตุผลในการประกาศใช้พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กล่าวคือในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเทอร์เน็ตโครงข่ายโทรคมนาคมหรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ดังนั้น เพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีสมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชนที่จะต้องมีการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่างๆรวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชนไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรงตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่องอันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ[39] จากเหตุผลดังกล่าว ได้ก่อให้เกิดคำถามต่อกองทัพในสองประการ คือ ประการแรก กองทัพต้องอยู่ภายใต้พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ในฐานะส่วนราชการหนึ่ง และประการที่สองคือ กองทัพจะต้องปฏิบัติการทางทหารด้านไซเบอร์เพื่อสนับสนุนการปฏิบัติการทางทหารอย่างเป็นสากลเช่นเดียวกับกองทัพมิตรประเทศ ซึ่งจำเป็นต้องศึกษาว่าทั้งสองประการเป็นเรื่องเดียวกัน หรือไม่มีความเชื่อมโยงสนับสนุนซึ่งกันและกัน หรือขัดแย้งกันอย่างไร และจะมีข้อเสนอแนะอย่างไร

2.พัฒนาการระบบงานไซเบอร์ของกองทัพมิตรประเทศ

พัฒนาการระบบงานไซเบอร์ของกองทัพมิตรประเทศ ไม่แตกต่างไปจากกองทัพไทยโดยแยกมาจากงานสื่อสารมาไม่นานตามความก้าวหน้าของเทคโนโลยีคอมพิวเตอร์และสารสนเทศที่เป็นไปอย่างรวดเร็ว จากการที่การเมืองระหว่างประเทศอยู่ในสภาวะอนาธิปไตยซึ่งไม่มีรัฐบาลกลางมาควบคุม ส่งผลทำให้พลังอำนาจทางทหารยังคงมีความจำเป็นต่อรัฐพลังอำนาจทางทหารจึงรวมเข้ากับการเมืองโดยไม่สามารถแยกออกจากนโยบายต่างประเทศได้และกำลังทหารสามารถใช้ในภารกิจที่

[39]“พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562”, ราชกิจจานุเบกษา. เล่ม 136, 27 พฤษภาคม 2562, หน้า 51.

หลากหลายทั้งวัตถุประสงค์ทางทหารและไม่ใช่ทางทหาร[40]หลังจากสงครามเย็นยุติลงในต้นทศวรรษ 1990 ความขัดแย้งจนถึงระดับการใช้กำลังทหารทำสงครามระหว่างรัฐ (Interstate War) ลดน้อยลง เหลือเพียงความขัดแย้งระดับต่ำ (Low Intensity Conflict) ทำให้มีแนวคิดนำกำลังทหารมาใช้ภายในรัฐมากขึ้นโดยเฉพาะหลังจากเหตุการณ์ 9/11 ได้ทำให้ประชาคมระหว่างประเทศเพิ่มบทบาทกองทัพต่อภัยคุกคามรูปแบบใหม่ (Non-traditional Threat) มากขึ้น โดยมีลักษณะภัยคุกคามซึ่งข้ามพรหมแดนเข้ามาภายในรัฐ

ถึงแม้ว่ารัฐจะมีอำนาจอธิปไตยภายในรัฐ แต่การใช้กำลังทหารภายในรัฐไม่ใช่เป็นสิ่งที่อ้างว่าเป็นอธิปไตยภายในที่รัฐจะสามารถใช้กำลังทหารอย่างไรก็ได้ โดยเฉพาะผลกระทบต่อประชาชนภายในรัฐเองแต่เป็นประเด็นสากลที่เกี่ยวข้องกับกฎหมายสิทธิมนุษยชนตามพันธกรณีที่ทุกรัฐได้เป็นสมาชิกองค์การระหว่างประเทศโดยเฉพาะหลังจากเหตุการณ์ 9/11 รัฐต่างๆได้นำกองทัพเข้ามาปฏิบัติภารกิจในการบังคับใช้กฎหมายภายในรัฐมากขึ้นตามตัวอย่างภารกิจในการบังคับใช้กฎหมายของรัฐต่างๆ ซึ่งรวมถึงการใช้กำลังทหารในการสนับสนุนฝ่ายพลเรือนในการปฏิบัติการไซเบอร์ด้วยตารางที่ 3 - 1

ตาราง 3 - 1 ภารกิจกองทัพในการบังคับใช้กฎหมายของรัฐต่างๆ

	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
การรักษาความสงบเรียบร้อย	√	√	√	√	√	√	√	√	√	√	√
การต่อต้านการก่อการร้าย	√	√	√	√	√	√	√	√	√	√	√
การควบคุมชายแดน	√	-	√	√	√	-	√	√	√	-	√
การปราบปรามยาเสพติด	√	√	√	√	√	√	-	√	√	-	√
การบังคับใช้กฎหมาย	√	√	√	√	√	-	√	√	√	-	-
การสอบสวนอาชญากรรม	√	-	√	√	√	-	-	√	√	-	√
การสนับสนุนงานสาธารณะ	√	√	√	√	√	√	√	√	√	√	-
การสร้างความปลอดภัยบุคคล	√	√	√	√	√	-	√	√	√	√	√
การปฏิบัติการไซเบอร์	-	-	√	√	-	-	-	√	√	√	√
การรวบรวมข่าวสาร	-	-	√	√	-	-	-	√	√	-	√

[40]Robert J. Art and Robert Jervis, "The fungibility of force", in International politics: Enduring concepts and contemporary issues, (New York : Pearson, 2009). p.205.

ที่มา : Albrecht Schnabel and Marc Krupanski, 2012 : 36-37.

หัวใจสำคัญที่สุดในการปฏิบัติการทางทหารคือการวางกำลังให้เหมาะสมกับเวลา (Time) และพื้นที่ (Space) ด้วยความก้าวหน้าทางเทคโนโลยีส่งผลทำให้การปฏิบัติการทางทหาร ซึ่งพื้นที่ในอดีตเดิมมีเฉพาะทางบก (Land) และทางทะเล (Sea) ตามประวัติศาสตร์สงคราม เพโลพอนนีเซียน สมัยกรีกโบราณ 431-404 ปี ก่อนคริสตกาล ต่อมาในศตวรรษที่ 18 มนุษย์สามารถพัฒนาอากาศยานและนำมาใช้ในกิจการทหารทำให้พื้นที่ขยายเพิ่มมาเป็นทางอากาศ (Air) หลังสงครามโลกครั้งที่ 2 ได้มีการแข่งขันการเดินทางไปสู่อวกาศท่ามกลางสงครามเย็นระหว่างสหรัฐอเมริกาและสหภาพโซเวียต โดยต่างฝ่ายต่างครอบครองขีปนาวุธข้ามทวีปและดาวเทียมทำให้พื้นที่ทางทหารขยายเพิ่มเป็นอวกาศ (Space) และด้วยความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์และการสื่อสารข้อมูลได้ทำให้พื้นที่ทางทหารเพิ่มมาเป็นไซเบอร์อย่างรวดเร็วโดยกองทัพสหรัฐอเมริกาได้แบ่งพื้นที่ไซเบอร์สำหรับการวางแผนและการปฏิบัติการทางทหารออกเป็น 3 ระดับ ซึ่งมีความแตกต่างแต่มีความเกี่ยวข้องกัน ทำให้การมุ่งเน้นในการวางแผน การปฏิบัติการ ในแต่ละระดับแตกต่างกัน ได้แก่

1)ระดับเครือข่ายทางกายภาพ (The physical network layer) ประกอบด้วยโครงสร้างพื้นฐานและอุปกรณ์ไอทีที่อยู่ในพื้นที่จัดเก็บ การขนส่ง และกระบวนการประมวลผลข้อมูลข่าวสารภายในพื้นที่ไซเบอร์รวมถึงความเชื่อมโยงระหว่างอุปกรณ์เครือข่าย ฮาร์ดแวร์และโครงสร้างอื่น โดยในระดับนี้ยังอยู่ในพื้นที่ทางภูมิศาสตร์และต้องการการรักษาความปลอดภัยทางกายภาพทั้งของรัฐและเอกชนไม่ให้ถูกทำลาย

2)ระดับเครือข่ายทางโลจิก (The logical network layer) ประกอบด้วยเครือข่ายที่เชื่อมโยงระหว่างกันต่อจากเครื่อข่ายทางกายภาพบนพื้นฐานของชุดคำสั่งที่ขับเคลื่อนอุปกรณ์เครือข่าย รวมถึงข้อมูล โปรแกรมประยุกต์ URL และ Internet Protocol ฮาร์ดแวร์และซอฟต์แวร์โดยไม่จำเป็นต้องรู้สถานที่ทางภูมิศาสตร์

3)ระดับบุคคล-ไซเบอร์ (The cyber-persona layer) ประกอบด้วยหมายเลขแอคเคานท์ของเครือข่ายหรือไอพีที่สัมพันธ์กัน ไม่ว่าจะเป็นมนุษย์หรือสิ่งใดที่เกี่ยวข้องโดยตรงระดับบุคคล เช่น อีเมลล์ เว็บเพจ หมายเลขโทรศัพท์ และรหัสผ่าน เป็นต้น

โครงสร้างการจัดหน่วยงานด้านไซเบอร์ของไทย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒มีหลักการและเหตุผลเพื่อให้การให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเทอร์เน็ตโครงข่ายโทรคมนาคมหรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจ

กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศดังนั้นเพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีสมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชนที่จะต้องมีการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่างๆรวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชนไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรงตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่องอันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ[41] จากพระราชบัญญัติดังกล่าว ทำให้การจัดโครงสร้างและอัตรากำลังรวมถึงระบบงานของไซเบอร์ในทุกระดับต้องพัฒนาตามไปด้วย สำหรับโครงสร้างการจัดหน่วยงานด้านไซเบอร์ของไทยในปัจจุบันมีดังนี้

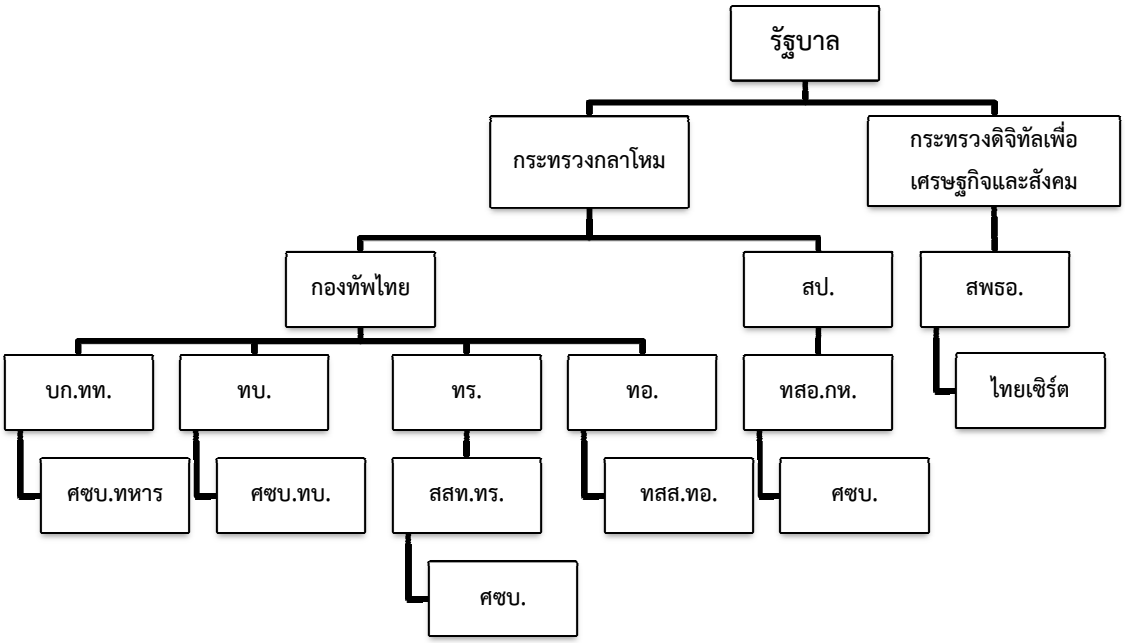
1.ระดับรัฐบาล

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ซึ่งไทยเซิร์ต มีหน้าที่ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้การสนับสนุนที่จำเป็นและให้คำแนะนำในการแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต นอกจากนี้ ยังมีบทบาทสำคัญในการประสานงานระหว่างหน่วยงานต่างประเทศกับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง เนื่องจากไทยเซิร์ตเป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค คือ APCERT/Asia Pacific Computer Emergency Response Team และระดับสากล คือ FIRST/Forum of Incident Response and Security Teams[42]ตามแผนภาพที่ 3 - 1

แผนภาพที่ 3 - 1 แสดงโครงสร้างการจัดหน่วยงานด้านไซเบอร์ระดับรัฐบาลและความเชื่อมโยงกับหน่วยงานด้านไซเบอร์ในกระทรวงกลาโหมไทย

[41]“พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562”, ราชกิจจานุเบกษา. เล่ม 136, 27 พฤษภาคม 2562, หน้า 51.

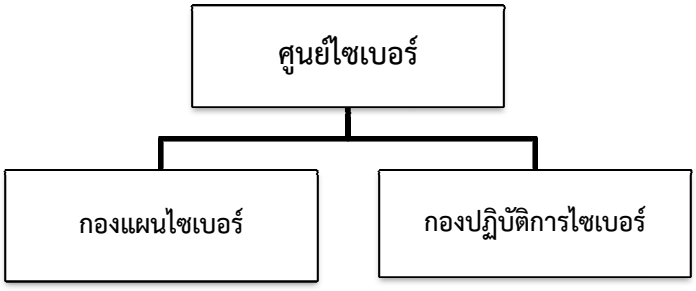
[42]ThaiCERT.“2016 ThaiCERT Annual Report”. (รายงานประจำปี. 2559). p.12.



2. ระดับกระทรวงกลาโหม

สำนักงานปลัดกระทรวงกลาโหม (สป.) ได้จัดตั้งศูนย์ไซเบอร์ขึ้นภายใต้กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ศซบ.ทสอ.กห.) มีภารกิจในการพิจารณา เสนอความเห็น วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับนโยบายและยุทธศาสตร์ด้านไซเบอร์ นำนโยบายด้านไซเบอร์ระดับรัฐบาลไปสู่การปฏิบัติ สนับสนุนภารกิจด้านไซเบอร์เพื่อความมั่นคงของประเทศ ส่งเสริมและสนับสนุนการปฏิบัติการข้อมูลข่าวสารและความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ รวมทั้งการสนับสนุนหน่วยไซเบอร์ระดับปฏิบัติ โดย ศซบ.ทสอ.กห. ประกอบด้วย 2 กอง คือ กองแผนไซเบอร์ และกองปฏิบัติการไซเบอร์[43] ตามแผนภาพที่ 3 - 2

แผนภาพที่ 3 - 2 แสดงโครงสร้างการจัดศูนย์ไซเบอร์สำนักงานปลัดกระทรวงกลาโหม



[43]ศูนย์ไซเบอร์ ทสอ.กห. “หน่วยขึ้นตรง”.(ออนไลน์). เข้าถึงได้จาก : http://csc.dist.mod.go.th, 2561.

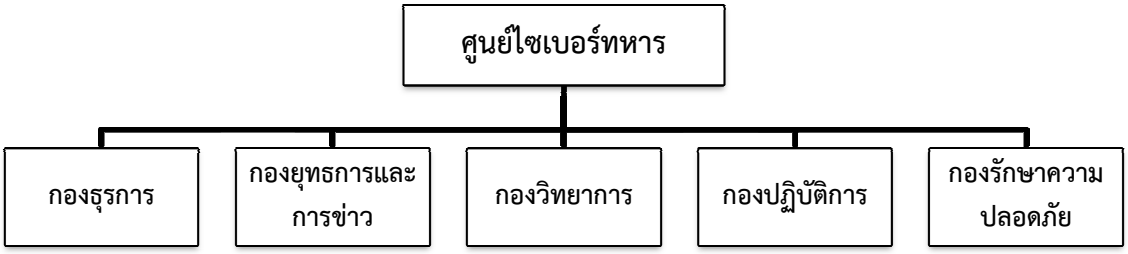
3.ระดับกองทัพไทย

พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551 และฉบับแก้ไข กำหนดการแบ่งราชการในกระทรวงกลาโหมออกเป็นสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย โดยกองบัญชาการกองทัพไทยแบ่งออกเป็นกองทัพบก กองทัพเรือ และกองทัพอากาศ

3.1 กองบัญชาการกองทัพไทย (บก.ทท.)

ได้จัดตั้ง ศูนย์ไซเบอร์ทหาร (ศซบ.ทหาร) อยู่ในส่วนบังคับบัญชาของกองบัญชาการกองทัพไทย โดยมีภารกิจ เสนอความเห็น กำหนดนโยบาย วางแผน อำนวยการประสานงาน บูรณาการ ปฏิบัติการ และกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ ดำเนินการจัดการศึกษา บูรณาการด้านการข่าวกรองทางไซเบอร์ และเป็นสายวิทยาการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพไทย ซึ่งประกอบด้วย 5 กอง คือ กองธุรการกองยุทธการและการข่าวกองวิทยาการ กองปฏิบัติการ และกองรักษาความปลอดภัยนอกจากนี้ยังมีการจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ ศูนย์บัญชาการทางทหาร (ศรซ.ศบท.) มีภารกิจ ป้องกันภัยคุกคามทางไซเบอร์ให้กับศูนย์บัญชาการทางทหารตลอด 24 ชั่วโมง รวมทั้งทำหน้าที่บูรณาการงานด้านไซเบอร์ให้กับเหล่าทัพและหน่วยงานที่เกี่ยวข้อง[44] ตามแผนภาพที่ 3 - 3

แผนภาพที่ 3 - 3 แสดงโครงสร้างการจัดศูนย์ไซเบอร์กองบัญชาการกองทัพไทย



3.2 กองทัพบก(ทบ.)

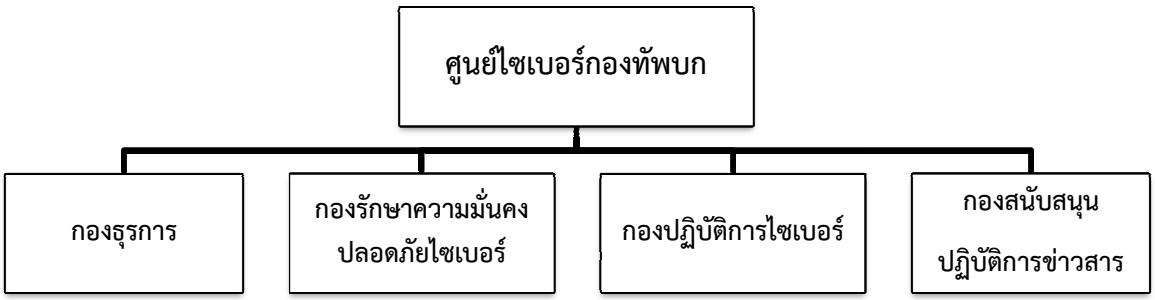
ได้จัดตั้งศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) เป็นหน่วยในฝ่ายกิจการพิเศษของกองทัพบก มีภารกิจดำเนินการเกี่ยวกับการปฏิบัติด้านไซเบอร์และพัฒนาความพร้อมด้านไซเบอร์ของกองทัพบก นอกจากนี้ ยังทำหน้าที่เฝ้าระวังความปลอดภัยให้กับระบบเครือข่ายกองทัพบก และเว็บไซต์ของหน่วยขึ้นตรงกองทัพบก ซึ่ง ศซบ.ทบ. ประกอบด้วย 4 กอง คือ กองธุรการ กองรักษา

[44]ศูนย์ไซเบอร์ทหาร, “Cyber Security Center, Royal Thai Armed Forces”. (CD-ROM), 2561.

ความมั่นคงปลอดภัยไซเบอร์ กองปฏิบัติการไซเบอร์ และกองสนับสนุนปฏิบัติการข่าวสาร[45]ตามแผนภาพที่ 3 - 4

หลังการแปรสภาพจากศูนย์เทคโนโลยีทางทหาร (ศทท.) ซึ่งเป็นหน่วยขึ้นตรงของกรมสื่อสารทหารบก มาเป็นศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) เมื่อ 1 ตุลาคม 2559[46] ได้ทำหน้าที่ดำเนินการปฏิบัติการด้านไซเบอร์ โดยการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับระบบเครือข่ายอินเตอร์เน็ตของกองทัพบก รวมถึงระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ในโครงการระบบสารสนเทศกองทัพบก (Management Information System : MIS)[47] ซึ่งอยู่ในความรับผิดชอบของกรมการทหารสื่อสาร นอกจากนี้ ศซบ.ทบ. ยังดำเนินการวิเคราะห์ข่าวสารทางไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบก[48] ซึ่งอยู่ในความรับผิดชอบของกรมยุทธการทหารบก

แผนภาพที่ 3 - 4 แสดงโครงสร้างการจัดศูนย์ไซเบอร์กองบัญชาการกองทัพบก



3.3กองทัพเรือ (ทร.)

กองทัพเรือมีการจัดตั้งศูนย์ไซเบอร์ขึ้นภายใต้ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (ศซบ.สสท.ทร.) ในส่วนบัญชาการของกองทัพเรือ มีภารกิจรับมือและตอบโต้ภัยคุกคามทางไซเบอร์ รวมทั้งตอบสนองต่อภารกิจต่างๆ ในการดำเนินการด้านสงคราม

---

[45]ศูนย์ไซเบอร์กองทัพบก. "คำสั่งศูนย์ไซเบอร์กองทัพบก (เฉพาะ) ที่ 1/59 เรื่องกำหนดหน้าที่และอัตรากำลังพลอัตราเฉพาะกิจ หมายเลข 2900 ศูนย์ไซเบอร์กองทัพบก". ลงวันที่ 3 ตุลาคม 2559.

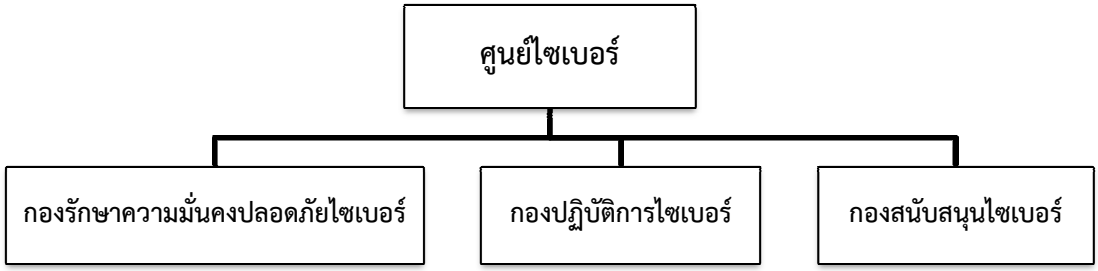
[46]กรมยุทธการทหารบก. “หนังสือ ลับ ด่วนมาก ที่ กห 0403/1074 เรื่องขออนุมัติจัดตั้งศูนย์ไซเบอร์กองทัพบก โดยการแปรสภาพหน่วย ศทท.”. ลงวันที่ 19 กันยายน 2559.

[47]กองทัพบก, โครงการจัดหาระบบสารสนเทศกองทัพบก (MIS), 2547.

[48]ศูนย์ไซเบอร์กองทัพบก. เรื่องเดิม.

ไซเบอร์ของ ทร. ซึ่ง ศซบ.สสท.ทร. ประกอบด้วย 3 กอง คือ กองรักษาความมั่นคงปลอดภัยไซเบอร์ กองปฏิบัติการไซเบอร์ และกองสนับสนุนไซเบอร์[49]ตามแผนภาพที่ 3 – 5

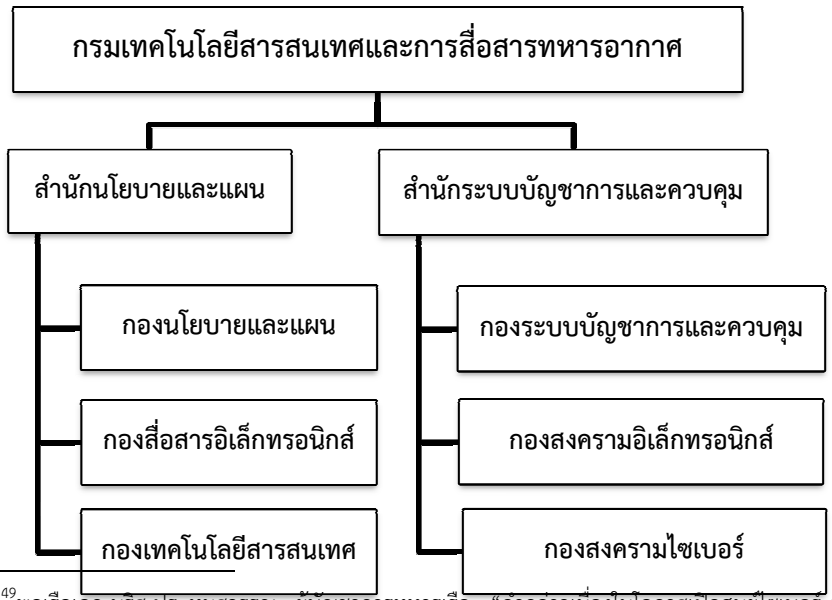
แผนภาพที่ 3 - 5 แสดงโครงสร้างการจัดศูนย์ไซเบอร์กองบัญชาการกองทัพเรือ



3.4 กองทัพอากาศ (ทอ.)

ยังไม่ได้จัดตั้งศูนย์ไซเบอร์ แต่มีกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ซึ่งอยู่ในส่วนบัญชาการกองทัพอากาศ ทำหน้าที่เกี่ยวกับไซเบอร์ คือ เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านระบบบัญชาการและควบคุมข่ายเครือข่ายเทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ รวมทั้งจัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์[50]ตามแผนภาพที่ 3 - 6

แผนภาพที่ 3 - 6 แสดงโครงสร้างการจัดศูนย์ไซเบอร์กองบัญชาการกองทัพอากาศ



[49]พลเรือเอก นริส ประทุมสุวรรณ, ผู้บัญชาการทหารเรือ. “คำกล่าวเนื่องในโอกาสเปิดศูนย์ไซเบอร์ สสท.ทร.”, ณ กองบัญชาการทหารเรือ, 9 กรกฎาคม 2561.

[50]กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. “ภารกิจ”. (ออนไลน์). เข้าถึงได้จาก :http://www.dict.rtaf.mi.th/index.php/2017-02-01-01-28-28/2017-02-01-01-53-22, 2559.

จากการศึกษาพบว่าหน้าที่และโครงสร้างการจัดมีความแตกต่างกันไปตามคุณลักษณะของเหล่าทัพ โดยหน่วยงานไซเบอร์ของกองทัพบก มีหน้าที่ปฏิบัติการด้านไซเบอร์ การเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับระบบเครือข่ายอินเตอร์เน็ตของกองทัพบก รวมถึงระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ในโครงการระบบสารสนเทศ ในขณะที่กองทัพเรือ มีหน้าที่รับมือและตอบโต้ภัยคุกคามทางไซเบอร์ รวมทั้งตอบสนองต่อภารกิจต่างๆ ในการดำเนินการด้านสงครามไซเบอร์ ส่วนกองทัพอากาศ มีหน้าที่เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการพัฒนา และดำเนินการด้านระบบบัญชาการและควบคุมเครือข่ายเทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ ดังนั้น การจัดโครงสร้างอัตรากำลัง เพื่อรองรับการพัฒนาระบบงานไซเบอร์ของแต่ละเหล่าทัพ จำเป็นต้องพิจารณาความแตกต่างของหน้าที่ด้วย

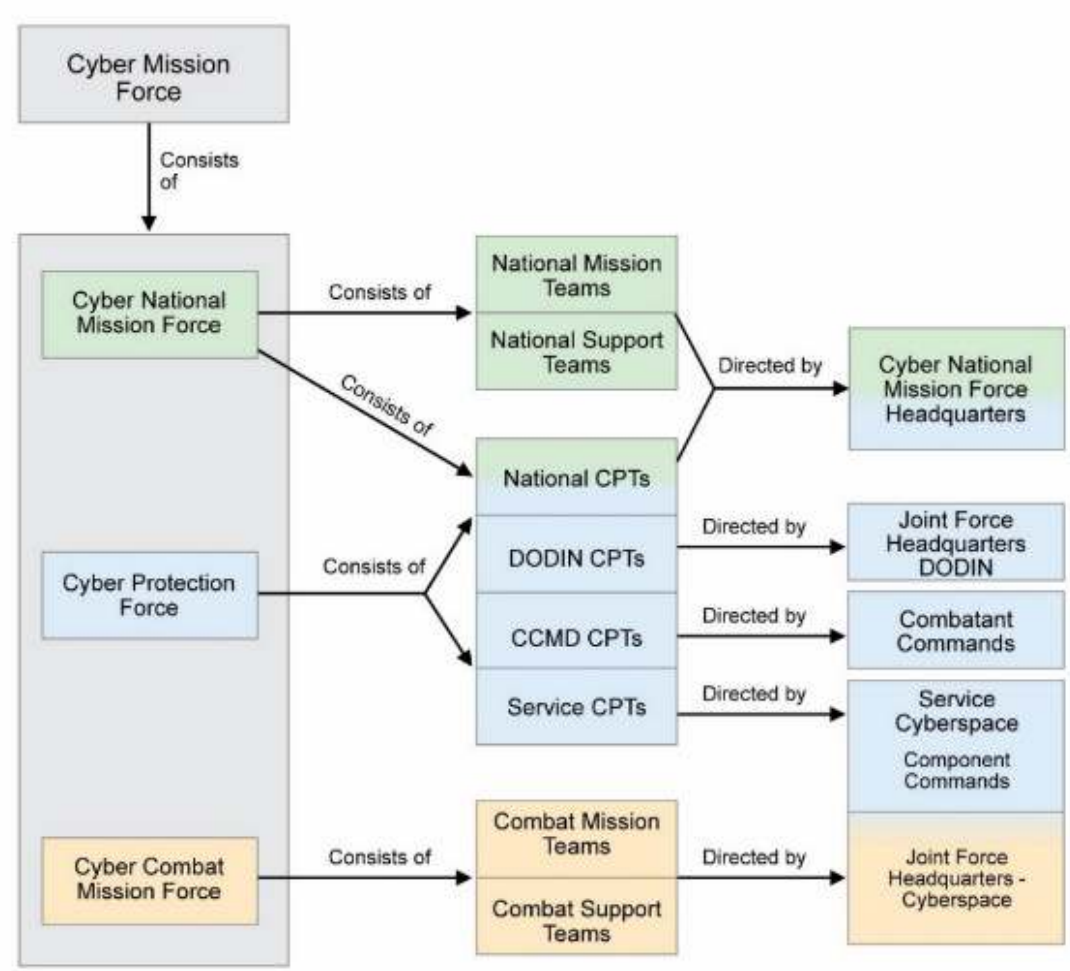
ระบบไซเบอร์ของกองทัพมิตรประเทศ

ถึงแม้ว่าทุกกองทัพมิตรประเทศจะมีระบบไซเบอร์ที่มีความเชื่อมโยงกับระบบของประเทศเหมือนกัน แต่ในรายละเอียดแล้วแต่ละประเทศย่อมความแตกต่างกัน โดยพื้นฐานระบบไซเบอร์จะประกอบด้วย ส่วนปฏิบัติการเครือข่าย (Network Operations) ส่วนปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operations) และชุดตอบสนองต่อภัยคุกคามทางไซเบอร์ (CSIRT) ซึ่งประเทศส่วนใหญ่จะไม่เปิดเผยข้อมูลระบบไซเบอร์ของกองทัพ เช่น สาธารณรัฐประชาชนจีน และสหพันธรัฐรัสเซีย และในบางประเทศที่มีระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับสูง แต่ยังไม่มีหน่วยงานทางทหารที่รับผิดชอบด้านไซเบอร์โดยเฉพาะ เช่น สาธารณรัฐสิงคโปร์ และประเทศญี่ปุ่น ข้อมูลระบบไซเบอร์ของกองทัพจึงได้มาจากการสัมมนาและการศึกษาดูงานระหว่างประเทศ ซึ่งสามารถรวบรวมข้อมูลอย่างกว้างๆ ของกองทัพ 2 ประเทศ คือ สหรัฐอเมริกา และรัฐอิสราเอล ซึ่งสรุปได้ดังนี้

1. สหรัฐอเมริกา

กองกำลังภารกิจไซเบอร์ของกองทัพสหรัฐ (Cyber Mission Force) ประกอบด้วย กองกำลังภารกิจไซเบอร์ระดับชาติ กองกำลังป้องกันไซเบอร์ กองกำลังภารกิจการรบไซเบอร์ ตามแผนภาพที่ 3 – 7

แผนภาพที่ 3 - 7 ความสัมพันธ์กองกำลังภารกิจไซเบอร์กระทรวงกลาโหมสหรัฐอเมริกา



ที่มา :Joint Chiefs of Staff, 2018 : I-10.

1)กองกำลังภารกิจไซเบอร์ระดับชาติ (Cyber National Mission Force) ประกอบด้วยชุดทำงานไซเบอร์ระดับชาติและชุดป้องกันไซเบอร์ระดับชาติโดยอยู่ในการอำนวยการของกองบัญชาการกองกำลังภารกิจไซเบอร์ระดับชาติ

2)กองกำลังป้องกันไซเบอร์ (Cyber Protection Force) ประกอบด้วยชุดป้องกันไซเบอร์ระดับชาติชุดป้องกันไซเบอร์ระดับกองบัญชาการผสม ชุดป้องกันไซเบอร์ผู้บัญชาการ

หน่วยกำลังรบ และชุดป้องกันไซเบอร์สนับสนุนโดยอยู่ในการอำนวยการของกองบัญชาการแต่ละระดับที่ไปสนับสนุน

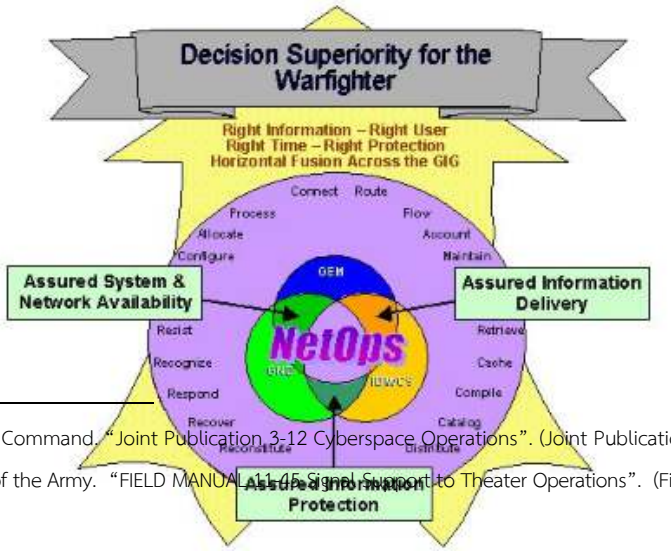
3)กองกำลังภารกิจการรบไซเบอร์ (Cyber Combat Mission Force) อยู่ในการอำนวยการของกองบัญชาการผสมไซเบอร์ ประกอบด้วย ชุดภารกิจการรบและชุดสนับสนุนการรบ

สาเหตุสำคัญที่ทำให้กองทัพสหรัฐอมริกาให้ความสำคัญกับการปฏิบัติการไซเบอร์ เพราะส่งผลกระทบต่อการปฏิบัติการร่วมของทหารสหรัฐอเมริกา พันธมิตร และชาติที่เป็นหุ้นส่วน เพื่อสร้างและดำรงความได้เปรียบในสภาวะแวดล้อมระดับยุทธการ และทำให้เกิดความมั่นคงทางด้านเศรษฐกิจและทางกายภาพของรัฐนั้น พื้นที่ไซเบอร์ข้ามพรหมแดนทางภูมิศาสตร์และทางการเมือง[51]

จากคู่มือการฝึก FM 11-45 ของกองทัพสหรัฐได้กล่าวถึงการปฏิบัติการเครือข่ายและการปฏิบัติการด้านการป้องกันทางไซเบอร์[52]สรุปได้ดังนี้

1. การปฏิบัติการเครือข่ายของสหรัฐ (Network Operations : NetOps) เป็นความสามารถในด้านการดำเนินการ การจัดระเบียบ และเทคนิคในการปฏิบัติการและป้องกันระบบเครือข่ายสารสนเทศของกองทัพ และหมายรวมถึงการบริหารจัดการองค์กร (Enterprise Management) การประกันเครือข่าย (Network Assurance) และการบริหารจัดการสารบบ (Content Management) ทำให้เชื่อมั่นได้ว่าข้อมูลข่าวสารของผู้บังคับบัญชาสามารถส่งไปถึงพลรบได้อย่างรวดเร็วและถูกต้องครบถ้วน โดยโครงข่ายตั้งแต่ระดับสูงสุดจนถึงระดับล่างสุดมีการออกแบบให้เชื่อมต่อกันอย่างเป็นระบบและสามารถทำงานตามขั้นตอนที่กำหนดร่วมกันได้ ดังนั้น การปฏิบัติการเครือข่าย จึงได้จัดให้มีการเฝ้าระวัง การติดตามสถานการณ์ การปกป้องการรั่วไหลของข้อมูลข่าวสาร การบริหารจัดการเครือข่าย การประกันเครือข่าย (Network Assurance) และการบริหารด้านการกระจายข้อมูลข่าวสาร ตามแผนภาพที่ 3 - 8

แผนภาพที่ 3 - 8 พื้นที่รับผิดชอบและพันธกิจของการปฏิบัติการเครือข่าย



[51]U.S. Strategic Command. “Joint Publication 3-12 Cyberspace Operations”. (Joint Publication. 2018). p.I-1.

[52]Department of the Army. “FIELD MANUAL 11-45 Signal Support to Theater Operations”. (Field Manual. 1999).

ที่มา : U.S. Strategic Command, 2005 : 3.

เป้าประสงค์ของการปฏิบัติการเครือข่ายของกองทัพสหรัฐ คือ

1.1 จัดให้ผู้ใช้งานทุกคนในกองทัพสามารถเข้าถึงบริการโครงข่ายสารสนเทศของกองทัพอย่างปลอดภัย โดยมีรหัสผ่านส่วนบุคคลโดยให้ลงทะเบียนใช้แบบ plug and play

1.2 โครงข่ายสารสนเทศสามารถแสดงผลลัพธ์ทั้งในภาพรวมและเฉพาะสถานการณ์ที่พึงระวังได้อย่างถูกต้องแม่นยำ

1.3 เจ้าหน้าที่ที่เกี่ยวข้องสามารถพยากรณ์หรือคาดเดาผลกระทบต่อโครงข่ายสารสนเทศของกองทัพที่อาจเกิดจากภัยคุกคามแบบใหม่ๆ และจัดทำแผนเผชิญเหตุฉุกเฉินเพื่อรับมือภัยคุกคามนั้น

1.4 เจ้าหน้าที่ที่เกี่ยวข้องสามารถทำ redirect หรือ reallocate แหล่งทรัพยากรของโครงข่ายสารสนเทศในโหมด Near Real Time เพื่อรองรับเหตุการณ์ฉุกเฉินในทุกพื้นที่ที่รับผิดชอบ

1.5 จัดทำการบริการที่มีความมั่นคงสามารถให้บริการขั้นพื้นฐานจากโครงข่ายสารสนเทศแก่ผู้ใช้งานทุกคนที่ได้รับสิทธิ์ในต้นทุนที่ต่ำที่สุดภายใต้ข้อจำกัดทางด้านยุทธการของกองทัพ

1.6 จัดทำบริการโครงข่ายสารสนเทศที่สูงกว่าขั้นพื้นฐาน เพื่อให้บริการแก่ผู้ใช้งานโดยมีค่าใช้จ่าย แต่ผู้ใช้งานสามารถนำใบเสร็จรับเงินมาเบิกเงินคืนได้

1.7 จัดให้มีการปฏิบัติการป้องกันการบุกรุกอย่างต่อเนื่องโดยไม่รบกวนต่อการปฏิบัติงาน เพื่อเพิ่มระดับการให้บริการ หรือเพื่อลดค่าใช้จ่ายของการบริการขั้นพื้นฐาน

1.8 สร้างขีดความสามารถให้กับบุคลากรในการวางแผนยุทธการได้อย่างต่อเนื่อง (Continuity of Operations)

2. การปฏิบัติการด้านการป้องกันทางไซเบอร์ของระบบเครือข่ายคอมพิวเตอร์ (Computer Network Defense หรือเรียกย่อว่า Cyber Defense) เป็นองค์ประกอบย่อยของระบบการประกันข้อมูล (Information Assurance: IA) ซึ่งอยู่ใน NetOps เป็นการปฏิบัติด้านการ

ป้องกัน การเฝ้าตรวจ การวิเคราะห์ การปกป้อง และการตอบโต้ต่อกิจกรรมที่ไม่ได้รับอนุญาตที่เกิดต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ รวมถึงทำการป้องกันระบบการประกันข้อมูล (IA)

เป้าประสงค์ของการปฏิบัติด้านการป้องกันทางไซเบอร์ (Cyber Defense) คือ

2.1 ความสามารถในการป้องกัน หมายรวมถึง การรักษาความปลอดภัยการสื่อสาร การรักษาความปลอดภัยคอมพิวเตอร์ และการรักษาความปลอดภัยอุปกรณ์สารสนเทศ เช่น การควบคุมการเข้าถึง การเข้ารหัสถอดรหัส การป้องกันเครือข่าย และระบบ Firewall

2.2 ความสามารถในการกลั่นกรอง หมายรวมถึง ความสามารถในการตรวจจับการใช้งานภายในเครือข่ายที่ผิดปกติและการบุกรุกระบบสารสนเทศ โดยสามารถตรวจสอบห้วงเวลาการโจมตี รวมทั้งความเสียหายหรือการเปลี่ยนแปลงที่เกิดขึ้น ซึ่งเป็นจุดเริ่มต้นของการปฏิบัติการตอบโต้และการฟื้นฟูระบบ

2.3 ความสามารถในการตอบโต้ ซึ่งหมายรวมถึงการฟื้นฟูระบบ โดยขึ้นอยู่กับกลไกต่างๆ ที่ถูกกำหนดขึ้นตามลำดับความสำคัญของระบบและเครือข่ายสารสนเทศ

3. ขอบเขตภารกิจของการปฏิบัติการเครือข่าย (NetOps) การประกันข้อมูล (IA) และการปฏิบัติการด้านการป้องกันทางไซเบอร์ของระบบเครือข่ายคอมพิวเตอร์ (Cyber Defense) คือ ทำให้เกิดความมั่นใจว่าข้อมูลถูกเก็บเป็นความลับ (Confidentiality) มีความถูกต้องครบถ้วน ไม่ถูกเปลี่ยนแปลง (Integrity) สามารถเรียกข้อมูลได้ตลอดเวลา (Availability) สามารถระบุตัวตนได้ (Authenticity) ตรวจสอบการเข้าถึงได้ (Auditability) และไม่สามารถปฏิเสธความรับผิดชอบ (Non-Repudiation) สำหรับการประกันข้อมูล (IA) เป็นการรวมเอาขีดความสามารถในการป้องกัน การกลั่นกรอง และการปฏิบัติการตอบโต้ รวมถึงการกู้คืนระบบข้อมูล ซึ่งเป็นการคุ้มครองตั้งแต่ต้นทางจนถึงปลายทาง (end-to-end) เพื่อให้มั่นใจว่าระบบจะไม่เสี่ยงต่อความเสียหายที่อาจเกิดขึ้นจากความประมาทเลินเล่อหรือจากการโจมตีจากผู้ไม่ประสงค์ดี กล่าวโดยสรุปคือ การประกันข้อมูลเน้นที่การสร้างระบบการป้องกันและดำเนินการกู้คืนระบบหากพบว่าการป้องกันนั้นไม่สมบูรณ์ ในขณะที่การปฏิบัติการป้องกันทางไซเบอร์ (Cyber Defense) เน้นด้านการปฏิบัติ (ป้องกัน เฝ้าตรวจ วิเคราะห์ ปกป้อง และตอบโต้)

2. อิสราเอล

รัฐบาลอิสราเอลให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) อย่างมาก โดยกำหนดเป็นนโยบายและยุทธศาสตร์สำคัญของชาติ ให้หน่วยงานทั้งภาคการทหารภาคเอกชน รวมถึงประชาชนต้องปฏิบัติตามอย่างเคร่งครัด มีการเรียนการสอนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ระดับอนุบาลจนถึงระดับมหาวิทยาลัย ภาครัฐให้การสนับสนุนการลงทุนทางด้านการวิจัยและพัฒนาอาวุธที่เกี่ยวกับคอมพิวเตอร์เพื่อการป้องกันประเทศจากภัยคุกคามทางไซเบอร์อย่างจริงจัง

ดังนั้นระบบไซเบอร์ของกองทัพอิสราเอลจะเชื่อมโยงกับภาครัฐซึ่งเน้นหนักทางด้านการเฝ้าตรวจและการแจ้งเตือนที่รวดเร็ว แม่นยำ รวมถึงมีระบบการแบ่งปันข้อมูลข่าวสารภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) ระหว่างหน่วยงานที่มีประสิทธิภาพ โดยมี Cyber Warfare Center(CWC) เป็นศูนย์รวบรวมและกระจายข้อมูลการถูกโจมตีและภัยคุกคามทางไซเบอร์ทุกรูปแบบ นอกจากนี้ ยังมีระบบการเก็บสำรองข้อมูลและแผนการกู้คืนระบบที่มีประสิทธิภาพ หากเกิดเหตุภาวะฉุกเฉินทางไซแบอร์ กองทัพสามารถกู้คืนระบบได้อย่างรวดเร็วโดยแทบไม่กระทบต่อการปฏิบัติงาน ทั้งนี้ CWC จะทำการค้นหาและเก็บรวบรวมข้อมูลทุกรูปแบบของภัยคุกคามทางไซเบอร์จากทุกแหล่งทั้งภายในประเทศและต่างประเทศ ไม่ว่าจะเป็นข้อมูลที่เป็นข้อความ รูปภาพ เว็บไซต์ โซเชียลมีเดียหรือแม้แต่ใน Darknet เพื่อทำการวิเคราะห์ แยกหมวดหมู่ ประเมินความเสี่ยง และจัดทำเป็นฐานข้อมูล พร้อมทั้งแจ้งเตือนไปยังหน่วยงานต่างๆ หากหน่วยงานใดตรวจพบภัยคุกคามรูปแบบใหม่ จะแจ้งมายัง CWC เพื่อทำการวิเคราะห์ เก็บรวบรวมข้อมูล และหาวิธีการแก้ไขที่เหมาะสมที่สุดต่อไป[53]

ความสัมพันธ์ระหว่างระบบไซเบอร์กับระบบงานอื่นๆ ในกองทัพบกไทยและกองทัพมิตรประเทศ

ระบบไซเบอร์ของกองทัพบกไทยไม่ใช่เป็นระบบอิสระเนื่องจากการปฏิบัติการทางทหารจะเป็นการปฏิบัติแบบรวมโดยแบ่งตามระดับตามที่ได้ทบทวนวรรณกรรมได้แก่ ระดับยุทธศาสตร์ ระดับยุทธการ และระดับยุทธวิธี สำหรับกองทัพบกนั้น ตามพระราชบัญญัติจัดระเบียบกระทรวงกลาโหม พ.ศ.2551 กำหนดให้เป็นหน่วยระดับยุทธการและยุทธวิธี นอกจากนั้นแล้ว การปฏิบัติการทางทหารได้กำหนดเป็นแผนป้องกันประเทศซึ่งกำหนดขั้นการปฏิบัติเป็น 3 ขั้น ได้แก่ ขั้นปกติ ขั้นตอบโต้ และขั้นป้องกันประเทศ ดังนั้น การพัฒนาระบบระบบไซเบอร์ของกองทัพบกไทยจะต้องสอดคล้องกับการแบ่งระดับและขั้นการปฏิบัติที่กล่าวมาด้วย

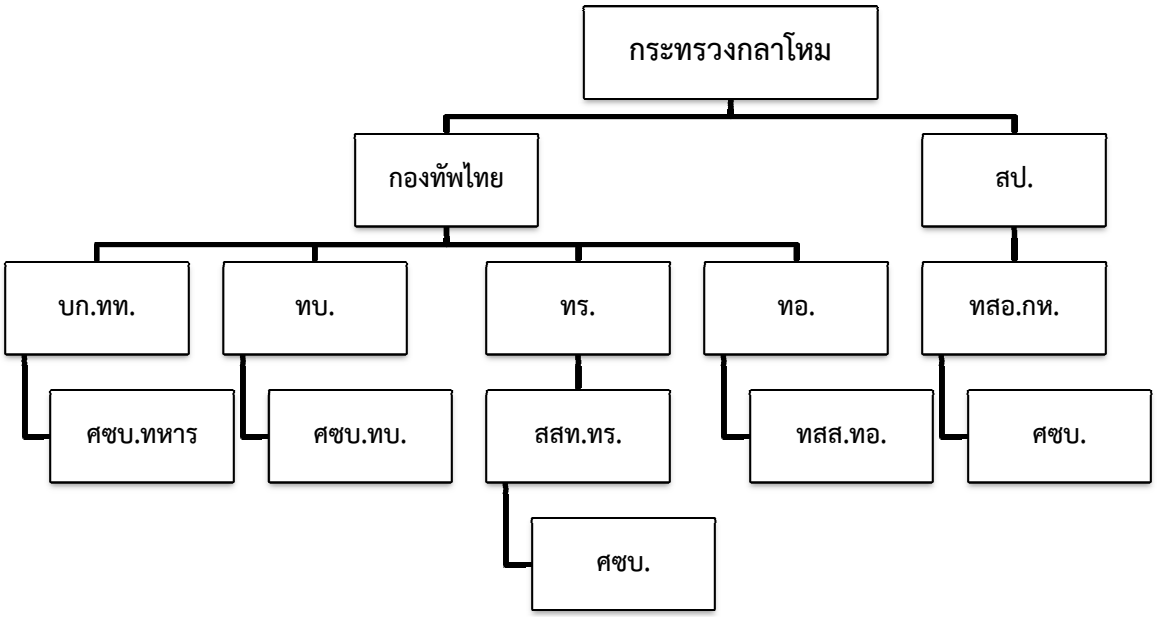
หน่วยงานภายในกระทรวงกลาโหมได้จัดตั้งหน่วยที่รับผิดชอบด้านไซเบอร์โดยเฉพาะเพื่อสนองนโยบายจากหน่วยเหนือในการป้องกันประเทศด้านไซเบอร์[54]โดยมีสายการบังคับบัญชาจากระดับกระทรวงกลาโหมถึงหน่วยงานด้านไซเบอร์ตามแผนภาพที่ 3 - 9

แผนภาพที่ 3 - 9 สายการบังคับบัญชาจากระดับกระทรวงกลาโหมถึงหน่วยงานด้านไซเบอร์

---

[53] Itamar Graff and Barak Sharabi, “Cyber Security Solutions”.(Paper Presented at Cyber Security Solution Seminar by Israel. 2016).

[54] กระทรวงกลาโหม, “แผนแม่บท กระทรวงกลาโหม”. (แผนแม่บท. 2559).



1.ความสัมพันธ์ระหว่างฝ่ายอำนวยการด้านไซเบอร์

จากการทบทวนวรรณกรรมสรุปในขั้นต้นได้ว่า ระบบไซเบอร์ซึ่งมีกรมฝ่ายเสนาธิการรับผิดชอบในการวางแผน อำนวยการ ประสานงาน และกำกับดูแลในระดับกองทัพบกนั้น จำเป็นต้องมีความชัดเจนว่าการปฏิบัติงานของกรมฝ่ายเสนาธิการดังกล่าวมีความชัดเจนประสานสอดคล้องกันเพียงใด โดยเฉพาะอย่างยิ่งในปัจจุบันกองทัพมิตรประเทศรวมทั้งการปฏิบัติการทางทหารในกรอบสหประชาชาติและองค์การสนธิสัญญาแอตแลนติกเหนือ รวมทั้งสหภาพยุโรปได้แบ่งการจัดสายงานฝ่ายอำนวยการใหม่ โดยเฉพาะการแบ่งสายงานยุทธการเดิมออกเป็นหลายสายงานย่อยซึ่งจำเป็นต้องศึกษาผลกระทบที่เกิดขึ้นต่อการพัฒนาระบบไซเบอร์จากความแตกต่างตามตารางที่ 3 - 2 ปัญหาสำคัญที่จะศึกษาในครั้งนี้คือผลกระทบที่เกิดขึ้นต่อระบบไซเบอร์ เมื่อกองทัพไทยนำระบบไซเบอร์มาจากกองทัพมิตรประเทศแล้ว แต่ไม่ได้มีการจัดระบบฝ่ายอำนวยการที่รับผิดชอบเหมือนกันจะนำมาสู่ปัญหาความสัมพันธ์ระหว่างสายงานที่รับผิดชอบ กับปัญหาระหว่างภายในสายงานกลุ่มงานเดียวกัน

ตารางที่ 3 - 2 เปรียบเทียบการจัดกรมฝ่ายเสนาธิการกองทัพบกไทยกับกองทัพมิตรประเทศ

G-1	G-2	G-3	G-4	G-5	G-6	G-7	G-8	G-9

Personnel	Intelligence	Operations	Logistics	Plans	Information	Training	Comptroller	Cimic
กพ.ทบ.	ขว.ทบ.	ยก.ทบ.	กบ. ทบ.	ยก. ทบ.	ยก.ทบ.	ยก. ทบ.	สปช.ทบ.	กร. ทบ.

ตามตารางที่ 3 - 2จากผลการศึกษาการแบ่งความรับผิดชอบฝ่ายอำนวยการด้านไซเบอร์ของกองทัพมิตรประเทศในปัจจุบันพบว่าทุกกองทัพได้แยกสายงานที่รับผิดชอบออกมาต่างหากโดยกองทัพบกสหรัฐอเมริกาจัดเป็นกรมฝ่ายเสนาธิการ G-6 เช่นเดียวกับนาโต สาเหตุที่ทุกกองทัพมิตรประเทศได้แยกการฝึกออกมาเป็นกรมฝ่ายเสนาธิการเฉพาะ คาดว่ามีเหตุผลมาจากระบบนี้มีความเป็นสายงานเฉพาะมากขึ้น และไม่ได้มีความสัมพันธ์โดยตรงกับสายงานยุทธการ (G-3 Operations) อย่างแน่นแฟ้นมาก จึงสามารถแยกออกมาเป็นระบบงานอิสระ เพียงแต่จัดความสัมพันธ์ระหว่างสายงานฝ่ายอำนวยการให้ชัดเจน

จากการสัมภาษณ์ผู้อำนวยการกองเทคโนโลยีสารสนเทศและการสื่อสาร สำนักปฏิบัติการ กรมยุทธการทหารบก ในประเด็นดังกล่าว มีความเห็นว่า การที่กองทัพบกไทยไม่ได้แยกงานไซเบอร์ รวมทั้งระบบงานอื่นในกลุ่มงานเดียวกัน ออกไปจัดตั้งเป็นกรมฝ่ายเสนาธิการเฉพาะเหมือนกับกองทัพมิตรประเทศนั้น ส่งผลกระทบในด้านโครงสร้างการจัดของกองงานที่รับผิดชอบงานด้านไซเบอร์ในระดับกองทัพบก ทำให้มีข้อจำกัดในการปฏิบัตหน้าที่ฝ่ายอำนวยการในการวางแผนอำนวยการ ประสานงาน และกำกับดูแลอย่างมีประสิทธิภาพ นอกจากนี้ยังมีข้อจำกัดด้านอัตรากำลังเจ้าหน้าที่ที่จะมาปฏิบัติงาน เพราะมีเพียง 4 แผนก ได้แก่ แผนกแผน แผนกเทคโนโลยีสารสนเทศ แผนกการสื่อสาร และแผนกปฏิบัติการข่าวสารแต่ละแผนกมีอัตรา 7 นาย (พ.ท.1, พ.ต.1, ร.อ.1, จ.ส.อ.2, ส.อ.2) รวมทั้งระดับชั้นยศของหัวหน้าแผนกยังสูงไม่พอที่จะไปประสานงานกับหน่วยงานอื่นทั้งภายในและภายนอกกองทัพบก ซึ่งทุกแผนกควรพิจารณายกระดับขึ้นมาเป็นระดับกอง และกองเทคโนโลยีสารสนเทศและการสื่อสาร ควรแยกออกมาเป็นสำนัก

ในส่วนความสัมพันธ์กับสายงานยุทธการอื่นๆ ที่อยู่ในกรมยุทธการทหารบกปัจจุบัน ได้แก่ สำนักนโยบายและแผน สำนักปฏิบัติการ และสำนักการฝึกและศึกษาทางทหารนั้นไม่ได้มีความจำเป็นที่จะต้องปฏิบัติงานร่วมกันอย่างใกล้ชิด โดยการวางแผนประสานงานสามารถกระทำได้ระหว่างสำนัก และการที่จัดไว้เป็นระดับแผนกภายใต้สำนักต่างๆ ทำให้งานไซเบอร์ถูกลดระดับความสำคัญลงไป และยากที่จะพัฒนาระบบงานให้มีประสิทธิภาพได้[55] ซึ่งเป็นข้อมูลสำคัญที่จะนำมาใช้ในการวิเคราะห์ต่อไป

2.ความสัมพันธ์ระหว่างระบบไซเบอร์กับระบบงานอื่น

[55]พันเอก นพดล แก้วกำเนิด, ผู้อำนวยการกองเทคโนโลยีสารสนเทศและการสื่อสาร สำนักปฏิบัติการ กรมยุทธการทหารบก. สัมภาษณ์. 6 มิถุนายน 2562.

ระบบไซเบอร์ไม่ได้มีที่มาจากตัวเอง แต่เป็นการพัฒนาแยกออกมาจากระบบการสื่อสาร อย่างไรก็ตามระบบงานไซเบอร์จำเป็นต้องพึ่งพาระบบสื่อสารในด้านของมัจฉิมทั้งทางคลื่นและทางสายทุกประเภท จึงทำให้ยากที่จะแยกงานไซเบอร์ออกจากงานสื่อสารโดยชัดเจน ตามที่ระบบไซเบอร์ หมายถึง ระบบที่เกี่ยวข้องหรือสัมพันธ์กับระบบเครือข่ายสื่อสารข้อมูล (Data Communication Systems) ระบบสารสนเทศ (Information Systems) ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition) และระบบควบคุมการทำงานของอุปกรณ์และอิเล็กทรอนิกส์ (Embedded Systems)[56]

จากผลการประชุมคณะอนุกรรมการนโยบายและมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารกองทัพบก ครั้งที่ 1/61 เมื่อ 25 เม.ย. 61 ได้กำหนดประเภทเครือข่ายสื่อข้อมูลที่มีใช้งานในกองทัพบก โดยแบ่งเป็น 4 ประเภท[57] คือ

- เครือข่ายสื่อสารข้อมูลประเภทที่ 1 เป็นโครงสร้างพื้นฐานวิกฤตแบบปิดของ ทบ. (RTA Critical Infrastructure)

- เครือข่ายสื่อสารข้อมูลประเภทที่ 2 เป็นเครือข่ายสื่อสารข้อมูลแบบปิด (Intranet) ที่หน่วยต่างๆ ใน ทบ. ใช้งานเป็นการภายใน

- เครือข่ายสื่อสารข้อมูลประเภทที่ 3 เป็นเครือข่ายสื่อสารข้อมูลที่เชื่อมต่อกับอินเทอร์เน็ต (Internet)

- เครือข่ายสื่อสารข้อมูลประเภทที่ 4 เครือข่ายเชื่อมต่อระหว่างเครือข่ายสื่อสารข้อมูลประเภทที่ 1 กับเครือข่ายสื่อสารข้อมูลประเภทที่ 3

ระบบไซเบอร์ของกองทัพบกเป็นการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้หน่วยงานต่างๆ ของกองทัพบกมั่นใจได้ว่าข้อมูลจะถูกเก็บเป็นความลับ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และพร้อมใช้งานเสมอ (Availability) ระบบไซเบอร์จึงเกี่ยวข้องกับเครือข่ายสื่อสารข้อมูลประเภทที่ 4 เพราะระบบไซเบอร์เปรียบเหมือนด่านหน้า หรือกองรักษาการณ์ที่ทำหน้าที่ตรวจหาและเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมง สำหรับการรักษาความมั่นคงปลอดภัยเครือข่ายสื่อสารข้อมูลประเภทที่ 1 (Critical Infrastructure) เป็นความรับผิดชอบของกรมการทหารสื่อสาร ส่วนอุปกรณ์ของเครือข่ายสื่อสารข้อมูลประเภทที่ 2 (Intranet) และเครือข่ายสื่อสารข้อมูลประเภทที่ 3 (Internet) อยู่ในความรับผิดชอบของหน่วยใช้งาน

ปัจจุบัน บก.ทท. ได้จัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์ ทท. และประชาคมไซเบอร์ ทท. เพื่อให้มีการแลกเปลี่ยนความรู้ ประสบการณ์ และแนวทางการดำเนินการ

---

[56]แผนแม่บทไซเบอร์กองทัพบก พ.ศ.2560-2564 หน้า 17.

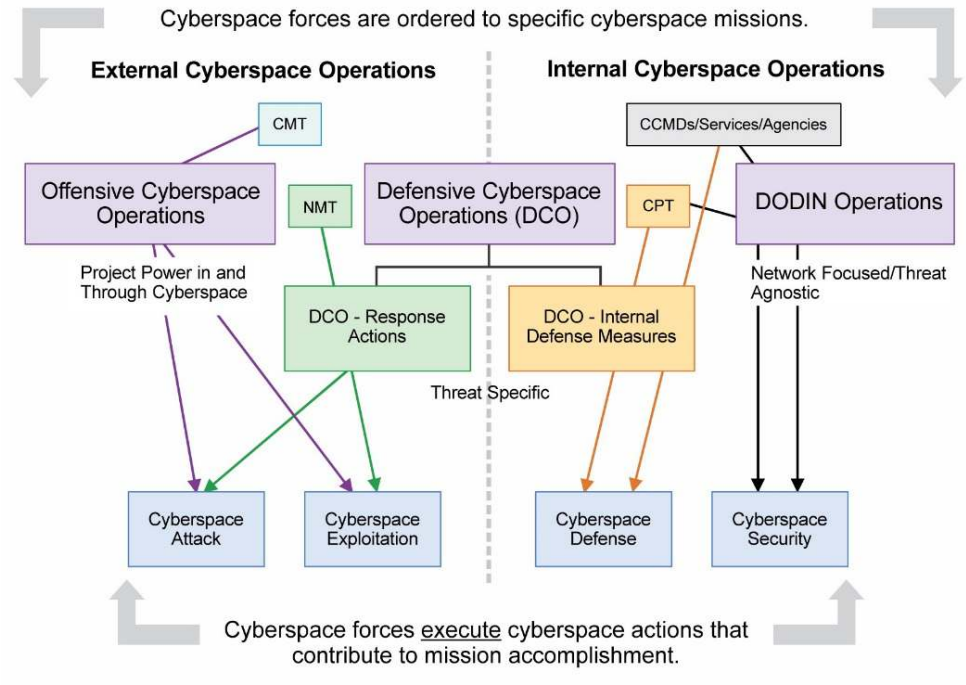
[57]กรมยุทธการทหารบก. “หนังสือ ยก.ทบ. ที่ กห 0403/5946 เรื่อง สรุปผลการประชุมคณะอนุกรรมการนโยบายและมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร ทบ. ครั้งที่ 1/61”. ลงวันที่ 30 เมษายน 2561.

ด้านไซเบอร์ระหว่างกองทัพไทยและหน่วยอื่นๆ ที่เกี่ยวข้องกับไซเบอร์ นอกจากนี้ ยังมีการฝึกร่วมทางไซเบอร์ระหว่างเหล่าทัพเพื่อฝึกการทำงานเป็นหน่วยในสถานการณ์ทางไซเบอร์ในภาวะปกติและไม่ปกติ หากเกิดข้อติดขัดสงสัย หน่วยงานสามารถประสานไปยังไทยเซิร์ตเพื่อปรึกษาหรือขอข้อมูลเพิ่มเติมได้

3.การปฏิบัติภารกิจไซเบอร์

การปฏิบัติภารกิจทางทหารโดยปกติจะแบ่งออกเป็นการปฏิบัติการเชิงรุกและการปฏิบัติการเชิงรับ การปฏิบัติภารกิจไซเบอร์ก็เช่นเดียวกัน เนื่องจากหน่วยงานไซเบอร์เพิ่งมีการจัดตั้งประกอบกับกฎหมายในระดับประเทศเพิ่งจะมีผลบังคับใช้ ดังนั้น ในปัจจุบันกองทัพไทยยังไม่ได้กำหนดหลักนิยมในการปฏิบัติภารกิจไซเบอร์ไว้ชัดเจน อย่างไรก็ตามในการศึกษาครั้งนี้จะนำแบบการปฏิบัติภารกิจไซเบอร์ของกองทัพสหรัฐอเมริกาซึ่งมีลักษณะคล้ายกับหลักนิยมของไทยมาศึกษาตามแผนภาพที่ 3 - 10

แผนภาพที่ 3 - 10 ภารกิจการปฏิบัติการไซเบอร์ การปฏิบัติ และกองกำลัง



ที่มา : Joint Chiefs of Staff, 2018 : II 2-3.

กองทัพสหรัฐอเมริกาได้แบ่งการปฏิบัติการพื้นที่ไซเบอร์ออกเป็น การปฏิบัติการพื้นที่ไซเบอร์ภายนอก และการปฏิบัติการพื้นที่ไซเบอร์ภายในโดยมีชุดปฏิบัติงานในระดับต่างๆ ได้แก่

ชุดภารกิจการรบ (Combat Mission Team: CMT) ชุดภารกิจระดับชาติ (National Mission Team : NMT) และชุดป้องกันพื้นที่ไซเบอร์ (Cyberspace Protection Team : CPT) เข้าปฏิบัติงานในแต่ละภารกิจตามแผนผังดังนี้

- การปฏิบัติการพื้นที่ไซเบอร์ภายนอก(External Cyberspace Operations) เป็นการปฏิบัติการพื้นที่ไซเบอร์เชิงรุก (Offensive Cyberspace Operations) และการปฏิบัติการพื้นที่ไซเบอร์เชิงรับ (Defensive Cyberspace Operations) บางส่วนประกอบด้วยการโจมตีพื้นที่ไซเบอร์ (Cyberspace Attack) และการขยายผลพื้นที่ไซเบอร์ (Cyberspace Exploitation)

- การปฏิบัติการพื้นที่ไซเบอร์ภายใน(Internal Cyberspace Operations) เป็นการปฏิบัติการเครือข่ายข้อมูลข่าวสารกระทรวงกลาโหม (Department of Defense Information Network Operations) และการปฏิบัติการพื้นที่ไซเบอร์เชิงรับ (Defensive Cyberspace Operations) บางส่วน ประกอบด้วยการป้องกันพื้นที่ไซเบอร์ (Cyberspace Defense) และการรักษาความปลอดภัยพื้นที่ไซเบอร์ (Cyberspace Security)

จากการกำหนดภารกิจการปฏิบัติการไซเบอร์ การปฏิบัติ และกองกำลังที่ชัดเจนของกองทัพสหรัฐอเมริกาตามแผนภาพที่ 3 - 10 ส่งผลทำให้การวางแผนที่เกี่ยวข้องในขั้นตอนต่อมาเป็นไปอย่างชัดเจนและมีระบบ ได้แก่ การจัดทำโครงสร้างการจัดและอัตรากำลัง การบริหารงานบุคคล การฝึกและศึกษา และการปฏิบัติภารกิจซึ่งจะได้นำมาวิเคราะห์ในการพัฒนาหน่วยงานไซเบอร์ในกองทัพไทยต่อไปเมื่อเตรียมบุคลากรพร้อมแล้ว ในการปฏิบัติงาน มีการกำหนดระเบียบปฏิบัติประจำ (รปจ.) ในแต่ละงาน จัดทำคู่มือ ขั้นตอนการทำงาน และวิธีการแก้ไขปัญหาเบื้องต้นเพื่อความเป็นระเบียบแบบแผน นอกจากนี้ ยังได้กำหนดช่องทางการสื่อสารกรณีเร่งด่วนหรือเมื่อเกิดเหตุฉุกเฉินตามลำดับสายการบังคับบัญชา

สำหรับการปฏิบัติภารกิจไซเบอร์ของกองทัพบกไทยนั้น เนื่องจากหน่วยงานด้านไซเบอร์ต้องมีการเฝ้าระวังภัยคุกคามตลอด 24 ชั่วโมงทุกวัน จึงมีการจัดกำลังพลปฏิบัติหน้าที่เฝ้าระวังสถานการณ์ โดยแบ่งเป็น 3 ระดับ คือ

- เจ้าหน้าที่ระวังภัยไซเบอร์ระดับ 1 ทำหน้าที่เฝ้าระวังผ่านอุปกรณ์และซอฟแวร์สำหรับตรวจจับสิ่งผิดปกติที่จะผ่านเข้าสู่ระบบเครือข่ายภายในกองทัพบก โดยจัดเจ้าหน้าที่แบ่งเป็น 3 ผลัดๆ ละ 8 ชั่วโมง และใน 1 ผลัดให้มีเจ้าหน้าที่ 2 นายเริ่มปฏิบัติหน้าที่ผลัดที่ 1 ตั้งแต่เวลา 0800 – 1600 ผลัดที่ 2 ตั้งแต่เวลา 1600 – 2400 และผลัดที่ 3 ตั้งแต่เวลา 0000 – 0800 โดยจะมีการรายงานสถานการณ์ทุกชั่วโมงผ่าน Application G-Chat

- เจ้าหน้าที่ระวังภัยไซเบอร์ระดับ 2 ทำหน้าที่วิเคราะห์และแก้ไขปัญหาเบื้องต้นเมื่อเจ้าหน้าที่ระวังภัยไซเบอร์ระดับ 1 รายงานการตรวจพบสิ่งผิดปกติ หรือเมื่อเกิดเหตุการณ์ฉุกเฉิน โดยจัดเจ้าหน้าที่ 1 ผลัดต่อ 1 นาย ปฏิบัติหน้าที่ 24 ชั่วโมง

- เจ้าหน้าที่ระวังภัยไซเบอร์ระดับ 3 ทำหน้าที่ตัดสินใจและสั่งการเมื่อเกิดเหตุการณ์ภัยคุกคามที่เกินขอบเขตความรับผิดชอบของเจ้าหน้าที่ระวังภัยไซเบอร์ระดับ 2 โดยจัดเจ้าหน้าที่ 1 ผลัดต่อ 1 นาย ปฏิบัติหน้าที่ 24 ชั่วโมง

ความสัมพันธ์ระหว่างระบบไซเบอร์ในกองทัพกับส่วนราชการอื่น

ตามที่ได้กล่าวมาแล้วว่าไซเบอร์ไม่ได้เป็นเรื่องที่จำกัดอยู่เฉพาะภายในกองทัพ แต่มีความเชื่อมโยงกับทุกองค์การในรัฐรวมถึงระดับโลก ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อธิบายความสัมพันธ์กับส่วนราชการต่างๆ ในประเทศไว้แล้ว อย่างไรก็ตามพระราชบัญญัติดังกล่าวยังคงมุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยจากภัยคุกคามไซเบอร์เพียงอย่างเดียวในขณะที่การปฏิบัติการทางทหารจะประกอบด้วยการปฏิบัติไซเบอร์เชิงรุกและการปฏิบัติการไซเบอร์เชิงรับด้วย เมื่อพิจารณาความสัมพันธ์ระบบไซเบอร์กับส่วนราชการอื่นในส่วนของสหรัฐอเมริกาได้กำหนดบทบาทและความรับผิดชอบของแต่ละส่วนราชการตามตารางที่ 3 - 3 ดังนี้

ตารางที่ 3 - 3 บทบาทและหน้าที่ของส่วนราชการในพื้นที่ไซเบอร์ของสหรัฐอเมริกา

เรื่อง	จุดมุ่งเน้นสำคัญ	องค์การหลัก	บทบาทในพื้นที่ไซเบอร์
ความมั่นคงภายในรัฐ	การป้องกันมาตุภูมิ	กระทรวงป้องกันมาตุภูมิ	การรักษาความปลอดภัยพื้นที่ไซเบอร์ของสหรัฐ
กองกำลัง	การป้องกันประเทศ	กระทรวงกลาโหม	คน การฝึก และกำลังพลติดอาวุธสำหรับการปฏิบัติการไซเบอร์
การก่ออาชญากรรมทางไซเบอร์และกระบวนการยุติธรรม	กองกำลังบังคับใช้กฎหมาย	กระทรวงยุติธรรม	การป้องกันการก่ออาชญากรรมในพื้นที่ไซเบอร์
กองกำลังป้องกันชาติ	การป้องกันประเทศและการสนับสนุนฝ่ายพลเรือนในการฝึกและการปฏิบัติการไซเบอร์ในสหรัฐ	กำลังป้องกันชาติทางพื้นดินและทางอากาศ	การจัดการสิ่งที่เกิดขึ้นภายในประเทศ
ทรัพย์สิน สิ่งก่อสร้าง แรงงานสาธารณะ		ทุกกระทรวงและหน่วยงาน	
การพิมพ์และเอกสารสาธารณะ	กำหนดองค์การรับผิดชอบและมีอำนาจในนโยบายความมั่นคงด้านข้อมูล	ทุกกระทรวงและหน่วยงาน	

	ข่าวสาร		
การสงครามและการป้องกันประเทศ	การปฏิบัติการทางทหารในย่านกว้าง การข่าวกรองต่างประเทศ และกิจกรรมการต่อต้านข่าวกรอง	กองบัญชาการ และเหล่าทัพ และองค์กรภายใต้กระทรวงกลาโหมและพันธมิตรด้านการข่าวภายใต้สำนักงานข่าวกรองแห่งชาติ	รักษาผลประโยชน์ของสหรัฐโดยการปฏิบัติการทางทหาร การปฏิบัติการข่าวกรองต่างประเทศในพื้นที่ไซเบอร์

ที่มา : Joint Chiefs of Staff, 2018 : III 2-3.

จากตารางที่ 3 - 3 สหรัฐอเมริกาได้กำหนดบทบาทและหน้าที่ของส่วนราชการในพื้นที่ไซเบอร์ไว้ชัดเจน ทำให้สามารถแบ่งความรับผิดชอบของหน่วยงานไซเบอร์ในกระทรวงกลาโหมสหรัฐอเมริกาได้อย่างชัดเจน และนำไปสู่การพัฒนาหน่วยงานไซเบอร์ให้มีขีดความสามารถในการปฏิบัติงานตามที่แบ่งความรับผิดชอบได้

การบริหารงานบุคคลในระบบไซเบอร์ของกองทัพบกไทย

การบริหารงานบุคคลมีความเชื่อมโยงกับโครงสร้างการจัดและอัตรากำลัง ซึ่งจากการทบทวนวรรณกรรมในบทที่ 2 จะพบว่าในปัจจุบันการบริหารงานบุคคลจะเริ่มด้วยขั้นตอนการวิเคราะห์งานขององค์การนั้นๆ และตามมาด้วยการจัดโครงสร้างและอัตรากำลัง หลังจากนั้นจึงจะเป็นการคัดสรรและบรรจุ รวมถึงการฝึกและศึกษา และสุดท้ายคือการประเมินผลการปฏิบัติงาน

การบริหารงานบุคคลในระบบงานไซเบอร์ของกองทัพบก เริ่มจากการผลิตบุคลากรที่เหมาะสมในแต่ละตำแหน่งงาน ตั้งแต่มีการกำหนดคุณลักษณะบุคลากรที่ต้องการให้ตรงตามภารกิจและหน้าที่ความรับผิดชอบที่กำหนดไว้ในอัตราเฉพาะกิจของหน่วย ทำการคัดเลือก มอบหมายงานให้ตรงกับความรู้ความสามารถของบุคลากร และประเมินผลการปฏิบัติงานเพื่อการปูนบำเหน็จรางวัล รวมทั้งมีการอบรมเพิ่มเติมตามแนวทางรับราชการและตามความเหมาะสมเพื่อเพิ่มขีดความสามารถในการปฏิบัติงาน

นอกจากนี้ กองทัพบกยังมีการประชุมและอบรมเพื่อเพิ่มพูนความรู้และแลกเปลี่ยนประสบการณ์ทางด้านไซเบอร์กับหน่วยงานภายนอกกระทรวงกลาโหมและกองทัพมิตรประเทศ เช่น

- การประชุม Cyber Defense Working Group (CDWG) ของกองทัพไทยและกองทัพสหรัฐ

- การประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์ (Cybersecurity Subject Matter Expert Exchange : Cyber SMEE) ของกองทัพบกไทยและกองทัพบกสหรัฐ

- การประชุมแลกเปลี่ยนผู้เชี่ยวชาญด้านไซเบอร์ (Cybersecurity Subject Matter Expert Exchange : Cyber SMEE) ของกองทัพบกไทยและกองทัพบกฟิลิปปินส์

- การอบรม CyberOffensive Workshop กับหน่วยงานภาครัฐและเอกชน

-การอบรมพื้นฐานด้านการรักษาความปลอดภัยไซเบอร์จากหน่วยงานต่างๆ ทั้งภาครัฐและเอกชน

- การศึกษาดูงานจากหน่วยงานในประเทศและต่างประเทศ

จากผลการตรวจสอบระบบการบริหารงานบุคคลสายงานไซเบอร์ของกองทัพไทยพบว่ายังมีความแตกต่างกันโดยเฉพาะศูนย์ไซเบอร์กองทัพบก ซึ่งมีพื้นฐานในการแปรสภาพมาจากศูนย์เทคโนโลยีสารสนเทศกองทัพบกเดิม และกองทัพไทยยังใช้อัตราทหาร ซึ่งมีความจำเป็นต้องย้ายตำแหน่งตลอดเวลาเพื่อความก้าวหน้าในแต่ละชั้นยศ

บทที่ 4
การวิเคราะห์ผลการวิจัย

จากผลการศึกษาข้อมูลในบทที่ 3 สามารถนำมาวิเคราะห์ผลเพื่อพัฒนาระบบไซเบอร์ของกองทัพบกให้สามารถสนับสนุนตามแผนแม่บทรองรับยุทธศาสตร์ชาติด้านความมั่นคงของรัฐตามที่กำหนดไว้ในกฎหมายได้ โดยมีประเด็นสำคัญที่จะทำการวิเคราะห์ ได้แก่ การจัดกลุ่มงานและระบบฝ่ายอำนวยการไซเบอร์ความเชื่อมโยงระบบไซเบอร์กองทัพบกกับทุกหน่วยในกระทรวงกลาโหมและรัฐความชัดเจนบทบาทและความรับผิดชอบหน่วยไซเบอร์ยามปกติและยามสงครามระบบโครงสร้างอัตรากำลังหน่วยงานด้านไซเบอร์และระบบการบริหารงานบุคคล ซึ่งจะได้วิเคราะห์ผลการวิจัยในแต่ละประเด็นดังนี้

การจัดกลุ่มงานและระบบฝ่ายอำนวยการไซเบอร์

งานไซเบอร์เช่นเดียวกับงานทางทหารอื่น ซึ่งจำเป็นต้องมีความสัมพันธ์กับทุกงานเพื่อให้การปฏิบัติภารกิจทั้งในยามปกติและยามสงครามเป็นไปอย่างประสานสอดคล้อง โดยเฉพาะความชัดเจนด้านการจัดกลุ่มงานและระบบฝ่ายอำนวยการด้านไซเบอร์

1. การจัดกลุ่มงานไซเบอร์

ผลจากการศึกษาพบว่าในปัจจุบันการจัดกลุ่มงานไซเบอร์ยังมีความไม่ชัดเจนว่ามีความสัมพันธ์กับงานสื่อสาร งานสารสนเทศ และงานการปฏิบัติการข่าวสารอย่างไร ดังจะเห็นได้จากโครงสร้างการจัดและหน้าที่ของหน่วยงานไซเบอร์ในกระทรวงกลาโหมมีความแตกต่างกัน โดยกองทัพอากาศยังรวมอยู่กับการสื่อสาร ในขณะที่ส่วนราชการอื่นได้แยกงานไซเบอร์ออกมาเฉพาะ แต่ก็ยังไม่ได้มีการจัดระบบความสัมพันธ์ที่ชัดเจน ผลที่ตามมาทำให้การกำหนดหน้าที่ความรับผิดชอบในแต่ละงานที่กล่าวมายังขาดความชัดเจน และทำให้การจัดโครงสร้าง อัตรากำลัง การพัฒนากำลังพลไม่สามารถทำได้อย่างมีประสิทธิภาพและก่อให้เกิดปัญหาในการประสานการปฏิบัติงานตามมาทั้งในยามปกติและในยามสงคราม

นอกจากปัญหาภายในกองทัพบกแล้ว ผลที่ตามมาทำให้การพัฒนาในด้านต่างๆ รวมทั้งการจัดความเชื่อมโยงงานไซเบอร์ของกองทัพบกให้การเชื่อมโยงกับเหล่าทัพต่างๆ ในทางระดับและการเชื่อมโยงกับระดับกองทัพไทยและระดับกระทรวงกลาโหมเป็นไปได้ยากส่งผลกระทบต่อการจัดทำระเบียบปฏิบัติร่วม การฝึกและการปฏิบัติการร่วมระหว่างเหล่าทัพและกองทัพไทย และยังทำ

ให้การปฏิบัติงานกับทุกส่วนราชการเพื่อสนับสนุนแผนแม่บทรองรับยุทธศาสตร์ชาติด้านความมั่นคง เป็นไปด้วยความยากลำบาก

2.การจัดระบบฝ่ายอำนวยการไซเบอร์

จากผลการศึกษาพบว่าในปัจจุบันการการจัดระบบฝ่ายอำนวยการไซเบอร์ของกองทัพไทยยังไม่มีความชัดเจนซึ่งเป็นผลมาจากการจัดกลุ่มฝ่ายอำนวยการของกองทัพไทย ยังคงยึดถือฝ่ายอำนวยการ 6 สายงาน ตามเดิม ในขณะที่กองทัพมิตรประเทศได้จัดใหม่เป็น 8-9 สายงานแล้ว โดยเฉพาะสายงานยุทธการของกองทัพไทยในปัจจุบันนั้น กองทัพมิตรประเทศได้แยกงานออกเป็นกรมแผน (Plan)กรมปฏิบัติการ (Operations)กรมการฝึก (Training) และกรมใหม่ที่รวมระบบงาน C4I ซึ่งรวมถึงงานไซเบอร์ด้วย ผลที่ตามมาจากการนำงานไซเบอร์ซึ่งไม่ได้มีความเกี่ยวข้องกันโดยตรงเข้าไปรวมไว้ในกลุ่มงานเดียวกันกับงานยุทธการ ทำให้เกิดปัญหาที่ส่งผลกระทบต่อการพัฒนาระบบต่างๆ ของไซเบอร์คือ การที่จะต้องจัดลำดับความสำคัญด้านกำลังพล งบประมาณ ให้กับงานที่มีความเร่งด่วนเฉพาะหน้าก่อน เช่น งานการใช้กำลัง งานฝึก หรืองานปฏิบัติอื่นๆ ที่มีลักษณะเฉพาะหน้า ส่วนงานระบบที่มีผลกระทบระยะยาวมักจะถูกจัดลำดับไปให้ความเร่งด่วนต่ำกว่า รวมถึงงานไซเบอร์[58] ดังนั้น การพัฒนางานไซเบอร์ในกองทัพไทยซึ่งรวมถึงกองทัพบกจึงมีลำดับความเร่งด่วนต่ำกว่างานอื่นในสายงานยุทธการ ทำให้ในปัจุบันยังไม่มีแผนกงาน ในกรมยุทธการทหารบกรับผิดชอบเป็นฝ่ายอำนวยการด้านไซเบอร์ในกองทัพบก ในขณะที่งานไซเบอร์ได้ขยายตัวออกไปเป็นวงกว้างแล้วทั้งประเทศและในกองทัพมิตรประเทศ

ความเชื่อมโยงระบบไซเบอร์กองทัพบกกับทุกหน่วยในกระทรวงกลาโหมและรัฐ

ทุกองค์การในโลกทั้งภาครัฐ ภาคเอกชน และฝ่ายทหาร ล้วนแล้วแต่ก็มีการควบคุมบังคับบัญชาตามหลักทฤษฎีองค์การซึ่งวิธีการเดิมผ่านตัวกลางที่เป็นสายโทรศัพท์และการนำสาร โดยการเก็บข้อมูลไว้ในแฟ้มเอกสาร แต่ความก้าวหน้าทางเทคโนโลยีสมัยใหม่ทำให้มีตัวกลางที่ทันสมัยและรวดเร็วส่งผลทำให้การติดต่อสื่อสารด้วยวิธีการเดิมได้เปลี่ยนไป แต่ก็ยังคงเป็นไปตามหลักการควบคุมบังคับบัญชาองค์การที่มีมาอย่างยาวนานจึงเกิดการเชื่อมโยงทุกองค์การภาครัฐเข้าไว้ด้วยกันโดยผ่านเครือข่ายความเร็วสูงดังนั้น การที่จะพัฒนาหน่วยงานไซเบอร์กองทัพบกไทยเพื่อรองรับการเปลี่ยนแปลงในอนาคตนั้น จำเป็นต้องมีความชัดเจนว่ากองทัพจะจัดระบบความเชื่อมโยงระหว่างระบบไซเบอร์กับทุกหน่วยในกระทรวงกลาโหมและหน่วยงานภายนอกอย่างไร เพราะการเชื่อมโยง

[58]พลตรี นพนันต์ ชั้นประดับ, นายทหารฝ่ายเสนาธิการ กรมยุทธการทหารบก. สัมภาษณ์.7มิถุนายน 2562.

ดังกล่าวจำเป็นต้องกำหนด กฎหมาย ระเบียบ เพื่อให้ปฏิบัติงานร่วมกันได้ ในขณะเดียวกันกองทัพก็ต้องมีหลักนิยมและวิธีการปฏิบัติการทางทหาร รวมทั้งความมุ่งหมายที่แตกต่างกันออกไปจากฝ่ายพลเรือน

1.ความเชื่อมโยงระบบไซเบอร์กองทัพบกกับทุกหน่วยในกระทรวงกลาโหม

หากพิจารณาตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งมีผลบังคับใช้กับทุกหน่วยงานของรัฐ และตามพระราชกฤษฎีกาแบ่งส่วนราชการและกำหนดหน้าที่ส่วนราชการของ สำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ได้แบ่งส่วนราชการเป็นหน่วยขึ้นตรงต่างๆ และทุกหน่วยมีหน้าที่ในการรักษาความมั่นคงของรัฐ จึงถือว่าเป็นหน่วยที่มี “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” ซึ่งหมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐความปลอดภัยสาธารณะความมั่นคงทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ โดยเกี่ยวข้องกับการใช้ไซเบอร์ส่งผลทำให้หน่วยเหล่านี้อยู่ในความหมายของ“ไซเบอร์” ซึ่งหมายความรวมถึงข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ระบบอินเทอร์เน็ตหรือโครงข่ายโทรคมนาคมรวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

จากโครงสร้างการจัดในกองทัพไทยตั้งแต่ระดับกระทรวงกลาโหมลงมา ทุกหน่วยมีความเชื่อมโยงกันหมดตามสายการบังคับบัญชาโดยกำหนดไว้ในพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.2551 และที่แก้ไขเพิ่มเติม ซึ่งได้กำหนดหน่วยขึ้นตรงภายในกระทรวงกลาโหม และพระราชกฤษฎีกาแบ่งส่วนราชการและกำหนดหน้าที่ส่วนราชการสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ โดยพระราชกฤษฎีกาแต่ละฉบับหน่วยได้กำหนดหน่วยย่อยลงไปและมีอัตราการจัดรองรับ ผลที่ตามมาทำให้เมื่อนำระบบการสื่อสารและคอมพิวเตอร์เข้ามาใช้ในช่วงทศวรรษ 2530 แล้ว ก็จะก่อให้เกิดความเชื่อมโยงของทุกหน่วยในกระทรวงกลาโหมเข้าไว้ด้วยกันผ่านระบบการควบคุมบังคับบัญชาทางทหารเดิมเกิดเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศขนาดใหญ่และซับซ้อน และเป็นเป้าหมายขนาดใหญ่ต่อภัยคุกคามด้านไซเบอร์ได้ง่าย ผลกระทบที่ตามมาคือกองทัพจำเป็นต้องมีระบบ หลักเกณฑ์ และวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ซึ่งได้กำหนดเป็นพระราชบัญญัติให้ทุกส่วนราชการยึดถือปฏิบัติแล้วเพื่อไม่ให้ข้อมูลข่าวสารที่เข้าและออกจากกองทัพบกส่งผลกระทบต่อเครือข่ายอื่นที่เชื่อมโยงกัน

2. ความเชื่อมโยงระบบไซเบอร์กองทัพบกกับส่วนราชการภายนอกกระทรวงกลาโหม

นอกจากทุกส่วนราชการในกระทรวงกลาโหมมีระบบการควบคุมบังคับบัญชาที่มีมายาวนานแล้ว และหลังจากนำระบบคอมพิวเตอร์และการสื่อสารเข้ามาใช้ในกองทัพบกทุกหน่วยก็คงยังสามารถเชื่อมโยงไปยังส่วนราชการภายในนอกได้โดยตรงโดยไม่ต้องผ่านตามสายการบังคับบัญชาตามกรอบอำนาจหน้าที่ที่มอบให้ ส่งผลกระทบต่อการวางระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทยไม่สามารถพิจารณาเฉพาะแค่ความเชื่อมโยงของระบบเครือข่ายภายในกองทัพได้อีกต่อไป นั่นหมายความว่ากองทัพจำเป็นต้องมีหน่วยงานรับผิดชอบเพื่อวางแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภายในกองทัพและระหว่างกองทัพ และปัญหาที่จะตามมาคือการดำเนินการดังกล่าวสามารถสนับสนุนการปฏิบัติการทางทหารในยามสงครามได้หรือไม่

ปัญหาประการสำคัญในการนำระบบงานพลเรือนไทยมาใช้กับกองทัพในยามปกติคือระบบงานพลเรือนไม่ได้ออกแบบมาใช้กับการปฏิบัติการทางทหารโดยตรง แต่เป็นการวางระบบในรูปแบบตามพระราชบัญญัติหรือระเบียบสำนักนายกรัฐมนตรีเพื่อบังคับใช้ทุกส่วนราชการในภาพรวม แต่ถ้าหากส่วนราชการใดเห็นว่าจำเป็นต้องมีระบบหรือระเบียบเป็นการเฉพาะ ก็ต้องเป็นหน้าที่ของส่วนราชการนั้นที่จะต้องดำเนินการแก้ไขจนได้ข้อยุติออกมาเป็นกฎหมายเพื่อยึดถือปฏิบัติให้ครอบคลุมกับภารกิจของทุกส่วนราชการที่มีความแตกต่างกันออกไปโดยเฉพาะอย่างยิ่งความแตกต่างระหว่างราชการฝ่ายพลเรือนกับราชการฝ่ายทหารที่มีความแตกต่างกันอย่างเป็นสากล

ตัวอย่างที่เห็นได้ชัดเจนคือการรักษาความปลอดภัยสถานที่ สำนักนายกรัฐมนตรีได้กำหนดระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552โดย “การรักษาความปลอดภัยแห่งชาติ” หมายถึงมาตรการและการดำเนินการที่กำหนดขึ้นเพื่อพิทักษ์รักษาและคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการตลอดจนหน่วยงานของรัฐเจ้าหน้าที่ของรัฐและทรัพย์สินมีค่าของแผ่นดินให้พ้นจากการรั่วไหลการจารกรรมการก่อวินาศกรรมการบ่อนทำลายการก่อการร้ายการกระทำที่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐและการกระทำอื่นใดที่เป็นการเปิดเผยสิ่งที่เป็นความลับของทางราชการ และให้คำนิยามคำว่า “ยุทธภัณฑ์” หมายถึงสิ่งของทั้งหลายที่ใช้ประจำกายหรือประจำหน่วยกำลังถืออาวุธของทางราชการและสิ่งอื่นที่คณะกรรมการนโยบายรักษาความปลอดภัยแห่งชาติ (กรช.)ประกาศกำหนด และให้นิยามคำว่า “ที่สงวน” หมายถึงสิ่งปลูกสร้างทุกชนิดสำหรับการป้องกันประเทศฐานทัพบกฐานทัพเรือฐานทัพอากาศโรงงานทำอาวุธหรือยุทธภัณฑ์โรงช่างแสงหรือคลังอาวุธยุทธภัณฑ์อู่เรือรบท่าเรืออันใช้เป็นฐานทัพเรือสถานีวิทยุหรือโทรเลขหรือสถานีส่งและรับอาณัติสัญญาณรวมทั้งสถานที่ใดๆซึ่งใช้ในการสร้างหรือซ่อมแซมเรือรบหรืออาวุธยุทธภัณฑ์หรือวัตถุใดๆสำหรับใช้ในการสงคราม[59]

[59]“ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติพ.ศ.2552”, ราชกิจจานุเบกษา. เล่มที่ 126, 13 มีนาคม 2552, หน้า 4 - 6.

ในขณะที่หน่วยทหารสากลต่างมีระบบการป้องกันกำลังรบ (Force Protection) เพื่อดำรงสภาพกำลังพลและยุทโธปกรณ์ให้มีความพร้อมในการปฏิบัติภารกิจได้ตลอดเวลา และมีการจัดทำแผนการต่อต้านการใช้กำลังเข้าโจมตีที่ตั้งหน่วยซึ่งเป็นแผนทางทหารโดยเฉพาะ ดังนั้น ในกรณีนี้จะเกิดปัญหาในทางปฏิบัติว่ากองทัพจะยึดถือระเบียบใดในการรักษาความปลอดภัยที่ตั้งทางทหาร เพราะทุกส่วนราชการของกองทัพล้วนเป็นส่วนราชการที่จะต้องปฏิบัติตามระเบียบที่ทางราชการกำหนดเหมือนกับส่วนราชการอื่น ในขณะเดียวกันกองทัพต้องยึดถือหลักนิยมและวิธีการปฏิบัติการทางทหารซึ่งมีความเป็นสากลตามสายวิชาชีพ ปัญหาดังกล่าวจะเกิดขึ้นในการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ในการเชื่อมโยงกับส่วนราชการภายนอกกระทรวงกลาโหมเช่นกัน

ความชัดเจนบทบาทและความรับผิดชอบไซเบอร์ยามปกติและยามสงคราม

จากการศึกษาพบว่าบทบาทไซเบอร์ในกองทัพเช่นเดียวกับทุกสายงานคือมีบทบาททั้งในยามยามปกติและยามสงคราม โดยในยามปกติอยู่ภายใต้กฎหมายของประเทศเช่นเดียวกับระบบทางทหารอื่นเช่น การปฏิบัติงานอากาศยานของกองทัพในยามปกติ ต้องปฏิบัติตามกฎหมายการควบคุมห้วงอากาศของกรมการบินพลเรือน แต่เมื่อมีการประกาศสงครามการควบคุมห้วงอากาศจึงจะอยู่ภายใต้การควบคุมของฝ่ายทหาร การปฏิบัติงานด้านไซเบอร์ก็เช่นเดียวกันในยามปกติต้องอยู่ภายใต้ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งมีผลบังคับใช้ต่อหน่วยงานของรัฐ ได้แก่ราชการส่วนกลางราชการส่วนภูมิภาคราชการส่วนท้องถิ่นรัฐวิสาหกิจองค์กรฝ่ายนิติบัญญัติองค์กรฝ่ายตุลาการองค์กรอิสระองค์การมหาชนและหน่วยงานอื่นของรัฐภายใต้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยนายกรัฐมนตรีเป็นประธาน รัฐมนตรีกระทรวงที่เกี่ยวข้องเป็นกรรมการ และมีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ ปลัดกระทรวงต่างๆ เป็นกรรมการ

ผลกระทบที่ตามมาคือการจัดบทบาทของกองทัพด้านไซเบอร์ทั้งในยามปกติและยามสงครามซึ่งจะนำไปสู่การพัฒนาระบบงานรองรับให้ชัดเจนเช่นเดียวกับกองทัพสหรัฐอเมริกาที่มีการจัดหน่วยงานไซเบอร์รองรับการสนับสนุนฝ่ายพลเรือนและการปฏิบัติการทางทหารทั้งในกองบัญชาการผสมและชุดไซเบอร์ที่ไปปฏิบัติงานยังหน่วยทหารทางยุทธวิธี ซึ่งในเรื่องดังกล่าวยังไม่มีใครกำหนดให้ชัดเจนดังนั้นสถานะของหน่วยงานด้านไซเบอร์ในแต่ละเหล่าทัพ รวมทั้งกองบัญชาการกองทัพไทยและสำนักงานปลัดกระทรวงกลาโหม จึงเป็นเพียงการจัดตั้งหน่วยงานขึ้นมารองรับซึ่งอาจจะมีฐานะเป็นเพียงกรมฝ่ายกิจการพิเศษ แต่ในระดับกองทัพภาคลงมายังไม่มีการกำหนดแนวทางปฏิบัติที่ชัดเจนว่าจะมีการจัดหน่วยไซเบอร์ในระดับกองทัพภาคลงไป หรือรับการสนับสนุนชุดปฏิบัติการไซเบอร์เช่นเดียวกับกองทัพสหรัฐอเมริกา

เหตุผลความจำเป็นที่จะต้องกำหนดบทบาทและหน้าที่ของหน่วยงานไซเบอร์ในกองทัพให้ชัดเจนเนื่องจากการปฏิบัติงานของกองทัพก็ไม่แตกต่างไปจากองค์การทุกองค์การ คือต้องจัดทำโครงสร้าง การจัด อัตรากำลังรองรับให้ชัดเจน และนำไปบรรจุกำลังพล การพัฒนากำลังพล รวมทั้งนำไปยึดถือปฏิบัติงาน และการประเมินผลการปฏิบัติ เพื่อนำมาใช้ในการรกำหนดค่าตอบแทน และการพัฒนาองค์การต่อไป ตามที่ปรากฏหน้าที่ของทุกส่วนราชการในกระทรวงกลาโหมในอัตราซึ่งเป็นคำสั่งกระทรวงกลาโหม โดยแบ่งออกเป็นอัตราการจัดและยุทโปกรณ์ หรือ อจย. (Table and Organization of Equipment: TOE) และอัตราการจัดเฉพาะกิจ หรือ อฉก. (Table of Distributions and Allowance: TDA)โดยทั้งสองแบบของอัตราดังกล่าวจะกำหนดหน้าที่ไว้ในตอนที่ 1 กล่าวทั่วไป ซึ่งถ้าหากกองทัพยังไม่กำหนดความชัดเจนบทบาทไซเบอร์ยามปกติและยามสงครามแล้ว ก็จะส่งผลตามมาทั้งระบบ โดยระบบอัตรากำลังของกองทัพไทยซึ่งนำมาจากกองทัพสหรัฐอเมริกาในแต่ละส่วนที่มีความเชื่อมโยงจากตอนที่ 1 ถึงตอนที่ 4 ตามตารางที่ 4 - 1 ดังนี้

ตารางที่ 4 - 1 รายละเอียดการจัดแบบอัตราการจัดของกองทัพบกไทย

	ตอนที่ 1	ตอนที่ 2	ตอนที่ 3	ตอนที่ 4
อัตราการจัดและยุทโปกรณ์ (อจย.) (Table and Organization of Equipment: TOE)	กล่าวทั่วไป	ผังการจัด	อัตรากำลังพล	ยุทโธปกรณ์
อัตราการจัดเฉพาะกิจ (อฉก.) (Table of Distributions and Allowance: TDA)	กล่าวทั่วไป	ผังการจัด	อัตรากำลังพล	คำชี้แจง

ตอนที่ 1 กล่าวทั่วไป ในส่วนของหน่วยที่มีการจัดแบบ อฉก. จะกำหนดหน้าที่และขอบเขตความรับผิดชอบที่สำคัญ ส่วนหน่วยที่มีการจัดแบบ อจย. ซึ่งเป็นหน่วยกำลังรบและใช้ร่วมกันหลายหน่วยจะกำหนดเป็นภารกิจและขีดความสามารถเพื่อให้สามารถนำไปวางแผนประกอบกำลังในการปฏิบัติการในสนามได้อย่างถูกต้อง สำหรับหน่วยไซเบอร์ในกองทัพซึ่งมีหน้าที่และลักษณะงานเป็นแบบ Staff Function โดยมีหน้าที่เฉพาะจึงควรกำหนดการจัดเป็นอัตราแบบ อฉก. ซึ่งกำหนดหน้าที่และขอบเขตความรับผิดชอบที่สำคัญไว้ เพื่อจะได้นำไปขยายเป็นผังการจัดหน่วยรองรับหน้าที่ดังกล่าว และนำไปจัดทำอัตรากำลังพลมาปฏิบัติงานในตอนที่ 3 ต่อไป ดังนั้นถ้าไม่สามารถกำหนด

ความชัดเจนบทบาทไซเบอร์ยามปกติและยามสงครามให้ชัดเจนแล้ว ก็จะทำให้กระบวนการที่ตามมาในตอนที่ 2-4 หยุดชะงักลง รวมไปถึงผลกระทบที่จะเกิดขึ้นจากการนำอัตราดังกล่าวไปใช้บรรจุกำลังพลและปฏิบัติงานตามวงรอบที่กล่าวมา

วิเคราะห์ผลกระทบต่อระบบโครงสร้างอัตรากำลังหน่วยงานด้านไซเบอร์

จากผลกระทบความไม่ชัดเจนของบทบาทไซเบอร์ในกองทัพไทยตั้งแต่บทบาทในยามปกติและยามสงคราม รวมถึงความไม่ชัดเจนในการปรับระบบฝ่ายอำนวยการให้มีกรมฝ่ายเสนาธิการเฉพาะรองรับ และความไม่ชัดเจนในการจัดชุดปฏิบัติการสนับสนุนในระดับต่างๆ ตั้งแต่ฝ่ายพลเรือนระดับชาติลงมาจนถึงกองกำลังทางยุทธวิธีส่งผลทำให้ระบบโครงสร้างอัตรากำลังของหน่วยงานด้านไซเบอร์ในกองทัพไทย ยังคงจำกัดบทบาทเป็นเพียงการจัดตั้งหน่วยงานไซเบอร์ทำหน้าที่กรมฝ่ายกิจการพิเศษรับผิดชอบเรื่องไซเบอร์ทั้งระบบในแต่ละเหล่าทัพในขณะที่ความก้าวหน้าภายในรัฐมีความตื่นตัวสูงรวมถึงการจัดเก็บข้อมูลขนาดใหญ่ (Big Data) ตามสั่งการของนายกรัฐมนตรีให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นเจ้าภาพในการรวบรวมข้อมูลจากส่วนราชการและหน่วยงานต่างๆ เกี่ยวกับแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ของทุกหน่วยงานเพื่อจัดทำเป็นภาพรวม[60]

ผลที่ตามมาคือหน่วยขึ้นตรงในกองทัพบกยังขาดเจ้าหน้าที่ปฏิบัติงานด้านไซเบอร์ โดยยังคงมีเพียงการจัดส่วนกรรมวิธีข้อมูลซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับคอมพิวเตอร์โดยมุ่งเน้นไปที่ระบบสารสนเทศมากกว่าระบบการรักษาความปลอดภัยไซเบอร์ ถึงแม้กองทัพจะกำหนดมอบงานให้ส่วนกรรมวิธีข้อมูลรับผิดชอบ ก็จะประสบปัญหาตามมาในทุกด้าน ได้แก่ หน้าที่ โครงสร้างการจัดระบบงาน รวมถึงบุคลากรที่มีความเชี่ยวชาญโดยตรง นอกจากนั้น กองทัพยังขาดความชัดเจนในเรื่องการปฏิบัติการข่าวสาร และระบบข้อมูลสารสนเทศซึ่งเป็นปัญหาที่มีสาเหตุความเป็นมาในลักษณะเดียวกันมาก่อนหน้านานกว่าระบบไซเบอร์อีกด้วย แต่ก็ยังไม่ได้รับการแก้ไข ดังนั้น จึงเป็นการยากที่จะแยกดำเนินการแก้ไขและพัฒนาเฉพาะปัญหาด้านไซเบอร์เพียงลำพังก่อน และปัญหาที่กล่าวมาทั้งหมดจำเป็นต้องได้รับการแก้ไขเชิงระบบไปพร้อมกัน

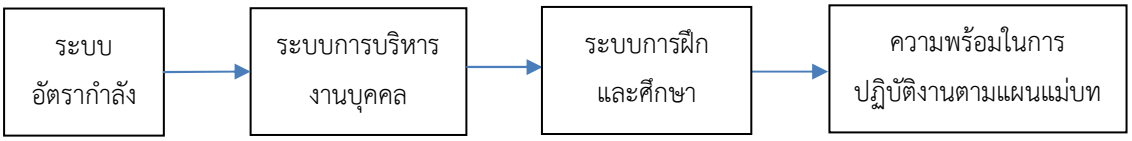
ตามที่ได้ศึกษาและวิเคราะห์มาแล้วว่าโครงสร้างการจัดและอัตรากำลัง เป็นจุดเริ่มต้นขององค์การทุกองค์การ ดังนั้น หากกองทัพต้องการพัฒนาหน่วยงานไซเบอร์ก็จำเป็นต้องจัดทำโครงสร้างการจัดและอัตรากำลังให้มีความสมบูรณ์เพื่อให้หน่วยที่เกี่ยวข้องในการพัฒนาหน่วยงานไซเบอร์และทุกกรมฝ่ายเสนาธิการใช้ยึดถือในการกำหนดงานของแต่ละหน่วยต่อไปโดยเฉพาะการบริหารงานบุคคลซึ่งเป็นเรื่องที่สำคัญที่สุดในการพัฒนาองค์การ

[60]สำนักงานเลขาธิการคณะรัฐมนตรี. “หนังสือด่วนที่สุด ที่ นร 0505/ว.187”.ลงวันที่13 พฤษภาคม 2562.

ระบบการบริหารงานบุคคลด้านไซเบอร์

เมื่อพิจารณาตามหลักการบริหารทรัพยากรบุคคลในบทที่ 2 และผลการศึกษาข้อมูลในบทที่ 3 แล้ว ระบบอัตรากำลังเป็นปัจจัยนำเข้าของระบบการบริหารงานบุคคล และระบบการบริหารงานบุคคลเป็นปัจจัยส่งออกไปยังระบบการฝึกและศึกษา โดยทั้ง 3 ระบบมีความเชื่อมโยงกันแบบอนุกรมกล่าวคือ ถ้าระบบก่อนหน้าไม่มีความสมบูรณ์ก็จะส่งผลทำให้ระบบต่อๆ มาขาดความสมบูรณ์เช่นกัน และนำไปสู่การขาดความพร้อมในการปฏิบัติหน้าที่ ดังนั้น กองทัพจึงจำเป็นต้องพัฒนาทั้ง 3 ระบบงานให้สมบูรณ์ตามแผนภาพที่ 4 - 1เพื่อให้มีความพร้อมในการปฏิบัติภารกิจตามที่กำหนดไว้ในแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคงได้

แผนภาพที่ 4 - 1 วิเคราะห์ความเชื่อมโยง ระบบอัตรากำลัง ระบบการบริหารงานบุคคล ระบบการฝึกและศึกษาตามทฤษฎีระบบ



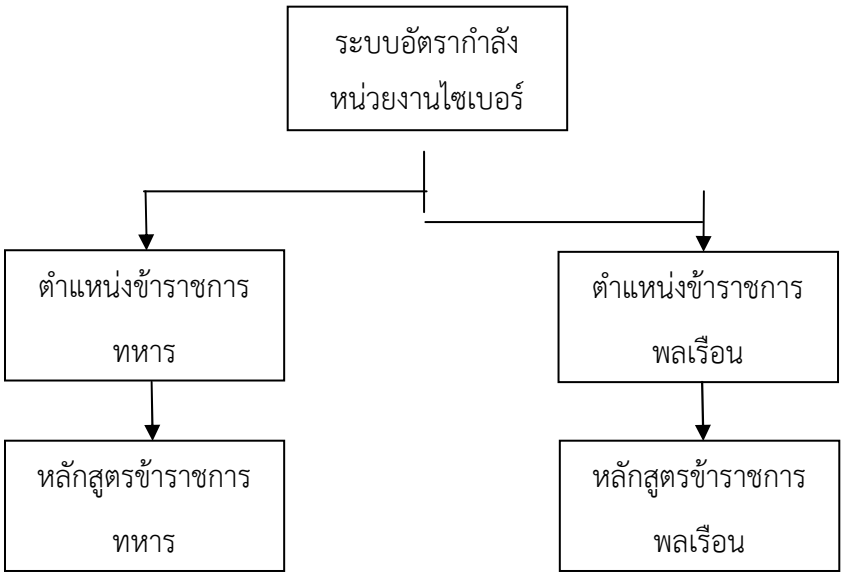
1.ระบบอัตรากำลัง

จากการศึกษาพบว่าระบบอัตรากำลังของกองทัพไทยทั้งสามเหล่าทัพ ได้นำมาจากสหรัฐอเมริกา หลังจากได้มีการลงนามความช่วยเหลือทางทหารจากสหรัฐอเมริกา โดยในส่วนกองทัพบกนำระบบอัตรากำลังทั้งแบบอัตราการจัดและยุทโธปกรณ์ และอัตราการจัดเฉพาะกิจมาเริ่มใช้ตั้งแต่ปี พ.ศ.2495 หลังจากนั้นได้นำระบบหมายเลขความชำนาญการทางทหารมาใช้กับนายทหารชั้นประทวนในปี พ.ศ.2499 และต่อมาเมื่อเห็นผลดีของระบบหมายเลขความชำนาญการทางทหารจึงนำมาพัฒนาใช้กับนายทหารสัญญาบัตรด้วยในปี พ.ศ.2501 พร้อมกับได้จัดทำหลักการจัดทำอัตรากองทัพบกขึ้นฉบับแรกในปีพ.ศ.2503 อย่างไรก็ตาม หลังจากที่สหรัฐอเมริกาได้ถอนกำลังออกจากประเทศไทยแล้ว การพัฒนาระบบอัตรากำลังของกองทัพไทยเป็นไปในลักษณะของการปรับปรุงเพิ่มเติมจากของเดิม ในขณะที่หลังจากนั้นเป็นต้นมาจนถึงปัจจุบัน ได้มีระบบงานใหม่ๆ เช่น งานด้านกิจการพลเรือน เป็นต้น โดยเฉพาะในช่วงสองทศวรรษที่ผ่านมาได้มีการเพิ่มงานด้านเทคโนโลยีสารสนเทศ งานไซเบอร์ รวมถึงงานพัฒนาระบบราชการ ในขณะที่อัตรากำลังของกองทัพยังคงใช้ระบบหมายเลขความชำนาญการทางทหารแบบเดิมโดยรวมทุกตำแหน่งไว้ในอัตราทหาร จึงทำให้เกิด

ปัญหาเรื่องแนวทางรับราชการตลอดจนการฝึกและศึกษาของตำแหน่งงานที่ปรากฏขึ้นใหม่และนำมาสู่ความไม่ชัดเจนของการจัดกำลังพลเข้ารับการฝึกและศึกษาตลอดจนการบรรจุเข้าปฏิบัติหน้าที่

หน่วยงานไซเบอร์เป็นสายงานทางด้านเทคนิคที่ต้องใช้ความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์ การสื่อสารข้อมูล รวมถึงความรู้ทางเทคนิคในการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับแทบทุกตำแหน่ง ในขณะที่โครงสร้างการจัดเป็นการนำหน่วยที่เป็นอัตราทหารทั้งหน่วยจากสายงานสื่อสารเดิมมาใช้ ผลกระทบที่เกิดขึ้นจากการที่ระบบอัตรากำลังไม่สมบูรณ์คือทำให้กองทัพไม่สามารถบริหารงานบุคคลได้ตรงตามความรู้ที่ต้องการในแต่ละตำแหน่ง และไม่สามารถจัดกำลังพลเข้ารับการฝึกและศึกษาได้ตรงตามตำแหน่งหน้าที่ รวมถึงไม่สามารถบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดได้อย่างเต็มประสิทธิภาพ โดยเฉพาะกำลังพลในกองทัพบกปัจจุบันบรรจุในอัตราไม่จำกัดเหล่าจำนวนมาก ทั้งที่อัตราเหล่านั้นควรกำหนดเป็นอัตราข้าราชการพลเรือนกลาโหม แต่เนื่องจากระบบข้าราชการพลเรือนดังกล่าวยังไม่มีผลบังคับใช้ในกระทรวงกลาโหมอย่างเป็นรูปธรรม จึงทำให้กำลังพลในหน่วยงานไซเบอร์ต้องเข้ารับการศึกษาตามหลักสูตรเพียงเพื่อใช้คุณวุฒิประกอบในการปรับตำแหน่งให้สูงขึ้นเท่านั้น ถึงแม้จะมีการอบรมหลักสูตรที่เกี่ยวข้องกับการปฏิบัติงานไซเบอร์บ้างแต่ก็ยังไม่เพียงพอที่จะมีความเชี่ยวชาญ ดังนั้น กองทัพสมควรแยกอัตรากำลังข้าราชการทหารและอัตรากำลังข้าราชการพลเรือนกลาโหมพร้อมกับจัดทำหลักสูตรรองรับให้เหมาะสมกับงานแต่ละตำแหน่งให้ชัดเจนตามแผนภาพที่ 4 - 2

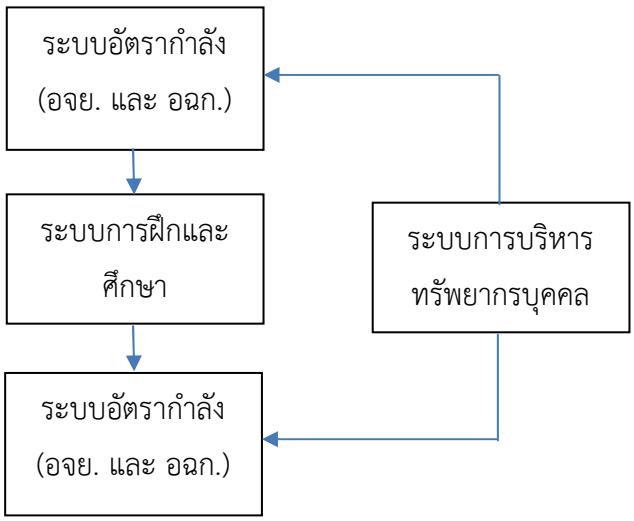
แผนภาพที่ 4 - 2 การแยกตำแหน่งและการฝึกศึกษาของข้าราชการทหารและข้าราชการพลเรือนในหน่วยงานไซเบอร์



2.ระบบการบริหารทรัพยากรบุคคล

ระบบการบริหารทรัพยากรบุคคลเป็นระบบที่ต่อเนื่องมาจากระบบอัตรากำลัง โดยเป็นการพัฒนากำลังพลให้มีความพร้อมในการปฏิบัติหน้าที่แต่ละตำแหน่งที่กำหนดไว้ในอัตราของหน่วย ดังนั้น จึงจำเป็นต้องมองกรอบในภาพใหญ่ของทุกระบบ โดยระบบการบริหารทรัพยากรบุคคลมีหน้าที่ในการคัดเลือกกำลังพลเข้ามาบรรจุให้ตรงตามอัตรากำลังมาเข้าสู่ระบบการฝึกและศึกษา หลังจากนั้น จึงนำกลับไปบรรจุในอัตราจึงจะครบสมบูรณ์ตามขั้นตอนการบริหารงานบุคคลในแผนภาพที่4 - 3 แต่จากการศึกษาข้อมูลในบทที่ 3 สามารถสรุปได้ว่าในปัจจุบันระบบการแต่งตั้งโยกย้ายของทุกส่วนราชการในกระทรวงกลาโหมยังไม่สามารถตอบสนองต่อระบบดังกล่าวได้ โดยเป็นการดำเนินการของบุคลากรที่จะแสวงหาตำแหน่งที่ตัวเองจะบรรจุเพื่อให้ได้เลื่อนชั้นยศสูงขึ้นหากผ่านหลักสูตรที่กำหนดและได้รับการถ่ายทอดยึดถือปฏิบัติจนกล่าวได้ว่าเป็นวัฒนธรรมองค์กรทหารไทยไปแล้วว่าไปเรียนเพื่อเลื่อนฐานะให้สูงขึ้น แต่ไม่ได้มีการพิจารณาถึงผลการประเมินค่ากำลังพลและนำมาพิจารณาในภาพรวมของกองทัพอย่างเป็นระบบเหมือนกองทัพมิตรประเทศดังนั้น จึงจำป็นต้องพัฒนาระบบการบริหารงานบุคคลด้านไซเบอร์ไปพร้อมกันตามแผนภาพที่ 4 - 3

แผนภาพที่ 4 - 3 ความสัมพันธ์ระหว่างการบริหารทรัพยากรบุคคล กับระบบอัตรากำลังระบบการฝึกและศึกษา



3.ระบบการฝึกและการศึกษา

จากคุณลักษณะของหน่วยงานไซเบอร์ที่เป็นสายงานเทคนิค ดังนั้นหลักสูตรการฝึกและศึกษาเกือบทั้งหมดจึงเป็นการศึกษาทางเทคนิคซึ่งมีความแตกต่างไปจากการฝึกและศึกษาทางทหารโดยสิ้นเชิงจากการสัมภาษณ์ผู้ที่มีส่วนเกี่ยวข้องสรุปว่าเนื่องจากระบบการเรียนการสอนทางทหารของกองทัพไทยเป็นการนำกำลังพลจำนวนมากมาเข้ารับการศึกษาตามหลักสูตรที่กำหนดไว้ในแผนงานประจำปีและได้รับการจัดสรรงบประมาณแล้วโดยไม่ได้แยกหลักสูตรทางทหารและพลเรือนให้ชัดเจน ดังนั้น จึงต้องรับผู้เข้ารับการศึกษาให้ครบตามจำนวน โดยไม่ได้มีการพิจารณาตรวจสอบให้ชัดเจนว่าผู้เข้ารับการศึกษาแต่ละคนมีความจำเป็นที่จะต้องเข้ารับการศึกษาและกลับไปปฏิบัติหน้าที่หรือไม่ โดยเฉพาะอย่างยิ่งการที่ไม่แยกข้าราชการทหารและข้าราชการพลเรือนกลาโหมออกจากกัน ทำให้กำลังพลทุกนายต้องเข้ารับการศึกษาหลักสูตรตามแนวทางรับราชการทั้งนายทหารสัญญาบัตรและนายทหารประทวนเพื่อให้สามารถติดยศสูงขึ้นได้ตามที่กำหนดไว้ในแนวทางรับราชการ

ในปัจจุบันแต่ละเหล่าทัพมีการเปิดหลักสูตรอบรมด้านไซเบอร์ที่แตกต่างกันออกไป

- ศูนย์ไซเบอร์ทหาร เปิดอบรม 3 หลักสูตร คือ หลักสูตรการฝึกอบรมเพิ่มพูนความรู้ทางด้านไซเบอร์ หลักสูตรปรับพื้นฐานบุคลากรด้านไซเบอร์ และหลักสูตรนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์

- ศูนย์ไซเบอร์กองทัพบกเปิดอบรม 2 หลักสูตร คือหลักสูตรการปฏิบัติการไซเบอร์ชั้นต้น และหลักสูตรการปฏิบัติการไซเบอร์ชั้นสูง

- ศูนย์ไซเบอร์กองทัพเรือเปิดอบรม 1 หลักสูตร คือ หลักสูตรเจ้าหน้าที่ดูแลระบบเครือข่าย

- กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เปิดอบรม 1 หลักสูตร คือ หลักสูตรนายทหารรักษาความปลอดภัยไซเบอร์

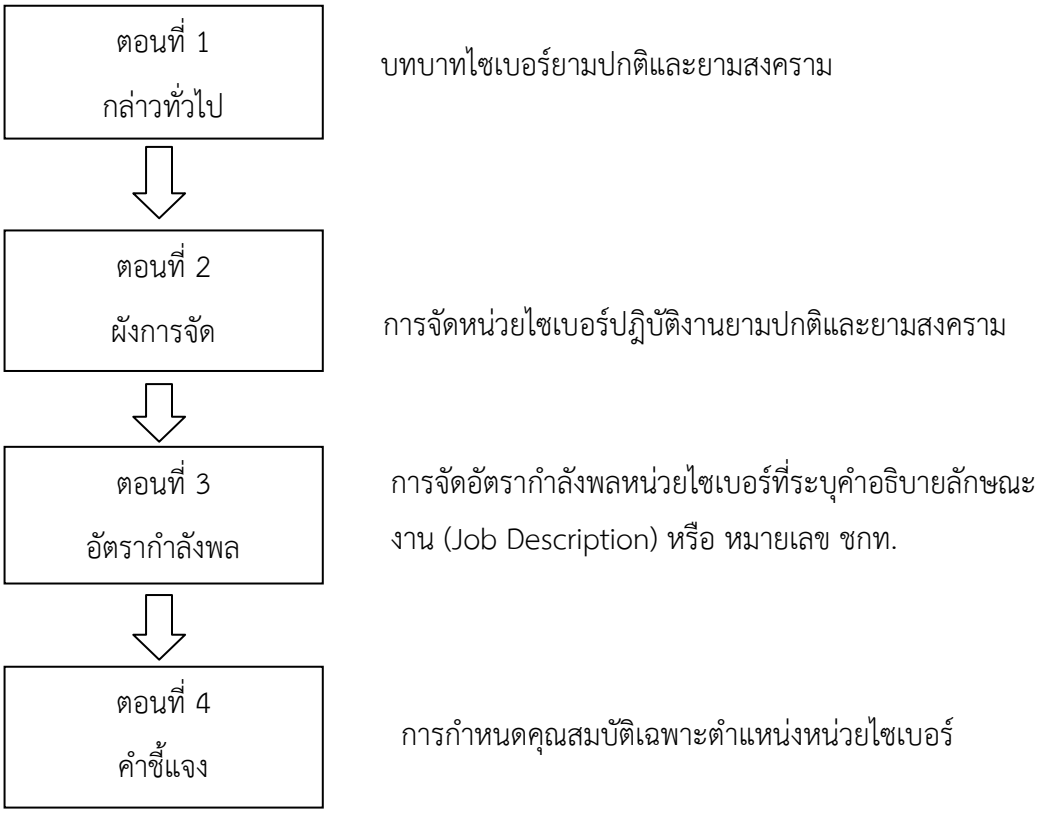
- ศูนย์ไซเบอร์ภายใต้กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เปิดอบรม 1 หลักสูตร คือ หลักสูตร Digital Forensics ซึ่งในแต่ละปีจะเปิดอบรมในหัวข้อที่ไม่ซ้ำกัน

กองทัพยังต้องพัฒนาหลักสูตรทางเทคนิคเฉพาะด้านสำหรับกำลังพลสายงานไซเบอร์ที่ปฏิบัติงานในทุกระดับ

สรุปการพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคง

ตามที่ได้วิเคราะห์มาแล้วว่า การที่จะพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้นั้น จะต้องเริ่มที่การกำหนดหน้าที่และความรับผิดชอบของหน่วยงานไซเบอร์ให้ชัดเจนซึ่งปกติกำหนดไว้ในอัตราการจัดของทุกหน่วยในกองทัพบก เนื่องจากงานไซเบอร์ไม่ใช่เป็นงานทางยุทธวิธี จึงจัดเป็นงานที่มีการจัดแบบอัตราเฉพาะกิจ โดยในตอนที่ 1กล่าวทั่วไป จะกล่าวถึง ภารกิจ ขอบเขตหน้าที่ที่สำคัญว่าหน่วยจะต้องปฏิบัติงานตอนที่ 2ผังการจัด จะกำหนดการจัดหน่วย ซึ่งถ้าจัดให้มีชุดปฏิบัติการไซเบอร์ไปสนับสนุนการปฏิบัติในระดับต่าง ๆ ก็ต้องกำหนดไว้ในผังการจัดให้ชัดเจน ตอนที่ 3อัตรากำลังพล จะเป็นการกำหนดรายละเอียดแต่ละตำแหน่งว่าในหน่วยนั้นประกอบด้วยตำแหน่งอะไรบ้าง มีจำนวนกี่คน และแต่ละคนมีคำอธิบายลักษณะงาน (Job Description) หรือที่กองทัพบกเรียกว่าหมายเลข ชกท. อย่างไร โดยหมายเลข ชกท. ดังกล่าวจะเชื่อมโยงกับมาตรฐานกำหนดตำแหน่ง (Job Specification) เพื่อกำหนดหลักสูตรที่ต้องสำเร็จการศึกษาเพื่อให้บรรจุปฏิบัติหน้าที่ในแต่ละตำแหน่งได้อย่างถูกต้อง ซึ่งการพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยจะต้องดำเนินการให้ครบทั้งระบบตามแผนภาพที่4 - 4

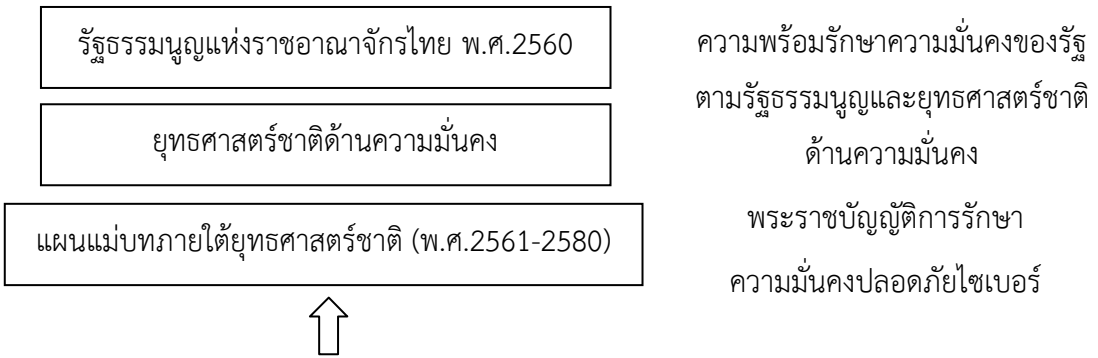
แผนภาพที่ 4 - 4กรอบการพัฒนาหน่วยงานไซเบอร์การพัฒนาบุคลากรไซเบอร์กองทัพไทย



เมื่อได้กำหนดหน้าที่และการจัดหน่วยงานย่อยมารองรับในแต่ละงานย่อย ตลอดจนการจัดอัตรากำลังที่ชัดเจนแล้ว จึงจะนำอัตราดังกล่าวมาดำเนินการขออนุมัติเพื่อใช้ในการบริหารงานบุคคลทั้งระบบ เริ่มจากการบรรจุกำลังพลให้ครบตามอัตรา การพัฒนาระบบการฝึกและศึกษาทางทหารโดยจะต้องเริ่มจากขั้นตอนการคัดกำลังพลจากอัตราหรือที่จะเตรียมบรรจุไว้ในอัตราออกมาแล้วจัดส่งเข้ารับการฝึกและศึกษาทางทหาร เมื่อสำเร็จการศึกษาตามหลักสูตรต่าง ๆ แล้วก็นำกลับเข้ามาบรรจุปฏิบัติงานตามตำแหน่งเมื่อกำลังพลที่ผ่านการศึกษาและกลับเข้ามาบรรจุปฏิบัติงานตามตำแหน่งได้ทุกตำแหน่งแล้วก็จะทำให้อัตราของหน่วยนั้นมีความพร้อมที่จะปฏิบัติงานตามที่ขีดความสามารถที่กำหนดไว้ในตอนที่ 1

กรณีของหน่วยไซเบอร์หากมีการจัดหน่วยแบบ อจย. ซึ่งจัดสำหรับสนับสนุนหน่วยปฏิบัติทางยุทธวิธีและปฏิบัติภารกิจร่วมกับหน่วยกำลังรบในระดับต่างๆ จึงจำเป็นต้องมีการฝึกการปฏิบัติในสนามร่วมกันดังนั้นหลังจากบรรจุกำลังพลและเข้ารับการฝึกและศึกษาในระดับตำแหน่ง (Individual Training) แล้วในหน่วยทหารทั้งหมดที่กล่าวมา จำเป็นต้องเข้ารับการฝึกเป็นหน่วย (Collective Training) เพื่อให้แต่ละหน่วยสามารถปฏิบัติงานได้อย่างสอดคล้องกันก่อน โดยมีหลักนิยมเป็นเครื่องมือที่จะช่วยทำให้ทุกหน่วยสามารถปฏิบัติหน้าที่ได้อย่างประสานสอดคล้องกัน เมื่อทุกหน่วยมีความพร้อมที่จะปฏิบัติภารกิจตามที่กำหนดไว้ในตอนที่ 1 แล้ว ก็จะทำให้ทุกเหล่าทัพมีความพร้อมรบสามารถปฏิบัติหน้าที่ตามที่กำหนดไว้ในพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหมและรัฐธรรมนูญแห่งราชอาณาจักรไทยซึ่งกำหนดให้รัฐจัดให้มีกำลังทหารเพื่อรักษาเอกราชและความมั่นคงของประเทศรวมทั้งแผนแม่บทรองรับยุทธศาสตร์ชาติด้านความมั่นคง โดยกำหนดหลักนิยมการปฏิบัติให้ชัดเจนตามแผนภาพที่ 4 - 5 ในขณะเดียวกันก็ต้องสนับสนุนการปฏิบัติงานของฝ่ายพลเรือนในยามปกติได้ด้วย

แผนภาพที่ 4 - 5 แบบจำลองระบบหน่วยงานด้านไซเบอร์ของกองทัพบกไทย
รองรับยุทธศาสตร์ชาติด้านความมั่นคง



บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

การปฏิบัติการไซเบอร์เป็นเรื่องที่กองทัพทั่วโลกให้ความสำคัญอย่างมาก เพราะมีส่วนสำคัญในการสนับสนุนการปฏิบัติการทางทหารและสนับสนุนฝ่ายพลเรือนในยามปกติได้ดังนั้นกองทัพไทยจึงมีความจำเป็นที่จะต้องพัฒนาหน่วยงานไซเบอร์ในกองทัพให้สามารถปฏิบัติภารกิจตามที่กำหนดไว้ในแผนแม่บทรองรับยุทธศาสตร์ชาติ (พ.ศ.2561-2580) ได้ และนำมาซึ่งความพร้อมในการปฏิบัติหน้าที่ในการรักษาความมั่นคงของรัฐตามที่กำหนดไว้ในรัฐธรรมนูญ

สรุปผลการวิจัย

จากการวิเคราะห์สามารถสรุปผลการวิจัยได้ว่าการที่จะพัฒนาหน่วยงานไซเบอร์ในกองทัพให้สามารถปฏิบัติภารกิจตามที่กำหนดไว้ในแผนแม่บทรองรับยุทธศาสตร์ชาติ (พ.ศ.2561-2580) ได้นั้น จำเป็นต้องสร้างความเข้าใจต่อทุกฝ่ายให้มีความรู้ในเรื่องไซเบอร์ก่อน หลังจากนั้นจึงจะทำให้การกำหนดหน้าที่ของหน่วยงานไซเบอร์ในกองทัพมีความชัดเจนในเรื่องบทบาท ภารกิจและหน้าที่เพื่อใช้ในการพิจารณาติดสินใจว่าควรเป็นเพียงกรมฝ่ายกิจการพิเศษดังเช่นปัจจุบัน หรือจัดตั้งให้เป็นหน่วยปฏิบัติงานด้านไซเบอร์อย่างสมบูรณ์สามารถสนับสนุนฝ่ายพลเรือนในยามปกติและสนับสนุนกองกำลังทางยุทธวิธีในการปฏิบัติการทางทหารเช่นเดียวกับกองทัพมิตรประเทศเมื่อเกิดความชัดเจนแล้วจึงจะสามารถพัฒนาทุกระบบที่เกี่ยวข้องไปพร้อมกัน ได้แก่ ระบบอัตรากำลัง ระบบการบริหารทรัพยากรบุคคล และระบบการฝึกศึกษา ที่สำคัญที่สุดคือในปัจจุบันได้มีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 แล้ว ดังนั้น จึงมีความจำเป็นต้องพัฒนาหน่วยงานไซเบอร์ในกองทัพให้มีความสอดคล้องกัน

1.การสร้างความเข้าใจให้ตรงกันในเรื่องที่เกี่ยวข้องกับระบบงานไซเบอร์ในกองทัพและในประเทศ

ผลการวิจัยสามารถสรุปได้ว่าปัญหาหลักประการหนึ่งของการพัฒนาหน่วยงานไซเบอร์ในกองทัพเพื่อปฏิบัติงานตามแผนแม่บทรองรับยุทธศาสตร์ชาติด้านความมั่นคงคือ การขาดความเข้าใจที่ตรงกันในหลายเรื่อง ทำให้หน่วยที่มีหน้าที่ความรับผิดชอบในการพัฒนาหน่วยงานไซเบอร์แต่ละด้านขาดมุมมองร่วมกัน และไม่สามารถนำพาไปสู่เป้าหมายเดียวกันได้ โดยเรื่องที่เกี่ยวข้องกับระบบงานไซเบอร์ในกองทัพและประเทศซึ่งสมควรสร้างความเข้าใจให้ตรงกันได้แก่

ความหมายและขอบเขตของระบบงานไซเบอร์ การจัดฝ่ายอำนวยการทางทหารในระบบงานไซเบอร์ ความแตกต่างภายในกระทรวงกลาโหม และความแตกต่างระหว่างทหารและพลเรือน

1.1 ความหมายและขอบเขตของระบบงานไซเบอร์

ผลการศึกษาจากการสังเกตการณ์แบบมีส่วนร่วมของผู้วิจัยทำให้ทราบว่า ความรู้เรื่องไซเบอร์ในกองทัพยังคงจำกัดอยู่เพียงหน่วยงานไซเบอร์และหน่วยที่เกี่ยวข้องเท่านั้น ทั้งนี้เป็นผลมาจากในห้วงที่ผ่านมาประเทศไทยยังไม่มีกฎหมายที่เกี่ยวข้องกับไซเบอร์ จึงทำให้ยังไม่มีความชัดเจนตั้งแต่ความหมายของไซเบอร์ และทำให้เกิดปัญหาการตีความเกี่ยวกับสายงานต่างๆ ตั้งแต่สายงานข่าวซึ่งเห็นว่าไซเบอร์เป็นข้อมูลข่าวสารส่วนหนึ่งของงานข่าว ส่วนสายงานสื่อสารเห็นว่าไซเบอร์เป็นส่วนหนึ่งของการสื่อสารเพราะต้องใช้ตัวกลางในการสื่อสารข้อมูล ในขณะที่สายงานสารสนเทศและประชาสัมพันธ์เห็นว่าไซเบอร์เป็นข้อมูลข่าวสาร ส่วนงานด้านการปฏิบัติการข่าวสารเห็นว่าไซเบอร์ต้องถูกเพิ่มเข้ามาเป็นส่วนหนึ่งของระบบปฏิบัติการข่าวสาร จากที่กล่าวมาทั้งหมดจะเห็นว่าเพียงเริ่มต้นก็สร้างความสับสนให้กับการพัฒนาหน่วยงานไซเบอร์แล้ว ดังนั้นจึงจำเป็นต้องกำหนดหน้าที่และแบ่งขอบเขตงานที่มีความคาบเกี่ยวหรือทับซ้อนกันให้มีความชัดเจน โดยเริ่มจากการนำความหมายของไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ภัยคุกคามทางไซเบอร์ ตลอดจนความหมายที่เกี่ยวข้องในเรื่องอื่นๆ มาขยายผลสร้างความเข้าใจร่วมกันในขั้นต้นก่อน

นอกจากการสร้างความเข้าใจความหมายของไซเบอร์แล้ว ที่สำคัญคือการสร้างความเข้าใจเรื่องขอบเขตงานไซเบอร์ในแต่ละระดับ โดยเฉพาะขอบเขตงานไซเบอร์ของกองทัพว่าจะให้มีฐานะเป็นกรมฝ่ายกิจการพิเศษที่เป็นอยู่ในปัจจุบัน หรือจะสร้างหน่วยปฏิบัติขึ้นภายในหน่วยงานไซเบอร์สำหรับการจัดออกไปสนับสนุนการปฏิบัติการไซเบอร์ในแต่ละระดับตั้งแต่ระดับชาติลงมาจนถึงระดับกองกำลังทางยุทธวิธี หรือจะจัดตั้งหน่วยงานไซเบอร์ขึ้นประจำในหน่วยต่างๆ ซึ่งถ้ายังกำหนดขอบเขตงานไซเบอร์ที่ชัดเจนไม่ได้ก็ย่อมส่งผลทำให้การพัฒนาในด้านต่างๆ เป็นไปอย่างไร้ทิศทางหรือเป็นไปได้อย่างจำกัดในขณะที่ขอบเขตงานไซเบอร์ทั้งระดับชาติและในกองทัพมิตรประเทศได้ขยายตัวไปอย่างรวดเร็ว

1.2 การจัดฝ่ายอำนวยการทางทหารรับผิดชอบระบบงานไซเบอร์

ปัญหาความไม่ชัดเจนในการพัฒนาหน่วยงานไซเบอร์คือการจัดฝ่ายอำนวยการทางทหารรับผิดชอบระบบงานไซเบอร์ซึ่งในปัจจุบันยังคงจัดอยู่ในสายงานยุทธการ ในขณะที่กองทัพมิตรประเทศได้จัดให้งานด้านการสื่อสาร ไซเบอร์ สารสนเทศ และการปฏิบัติการข่าวสารแยกออกเป็นกรมฝ่ายเสนาธิการโดยเฉพาะ การรวมระบบงานดังกล่าวให้อยู่ในกรมยุทธการของแต่ละเหล่าทัพทำให้เกิดปัญหาด้านการพัฒนาเนื่องจากงานด้านการปฏิบัติการไซเบอร์เป็นงาน

เร่งด่วนเช่นเดียวกับการปฏิบัติการทางทหารอื่นๆ ในขณะเดียวกันหน่วยงานไซเบอร์จำเป็นต้องได้รับการพัฒนาในหลายด้านไปพร้อมกัน หากแต่สายงานยุทธการมีภารกิจมาก งานด้านไซเบอร์จึงถูกจัดอยู่ในความเร่งด่วนลำดับท้ายๆ จึงสมควรแยกสายงานในกลุ่มนี้ออกแล้วสร้างความเชื่อมโยงให้เข้ากับระบบกรมฝ่ายเสนาธิการต่างๆ ซึ่งจากการที่มีกรมฝ่ายเสนาธิการรับผิดชอบโดยตรงย่อมจะทำให้มีประสิทธิภาพมากกว่า

1.3 ความแตกต่างภายในกระทรวงกลาโหม

ผลการวิเคราะห์สรุปปัญหาสำคัญประการหนึ่งซึ่งพบได้ในการพัฒนาระบบงานในกระทรวงกลาโหมคือความพยายามที่จะออกแบบระบบทุกเหล่าทัพให้มีความเหมือนกัน ซึ่งไม่มีทางเป็นไปได้ เพราะตามทฤษฎีองค์การแล้วระบบย่อยภายในเหล่าทัพ ออกแบบมาเพื่อตอบสนองการปฏิบัติงานของเหล่าทัพนั้นๆ ในเมื่อหน้าที่ของแต่ละเหล่าทัพมีความแตกต่างกันตามที่ปรากฏในพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม ย่อมทำให้ระบบงานย่อยมีความแตกต่างกันไปด้วยและเป็นความแตกต่างที่มีความเป็นสากล ผลจากหลักการดังกล่าวทำให้การจัดหน่วยงานของสำนักงานปลัดกระทรวงกลาโหมและกองบัญชาการกองทัพไทย หน่วยไซเบอร์จะเป็นหน่วยขึ้นตรง ในขณะที่กองทัพเรือและกองทัพอากาศหน่วยไซเบอร์เป็นกรมฝ่ายกิจการพิเศษรวมอยู่กับหน่วยสื่อสาร ส่วนกองทัพบกได้แยกหน่วยไซเบอร์ออกมาจากหน่วยสื่อสารและขึ้นตรงกับกองทัพบก

1.4 ความแตกต่างของส่วนราชการพลเรือนและทหาร

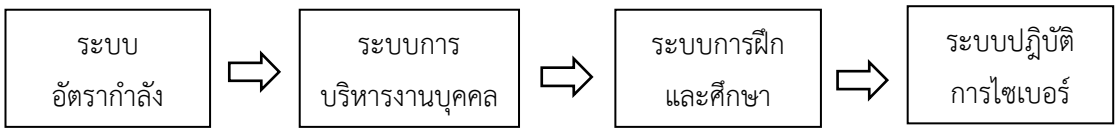
ผลการวิเคราะห์สรุปได้ว่าถึงแม้การรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศจะมีกฎหมายและกระทรวงที่รับผิดชอบแล้ว แต่ความแตกต่างที่สำคัญคืองานไซเบอร์ของพลเรือนมีเพียงการรักษาความมั่นคงปลอดภัยจากภัยคุกคามไซเบอร์ ในขณะที่งานไซเบอร์ของกองทัพมีความมุ่งหมายสำคัญในการสนับสนุนการปฏิบัติการทางทหารให้บรรลุผลสำเร็จ รวมถึงมีขีดความสามารถในการเป็นภัยคุกคามต่อฝ่ายตรงข้ามซึ่งไม่ได้กำหนดไว้ในกฎหมายใดๆ แต่เป็นส่วนที่กองทัพต้องกำหนดขึ้นมาเอง ดังนั้น การที่จะพัฒนาหน่วยงานไซเบอร์ให้มีขีดความสามารถในเรื่องดังกล่าวได้นั้น ต้องสร้างความเข้าใจในความแตกต่างของภารกิจ ไม่เช่นนั้นแล้วจะทำให้มุมมองที่มีต่อกองทัพเป็นการทำเกินภาระหน้าที่ตามที่กำหนดไว้ในกหมายทั้งนี้ อาจต้องรวบรวมแนวคิดจากกองทัพมิตรประเทศนำมาประยุกต์และกำหนดเป็นหลักนิยมด้านไซเบอร์ของกองทัพให้ชัดเจนเพื่อเป็นหลักในการพัฒนาหน่วยไซเบอร์ในกองทัพต่อไป

2. การพัฒนาระบบที่เกี่ยวข้อง

ผลการวิเคราะห์สรุปว่าหลังจากการสร้างความเข้าใจให้ตรงกันในเรื่องบทบาทและหน้าที่ของหน่วยไซเบอร์ในกองทัพแล้ว จะต้องนำมาพัฒนาระบบงานให้รองรับ โดยเริ่มจากการพัฒนาระบบอัตรากำลังในรูปแบบของ อจย. และ อฉก.ซึ่งประกอบด้วยตอนต่างๆ เพื่อนำไปเป็นหลักใน

ระบบการบริหารทรัพยากรบุคคล ระบบการฝึกและศึกษา และการปฏิบัติการไซเบอร์ โดยทุกระบบมีความต่อเนื่องกันตามทฤษฎีระบบจึงไม่สามารถเว้นระบบใดระบบหนึ่งได้ตามแผนภาพที่ 5–1

แผนภาพที่ 5 - 1 การพัฒนาระบบที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์



2.1 ระบบอัตรากำลัง

ผลการวิเคราะห์สรุปว่าระบบอัตรากำลังเป็นจุดเริ่มต้นของทุกองค์การเพื่อนำไปสู่ความสำเร็จในการปฏิบัติงาน รวมถึงการปฏิบัติการไซเบอร์ระบบอัตรากำลังที่ดีจะทำให้หน่วยไซเบอร์มีหน้าที่ที่ชัดเจนและมีโครงสร้างการจัดที่เหมาะสมในการปฏิบัติหน้าที่ และเป็นจุดเริ่มต้นให้กับระบบการบริหารงานบุคคล อย่างไรก็ตามเนื่องจากกองทัพบกไทยยังมีปัญหาในเรื่องอัตรากำลังเนื่องจากได้นำมาจากกองทัพสหรัฐอเมริกามานานกว่า 60 ปี จึงจำเป็นต้องกำหนดเหล่าและหมายเลขชำนาญการทางทหารในแต่ละตำแหน่งให้ชัดเจน รวมถึงการแยกอัตรากำลังข้าราชการพลเรือนออกจากอัตรากำลังทหารเพื่อให้สอดคล้องกับหน่วยไซเบอร์ที่ต้องการพลเรือนที่มีความรู้ความเชี่ยวชาญทางเทคนิคจำนวนมาก

2.2 ระบบการบริหารงานบุคคล

ผลการวิเคราะห์สรุปว่าการบริหารงานบุคคลที่ดีจะทำให้กองทัพสามารถบรรจุกำลังพลที่เหมาะสมตามหน้าที่ที่กำหนดไว้ในแต่ละตำแหน่ง ทำให้ในระดับบุคคลมีความพร้อมในการปฏิบัติหน้าที่ ซึ่งส่งผลทำให้ระดับหน่วยมีความพร้อมตามไปด้วย และทำให้เหล่าทัพสามารถปฏิบัติหน้าที่ตามกฎหมายได้นอกจากการบริหารงานบุคคลจะส่งผลโดยตรงกับการปฏิบัติงานของหน่วยแล้วยังทำให้การบริหารจัดการด้านการฝึกและศึกษาเป็นไปอย่างมีประสิทธิภาพและประหยัดงบประมาณที่จะต้องใช้ในการจัดการฝึกและศึกษาให้ตรงกับความต้องการอย่างแท้จริงอีกด้วย

กองทัพไทยควรปรับระบบการบริหารงานบุคคลใหม่โดยใช้ระบบการบริหารงานบุคคลแบบรวมการไว้ที่กองบัญชาการเหล่าทัพซึ่งจะทำให้กองทัพสามารถบริหารจัดการกำลังพลได้ทั้งระบบรวมถึงการฝึกและศึกษา ซึ่งปัญหาในปัจจุบันของกองทัพไทยคือการมอบอำนาจการบริหารงานบุคคลให้กับหน่วยขึ้นตรงเหล่าทัพทำให้กองทัพไม่สามารถควบคุมการบริหารจัดการได้และส่งผลกระทบต่อการพัฒนาหน่วยงานไซเบอร์

2.3 การพัฒนาระบบการฝึกและศึกษา

ระบบการฝึกและศึกษาเป็นเรื่องที่ต่อเนื่องมาจากการบริหารงานบุคคลบ่อยครั้งที่ถูกรวมเข้าไว้ในระบบการบริหารงานบุคคล ซึ่งเป็นเรื่องสำคัญที่จะทำให้กำลังพลมีความพร้อมปฏิบัติงานในแต่ละตำแหน่ง จากการที่หน่วยงานไซเบอร์เพิ่งได้รับการจัดตั้งการพัฒนาหลักสูตรการฝึกและศึกษาในสายงานไซเบอร์จึงยังคงมีข้อจำกัด นอกจากการฝึกเป็นบุคคลโดยการจัดให้เข้ารับการฝึกอบรมตามหลักสูตรแล้ว ยังจำเป็นต้องทำการฝึกรวมกันทั้งหน่วยและการฝึกกับหน่วยอื่นซึ่งอาจรวมถึงส่วนราชการพลเรือนที่อยู่ในโครงสร้างพื้นฐานไซเบอร์อีกด้วย

ผลจากการวิจัยสรุปว่าการพัฒนาหน่วยงานไซเบอร์รองรับยุทธศาสตร์ชาติด้านความมั่นคงนั้น จำเป็นต้องพัฒนาระบบที่เกี่ยวข้องไปพร้อมกันตามที่กล่าวมาได้แก่ ระบบอัตรากำลัง ระบบการบริหารงานบุคคล และระบบการฝึกและศึกษา แต่เนื่องจากทั้งสามระบบของกองทัพบกไทยอยู่ในระหว่างการพัฒนา จึงสมควรพัฒนาในส่วนที่เกี่ยวข้องกับไซเบอร์ไปพร้อมกัน

ข้อเสนอแนะ

การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยเป็นเรื่องที่เกี่ยวข้องกับหลายฝ่าย ซึ่งมีสาเหตุมาจากการยกระดับการปฏิบัติการทางทหารให้สอดคล้องกับการพัฒนาทางด้านเทคโนโลยีสารสนเทศ จึงทำให้บทบาทของงานด้านไซเบอร์ซึ่งเคยเป็นงานย่อยของระบบงานด้านสื่อสารและอยู่ในฐานะฝ่ายกิจการพิเศษ (Special Staff) ที่มีภารกิจเฉพาะด้านถูกยกระดับมาเป็นงานหลักในกรอบการปฏิบัติการทางทหาร (Military Operations) ส่งผลให้ต้องเกี่ยวข้องกับทุกสายงานฝ่ายอำนวยการและทุกหน่วยปฏิบัติดังนั้น การพัฒนาจึงจำเป็นต้องดำเนินการในทุกระดับ โดยผลการวิจัยสามารถสรุปข้อเสนอแนะได้ดังนี้

2.1 การพัฒนาความรู้กำลังพลทุกนายตลอดจนผู้บังคับบัญชาทุกระดับชั้น ให้ตระหนักถึงความสำคัญของงานด้านการปฏิบัติการไซเบอร์ในการปฏิบัติการทางทหารสมัยใหม่รวมถึงให้เข้าใจงานที่เกี่ยวข้องในกลุ่มงานเดียวกันได้แก่ การสื่อสาร การปฏิบัติการข่าวสาร การสารสนเทศ ตลอดจนงานในระบบการควบคุมบังคับบัญชาอื่นๆเพื่อนำไปสู่ความเข้าใจร่วมกันในการกำหนดบทบาท หน้าที่ของหน่วยงานไซเบอร์ การพัฒนาเสริมสร้างหน่วยงานไซเบอร์ ตลอดจนการกำหนดความสัมพันธ์กับระบบงานอื่นในกองทัพให้มีความชัดเจน

2.2 พัฒนาระบบอื่นในกลุ่มงานที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ตามข้อ 2.1ได้แก่ การสื่อสาร การปฏิบัติการข่าวสาร การสารสนเทศโดยแยกหน้าที่ให้มีความชัดเจนและมีความประสานสอดคล้องเชื่อมโยงกันอย่างเป็นระบบตามหลักการจัดกลุ่มงานที่มีความเชื่อมโยงในระดับเดียวกันเข้าไว้ด้วยกัน

2.3 พัฒนาระบบฝ่ายอำนวยการทางทหาร ให้มีความพร้อมในการปฏิบัติการทางทหารเช่นเดียวกับการปฏิบัติการทางทหารแบบอื่นโดยเฉพาะการขยายขอบเขตกรมฝ่ายเสนาธิการในระดับ

กองบัญชาการกองทัพบกขึ้นไปให้มีกรมฝ่ายเสนาธิการ (G-6 Army Staff) ที่รับผิดชอบโดยตรงแยกออกจากกรมฝ่ายยุทธการ (G-3 Army Staff) เช่นเดียวกับกองทัพมิตรประเทศทั้งในและนอกอาเซียน

2.4 พัฒนาความเชื่อมโยงของระบบการปฏิบัติการไซเบอร์ของกองทัพบกให้มีความเชื่อมโยงกับทุกหน่วยในกระทรวงกลาโหม ตลอดจนบทบาทของกองทัพบกในระดับประเทศเช่นเดียวกับกองทัพมิตรประเทศทั้งในยามปกติในบทบาทการสนับสนุนฝ่ายพลเรือนต่อความมั่นคงรูปแบบใหม่ และในยามสงครามเพื่อสนับสนุนการปฏิบัติการทางทหาร

2.5พัฒนาระบบโครงสร้างอัตรากำลังหน่วยงานด้านไซเบอร์ให้มีทั้งองค์การทางดิ่งซึ่งเป็นอัตราทหารเพื่อสนับสนุนงานการปฏิบัติการทางทหารและองค์การทางราบซึ่งเป็นอัตราพลเรือนเพื่อสนับสนุนงานทางเทคนิคที่มีความชำนาญเฉพาะด้าน เป็นการชดเชยจุดอ่อนของการจัดองค์การแต่ละแบบและสามารถตอบสนองการปฏิบัติการด้านไซเบอร์ได้

2.6 พัฒนาระบบการบริหารงานบุคคลโดยเฉพาะในเรื่องมาตรฐานการกำหนดตำแหน่งและแนวทางการรับราชการในตำแหน่งที่มีความชำนาญเฉพาะ ตลอดจนระบบการฝึกและศึกษาทางด้านไซเบอร์ให้สามารถสนับสนุนการปฏิบัติการไซเบอร์ได้อย่างมีประสิทธิภาพ

2.7เผยแพร่ทำความเข้าใจในเรื่องความแตกต่างระหว่างส่วนราชการภายในกระทรวงกลาโหม ทั้งความแตกต่างทางดิ่งตามหลักระดับการปฏิบัติการทางทหารทางยุทธศาสตร์ ยุทธการและยุทธวิธี และความแตกต่างทางระดับระหว่างเหล่าทัพตามคุณสมบัติของเหล่าที่เป็นสากล โดยกองทัพบกจะมุ่งเน้นไปที่การฝึกกำลังพลจำนวนมากเพื่อเข้าปฏิบัติการเป็นหน่วยขนาดใหญ่จึงมุ่งเน้นไปที่การปฏิบัติการไซเบอร์ของหน่วยทางยุทธวิธีในขณะที่กองทัพเรือและกองทัพอากาศเป็นการปฏิบัติงานของยุทโธปกรณ์ที่มีเป้าหมายระดับยุทธศาสตร์จึงมีการให้ความรู้แก่กำลังพลทางด้านเทคนิคอย่างต่อเนื่อง เพื่อมุ่งเน้นการปฏิบัติการไซเบอร์ในระดับสูง

2.8นำระบบข้าราชการพลเรือนกลาโหมมาใช้ในกระทรวงกลาโหมให้เป็นรูปธรรมเพื่อให้สามารถสร้างบุคลากรด้านไซเบอร์ที่มีความเชี่ยวชาญเฉพาะด้านได้ โดยการจัดการฝึกและศึกษาให้เหมาะสมกับงานของข้าราชการแต่ละประเภท ซึ่งจะทำให้สามารถบริหารจัดการทรัพยากรที่มีจำกัดให้มุ่งไปสู่ตำแหน่งที่ปฏิบัติงานจริงโดยไม่ต้องย้ายออกจากสายงานเมื่อมีการปรับชั้นยศใหม่ตามข้อจำกัดของอัตราทหาร

2.9สร้างความเข้าใจต่อหน่วยงานภายนอกในด้านความแตกต่างระหว่างกองทัพกับส่วนราชการพลเรือนโดยเฉพาะกองทัพเป็นองค์การที่ออกแบบมาเพื่อปฏิบัติหน้าที่ทางทหาร ดังนั้นระบบงานบางระบบรวมถึงระบบงานไซเบอร์ในบางเรื่องจำเป็นต้องมีการยกเว้นกฎ ระเบียบ การปฏิบัติเพื่อตอบสนองความต้องการเฉพาะของกองทัพในภาพรวมซึ่งเป็นความแตกต่างที่เป็นสากลเหมือนกันในทุกประเทศ

บรรณานุกรม

ภาษาไทย

เอกสารที่มีชั้นความลับ

เอกสารไม่ตีพิมพ์

กรมยุทธการทหารบก. “หนังสือ ลับ ด่วนมาก ที่ กห 0403/1074 เรื่องขออนุมัติจัดตั้งศูนย์ไซเบอร์กองทัพบก โดยการแปรสภาพหน่วย ศทท.”. ลงวันที่ 19 กันยายน 2559.

กระทรวงกลาโหม, “แผนแม่บทไซเบอร์ เพื่อการป้องกันประเทศกระทรวงกลาโหม (พ.ศ.2560-2564)”. 2559.

กองทัพบก. “แผนแม่บทไซเบอร์กองทัพบก พ.ศ.2560-2564”. 2560.

ศูนย์ไซเบอร์กองทัพบก. "คำสั่งศูนย์ไซเบอร์กองทัพบก (เฉพาะ) ที่ 1/59 เรื่องกำหนดหน้าที่และอัตรากำลังพลอัตราเฉพาะกิจ หมายเลข 2900 ศูนย์ไซเบอร์กองทัพบก". ลงวันที่ 3 ตุลาคม 2559.

เอกสารที่ไม่มีชั้นความลับ

หนังสือ

จุลชีพ ชินวรรโณ.“สหรัฐอเมริกากับประเทศไทยในบริบทของความมั่นคงร่วมกันในเอเชียอาคเนย์”, ใน เส้นทางมหาอำนาจ : เอกสารด้านนโยบายต่างประเทศอเมริกาต่อเอเชีย.กรุงเทพ : โครงการจัดพิมพ์คบไฟ, 2544.หน้า 271.

ศุภชัย เยาวะประภาษ.การบริหารงานบุคคลภาครัฐไทย; กระแสใหม่และสิ่งท้าทาย. พิมพ์ครั้งที่ 2, กรุงเทพ : จุดทอง, 2548. หน้า 27, 119-120.

สัมภาษณ์

นพดล แก้วกำเนิด, พันเอก, ผู้อำนวยการกองเทคโนโลยีสารสนเทศและการสื่อสาร สำนักปฏิบัติการ กรมยุทธการทหารบก. สัมภาษณ์.6 มิถุนายน 2562.

นพนันต์ ชั้นประดับ, พลตรี, นายทหารฝ่ายเสนาธิการ กรมยุทธการทหารบก. สัมภาษณ์. 7มิถุนายน 2562.

บรรยาย

นริส ประทุมสุวรรณ, พลเรือเอก, ผู้บัญชาการทหารเรือ. “คำกล่าวเนื่องในโอกาสเปิดศูนย์ไซเบอร์ สสท.ทร.”, ณ กองบัญชาการทหารเรือ, 9 กรกฎาคม 2561.

กฎหมาย

“ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ.2561 - 2580)”, ราชกิจจานุเบกษา. เล่มที่ 135, 13 ตุลาคม 2561, หน้า 3-16.

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562”, ราชกิจจานุเบกษา. เล่มที่136, 27 พฤษภาคม2562, หน้า 21-22, 51.

“พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. 2551”. ราชกิจจานุเบกษา. เล่มที่ 125, 1 กุมภาพันธ์ 2551, หน้า 43.

“ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติพ.ศ. 2552”, ราชกิจจานุเบกษา. เล่มที่ 126, 13 มีนาคม 2552, หน้า 4-6.

ก.จ.ช. เอกสาร ร.5 ก.13.2/37 สำเนา ที่ 31/17914 กรมหมื่นนครไชยศรีสุรเดช กราบบังคมทูลพระบาทสมเด็จพระเจ้าอยู่หัว ลง วันที่ 4 กุมภาพันธ์ ร.ศ.126 (พ.ศ.2452).

ราชกิจจานุเบกษา เล่มที่ 26 น่า 1103 วันที่ 22 สิงหาคม ร.ศ.128.

ศาลายุทธนาธิการ ข้อบังคับกรมทหารบก คำสั่งที่ 2 ว่าด้วยน่าที่ของออฟฟิศเซอบังคับทหารรักษาราชการตามหัวเมือง จุลศักราช 1249.

เอกสารไม่ตีพิมพ์

กรมยุทธการทหารบก. “หนังสือ ยก.ทบ. ที่ กห 0403/5946 เรื่อง สรุปผลการประชุมคณะอนุกรรมการนโยบายและมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร ทบ. ครั้งที่ 1/61”. ลงวันที่ 30 เมษายน 2561.

กองทัพบก. “แผนพัฒนากองทัพบก ปี 2560 – 2564”. 2560.

ไทยเซิร์ต. “2016 ThaiCERT Annual Report”. (รายงานประจำปี. 2559). p.12.

สำนักงานเลขาธิการคณะรัฐมนตรี. “หนังสือด่วนที่สุด ที่ นร 0505/ว.187”.ลงวันที่13 พฤษภาคม 2562.

ฐานข้อมูลอิเล็กทรอนิกส์

กรมการทหารสื่อสาร. “กำเนิดกรมการทหารสื่อสาร”.(ออนไลน์). เข้าถึงได้จาก :http://signal.rta.mi.th/web/history.php, 2559.

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. “ภารกิจ”. (ออนไลน์). เข้าถึงได้จาก :http://www.dict.rtaf.mi.th/index.php/2017-02-01-01-28-28/2017-02-01-01-53-22, 2559.

ศูนย์ไซเบอร์กองทัพบก. “ศูนย์ไซเบอร์กองทัพบก”. (ออนไลน์). เข้าถึงได้จาก :http://cyber.rta.mi.th, 2560.

ศูนย์ไซเบอร์ทหาร, “Cyber Security Center, Royal Thai Armed Forces”. (CD-ROM), 2561.

ศูนย์ไซเบอร์ ทสอ.กห.“หน่วยขึ้นตรง”.(ออนไลน์). เข้าถึงได้จาก : http://csc.dist.mod.go.th, 2561.

ภาษาต่างประเทศ

Books

Art, Robert J. and Jervis, Robert. "The fungibility of force”, inInternational politics: Enduring concepts and contemporary issues. (New York : Pearson, 2009). p.205

Dessler, Gary Human Resource Management, 12th ed., (New Jersey : Pearson, 2011). p.179-332-348.

Gray, Colin S. Modern Strategy. (New York : Oxford University press, 1999). p.17, 58.

Grote, Dick The performance appraisal question and answer book : A survival guide for managers, (New York : American Management Association, 2002)

Maitland,Iain How to recruit. (England : Gower, 1991), p.3-11.

Mintzberg, Henry. Structure in Fives: Designing Effective Organizations. (New Jersey : Prentice-Hall, 1983). p.283-284.

Thompson, James D.“Organizations in Action”,inClassics of Organization Theory. J. M. Shafritz; and others. (California : Thomson/Wadsworth, 2005), p.499-450.

Weber, Max. “Bureaucracy”, in Classics of Organization Theory. J. M. Shafritz and others. (California : Thomson/Wadsworth, 2005). p.73-74.

Lecture, Speech

Graff, Itamar and Sharabi,Barak “Cyber Security Solutions”.(Paper Presented at Cyber Security Solution Seminar by Israel. 2016).

Non-Published Document

Department of the Army. “FIELD MANUAL 11-45 Signal Support to Theater Operations”. (Field Manual. 1999).

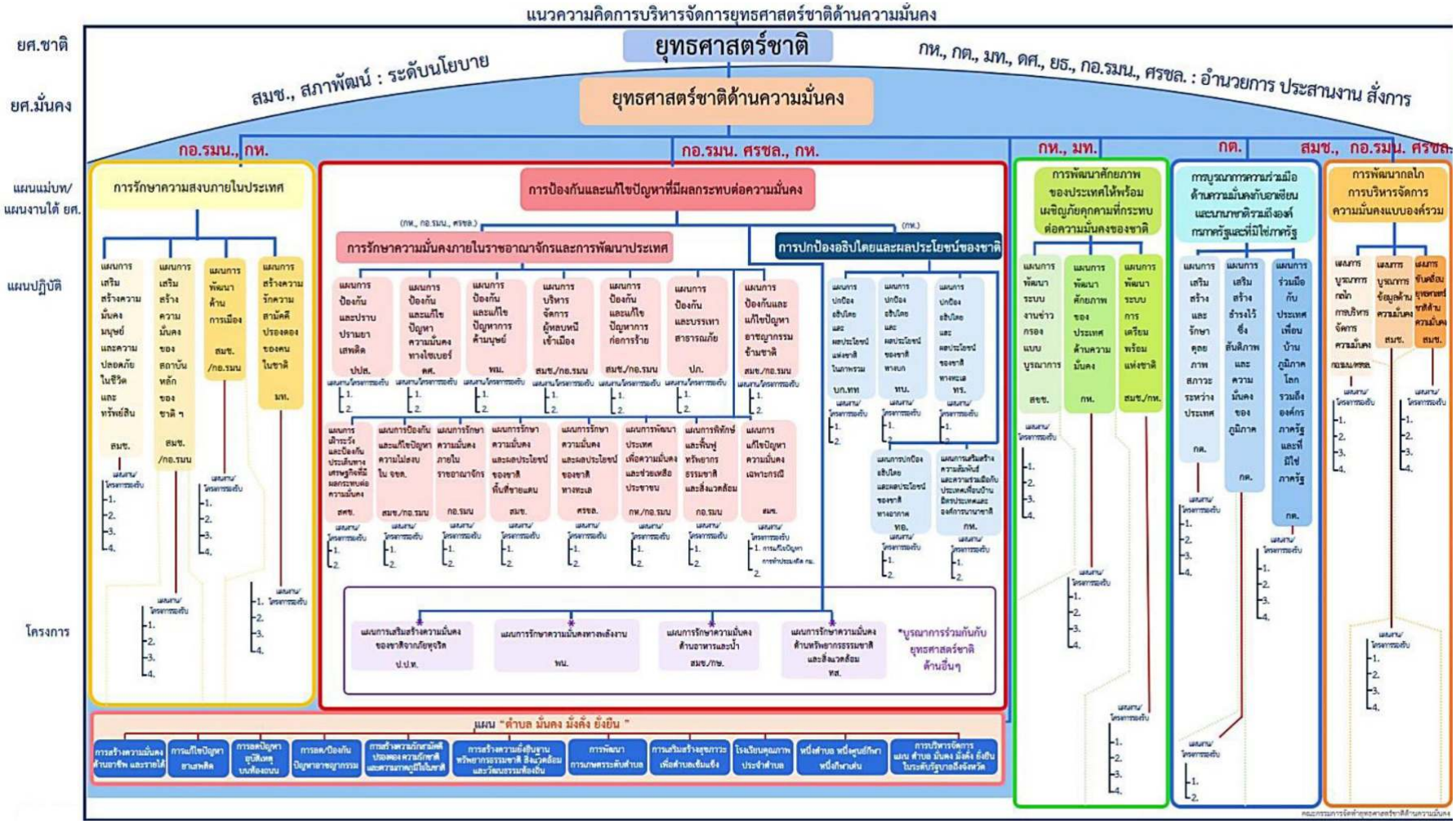
The U.S. Army. “The Army Strategy”. (Headquarters, Deputy Chief of Staff, G-3-5-7. 2018). p.1,8.

U.S. Strategic Command. “Joint Publication 3-12 Cyberspace Operations”. (Joint Publication. 2018). p.I-1.

ภาคผนวก

ผนวก ก

แนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง



ที่มา: ประกาศสำนักนายกรัฐมนตรี เรื่อง การประกาศแผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ.2561-2580)”,ราชกิจจานุเบกษา. เล่มที่ 136, 18 เมษายน 2562, หน้า 5.

ผนวก ข
หลักสูตรอบรมทางไซเบอร์ของเหล่าทัพและ ทสอ.กห.

หน่วยจัดการอบรม	ชื่อหลักสูตร	ห้วงอบรม	จำนวนผู้เข้ารับการอบรม
ศซบ.ทหาร	1. การฝึกอบรมเพิ่มพูนความรู้ทางด้านไซเบอร์ 2. หลักสูตรปรับพื้นฐานบุคลากรด้านไซเบอร์ 3. หลักสูตรนายทหารรักษาความมั่นคงปลอดภัยไซเบอร์ นขต.บก.ทท.	เดือน ก.พ. - พ.ค. 62 30 ม.ค.- 24 พ.ค.62 3 มิ.ย. - 5 ก.ค. 62	เปิดอบรม 5 ครั้ง ครั้งละ 30 นาย
ศซบ.ทบ.	1. หลักสูตรการปฏิบัติการไซเบอร์ชั้นต้น 2. หลักสูตรการปฏิบัติการไซเบอร์ชั้นสูง	17 - 21 ธ.ค. 61 4 - 8 ก.พ. 61	40 นาย 40 นาย
ศซบ.ทร.	หลักสูตรเจ้าหน้าที่ดูแลระบบเครือข่าย	22 ต.ค. - 9 พ.ย. 61	15 นาย
ทสส.ทอ.	หลักสูตรนายทหารรักษาความปลอดภัยไซเบอร์	ปีงบประมาณ 63 (ยังไม่กำหนดห้วง)	ยังไม่กำหนด
ศซบ.ทสอ.กห.	Digital Forensics	ปีงบประมาณ 62 (ยังไม่กำหนดห้วง)	15 - 30 นาย

ประวัติย่อผู้วิจัย

ชื่อ – นามสกุล : พลตรี มานพ สัมมาขันธ์
Major General Manop Summakhan

วันเดือน ปี เกิด : 8เมษายน2507

การศึกษาพลเรือน:

- โรงเรียนอยุธยาวิทยาลัย
- โรงเรียนเตรียมทหาร
- โรงเรียนนายร้อยพระจุลจอมเกล้า (วิทยาศาสตรบัณฑิต)
- สถาบันบัณฑิตพัฒนบริหารศาสตร์ - นิด้า (วิทยาศาสตรมหาบัณฑิต)

การศึกษาทางทหาร :

- หลักสูตรชั้นนายร้อยเหล่าทหารปืนใหญ่
- หลักสูตรชั้นนายพันเหล่าทหารปืนใหญ่
- หลักสูตรหลักประจำโรงเรียนเสนาธิการทหารบก
- หลักสูตรนายทหารปลัดบัญชี

ประวัติการทำงาน :

- ผู้บังคับกองร้อย กองพันทหารปืนใหญ่ที่ 21 รักษาพระองค์
- ผู้บังคับกองพันทหารปืนใหญ่ที่ 2 รักษาพระองค์
- ผู้บังคับกองพันทหารปืนใหญ่ที่ 21 รักษาพระองค์
- เสนาธิการกรมทหารปืนใหญ่ที่ 2 รักษาพระองค์
- รองผู้บังคับการกรมทหารปืนใหญ่ที่ 2 รักษาพระองค์
- รองผู้อำนวยการศูนย์ไซเบอร์กองทัพบก

ตำแหน่งปัจจุบัน :

- ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก

- ผู้อำนวยการศูนย์ดิจิทัลเพื่อความมั่นคง กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยรองรับยุทธศาสตร์ชาติด้านความมั่นคง

ผู้วิจัย พลตรี มานพ สัมมาขันธ์ **หลักสูตร** วปอ. **รุ่นที่** 61

ตำแหน่ง ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก

ความเป็นมาและความสำคัญของปัญหา

ยุทธศาสตร์ชาติด้านความมั่นคง เป็น 1 ใน 6 ยุทธศาสตร์ซึ่งถูกกำหนดอยู่ในยุทธศาสตร์ชาติ 20 ปี (พ.ศ.2561-2580)ได้กล่าวถึงประเด็นเรื่องการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง และหนึ่งในภัยคุกคามที่สำคัญ คือ อาชญากรรมทางไซเบอร์ และรูปแบบการก่อสงครามที่ใช้เทคโนโลยีเป็นเครื่องมือ นอกจากนี้ ยังมีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งมีผลบังคับใช้กับทุกส่วนราชการ เพื่อป้องกันภัยคุมคามทางไซเบอร์ซึ่งเป็นภัยคุกคามรูปแบบใหม่และทวีความรุนแรงขึ้น กองทัพไทยซึ่งเป็นหน่วยงานที่มีหน้าที่รักษาความมั่นคงของประเทศ รวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงต้องมีการพัฒนาระบบงานไซเบอร์ขึ้นเพื่อรองรับภารกิจ แต่หลังจากปฏิบัติงานไปได้ระยะหนึ่งพบว่าความก้าวหน้าของงานไซเบอร์ยังไม่ดีเท่าที่ควรยังมีข้อจำกัดอีกหลายด้านที่ยังไม่ได้ดำเนินการพัฒนาไปพร้อมการจัดตั้งหน่วยงานไซเบอร์ คาดว่ามีสาเหตุ 3 ประการ คือ

1. อาจเกิดจากงานไซเบอร์ได้ถูกแยกมาจากงานด้านการสื่อสารด้วยวิธีการแยกหน่วยรองมาจัดตั้งเป็นหน่วยใหม่เพื่อรองรับงานไซเบอร์ ในขณะที่ระบบงานสื่อสารเดิมก็ยังไม่ได้รับการปรับบทบาทหรือกำหนดขอบเขตหน้าที่ความรับผิดชอบงานให้ชัดเจน จึงทำให้เกิดปัญหาความซ้ำซ้อนและความไม่ชัดเจนในการเชื่อมโยงระบบงานตั้งแต่ภารกิจ ขอบเขตหน้าที่และความรับผิดชอบที่สำคัญในอัตรา ซึ่งส่งผลกระทบถึงการจัดโครงสร้างอัตรากำลัง และการบริหารงานบุคคล รวมถึงการปฏิบัติภารกิจต่างๆ

2. การจัดฝ่ายอำนวยการรับผิดชอบงานไซเบอร์ในระดับเหล่าทัพขึ้นไปยังขาดความชัดเจนเนื่องจากระบบงานกรมฝ่ายเสนาธิการของกองทัพไทยยังคงยึดถือตามระบบเดิมที่แบ่งออกเป็น 6 สายงาน ได้แก่ สายงานกำลังพล สายงานข่าว สายงานยุทธการ สายงานส่งกำลังบำรุง สายงานกิจการพลเรือน และสายงานปลัดบัญชี ส่งผลทำให้งานด้านไซเบอร์ งานด้านการสื่อสาร และงานด้านสารสนเทศยังคงรวมอยู่ในความรับผิดชอบของสายงานยุทธการหรือกรมยุทธการของ

เหล่าทัพและกองบัญชากองทัพไทยซึ่งมีภาระหน้าที่เร่งด่วนจำนวนมาก ทำให้ความเร่งด่วนในการพัฒนาหน่วยงานไซเบอร์ถูกให้ความสำคัญเป็นลำดับท้ายๆ

3. กองทัพบกก็เป็นส่วนราชการหนึ่งที่จะต้องปฏิบัติตามกฎหมาย ระเบียบ ที่กำหนดให้ทุกส่วนราชการปฏิบัติ แต่ในความเป็นจริงแล้วกองทัพมีความมุ่งหมายในการจัดตั้งที่แตกต่างไปจากพลเรือนโดยเฉพาะต้องปฏิบัติตามหลักนิยมเพื่อสนับสนุนการปฏิบัติการทางทหารซึ่งแบ่งออกเป็นการปฏิบัติการไซเบอร์เชิงรุก (Offensive Cyber Operations)และการปฏิบัติการไซเบอร์เชิงรับ (Defensive Cyber Operations) ในขณะที่กฎหมายของฝ่ายพลเรือนมีเพียงเฉพาะการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เท่านั้น ซึ่งจะมีความคล่องตัวกว่าทางทหาร

กองทัพไทยมุ่งไปที่การจัดตั้งหน่วยไซเบอร์เพื่อรองรับงาน แต่ไม่ได้ปรับปรุงระบบงานอื่นๆ ให้สอดคล้องกันไปด้วย จากสาเหตุข้างต้น ทำให้กองทัพขาดความชัดเจนในเรื่องโครงสร้างการจัดอัตรากำลังหน่วยงานไซเบอร์จึงจำเป็นต้องศึกษาวิจัยการพัฒนาหน่วยงานด้านไซเบอร์ เพื่อให้รองรับงานตามยุทธศาสตร์ชาติได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาหน่วยงานด้านไซเบอร์ของกองทัพบกไทย ในด้านความเหมาะสม ความเพียงพอที่จะสามารถรองรับภัยคุกคามด้านไซเบอร์ตามยุทธศาสตร์ชาติด้านความมั่นคง

2. เพื่อศึกษาความเชื่อมโยงระหว่างระบบไซเบอร์กับระบบที่เกี่ยวข้องซึ่งขยายมาจากกลุ่มงานของกองทัพบกเดิม ได้แก่ ระบบสื่อสาร ระบบสารสนเทศ ระบบปฏิบัติการข้อมูลข่าวสาร และระบบควบคุมบังคับบัญชา

3. เพื่อศึกษาการพัฒนากำลังพลในหน่วยงานไซเบอร์ของกองทัพบกไทยให้สามารถรองรับยุทธศาสตร์ชาติด้านความมั่นคงได้

ขอบเขตของการวิจัย

การวิจัยนี้จะจำกัดขอบเขตระดับในการวิเคราะห์ (Level of Analysis) และหน่วยในการวิเคราะห์(Unit of Analysis) ที่ระดับกองทัพบกไทย เพื่อให้เหมาะสมกับข้อจำกัดด้านเวลาและระดับของเอกสารวิจัยในหลักสูตรวิทยาลัยป้องกันราชอาณาจักร โดยการจำกัดขอบเขตที่กองทัพบกดังกล่าวไม่ได้ส่งผลกระทบต่อการวิจัยข้ามระดับในการเชื่อมโยงถึงระดับยุทธศาสตร์ชาติด้านความมั่นคง เนื่องจากกองทัพบกไทยเป็นหน่วยปฏิบัติหลักด้านความมั่นคงของรัฐที่กำหนดในแผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคงด้วย และปัญหาของระบบงานไซเบอร์ของทุกส่วนราชการในกระทรวงกลาโหมจะคล้ายกัน ซึ่งการวิจัยจะได้อธิบายความเชื่อมโยงระหว่างระดับกระทรวงกลาโหม

กองบัญชาการกองทัพไทย และเหล่าทัพอื่นด้วยแล้วจึงสามารถนำผลการวิจัยที่ค้นพบไปอธิบายปรากฏการณ์ที่เกิดขึ้นกับส่วนราชการอื่นในกระทรวงกลาโหมได้

วิธีดำเนินการวิจัย

การวิจัยในครั้งนี้มุ่งเน้นไปที่โครงสร้างการจัดและระบบงานด้านไซเบอร์ ซึ่งจัดอยู่ในสาขาสังคมศาสตร์ที่เป็นปฏิสัมพันธ์ระหว่างคน โดยเป็นการวิจัยเพื่อหาข้อสรุปเชิงนโยบาย ดังนั้น จึงใช้ระเบียบวิธีวิจัยเชิงคุณภาพซึ่งมีความเหมาะสมกับวัตถุประสงค์ในการวิจัย โดยใช้การเก็บข้อมูลจากเอกสารที่เกี่ยวข้อง การสัมภาษณ์ผู้ให้ข้อมูลสำคัญที่มีประสบการณ์ในการปฏิบัติงาน และการสังเกตการณ์แบบมีส่วนร่วมของผู้วิจัย ร่วมกับการเก็บข้อมูลระบบงานไซเบอร์ของกองทัพไทยและส่วนราชการขึ้นตรง ระบบไซเบอร์ของประเทศไทย และประเทศอื่น รวมทั้งความเชื่อมโยงในด้านต่างๆ ที่เกี่ยวข้อง ได้แก่ การฝึกและศึกษาทางทหาร ระบบอัตรากำลัง และระบบการบริหารงานบุคคล แล้วนำข้อมูลที่ได้มาจัดระเบียบ ตีความ และสรุปผลออกมาเป็นข้อสรุปและข้อเสนอของการวิจัย

ผลการวิจัย

การที่จะพัฒนาหน่วยงานไซเบอร์ในกองทัพให้สามารถปฏิบัติภารกิจตามที่กำหนดไว้ในแผนแม่บทรองรับยุทธศาสตร์ชาติ (พ.ศ.2561-2580) ได้นั้น จำเป็นต้องสร้างความเข้าใจต่อทุกฝ่ายให้มีความรู้ในเรื่องไซเบอร์ก่อน หลังจากนั้นจึงจะทำให้การกำหนดหน้าที่ของหน่วยงานไซเบอร์ในกองทัพมีความชัดเจนในเรื่องบทบาท ภารกิจและหน้าที่เพื่อใช้ในการพิจารณาติดสินใจว่าควรเป็นเพียงกรมฝ่ายกิจการพิเศษดังเช่นปัจจุบัน หรือจัดตั้งให้เป็นหน่วยปฏิบัติงานด้านไซเบอร์อย่างสมบูรณ์สามารถสนับสนุนฝ่ายพลเรือนในยามปกติและสนับสนุนกองกำลังทางยุทธวิธีในการปฏิบัติการทางทหารเช่นเดียวกับกองทัพมิตรประเทศเมื่อเกิดความชัดเจนแล้วจึงจะสามารถพัฒนาทุกระบบที่เกี่ยวข้องไปพร้อมกัน ได้แก่ ระบบอัตรากำลัง ระบบการบริหารทรัพยากรบุคคล และระบบการฝึกศึกษา ที่สำคัญที่สุดคือในปัจจุบันได้มีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 แล้ว ดังนั้น จึงมีความจำเป็นต้องพัฒนาหน่วยงานไซเบอร์ในกองทัพให้มีความสอดคล้องกัน

ข้อเสนอแนะ

การพัฒนาหน่วยงานด้านไซเบอร์ของกองทัพบกไทยเป็นเรื่องที่เกี่ยวข้องกับหลายฝ่าย ซึ่งมีสาเหตุมาจากการยกระดับการปฏิบัติการทางทหารให้สอดคล้องกับการพัฒนาทางด้านเทคโนโลยีสารสนเทศ จึงทำให้บทบาทของงานด้านไซเบอร์ซึ่งเคยเป็นงานย่อยของระบบงานด้านสื่อสารและอยู่ในฐานะฝ่ายกิจการพิเศษ (Special Staff) ที่มีภารกิจเฉพาะด้านถูกยกระดับมาเป็นงานหลักใน

กรอบการปฏิบัติการทางทหาร (Military Operations) ส่งผลให้ต้องเกี่ยวข้องกับทุกสายงานฝ่ายอำนวยการและทุกหน่วยปฏิบัติดังนั้น การพัฒนาจึงจำเป็นต้องดำเนินการในทุกระดับ โดยผลการวิจัยสามารถสรุปข้อเสนอแนะได้ดังนี้

1.การพัฒนาความรู้กำลังพลทุกนายตลอดจนผู้บังคับบัญชาทุกระดับชั้น ให้ตระหนักถึงความสำคัญของงานด้านการปฏิบัติการไซเบอร์ในการปฏิบัติการทางทหารสมัยใหม่ รวมถึงให้เข้าใจงานที่เกี่ยวข้องในกลุ่มงานเดียวกันได้แก่ การสื่อสาร การปฏิบัติการข่าวสาร การสารสนเทศ ตลอดจนงานในระบบการควบคุมบังคับบัญชาอื่นๆเพื่อนำไปสู่ความเข้าใจร่วมกันในการกำหนดบทบาท หน้าที่ของหน่วยงานไซเบอร์ การพัฒนาเสริมสร้างหน่วยงานไซเบอร์ ตลอดจนการกำหนดความสัมพันธ์กับระบบงานอื่นในกองทัพให้มีความชัดเจน

2. พัฒนาระบบอื่นในกลุ่มงานที่เกี่ยวข้องกับการปฏิบัติการไซเบอร์ตามข้อ 1 ได้แก่ การสื่อสาร การปฏิบัติการข่าวสาร การสารสนเทศโดยแยกหน้าที่ให้มีความชัดเจนและมีความประสานสอดคล้องเชื่อมโยงกันอย่างเป็นระบบตามหลักการจัดกลุ่มงานที่มีความเชื่อมโยงในระดับเดียวกันเข้าไว้ด้วยกัน

3.พัฒนาระบบฝ่ายอำนวยการทางทหาร ให้มีความพร้อมในการปฏิบัติการทางทหารเช่นเดียวกับการปฏิบัติการทางทหารแบบอื่นโดยเฉพาะการขยายขอบเขตกรมฝ่ายเสนาธิการในระดับกองบัญชาการกองทัพบกขึ้นไป ให้มีกรมฝ่ายเสนาธิการ (G-6 Army Staff) ที่รับผิดชอบโดยตรงแยกออกจากกรมฝ่ายยุทธการ (G-3 Army Staff) เช่นเดียวกับกองทัพมิตรประเทศทั้งในและนอกอาเซียน

4.พัฒนาความเชื่อมโยงของระบบการปฏิบัติการไซเบอร์ของกองทัพบกให้มีความเชื่อมโยงกับทุกหน่วยในกระทรวงกลาโหม ตลอดจนบทบาทของกองทัพบกในระดับประเทศเช่นเดียวกับกองทัพมิตรประเทศทั้งในยามปกติในบทบาทการสนับสนุนฝ่ายพลเรือนต่อความมั่นคงรูปแบบใหม่ และในยามสงครามเพื่อสนับสนุนการปฏิบัติการทางทหาร

5.พัฒนาระบบโครงสร้างอัตรากำลังหน่วยงานด้านไซเบอร์ให้มีทั้งองค์การทางดิ่งซึ่งเป็นอัตราทหารเพื่อสนับสนุนงานการปฏิบัติการทางทหาร และองค์การทางราบซึ่งเป็นอัตราพลเรือนเพื่อสนับสนุนงานทางเทคนิคที่มีความชำนาญเฉพาะด้าน เป็นการชดเชยจุดอ่อนของการจัดองค์การแต่ละแบบและสามารถตอบสนองการปฏิบัติการด้านไซเบอร์ได้

6.พัฒนาระบบการบริหารงานบุคคลโดยเฉพาะในเรื่องมาตรฐานการกำหนดตำแหน่งและแนวทางการรับราชการในตำแหน่งที่มีความชำนาญเฉพาะ ตลอดจนระบบการฝึกและศึกษาทางด้านไซเบอร์ ให้สามารถสนับสนุนการปฏิบัติการไซเบอร์ได้อย่างมีประสิทธิภาพ

7.เผยแพร่ทำความเข้าใจในเรื่องความแตกต่างระหว่างส่วนราชการภายในกระทรวงกลาโหม ทั้งความแตกต่างทางดิ่งตามหลักระดับการปฏิบัติการทางทหารทางยุทธศาสตร์ ยุทธการ และยุทธวิธี และความแตกต่างทางระดับระหว่างเหล่าทัพตามคุณสมบัติของเหล่าที่เป็นสากล โดยกองทัพบกจะมุ่งเน้นไปที่การฝึกกำลังพลจำนวนมากเพื่อเข้าปฏิบัติการเป็นหน่วยขนาดใหญ่จึงมุ่งเน้นไปที่การปฏิบัติการไซเบอร์ของหน่วยทางยุทธวิธีในขณะที่กองทัพเรือและกองทัพอากาศเป็นการปฏิบัติงานของยุทโธปกรณ์ที่มีเป้าหมายระดับยุทธศาสตร์และมีการให้ความรู้แก่กำลังพลทางด้านเทคนิคดังนั้น การปฏิบัติการไซเบอร์จึงมุ่งเน้นในระดับสูง

8.นำระบบข้าราชการพลเรือนกลาโหมมาใช้ในกระทรวงกลาโหมให้เป็นรูปธรรม เพื่อให้สามารถสร้างบุคลากรด้านไซเบอร์ที่มีความเชี่ยวชาญเฉพาะด้านได้ โดยการจัดการฝึกและศึกษาให้เหมาะสมกับงานของข้าราชการแต่ละประเภท ซึ่งจะทำให้สามารถบริหารจัดการทรัพยากรที่มีจำกัดให้มุ่งไปสู่ตำแหน่งที่ปฏิบัติงานจริงโดยไม่ต้องย้ายออกจากสายงานเมื่อมีการปรับชั้นยศใหม่ตามข้อจำกัดของอัตราทหาร

9.สร้างความเข้าใจต่อหน่วยงานภายนอก ในด้านความแตกต่างระหว่างกองทัพกับส่วนราชการพลเรือน โดยเฉพาะกองทัพเป็นองค์การที่ออกแบบมาเพื่อปฏิบัติหน้าที่ทางทหาร ดังนั้นระบบงานบางระบบรวมถึงระบบงานไซเบอร์ในบางเรื่องจำเป็นต้องมีการยกเว้นกฎ ระเบียบ การปฏิบัติเพื่อตอบสนองความต้องการเฉพาะของกองทัพในภาพรวมซึ่งเป็นความแตกต่างที่เป็นสากลเหมือนกันในทุกประเทศ