มิติไซเบอร์

การสรรหาและพัฒนากำลังพล

รองรับสงครามสมัยใหม่



ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
เอกสารศึกษาเฉพาะกรณี (Case Study) เรื่อง มิติไซเบอร์ : การสรรหาและพัฒนากำลังพลรองรับสงครามสมัยใหม่
พิมพ์ครั้งที่ ๑ กรุงเทพฯ จำนวน ๔๐๐ เล่ม
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, ๒๕๖๙ จำนวน ๘๘ หน้า

© สิทธิ์ภาษาไทยเป็นของศูนย์ศึกษายุทธศาสตร์
สถาบันวิชาการป้องกันประเทศอย่างถูกต้องตามกฎหมาย

ผู้อำนวยการ	:	พล.อ.ต. ไชยา	ออกแดง
รองผู้อำนวยการ	:	น.อ. สาดิศย์	พริ้งประยูร
	:	น.อ. ปัญญา	ศรีสิงห์
หัวหน้าโครงการ	:	พ.อ. อนุพนธ์	นาคสุทธิ์
รองหัวหน้าโครงการ	:	พ.อ.หญิง สุนิสา	ธิปัตย์
นักวิจัย	:	น.ส. กาญจนา	เพิ่มพูน
คณะวิจัย	:	น.ท.หญิง ภัสวรรณ	ศรีธนวิบุญชัย ร.น.
	:	น.ท.หญิง จิตราภรณ์	จิตรธร ร.น.
	:	ร.อ.หญิง ภิรัญชญา	อุไรรัตน์
	:	ร.ท.หญิง ปาณิสรา	เทียนอ่อน ร.น.
พิสูจน์อักษร	:	น.อ. ธีรพล	วุฒิทวีพัฒน์
	:	ส.อ. จิรายุ	กลัดบุบผา
	:	น.ส. อุไรวรรณ	สุสัมฤทธิ์
	:	น.ส. สุเมตตา	สารราช
	:	นาย ภาสพงษ์	อุทัยแสง

จัดพิมพ์โดย

กองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๔๐๐
โทร ๐ ๒๕๗๒ ๒๙๓๒ เว็บไซต์ www.ssctthailand.org

มิติไซเบอร์

การสรรหาและพัฒนากำลังพล

รองรับสงครามสมัยใหม่



คำนำ

ในยุคที่เทคโนโลยีสารสนเทศกลายเป็นหัวใจหลักของการขับเคลื่อนโลก มิติไซเบอร์ไม่ได้เป็นเพียงพื้นที่แห่งการสื่อสารอีกต่อไป แต่ได้กลายเป็นสมรภูมิใหม่ ที่มีอิทธิพลต่อความมั่นคงของชาติอย่างไม่อาจหลีกเลี่ยงได้ ทั้งนี้ ในปัจจุบันสงครามสมัยใหม่ไม่ได้ตัดสินกันเพียงด้วยกำลังอาวุธยุทโธปกรณ์เท่านั้น แต่ยังหมายรวมถึงขีดความสามารถในมิติทางดิจิทัล ทำให้ปัจจัยสำคัญประการหนึ่งสำหรับการเตรียมความพร้อมของกองทัพคือ “กำลังพล” ดังนั้น เพื่อเป็นหลักประกันความสำเร็จ กองทัพไทยจึงควรมุ่งเน้นสำหรับการสรรหาและพัฒนากำลังพลด้านไซเบอร์ให้มีทักษะที่เท่าทันต่อเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว เพื่อสร้างกองกำลังพลด้านไซเบอร์ที่มีประสิทธิภาพ พร้อมรับมือกับภัยคุกคามในรูปแบบใหม่ที่ไร้พรมแดนในปัจจุบัน

ด้วยเหตุปัจจัยที่กล่าวมา ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ ในฐานะหน่วยงานด้านความมั่นคงและคลังสมองของกองทัพไทย ได้เล็งเห็นถึงความสำคัญของกำลังพลด้านไซเบอร์กองทัพไทย จึงได้จัดทำเอกสาร กรณีศึกษา (Case Study) เรื่อง “มิติไซเบอร์ : การสรรหาและพัฒนากำลังพลรองรับสงครามสมัยใหม่ เพื่อให้ทราบถึงแนวทางและข้อเสนอแนะสำหรับการกำหนดนโยบายในการสรรหาและพัฒนากำลังพลด้านไซเบอร์อันเป็นประโยชน์ต่อการกำหนดนโยบายในการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยต่อไป

ศูนย์ศึกษายุทธศาสตร์
สถาบันวิชาการป้องกันประเทศ
พฤษภาคม ๒๕๖๙

สารบัญ

เรื่อง	หน้า
คำนำ	ก
สารบัญ	ค
สารบัญภาพ	จ
ส่วนที่ ๑ บทนำ	๑
๑.๑ ที่มาและความสำคัญของปัญหา	๑
๑.๒ วัตถุประสงค์	๒
๑.๓ ขอบเขตของการศึกษา	๒
๑.๔ กรอบแนวคิดในการศึกษา	๓
๑.๕ วิธีการศึกษา	๓
๑.๖ การวิเคราะห์และสรุปข้อมูล	๔
๑.๗ ประโยชน์ที่คาดว่าจะได้รับ	๔
ส่วนที่ ๒ ปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน	๗
๒.๑ ปัจจัยภายนอก	๗
- บริบทสงครามสมัยใหม่	๗
- ความก้าวหน้าทางเทคโนโลยี	๙
- ความก้าวหน้าด้านไซเบอร์ของกองทัพในต่างประเทศ	๑๒
๒.๒ ปัจจัยภายใน	๑๖
- บทบาทและภารกิจของกองทัพไทยในมิติไซเบอร์	๑๖
- หน่วยบัญชาการไซเบอร์ทหาร	๑๙
ส่วนที่ ๓ การสรรหาและพัฒนากำลังพลด้านไซเบอร์ในอนาคตโดยใช้เครื่องมือ Strategic Foresight	๓๓
๓.๑ การคาดการณ์ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์	๓๖
ฉากทัศน์ที่ ๑ : กองทัพไซเบอร์เกรียงไกร (The Cyber Vanguard)	๓๘
ฉากทัศน์ที่ ๒ : นักรบอุดมการณ์พลีชีพ (The Patriotic Martyrs)	๔๐

สารบัญ

เรื่อง	หน้า
ฉากทัศน์ที่ ๓ : ปราการไซเบอร์ล่มสลาย (The Defenseless Frontier)	๔๒
ฉากทัศน์ที่ ๔ : กรงทองของนักรบไร้ใจ (The Gilded Cage)	๔๔
๓.๒ แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่	๔๗
ส่วนที่ ๔ บทสรุปและข้อเสนอแนะ	๕๕
๔.๑ บทสรุป	๕๕
๔.๒ ข้อเสนอแนะ	๕๖
บรรณานุกรม	๖๐
ภาคผนวก	๖๗
ภาคผนวก ก ภาพประกอบการสัมมนาฯ	๖๗
ภาคผนวก ข ภาพประกอบการแถลงและวิพากษ์ผลงานทางวิชาการฯ	๖๙

สารบัญภาพ

	หน้า
ภาพที่ ๑ กรอบแนวคิดในการศึกษา (Conceptual Framework)	๓
ภาพที่ ๒ แผนผังโครงสร้างยุทธศาสตร์/กรอบการดำเนินงาน ของกองบัญชาการกองทัพไทย (Royal Thai Armed Forces Headquarters)	๑๖
ภาพที่ ๓ แสดงการตัดกันของแกน X และ แกน Y ในการสร้างภาพอนาคต	๓๗
ภาพที่ ๔ แสดง ภาพอนาคตของการสรรหาและพัฒนากำลังพล ด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า	๔๗

ส่วนที่ ๑
บทนำ



ส่วนที่ ๑ บทนำ

๑.๑ ที่มาและความสำคัญของปัญหา

จากสถานการณ์ความมั่นคงระหว่างประเทศในปัจจุบันที่กำลังเผชิญการเปลี่ยนแปลงเชิงยุทธศาสตร์ทำให้ภัยคุกคามรูปแบบใหม่เกิดขึ้นในหลายมิติ ทั้งด้านไซเบอร์ อวกาศ ปัญญาประดิษฐ์ ระบบอัตโนมัติ และสงครามข้อมูลส่งผลให้ลักษณะของสงครามสมัยใหม่ (Modern Warfare) แตกต่างไปจากอดีตโดยสิ้นเชิง ทั้งนี้ จะไม่ได้จำกัดอยู่เพียงการใช้กำลังรบในสนามรบทางกายภาพเท่านั้น แต่ได้ขยายไปสู่การใช้ข้อมูล เทคโนโลยี และระบบเครือข่ายอัจฉริยะเป็นอาวุธสำคัญ อนึ่ง มิติไซเบอร์เป็น “พื้นที่ยุทธศาสตร์ใหม่” ที่ส่งผลกระทบต่อมิติอื่น ๆ เป็นพื้นที่ปฏิบัติการหรือสมรภูมิที่ ๕ (ต่อจาก บก ทะเล อากาศ และอวกาศ)[๑] ที่ส่งผลต่อพื้นที่ทางกายภาพและไม่ใช่กายภาพ เช่น ระบบโครงสร้างพื้นฐานที่สำคัญ รวมทั้งด้านเศรษฐกิจ และสังคม ตลอดจนความรู้สึกนึกคิดของประชาชนที่อาจถูกชี้นำผ่านการทำสงครามข้อมูลข่าวสาร เป็นต้น ดังนั้น จะเห็นได้ว่ามิติไซเบอร์คือ **“โครงสร้างพื้นฐานของโลกยุคใหม่”** ที่หากขาดระบบป้องกันที่ดี อาจกลายเป็นภัยคุกคามที่ร้ายแรงต่อชาติและกองทัพได้

ในบริบทนี้ **“กำลังพลด้านไซเบอร์”** จึงกลายเป็นทรัพยากรทางยุทธศาสตร์หลักของกองทัพที่ต้องได้รับการพัฒนาอย่างมีทิศทางและต่อเนื่อง เพื่อให้สามารถปรับตัวและตอบสนองต่อรูปแบบสงครามใหม่ได้อย่าง มีประสิทธิภาพ ทั้งนี้ กองบัญชาการกองทัพไทย (บก.ทท.) ซึ่งมีบทบาทสำคัญในการบูรณาการกำลังรบระหว่างเหล่าทัพและการวางแผนยุทธศาสตร์ร่วม จึงให้ความสำคัญกับการสรรหาและพัฒนากำลังพลให้มีความรู้ความสามารถ เพื่อเป็นรากฐานในการเสริมสร้างขีดความสามารถในการปฏิบัติการร่วมสำหรับการป้องกันประเทศในอนาคต

ปัจจุบันการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของ บก.ทท. ยังมีพื้นที่สำหรับโอกาสในการดึงดูดบุคลากรที่มีศักยภาพเฉพาะทางที่มีความรู้ความสามารถในระดับสูง โดยเฉพาะผู้ที่มีทักษะในการรับมือกับภัยคุกคามที่เฉพาะเจาะจง เช่น การโจมตีทางไซเบอร์ อาชญากรรมทางไซเบอร์ การป้องกันการแฮกข้อมูล เป็นต้น ซึ่งบุคลากรเหล่านี้สามารถเป็นหัวใจสำคัญในการปกป้องโครงสร้างพื้นฐานสำคัญทางทหารในอนาคต

การสรรหาและพัฒนากำลังพลเป็นปัจจัยหลักในการสร้าง “ความพร้อมรบของกองทัพ” ดังนั้น การมีบุคลากรที่มีสมรรถนะและทักษะทางไซเบอร์สูงและที่สำคัญคือจิตสำนึกของ

[๑] กรมยุทธศึกษาทหารบก. (2563). *หลักนิยมกองทัพบกด้านไซเบอร์.* โรงพิมพ์กองสงเคราะห์ทหารผ่านศึก

ความเป็นทหารและการป้องกันประเทศ จึงเป็นหัวใจสำคัญของการรักษาอธิปไตยและความมั่นคงของประเทศในระยะยาว บก.ทท. จึงมีความจำเป็นในการพัฒนายุทธศาสตร์ด้านการบริหารกำลังพลด้านไซเบอร์ให้ทันต่อภัยคุกคามในปัจจุบัน โดยเฉพาะกระบวนการ **"สรรหา" และ "พัฒนา"** กำลังพล ด้วยเหตุนี้ ศูนย์ศึกษายุทธศาสตร์ฯ ซึ่งเป็นหน่วยงานที่ศึกษาวิจัยและให้ข้อคิดเห็นด้านยุทธศาสตร์ความมั่นคงแก่หน่วยงานของกองทัพ จึงได้จัดทำเอกสารกรณีศึกษา (Case Study) เรื่อง "มิติไซเบอร์ : การสรรหาและพัฒนากำลังพลรองรับสงครามสมัยใหม่" ซึ่งจะเป็นประโยชน์ต่อการบริหารจัดการกำลังพลด้านไซเบอร์ของ บก.ทท. ให้มีประสิทธิภาพสามารถรองรับกับภัยคุกคามและสงครามสมัยใหม่ต่อไป

๑.๒ วัตถุประสงค์

๑). เพื่อศึกษาปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน

๒). เพื่อคาดการณ์ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์

๓). เพื่อวิเคราะห์ภาพอนาคตและเสนอแนะแนวทางการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยรองรับสงครามสมัยใหม่

๑.๓ ขอบเขตของการศึกษา (Scope)

การจัดทำเอกสารศึกษาเฉพาะกรณี เรื่อง มิติไซเบอร์ : การสรรหาและพัฒนากำลังพลรองรับสงครามสมัยใหม่ มีรายละเอียดดังนี้

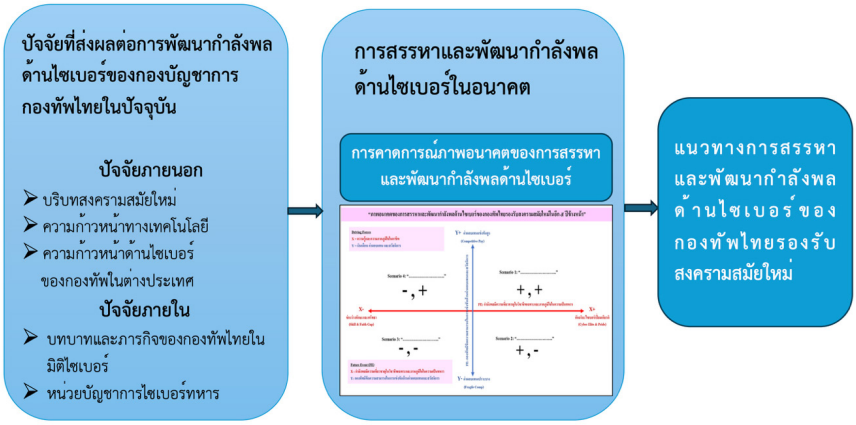
๑). ด้านเนื้อหาที่ศึกษา : ผู้วิจัยได้ศึกษาครอบคลุมประเด็นปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน แบ่งออกเป็นปัจจัยภายใน (บทบาทและภารกิจของกองทัพไทยในมิติไซเบอร์, หน่วยบัญชาการไซเบอร์ทหาร) และปัจจัยภายนอก (บริบทสงครามสมัยใหม่, ความก้าวหน้าทางเทคโนโลยี และความก้าวหน้าด้านไซเบอร์ของกองทัพในต่างประเทศ) การสรรหาและพัฒนากำลังพลด้านไซเบอร์ในอนาคตของ นซบ. ทหาร และหน่วยงานด้านไซเบอร์ที่เกี่ยวข้อง รวมถึงภาพอนาคตและแนวทางที่เหมาะสมในการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยรองรับสงครามสมัยใหม่

๒). ด้านประชากร **:** ผู้กำหนดนโยบายและผู้ปฏิบัติของ นซบ. ทหาร และหน่วยงานที่เกี่ยวข้อง ได้แก่ หน่วยงานด้านกำลังพล หน่วยงานด้านยุทธการ หน่วยงานด้านวิชาการ และภาคเอกชน

๓). ด้านพื้นที่ : หน่วยงานด้านไซเบอร์ และหน่วยงานที่เกี่ยวข้อง ในพื้นที่กรุงเทพมหานคร

๔). ด้านระยะเวลา : ดำเนินงานวิจัย ระหว่างเดือนมกราคม – พฤษภาคม ๒๕๖๙ รวมระยะเวลา ในการศึกษาทั้งสิ้น ๕ เดือน

๑.๔ กรอบแนวคิดในการศึกษา (Conceptual Framework)



ภาพที่ ๑ กรอบแนวคิดในการศึกษา (Conceptual Framework)

๑.๕ วิธีการศึกษา

การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีการศึกษาประกอบด้วย

๑). การศึกษาเอกสาร (Documentary Review) : ทบทวนเอกสาร เปรียบเทียบขีดความสามารถของกองทัพในต่างประเทศ สมุดปกขาว

๒). การสัมภาษณ์เชิงลึก (In–depth Interview) : กระทรวงกลาโหม, บก.ทท. ๓ เหล่าทัพ, สกมช. หน่วยงานภาคเอกชน และหน่วยงานวิชาการ

๓). การจัดสัมมนาปัญหายุทธศาสตร์ ครั้งที่ ๑/๖๙ หัวข้อ “แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่”

๓.๑ การบรรยายพิเศษ เรื่อง “Cyber Workforce เพื่อความมั่นคงของชาติ”

๓.๒ เวทีสนทนา เรื่อง “กำลังรบด้านไซเบอร์กับสงครามสมัยใหม่”

๓.๓ การสัมมนากลุ่มย่อย หัวข้อ “แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของ กองทัพไทยรองรับสงครามสมัยใหม่”

๑.๖ การวิเคราะห์และสรุปผล

วิเคราะห์และสรุปผลจากการนำข้อมูลปฐมภูมิ (Primary Data) และข้อมูลทุติยภูมิ (Secondary Data) ที่ได้มารวบรวมและวิเคราะห์เนื้อหา (Content Analysis) ตามประเด็นที่กำหนดไว้ เพื่อจัดทำเป็นข้อสรุปและข้อเสนอแนะต่อไป

๑.๗ ผลที่คาดว่าจะได้รับ

๑). ทราบถึงปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน

๒). ทราบความต้องการของกำลังพลที่มีความเชี่ยวชาญด้านไซเบอร์ รวมทั้งปัญหาและข้อจำกัดของหน่วยบัญชาการไซเบอร์ทหาร (นซบ. ทหาร) และความคิดเห็นของหน่วยงานที่เกี่ยวข้อง

๓). ได้ภาพอนาคตและแนวทางการพัฒนากำลังพลด้านไซเบอร์ซึ่งจะเป็นประโยชน์ต่อหน่วยงานด้าน ไซเบอร์ทั้งกองบัญชาการกองทัพไทยและภาคส่วนที่เกี่ยวข้อง

ส่วนที่ ๒
ปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน



ส่วนที่ ๒ ปัจจัยที่ส่งผลต่อการพัฒนากำลังพลด้านไซเบอร์ของกองบัญชาการกองทัพไทยในปัจจุบัน

๒.๑ ปัจจัยภายนอก

บริบทสงครามสมัยใหม่

ในศตวรรษที่ ๒๑ นิยามของคำว่าสงคราม ได้วิวัฒนาการไปไกลกว่าการปะทะกันด้วยกำลังทางทหารในสมรภูมิทางกายภาพเพียงอย่างเดียว ทั้งนี้ การขยายตัวของเทคโนโลยีดิจิทัลโลกได้ผลักดันให้เกิดสภาวะสงครามสมัยใหม่ (Modern Warfare) ที่มีความเป็น (Hybrid) และเบ็ดเสร็จมากยิ่งขึ้น อนึ่ง สงครามสมัยใหม่ถูกนิยามผ่านแนวคิดสงครามเบ็ดเสร็จที่วิวัฒนาการไปสู่สงครามไฮบริด (Hybrid Warfare) กองทัพไทยในปัจจุบัน[๒] ดังนี้

๑). การเปลี่ยนผ่านสู่สงครามไฮบริด (Hybrid Warfare) : ในอดีตชัยชนะทางสงครามจะหมายถึงการยึดครองพื้นที่ทางกายภาพเป็นหลัก แต่ในปัจจุบันพื้นที่สีเทา (Gray Zone) กลายเป็นสมรภูมิสำคัญ ทั้งนี้ สงครามสมัยใหม่มักเป็นการผสมผสานระหว่าง การใช้กำลังทหาร (Conventional Force) และกลยุทธ์ ที่ไม่ใช่การทหาร (Non-military means) เพื่อบ่อนทำลายความมั่นคงของฝ่ายตรงข้ามจากภายใน อาทิ การปฏิบัติการข้อมูลข่าวสาร (Information Operations: IO) ที่มุ่งทำลายขีดความสามารถฝ่ายตรงข้าม ผ่านการใช้ (Fake News) หรือการโฆษณาชวนเชื่อเพื่อสร้างความแตกแยกทางความคิดรวมถึงการสร้างแนวร่วมมุมกลับ นอกจากนี้ยังรวมถึงการใช้สงครามไซเบอร์ เพื่อโจมตีโครงสร้างพื้นฐาน เช่น ระบบไฟฟ้า ธนาคาร หรือระบบสื่อสาร ที่สามารถสร้างความเสียหายเป็นวงกว้างได้อย่างรวดเร็ว[๓]

๒). เทคโนโลยีอุบัติใหม่และปัญญาประดิษฐ์ (Emerging Tech & AI) : เทคโนโลยีปัจจุบันได้เปลี่ยนโฉมหน้าของการทำสงครามให้มีความแม่นยำสูงและลดความเสี่ยงด้านกำลังพล เช่น การใช้อากาศยานไร้คนขับและปัญญาประดิษฐ์ (AI) ในการลาดตระเวนและการโจมตีเป้าหมายที่ได้สร้างผลกระทบต่อยุทธศาสตร์การป้องกันประเทศอย่างมากในความขัดแย้งปัจจุบัน เช่น สงครามรัสเซีย-ยูเครน และ สหรัฐฯ - อิหร่าน[๔]

---

[๒] Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Potomac Institute for Policy Studies.

[๓] International Committee of the Red Cross. (2024). *Modern warfare and its impact on civilians.*

[๔] สถาบันเทคโนโลยีป้องกันประเทศ. (2565). *แนวโน้มเทคโนโลยีป้องกันประเทศและสงครามในอนาคต.*

นอกจากนี้ การนำปัญญาประดิษฐ์ (AI) มาใช้ในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่ออำนาจในการตัดสินใจในสนามรบอย่างรวดเร็ว รวมถึงอาวุธความเร็วเหนือเสียง (Hypersonic Weapons) ได้สร้างผลกระทบต่อยุทธศาสตร์ความมั่นคงในปัจจุบัน

๓). ตัวแสดงที่ไม่ใช่รัฐ (Non-State Actors) : สงครามสมัยใหม่มิได้ทำการรบระหว่างกองทัพเพียงสองประเทศ แต่เป็นสงครามแบบอสมมาตร (Asymmetric Warfare) ที่รัฐต้องต่อสู้กับกลุ่มติดอาวุธ องค์กรก่อการร้าย หรือกลุ่มอิทธิพลที่ได้รับการสนับสนุนจากรัฐอื่น (Proxy War) ซึ่งกลุ่มเหล่านี้มักแฝงตัวอยู่กับพลเรือน ทำให้การพิสูจน์ทราบเป้าหมายทำได้ยากขึ้น[๕]

ดังนั้น การทำสงครามในปัจจุบันจำเป็นต้องรวมทุกพลังอำนาจแห่งชาติเพื่อตอบโต้ภัยคุกคามทั้งปวง เนื่องจากสงครามในยุคปัจจุบันไม่ได้จำกัดเฉพาะการใช้กำลังทหาร แต่เป็นการปรับเปลี่ยนยุทธวิธีผสาน รวมถึงการใช้เทคโนโลยีและยุทธศาสตร์ที่ซับซ้อนเข้าด้วยกันเพื่อเพิ่มประสิทธิภาพสำหรับการบรรลุภารกิจ

นอกจากนี้ การวิเคราะห์พลวัตของรูปแบบการทำสงครามในยุคปัจจุบัน (Modern Warfare Trends) สามารถแบ่งออกเป็น ๓ รูปแบบ เพื่อสร้างความได้เปรียบโดยไม่ต้องใช้กำลังทหาร มีรายละเอียดดังนี้

๑). การปฏิบัติการ Multi-Domain Operations (MDO)[๖] คือปฏิบัติการที่ไม่ใช่การประกอบกำลังเพียงแค่การปฏิบัติการทางบก, เรือและอากาศ (Joint Operations) เหมือนในอดีต แต่คือการประสานทุกมิติเข้าด้วยกันอย่างไร้รอยต่อ (Seamless Integration) เพื่อสร้างความได้เปรียบโดยการทำให้ฝ่ายตรงข้ามเกิดภาวะชะงักงันทางการตัดสินใจ จากการถูกโจมตีในทุกมิติ อาทิ การใช้โดรนโจมตีทางอากาศ พร้อมกับการตัดสัญญาณดาวเทียมและการเจาะระบบสื่อสารภาคพื้นดิน รวมถึงการใช้กำลังผ่านอวกาศและไซเบอร์ (Space & Cyber) เพื่อทำลายระบบควบคุมบังคับบัญชาการของฝ่ายตรงข้าม

๒). สงครามทางการรับรู้ Cognitive Warfare[๗] คือ วิวัฒนาการขั้นสูงสุดของปฏิบัติการทางจิตวิทยา (Psychological Operations) โดยเปลี่ยนเป้าหมายจากการโฆษณาชวนเชื่อมาเป็นการเปลี่ยนกระบวนการรับรู้ของมนุษย์ ผ่านกลไกการใช้ประโยชน์จากสื่อสังคมออนไลน์

---

[๕] Biddle, S. (2021). The future of warfare: Non-state actors and high-tech weapons. *International Security, 45(3),* 7-48.

[๖] Townsend, S. J. (2018). Multi-domain operations: Preparing for future war. *Military Review, 98(3),* 4-11.

[๗] Rosner, Y., & Siman-Tov, D. (2018). *Cognitive warfare: The rise of the sixth domain.* Institute for National Security Studies (INSS).

เพื่อสร้างห้องแห่งเสียงสะท้อน (Echo Chambers) หรือการแพร่กระจาย (Fake News) ที่ตรงกับความอคติของผู้รับสาร โดยมีวัตถุประสงค์มุ่งเน้นไปที่การสร้างความแตกแยกภายในสังคม ทำให้ประชาชนเสื่อมศรัทธาในสถาบันหลักของรัฐหรือสร้างความสับสนจนแยกแยะความจริงไม่ได้ ซึ่งเป็นการชนะสงครามโดยไม่ต้องใช้กำลังทางทหาร

๓). เครื่องมือทางเศรษฐกิจเชิงยุทธศาสตร์ Economic Statecraft [๘] ในสงครามสมัยใหม่ อำนาจทางเศรษฐกิจ ถูกนำมาใช้เป็นอาวุธทำลายล้างที่มีประสิทธิภาพไม่แพ้ขีปนาวุธ โดยเปลี่ยนการพึ่งพากันระหว่างประเทศให้กลายเป็นความเปราะบาง อีกทั้ง การที่ประเทศหนึ่งควบคุมโครงสร้างพื้นฐานสำคัญ เช่น ระบบการโอนเงินระหว่างประเทศ (SWIFT) เทคโนโลยีเซมิคอนดักเตอร์ รวมไปถึงการควบคุมห่วงโซ่อุปทานเพื่อสร้างอำนาจต่อรองทางการเมืองและการทหาร

โดยสรุป สงครามสมัยใหม่ในปัจจุบันการปฏิบัติการมิใช่เพียงเรื่องของชัยชนะในสนามรบเพียงอย่างเดียว แต่หากรวมถึงชัยชนะเหนือโครงสร้างพื้นฐาน ความเชื่อและความมั่งคั่งของชาติฝ่ายตรงข้าม ผ่านการบูรณาการระหว่าง MDO ที่เชื่อมโยงมิติ บก ทะเล อากาศ อวกาศ และไซเบอร์เข้าด้วยกัน ในขณะที่ (Cognitive Warfare) และ (Economic Statecraft) ทำหน้าที่เป็นเครื่องมือในพื้นที่สีเทา (Gray Zone) ที่สามารถบั่นทอนอำนาจของรัฐจากภายในได้อย่างมีประสิทธิภาพ ดังนั้นความท้าทายของผู้กำหนดนโยบายและความมั่นคงในอนาคตจึงไม่ใช่เพียงการเสริมสร้างแสนยานุภาพทางอาวุธ แต่คือการสร้างความยืดหยุ่นและภูมิคุ้มกันในทุกมิติ เพื่อรับมือกับภัยคุกคามที่ไร้รูปแบบและไม่มีเส้นแบ่งของเวลาที่ชัดเจนระหว่างสภาวะสันติภาพและสภาวะสงคราม

ความก้าวหน้าทางเทคโนโลยี

ในปัจจุบัน ความก้าวหน้าทางเทคโนโลยี (Technological Advancement) ไม่ได้จำกัดอยู่เพียงการพัฒนาประสิทธิภาพของเครื่องมือหรือการสื่อสาร แต่ได้กลายเป็นรากฐานสำคัญของการปรับเปลี่ยนกระบวนทัศน์ด้านความมั่นคงระดับโลก[๙] โดยเฉพาะเมื่อเข้าสู่สงครามยุคที่ ๕ ที่เส้นแบ่งระหว่างสมรภูมิทางกายภาพและพื้นที่เสมือนจริงไม่อาจแยกได้ ทั้งนี้ ในปัจจุบันความก้าวหน้าทางเทคโนโลยีในมิติไซเบอร์ เช่น ปัญญาประดิษฐ์ (AI), เทคโนโลยี

[๘] Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44(1),* 42-79. https://doi.org/10.1162/isec_a_00351

[๙] United Nations Institute for Disarmament Research (UNIDIR). *(2021). The role of technological advancement in modern warfare: Challenges and opportunities.* https://unidir.org/publication/role-technological-advancement-modern-warfare

ควอนตัม (Quantum Computing) และระบบเครือข่ายไร้สายความเร็วสูง ได้กลายเป็นปัจจัยชี้ขาดในการสร้างความได้เปรียบทางยุทธวิธี[๑๐]

ดังนั้น การสรรหาและพัฒนากำลังพลจึงมิใช่เพียงการคัดเลือกบุคลากรที่มีทักษะการรบแบบดั้งเดิม แต่เป็นการเฟ้นหา “นักรบไซเบอร์” (Cyber Warriors) ที่สามารถเข้าใจและประยุกต์ใช้เทคโนโลยีที่ซับซ้อนภายใต้สภาวะกดดันได้ ความก้าวหน้าทางเทคโนโลยีจึงเป็นทั้งโอกาสและอุปสรรคที่ทำให้กองทัพต้องเร่งปฏิรูปโครงสร้างกำลังพลเพื่อรองรับการเผชิญหน้ากับภัยคุกคามรูปแบบใหม่ที่รวดเร็วและไร้พรมแดน[๑๑]

ทั้งนี้ เมื่อประมาณ ๓๐ ปีที่แล้ว กองทัพอากาศของสหรัฐฯ ได้ยกระดับความสำคัญในเรื่อง Space และ Cyber ให้เป็นยุทธศาสตร์หลัก (priority) นอกเหนือจาก Air – Land Operation ในอดีต ส่งผลให้เป็นจุดเริ่มต้นของการให้ความสำคัญกับ Air– Land Operation, Cyber และ Space ที่มีผลกระทบด้านยุทธศาสตร์ความมั่นคงมาถึงปัจจุบันซึ่งสะท้อนให้เห็นถึงความสำคัญในเรื่องความก้าวหน้าทางเทคโนโลยี นอกจากนี้ ในปี พ.ศ. ๒๕๖๘ กระทรวงการสงครามสหรัฐฯ (U.S. Department of War) ได้ประกาศมุ่งเน้นการพัฒนาเทคโนโลยี ๖ ด้าน เพื่อนำมาใช้พิจารณาสำหรับยุทธศาสตร์ด้านความมั่นคงของสหรัฐฯ ได้แก่

๑. เทคโนโลยี Directed Energy ใช้สำหรับระบบป้องกันภัยทางอากาศ, ต่อต้านอากาศยานไร้คนขับ, เรือบิน, จรวด, และปืนใหญ่ ซึ่งจะช่วยให้หน่วยงานสามารถขยายการใช้เลเซอร์พลังงานสูงและไมโครเวฟพลังงานสูงที่มีต้นทุนต่อการยิงต่ำและเข้าถึงได้กว้าง

๒. เทคโนโลยีไฮเปอร์โซนิค (Hypersonics) ได้แก่ อากาศยาน และระบบอาวุธที่สามารถทำการยิงด้วยความเร็วสูง ตั้งแต่ ๕ มัค ขึ้นไป ซึ่งจะส่งผลโดยตรงต่อการวางกำลังทางทหาร โดยจะมุ่งเน้นที่การผลิตในระดับขนาดใหญ่ ลดต้นทุนและการนำไปใช้ในหน่วยปฏิบัติการทั่วไป

๓. เทคโนโลยีปัญญาประดิษฐ์ (AI) คือ เทคโนโลยีการพัฒนาซอฟต์แวร์และระบบคอมพิวเตอร์ให้มีความสามารถในการคิด วิเคราะห์ เรียนรู้ และตัดสินใจได้คล้ายกับสติปัญญาของมนุษย์

---

[๑๐] ชัยชนะ จารุศิลาวงศ์. (2566). *ยุทธศาสตร์การพัฒนากำลังพลไซเบอร์: แนวคิดและการปฏิบัติ.* วารสารความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 4(2), 45-60.

[๑๑] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

๔. เทคโนโลยีข้อมูลข่าวสารสนามรบควอนตัม (Quantum Battlefield Information Dominance) ทำให้ความได้เปรียบด้านข้อมูล, การสั่งการและการเชื่อมโยงระบบซึ่งสำคัญมากกับศูนย์บัญชาการอากาศยาน, โดรนและระบบ C2 (บังคับ-ควบคุม)

๕. เทคโนโลยีชีวะการผลิต (Biomanufacturing) คือการใช้สิ่งมีชีวิตที่ถูกออกแบบทางพันธุกรรม เช่น แบคทีเรีย เพื่อผลิตวัสดุที่จำเป็น

๖. โลจิสติกส์ในสภาพแวดล้อมแข่งขัน (Contested Logistics Technology) คือระบบและเทคโนโลยีการส่งกำลังบำรุง เช่น การขนส่ง เสบียง อาวุธ ยุทโธปกรณ์ และการแพทย์ในสภาวะที่เส้นทางลำเลียงถูกขัดขวาง คุกคาม หรือถูกโจมตีจากฝ่ายตรงข้ามอย่างรุนแรง

อนึ่ง จากการพัฒนาเทคโนโลยีของสหรัฐฯ ดังกล่าวสามารถวิเคราะห์ประเด็นที่สำคัญได้ดังนี้ การมุ่งเน้นการพัฒนาเทคโนโลยีให้เหลือเพียง ๖ ด้าน ซึ่งอาจสะท้อนให้เห็นว่ากระทรวงการสงครามสหรัฐฯ มีความมุ่งหมายสำหรับการพัฒนาเทคโนโลยียุทธศาสตร์ดังกล่าวให้สามารถกระทำได้อย่างรวดเร็ว และมีประสิทธิภาพ โดยเลือกด้านที่ถือเป็นข้อบังคับ (Imperatives) ที่สำคัญเท่านั้น นอกจากนี้ ประเทศไทยถือเป็นพันธมิตรของสหรัฐฯ หากประสงค์จะเข้าร่วมหรือมีความร่วมมือย่อมจะมีโอกาสที่สหรัฐฯ จะเปิดรับในบริบทของเทคโนโลยีที่อยู่ใน ๖ ด้านนี้ ทั้งนี้ สหรัฐฯ ต้องการมุ่งเป้าผลผลิตทางเทคโนโลยีที่รวดเร็วและตรงความต้องการในเชิงยุทธศาสตร์ด้านความมั่นคง ดังนั้น กองทัพไทยจึงควรวางแผนและเตรียมความพร้อมให้ทันกับจังหวะที่เร็วขึ้นในเทคโนโลยีดังกล่าว เนื่องจากหากสหรัฐฯ พัฒนาเทคโนโลยีดังกล่าวได้ตามแผนและหากไทยสามารถสร้างความร่วมมือกับสหรัฐฯ ได้จะสร้างความได้เปรียบทางการทหารให้กับกองทัพไทยมากขึ้น

โดยสรุป ความก้าวหน้าทางเทคโนโลยีเปรียบเสมือนดาบสองคมในมิติไซเบอร์ แม้เทคโนโลยีจะช่วยเพิ่มขีดความสามารถในการป้องกันและโจมตีอย่างแม่นยำ แต่ขณะเดียวกันก็ได้สร้างช่องโหว่ใหม่ๆ ที่ต้องการระบบระวังป้องกันอย่างใกล้ชิด ดังนั้นหัวใจสำคัญของการรองรับสงครามสมัยใหม่จึงไม่ได้อยู่ที่การครอบครองเทคโนโลยีที่ทันสมัยที่สุดเพียงอย่างเดียว แต่อยู่ที่การพัฒนาทุนมนุษย์ (Human Capital) ให้มีความสามารถในการปรับตัว (Adaptability) และการเรียนรู้อย่างต่อเนื่อง[๑๒] ทั้งนี้ การสรรหาและพัฒนากำลังพลในอนาคตจำเป็นต้องบูรณาการความเชี่ยวชาญทางเทคนิคเข้ากับยุทธศาสตร์ด้านความมั่นคงเพื่อให้มั่นใจ

[๑๒] Arquilla, J., & Ronfeldt, D. (2020). *The emergence of noopolitik: Toward an American information strategy*. RAND Corporation.

ได้ว่าเทคโนโลยีที่ก้าวหน้าในปัจจุบันจะถูกนำมาใช้เป็นเครื่องมือหลักในการรักษาอธิปไตยทางไซเบอร์และสร้างความมั่นคงที่ยั่งยืนให้แก่ชาติ ท่ามกลางความผันผวนของภูมิทัศน์ความมั่นคงโลกในศตวรรษที่ ๒๑[๑๓]

ความก้าวหน้าด้านไซเบอร์ของกองทัพในต่างประเทศ

ปัจจุบันกองทัพประเทศมหาอำนาจและประเทศผู้นำด้านเทคโนโลยีมิได้มองว่าไซเบอร์เป็นเพียงเครื่องมือสนับสนุนทางการสื่อสารเท่านั้น แต่คืออาวุธทางยุทธศาสตร์ที่สามารถตัดสินผลแพ้ชนะในสนามรบได้เช่นกัน ทั้งนี้ ความก้าวหน้าด้านไซเบอร์ของกองทัพในต่างประเทศสะท้อนผ่านการเปลี่ยนแปลงใน ๓ มิติหลัก ดังนี้ **๑). จากตั้งรับเชิงรุกสู่การป้องปราม (From Passive Defense to Deterrence)** โดยกองทัพชั้นนำ เช่น สหรัฐอเมริกา (US Cyber Command)[๑๔] ได้เปลี่ยนหลักนิยมจากการเพียงป้องกันจากระบบภายในมาเป็นการตรวจจับและยับยั้งภัยคุกคามตั้งแต่ต้นทางรวมถึงการสร้างขีดความสามารถในการตอบโต้ (Counter-offensive) เพื่อสร้างอำนาจการป้องปรามทางไซเบอร์ **๒). การบูรณาการเทคโนโลยีอุบัติใหม่ (Emerging Tech Integration)** [๑๕] โดยการนำ Artificial Intelligence (AI) และ Machine Learning มาใช้ในการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อหาช่องโหว่แบบ Real-time รวมถึงการพัฒนาเทคโนโลยี Quantum Computing ที่อาจทำลายระบบรหัสผ่านเดิมของโลกไปอย่างสิ้นเชิง และ **๓). สงครามลูกผสม (Hybrid Warfare)** ผ่านการใช้ปฏิบัติการทางไซเบอร์ควบคู่ไปกับปฏิบัติการข้อมูลข่าวสารเพื่อสร้างความบิดเบือนในกระบวนการตัดสินใจซึ่งเป็นยุทธวิธีที่เห็นได้อย่างชัดเจนในความขัดแย้งร่วมสมัยในสมรภูมิยุโรปตะวันออกและตะวันออกกลางในปัจจุบัน[๑๖]

ทั้งนี้ ความก้าวหน้าด้านไซเบอร์ของกองทัพสหรัฐฯ และสิงคโปร์ในปัจจุบันสะท้อนให้เห็นอย่างชัดเจนสำหรับการพัฒนาด้านเทคโนโลยีดังกล่าว มีรายละเอียด ดังนี้

---

[๑๓] กฤษฎา มณีวงศ์. (2565). *ความก้าวหน้าทางเทคโนโลยีกับการปรับตัวของกองทัพในศตวรรษที่ 21.* สำนักพิมพ์มหาวิทยาลัยป้องกันประเทศ.

[๑๔] U.S. Department of Defense. (2023). *Summary of the 2023 Department of Defense cyber strategy.* https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023-DOD-CYBER-STRATEGY-SUMMARY.PDF

[๑๕] Synergia Foundation. (2026). *Global futures 2035: Scaling cyber resilience in an era of quantum computing.* Proceedings of the Synergia Conclave 2026.

[๑๖] Jensen, B., & Valeriano, B. (2024). The future of cyber power: Lessons from the integration of cyber operations in modern theater. *Journal of Strategic Studies, 47(2),* 145-168. https://doi.org/10.1080/01402390.2024.xxxxxx

๑). ความก้าวหน้าด้านไซเบอร์ของกองทัพสหรัฐอเมริกา

กองทัพสหรัฐฯ ได้ยกระดับมิติไซเบอร์จากระบบสนับสนุนไปสู่ขีดความสามารถหลักในการรบ (Core Warfighting Capability) [๑๗] ทั้งนี้ สหรัฐฯ มีการเปลี่ยนแปลงเชิงยุทธศาสตร์และเทคโนโลยีที่สำคัญผ่านการใช้ยุทธศาสตร์ไซเบอร์ฉบับใหม่ปี ๒๕๖๙ ดังนี้

๑.๑) ยุทธศาสตร์การป้องปรามเชิงรุก (Defend Forward & Integrated Deterrence) : สหรัฐฯ ปรับเปลี่ยนแนวคิดจากเดิมที่เน้นการตั้งรับภายในเครือข่ายของตนมาเป็นการใช้แนวคิด “Defend Forward” ซึ่งระบุให้กองบัญชาการไซเบอร์สามารถปฏิบัติการนอกเครือข่ายของตนเพื่อขัดขวางภัยคุกคามตั้งแต่ต้นทางก่อนจะถึงแผ่นดินสหรัฐฯ ทั้งนี้ ยุทธศาสตร์ปี ๒๕๖๙ ได้เน้นความสำคัญของ “Integrated Deterrence” หรือการป้องปรามแบบบูรณาการที่ใช้เครื่องมือในทุกมิติ ทั้งทางทหาร การทูต และไซเบอร์ควบคู่กัน [๑๘] อนึ่ง ภายใต้ยุทธศาสตร์ไซเบอร์ปี ๒๕๖๙ (President Trump’s Cyber Strategy 2026) สหรัฐฯ ได้ประกาศใช้หลัก **“Deter and Disrupt”** ซึ่งเน้นการสร้างความรับผิดชอบ (Accountability) สำหรับผู้ที่โจมตีผลประโยชน์ของสหรัฐฯ กล่าวคือการบังคับให้ผู้โจมตีต้องรับผิดชอบและชดใช้ต่อผลของการกระทำ (Holding Adversaries Accountable) โดยยุทธศาสตร์นี้ประกอบไปด้วย ๖ เสาหลัก ได้แก่ การปรับเปลี่ยนพฤติกรรมฝ่ายตรงข้าม, การปฏิรูปกฎระเบียบให้เอื้อต่อเอกชน, การยกระดับเครือข่ายรัฐบาลด้วย AI, การป้องกันโครงสร้างพื้นฐานวิกฤต (CII), การครองความเป็นผู้นำในเทคโนโลยีเกิดใหม่ และการสร้างบุคลากรไซเบอร์[๑๙]

๑.๒) การบูรณาการ AI และระบบอัตโนมัติ (Algorithmic Warfare) : ในปี ๒๕๖๘ – ๒๕๖๙ กองทัพสหรัฐฯ ได้เริ่มนำ Agentic AI และระบบการเรียนรู้ของเครื่องมือ (Machine Learning) มาใช้ในการตรวจจับภัยคุกคามแบบเรียลไทม์ซึ่งช่วยให้สามารถวิเคราะห์รูปแบบการโจมตีที่ซับซ้อน (Advanced Persistent Threats: APTs) และตอบโต้โดยอัตโนมัติ

---

[๑๗] U.S. Army. (2024). *Army digital transformation strategy 2024-2028: Integrating artificial intelligence and cyber resilience.* Department of the Army.

[๑๘] U.S. Department of Defense. (2023, May 26). *Fact sheet: 2023 DoD cyber strategy.* https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

[๑๙] Executive Office of the President. (2026). *President Trump’s cyber strategy 2026: Deter and disrupt.* The White House. https://www.whitehouse.gov/

ในระดับความเร็วระดับมิลลิวินาที[๒๐] นอกจากนี้ยังมีโครงการ Cyber Vision 2025 ของกองทัพอากาศที่มุ่งเน้นการสร้างเครือข่ายที่สามารถฟื้นฟูระบบได้โดยอัตโนมัติ

๑.๓) การยกระดับอุตสาหกรรมป้องกันประเทศ (Defense Industrial Base - DIB) : ความก้าวหน้าที่สำคัญอีกประการคือการขยายขอบเขตการคุ้มครองไปยังภาคอุตสาหกรรมป้องกันประเทศผ่านโครงการ Cybersecurity Maturity Model Certification (CMMC) เพื่อให้มั่นใจว่าห่วงโซ่อุปทานของกองทัพจะไม่ตกเป็นเป้าหมายของจารกรรมไซเบอร์จากคู่แข่งทางยุทธศาสตร์[๒๑] ทั้งนี้ กองบัญชาการไซเบอร์สหรัฐฯ (USCYBERCOM) ได้เริ่มย้ายโครงสร้างพื้นฐานข้อมูลระดับความมั่นคงสูงไปสู่มาตรฐาน Post-Quantum Cryptography เพื่อป้องกันภัยคุกคามจากคอมพิวเตอร์ควอนตัมที่คาดว่าจะสามารถถอดรหัสลับในปัจจุบันได้ในอนาคตอันใกล้ ทั้งนี้ หน่วยงานรัฐจะเริ่มแผนเปลี่ยนผ่านเต็มรูปแบบ ภายในปี ๒๕๖๙ [๒๒]

๒). ความก้าวหน้าด้านไซเบอร์ของกองทัพสิงคโปร์ (Singapore)

สิงคโปร์เป็นตัวอย่างที่โดดเด่นของรัฐขนาดเล็กที่มีขีดความสามารถด้านไซเบอร์ระดับโลกโดยมีระบบในการจัดโครงสร้างองค์กรและการร่วมมือแบบพหุภาคี ดังนี้

๒.๑) การจัดตั้งเหล่าทัพที่ ๔ Digital and Intelligence Service (DIS) : สิงคโปร์เป็นหนึ่งในไม่กี่ประเทศในประชาคมโลกที่จัดตั้งหน่วยไซเบอร์เป็นเหล่าทัพที่ ๔ อย่างเต็มรูปแบบควบคู่กับกองทัพบก, เรือและอากาศ โดยใช้ชื่อ Digital and Intelligence Service (DIS) ที่มีภารกิจมุ่งเน้นการรวบรวมขีดความสามารถด้านข่าวกรองดิจิทัล การปฏิบัติการสงครามข้อมูลข่าวสารและการป้องกันโครงสร้างพื้นฐานวิกฤตไว้ภายใต้สายการบังคับบัญชาเดียว [๒๓]

๒.๒) การบูรณาการ “ทหาร - พลเรือน” (Whole-of-Government Approach) : กองทัพสิงคโปร์โดย DIS จะดำเนินงานร่วมกับสำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (CSA) ผ่านหน่วยงานใหม่ที่ชื่อว่า Defense Cyber Command (DCCOM) ซึ่งมีการจัดตั้ง

---

[๒๐] Luckenbaugh, J. (2026, March 10). ALGORITHMIC WARFARE: Cyber ops increasingly melding with kinetic conflict. National Defense Magazine. https://www.nationaldefensemagazine.org/articles/2026/3/10/cyber-ops-increasingly-melding-with-kinetic-conflict

[๒๑] SOCRadar. (2026, January 23). The U.S. 2026 National Defense Strategy: A cybersecurity perspective. https://socradar.io/blog/us-2026-national-defense-strategy-cybersecurity/

[๒๒] Thales. (2026, January 6). AI, Quantum, and the cybersecurity threats defining 2026. https://cpl.thalesgroup.com/blog/data-security/ai-quantum-cybersecurity-threats-2026

[๒๓] Ministry of Defence, Singapore. (2025, March 3). *Fact sheet: Defence Cyber Command and SAF C4 & digitalisation command.* https://www.mindef.gov.sg/news-and-events/latest-releases/03mar25_fs/

Sectoral Cyber Defense Teams (SCDTs) เพื่อดูแลความมั่นคงด้านไซเบอร์ใน ๑๑ ภาคส่วนสำคัญของประเทศ เช่น พลังงานและการเงิน [๒๔] ทั้งนี้ ในปี ๒๕๖๙ สิงคโปร์ได้เปิดใช้งาน Digital Range ภายใต้ศูนย์ Cytec ที่ได้รับการพัฒนาเพื่อรองรับการฝึกด้วย AI-Simulated Cyber Defense ซึ่งสามารถจำลองสถานการณ์การโจมตีที่ซับซ้อนระดับสูง (Advanced Persistent Threat - APT) และรองรับการฝึกร่วมกับต่างประเทศผ่านระบบทางไกล [๒๕]

๒.๓) โครงการ Sentinel และการสร้าง "AI-for-Cyber" Talent : สิงคโปร์มุ่งเน้นการสร้างบุคลากรตั้งแต่ระดับเยาวชนผ่านโครงการ Sentinel Program me โดยในปี ๒๕๖๙ ได้เพิ่มหลักสูตร Applied AI Core Competencies เพื่อเตรียมความพร้อมให้นักเรียนทหารและเยาวชนได้สามารถใช้ AI ในการวิเคราะห์มัลแวร์และตรวจสอบนิติวิทยาศาสตร์ทางดิจิทัลได้อย่างเชี่ยวชาญ[๒๖] รวมถึงมีการเปิดตัวศูนย์ Cyber Defense Test and Experimentation Centre (Cytec) ที่ใช้เทคโนโลยี Virtualization ระดับสูงสำหรับจำลองเครือข่ายของประเทศและฝึกซ้อมการรับมือการโจมตีระดับรัฐ (State-sponsored attacks) รวมถึงการทดสอบเทคโนโลยี 5G และ AI ในภารกิจทางทหาร [๒๗]

---

[๒๔] Ministry of Defence, Singapore. (2026b, February 27). *Fact sheet: Cyber Defence Test and Experimentation Centre (CyTEC) and sectoral cyber defence teams (SCDTs).* https://www.mindef.gov.sg/news-and-events/latest-releases/27feb26-fs2/

[๒๕] Ministry of Defence, *Singapore. (2026, February 11). Singapore's Digital and Intelligence Service participates in multilateral cyber defence exercise.* https://www.mindef.gov.sg/news-and-events/latest-releases/11feb26-nr/

[๒๖] Ministry of Defence, Singapore. (2025, November 28). *SAF expands cybersecurity student talent development programme to include AI skills in 2026.* https://www.mindef.gov.sg/news-and-events/latest-releases/28nov25-nr2/

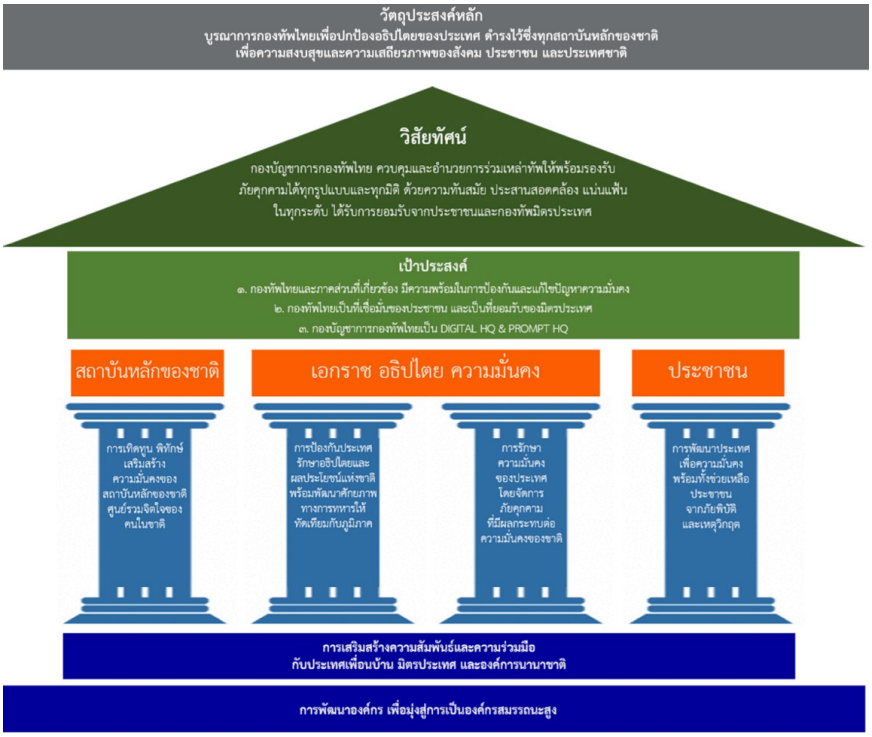
[๒๗] Cyber Security Agency of Singapore. (2025, November 12). *AI-enabled capabilities and collaboration with industry elevate defence of critical infrastructure at national cyber defence exercise.* https://www.csa.gov.sg/news-events/press-releases/ai-enabled-capabilities-and-collaboration-with-industry-elevate-defence-of-critical-infrastructure-at-national-cyber-defence-exercise/

๒.๒ ปัจจัยภายใน

บทบาทและภารกิจของกองทัพไทยในมิติไซเบอร์

ภารกิจ

กองบัญชาการกองทัพไทย มีหน้าที่ควบคุม อำนวยการ สั่งการ และกำกับดูแลการดำเนินงานของส่วนราชการในกองทัพไทยในการเตรียมกำลังการป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้ กำลังทหารตามอำนาจหน้าที่ของกระทรวงกลาโหมให้เกิดประสิทธิภาพสูงสุดมีผู้บัญชาการทหารสูงสุดเป็นผู้บังคับบัญชารับผิดชอบ[๒๘]



ภาพที่ ๒ แผนผังโครงสร้างยุทธศาสตร์/กรอบการดำเนินงานของกองบัญชาการกองทัพไทย (Royal Thai Armed Forces Headquarters)

---

[๒๘] แผนปฏิบัติราชการ ระยะ ๕ ปี (พ.ศ.๒๕๖๖-๒๕๗๐) กองบัญชาการกองทัพไทย (ฉบับแก้ไขเพิ่มเติม) https://strapi.rtarf.mi.th/uploads/0_2_c277c4a85d.pdf

อย่างไรก็ตาม การปฏิบัติการในมิติไซเบอร์ได้กลายเป็นยุทธบริเวณที่ ๕ ต่อจากทางบก ทางทะเล ทางอากาศ และอวกาศ โดยกองทัพไทยได้ปรับเปลี่ยนแนวทางและยุทธศาสตร์มุ่งสู่การปฏิบัติการหลายมิติ (Multi-Domain Operations: MDO) และยกระดับโครงสร้างการบริหารจัดการจากศูนย์ไซเบอร์ทหารไปสู่หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย เพื่อรองรับภัยคุกคามรูปแบบใหม่ที่มีความซับซ้อน รวดเร็ว และไร้พรมแดน[๒๙] ทั้งนี้ บทบาทและภารกิจของกองทัพไทยในมิติไซเบอร์ตามกรอบแผนยุทธศาสตร์และสมุดปกขาวทางทหาร สามารถสรุปออกเป็น ๕ ด้านหลัก ดังนี้

๑). การป้องกันและการปฏิบัติการทางไซเบอร์เชิงรับ (Defensive Cyber Operations: DCO

๑.๑). การสำรวจและจัดทำบัญชีทรัพย์สินดิจิทัล ได้ทำการรวบรวมและประเมินระบบสารสนเทศ โครงข่ายการสื่อสาร และระบบบังคับบัญชาและระบบควบคุม (C4ISR) ของกองทัพไทยและสามเหล่าทัพ เพื่อระบุจุดอ่อนและช่องโหว่ทางไซเบอร์ [๓๐]

๑.๒). การเฝ้าระวังและตอบสนองภัยคุกคามแบบเรียลไทม์ ได้จัดตั้งและพัฒนานวัตกรรมศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Joint Cyber Operations Center: JCOC) ควบคู่กับการนำสถาปัตยกรรมความมั่นคงปลอดภัยแบบ Zero Trust Architecture (ZTA) มาใช้ในการปกป้องระบบเครือข่ายทางทหารตลอด ๒๔ ชั่วโมง

๑.๓). การจัดการความเสี่ยงและบรรเทาเหตุการณ์ กำหนดโปรโตคอลการรับมือกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์เพื่อรักษาสภาพความพร้อมรบของระบบเทคโนโลยีทางทหาร [๓๑]

๒). การปฏิบัติการทางไซเบอร์เชิงรุกและการข่าวกรองไซเบอร์ (Offensive Cyber Operations & Cyber Intelligence)

๒.๑). การยับยั้ง ขัดขวาง และตอบโต้ มีการพัฒนาขีดความสามารถในการปฏิบัติตามกฎการใช้กำลัง (Rules of Engagement: ROE) ในการลดขีดความสามารถ ขัดขวาง หรือ

---

[๒๙] กระทรวงกลาโหม. (2568). *สมุดปกขาว หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2568.* หน่วยบัญชาการไซเบอร์ทหาร.

[๓๐] จินดา สระสมบูรณ์. (2558). ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย. รัฏฐาภิรักษ์, 57(2), 57–69.

[๓๑] ศูนย์ไซเบอร์กองทัพบก. (2558). แนวทางการปฏิบัติการและความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพบก. เอกสารเผยแพร่ทางวิชาการการทหาร.

ทำลายโครงสร้างพื้นฐานทางไซเบอร์ของฝ่ายตรงข้าม หากเกิดสถานการณ์สงครามไซเบอร์หรือการโจมตีรุนแรงที่กระทบต่ออธิปไตยของชาติ [๓๒]

๒.๒). ระบบบังคับบัญชาและระบบควบคุมทางไซเบอร์ การเชื่อมโยงสายการบังคับบัญชาและอำนวยการสั่งการปฏิบัติการทางไซเบอร์ของทุกเหล่าทัพให้อยู่ภายใต้กรอบการปฏิบัติการร่วม

๒.๓). การข่าวกรองทางไซเบอร์ ได้ทำการรวบรวม วิเคราะห์ และประเมินแนวโน้มภัยคุกคาม รวมถึงวิเคราะห์พฤติกรรมกลุ่มผู้ไม่หวังดี (Advanced Persistent Threats: APTs) เพื่อพาดพิงตัวตนและคาดการณ์การโจมตีล่วงหน้า [๓๓]

๓). การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของชาติ (Critical Information Infrastructure Protection: CIIP)

๓.๑). การบูรณาการความมั่นคงระดับชาติ ทำหน้าที่เป็นกลไกหลักทางทหารในการประสานงานร่วมกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๒). การสนับสนุนพื้นที่นอกกองทัพ ให้การสนับสนุนกำลังพล เครื่องมือ และความเชี่ยวชาญแก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศ เช่น ระบบพลังงาน การขนส่ง การธนาคาร และโทรคมนาคม ในภาวะวิกฤตไซเบอร์ระดับชาติ [๓๔]

๔). การพัฒนาขีดความสามารถของกำลังพลและเทคโนโลยีอุบัติใหม่ (Capacity Building & Emerging Technologies)

๔.๑). การสร้างกำลังพลทางไซเบอร์ ยกระดับการฝึกอบรมผ่านโรงเรียนไซเบอร์ทหาร และพัฒนาทักษะด้าน Cyber Range, Forensics, Ethical Hacking รวมถึงการใช้เครื่องมือจำลองสถานการณ์สงคราม ไซเบอร์ (Cyber Simulation)

๔.๒). การประยุกต์ใช้เทคโนโลยีขั้นสูง ได้ทำการวิจัยและบูรณาการเทคโนโลยีปัญญาประดิษฐ์ (AI-Driven Cyber Defense), ระบบวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data

---

[๓๒] กระทรวงกลาโหม. (2560). *ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560–2579.* สำนักงานนโยบายและแผนกลาโหม.

[๓๓] กองบัญชาการกองทัพไทย. (2561). *ยุทธศาสตร์ไซเบอร์กองทัพไทย พ.ศ. 2561–2565.* ศูนย์ไซเบอร์ทหาร.

[๓๔] สำนักงานสภาความมั่นคงแห่งชาติ. (2560). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560–2564).* สำนักนายกรัฐมนตรี.

Analytics) และระบบการเข้ารหัสลับยุคหลังควอนตัม (Post-Quantum Cryptography: PQC) เพื่อยกระดับมิติรบไซเบอร์เข้าสู่ “กองทัพดิจิทัล” [๓๕]

๕). ความร่วมมือระหว่างประเทศและการปฏิบัติการร่วม-ผสม (Joint & Coalition Cyber Operations)

๕.๑). การฝึกซ้อมทางไซเบอร์ระดับนานาชาติ ได้เข้าร่วมและจัดตั้งกรอบการฝึกซ้อมทางไซเบอร์ร่วมกับประเทศพันธมิตร เช่น การฝึก Cobra Gold (Cyber Domain), Cyber Flag และการประชุมกลุ่มทำงานด้านการป้องกันประเทศทางไซเบอร์ (Cyber Defense Working Group: CDWG) [๓๖]

๕.๒). การแลกเปลี่ยนข่าวสารการข่มขู่คุกคาม สร้างเครือข่ายความร่วมมือด้านความมั่นคงไซเบอร์ระดับภูมิภาคอาเซียนและมิตรประเทศ เพื่อเฝ้าระวังภัยคุกคามข้ามชาติ

อย่างไรก็ตาม ในส่วนของภารกิจกองทัพไทยในมิติไซเบอร์จะมีหน่วยขึ้นตรง คือ หน่วยบัญชาการ ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ซึ่งเป็นหน่วยผู้รับผิดชอบหลักในการอำนวยการและปฏิบัติการเชิงบูรณาการร่วมกับสามเหล่าทัพ[๓๗]

หน่วยบัญชาการไซเบอร์ทหาร

๑). วิสัยทัศน์และภารกิจหน่วยบัญชาการไซเบอร์ทหาร

หน่วยบัญชาการไซเบอร์ทหาร (เดิมคือ ศูนย์ไซเบอร์ทหาร) มีความสามารถในการปฏิบัติการทางไซเบอร์ และการปฏิบัติการร่วมทางไซเบอร์ ซึ่งเป็นหนึ่งในห้ามิติการรบในการปฏิบัติการหลายมิติ และประสานสอดคล้องกับการปฏิบัติการคลื่นแม่เหล็กไฟฟ้า และการปฏิบัติการรบด้านอื่น ๆ ทั้งในและนอกการปฏิบัติการหลายมิติของกองทัพไทย อีกทั้งยังมีความสามารถในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศตลอดจนแก้ปัญหาทางไซเบอร์กับหน่วยงานที่เกี่ยวข้องให้เกื้อกูลกับการรักษาผลประโยชน์ของชาติ และ

[๓๕] กระทรวงกลาโหม. (2568). *สมุดปกขาว หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2568.* หน่วยบัญชาการไซเบอร์ทหาร.

[๓๖] กองบัญชาการกองทัพไทย. (2561). *ยุทธศาสตร์ไซเบอร์กองทัพไทย พ.ศ. 2561–2565.* ศูนย์ไซเบอร์ทหาร.

[๓๗] ศิริพงษ์ พงษ์เพียรชอบ. (2565). การพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยเพื่อรองรับภัยคุกคามรูปแบบใหม่. *วารสารเสธาธิปัตย์, 71(2),* 45–58.

ความมั่นคงของประเทศ รวมถึงมีขีดความสามารถในการปฏิบัติการร่วม-ผสมทางไซเบอร์ที่เพียงพอกับหน่วยงานทางไซเบอร์ของกองทัพนานาชาติ

ภารกิจ วางแผน กำกับดูแล

ประสานสอดคล้องกับการปฏิบัติการทางไซเบอร์และการปฏิบัติการร่วมทางไซเบอร์ทั้งในและผ่านมิติทางไซเบอร์ ให้เกิดเสรีในการเตรียมกำลังและใช้กำลังในทุกมิติ ตลอดจนประสานสอดคล้องกับการปฏิบัติการคลื่นแม่เหล็กไฟฟ้า และปฏิบัติการรบด้านอื่น ๆ ของกองทัพไทย นำไปสู่การตัดสินใจที่เหนือกว่าฝ่ายตรงข้าม รวมทั้งการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ดำรงไว้ซึ่งสภาวะที่เกื้อกูลต่อการปฏิบัติการทางทหาร และพร้อมเข้าสู่สงครามที่มีมิติไซเบอร์เป็นมิติการรบในการปฏิบัติการหลายมิติ เพื่อรักษาผลประโยชน์ของชาติและความมั่นคงของประเทศ

๒). แนวความคิดในการปฏิบัติการทางไซเบอร์

ป้องกันมิติไซเบอร์ในความรับผิดชอบ ทั้งในระดับยุทธการและยุทธศาสตร์ ตั้งแต่ยามปกติ ประกอบด้วย การปฏิบัติการทางไซเบอร์ เชิงป้องปราม (Offensive Cyberspace Operations: OCO) , การปฏิบัติการทางไซเบอร์เชิงรับ (Defensive Cyberspace Operations: DCO) และการปฏิบัติการสารสนเทศและเครือข่าย (Information Network Operations: INO) เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์จากการโจมตีของฝ่ายตรงข้าม สามารถป้องกันไม่ให้ฝ่ายตรงข้ามเข้ามาในมิติทางไซเบอร์ของฝ่ายเรา ขณะเดียวกันสนับสนุนให้ฝ่ายเราสามารถเข้าไปในมิติทางไซเบอร์ของฝ่ายตรงข้าม สอดคล้องตามขั้นตอนการปฏิบัติ ตลอดห้วงเวลาการปฏิบัติการ และมีความพร้อมในการใช้การปฏิบัติการทางไซเบอร์ได้ทันที เมื่อความขัดแย้งระหว่างกำลังฝ่ายเรากับฝ่ายตรงข้ามไม่สามารถยุติได้ การปฏิบัติการดังกล่าวครอบคลุมการป้องกันระบบเครือข่ายสารสนเทศของกองบัญชาการกองทัพไทย การบูรณาการให้เกิดการปฏิบัติการร่วม ในมิติไซเบอร์ในระดับกองทัพไทย และเป็นหน่วยงานหลักในการแก้ไขปัญหาเหตุการณ์ทางไซเบอร์ในระดับประเทศ ผ่านสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓). เป้าหมายของหน่วยบัญชาการไซเบอร์ทหาร

๓.๑ เป้าหมาย: Ends ในการขับเคลื่อนการเสริมสร้างความมั่นคงปลอดภัยและปกป้องผลประโยชน์ของประเทศอย่างยั่งยืน จำเป็นต้องมุ่งเน้นการเสริมสร้างขีดความสามารถ

ในด้านการปฏิบัติการทางไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญ ตลอดจนการสนับสนุนความร่วมมือในระดับชาติและนานาชาติ ได้กำหนดเป้าหมายสำคัญไว้ดังนี้

เป้าหมายที่ ๑ มีขีดความสามารถปฏิบัติการทางไซเบอร์และการปฏิบัติการร่วมทางไซเบอร์ ซึ่งเป็นหนึ่งใน ๕ มิติการรบในการปฏิบัติการหลายมิติ และประสานสอดคล้องกับการปฏิบัติการต่างๆ ทั้งในและนอกการปฏิบัติการรบหลายมิติ เช่น การปฏิบัติการคลื่นแม่เหล็กไฟฟ้า

เป้าหมายที่ ๒ มีขีดความสามารถปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ตลอดจนแก้ปัญหาทางไซเบอร์กับหน่วยงานที่เกี่ยวข้องให้เกื้อกูลกับความมั่นคงของประเทศและปกป้องผลประโยชน์ของชาติ

เป้าหมายที่ ๓ มีขีดความสามารถปฏิบัติการร่วม-ผสมทางไซเบอร์ที่เพียงพอกับหน่วยงานทางไซเบอร์ของกองทัพนานาชาติ

เป้าหมายที่ ๔ มีขีดความสามารถในการลดขีดความสามารถ ขัดขวาง ทำลาย และควบคุมฝ่ายตรงข้าม

๓.๒ วิธีการ: Ways เพื่อให้การเดินทางไปสู่เป้าหมายต่าง ๆ ได้อย่างถูกต้องและมีทิศทาง โดยใช้การพิจารณา ๓ เสาหลัก ได้แก่ ทรัพยากรบุคคลกระบวนการ และเทคโนโลยี (People-Process-Technology) ดังนี้

เป้าหมายที่ ๑ People ➔ ทรัพยากรบุคคล ประกอบด้วย ผู้บังคับบัญชาฝ่ายอำนวยการ ชุดปฏิบัติการทางไซเบอร์ (CPT), ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT), ทีมสนับสนุนและช่วยสนับสนุนการปฏิบัติการทางไซเบอร์ ได้แก่ ข่าวกรองภัยคุกคามทางไซเบอร์ (CTI), ทีมสนับสนุนวิเคราะห์ทางไซเบอร์ (AST), ทีมประเมินภัยคุกคามทางไซเบอร์ (CAT), ทีมสนับสนุนภารกิจทางไซเบอร์ (MST) แนวร่วมนักรบอาสาทางไซเบอร์ พันธมิตรในการปฏิบัติการร่วมพนักงานราชการเชี่ยวชาญพิเศษ มีการพัฒนาบุคลากร โดยโรงเรียนไซเบอร์ทหารที่มีหลักสูตรทางไซเบอร์ขั้นพื้นฐาน ขั้นกลาง ขั้นสูง และด้านฝ่ายอำนวยการมีศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ ในการสร้างเครือข่ายบุคลากรไซเบอร์งานวิจัยทางไซเบอร์ งานประชาสัมพันธ์สร้างความตระหนักรู้ทางไซเบอร์ งานวิชาการทางไซเบอร์ รวมถึงการพัฒนาบุคลากรผ่านหลักสูตรภายนอกโดยสถาบันรับรองที่มีมาตรฐาน และสถาบันการศึกษาทั้งในและต่างประเทศ มีการฝึกฝนความชำนาญให้กับบุคลากรผ่านการฝึกร่วมของกองทัพไทย การฝึกเป็นหน่วย การฝึกตามหน้าที่การจัดการฝึกบริหารวิกฤตการณ์ระดับชาติ การฝึกกับศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล

การแข่งขันทักษะทางไซเบอร์ครอบคลุมทุกระดับการศึกษา การจัด Cyber Bootcamp ระดับมัธยมศึกษามีระบบ Recruit and Talent Management

Process ➔ กรอบแนวคิด ยุทธศาสตร์ (White Paper) หลักนิยมการปฏิบัติการร่วมทางไซเบอร์ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ รัฐมนตรีว่าการกระทรวงกลาโหมและผู้บัญชาการทหารสูงสุด แผนรับมือภัยคุกคามทางไซเบอร์ กองบัญชาการกองทัพไทย สนับสนุนสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แผนปฏิบัติการทางไซเบอร์ประกอบ แผนป้องกันประเทศ กฎหมาย พระราชบัญญัติ กฎกระทรวง กฎการใช้กำลังที่เกี่ยวข้อง และมาตรฐานขั้นตอนการทำงาน การดำเนินการต่าง ๆ ได้แก่ การประเมินความเสี่ยง การตรวจประเมินทางไซเบอร์ที่เป็นมาตรฐาน การปฏิบัติการด้านการข่าวกรองทางไซเบอร์ที่มีประสิทธิภาพ การสร้างความร่วมมือด้านข้อมูลข่าวสารกับหน่วยงานทั้งในและนอกประเทศ รวมทั้งการดำเนินงานภายใต้กรอบความร่วมมือประชาคมไซเบอร์กองทัพไทย

Technology ➔ เทคโนโลยี ประกอบด้วย โรงเรียนไซเบอร์ทหาร มี Online Course System, Cyber Range & Simulation, Training Center, Training Labs, Operational Technology (OT) Labs ศูนย์ปฏิบัติการร่วมทางไซเบอร์ มี Joint Cyber Operation Center (JCOC), Cyber-C2 Technology, Protect & Detect Response, Cyber Threat Intelligence, Cloud & Edge Computing, Post-Quantum Cryptography (PQC) Technology, Zero Trusted Architecture Technology, Internet of Things (IOT), Industrial Internet of Things (IIOT) มีเทคโนโลยีในการสนับสนุนทีมปฏิบัติการ Cyber Deployment Platform Technologies, Forensics, Big DATA, Artificial Intelligence (AI), Geographic Information System

เป้าหมายที่ ๒ People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เน้นชุดปฏิบัติการทางไซเบอร์สองชุด คือ ชุดปฏิบัติการทางไซเบอร์ (CPT), ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT) และ เพิ่มเติมการฝึก รับมือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) กับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เน้นแผนรับมือภัยคุกคามทางไซเบอร์ กองทัพไทย (ทท.) สนับสนุน สำนักงานคณะกรรมการการรักษาความมั่นคง

ปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และเพิ่มเติมการดำเนินการ สร้างความร่วมมือด้านข่าวสารข้อมูลกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เน้นห้องปฏิบัติการเทคโนโลยีปฏิบัติการ (OT Labs) และเพิ่มเติมห้องปฏิบัติการ ห้องจำลองการฝึกเฝ้าระวังเหตุการณ์ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งครอบคลุม ๗+๑

เป้าหมายที่ ๓ People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติมการฝึกการฝึกร่วม/ผสม กับเหล่าทัพและกองกำลังต่างชาติ ประกอบด้วยกลุ่ม Bilateral เช่น US, UK, AUS, Singapore, Malaysia, Indonesia เป็นต้น และกลุ่ม Multilateral เช่น Cobra Gold, Cyber Flag, Cyber Marvel, Talisman Sabre เป็นต้น รวมถึงการฝึกปฏิบัติการร่วมทางไซเบอร์ขั้นสูง เชิญหน่วยงานต่างประเทศเข้าร่วมการแข่งขันทักษะทางไซเบอร์

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติมการดำเนินการ การประสานความร่วมมือกับต่างประเทศ ได้แก่ Cyber Defense Working Group (CDWG), Significant Security Cooperation Initiative (SSCI), ASEAN Defense Ministers' Meeting (ADMM) ด้าน Cyber และการปฏิบัติการ Joint Cyberspace Operations Task Force Deployment, Cyber Threat Intelligence (CTI) Sharing เป็นต้น

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติมในส่วนโรงเรียนฯ ให้สามารถสนับสนุนระบบ Integrated Multinational Cyber Information sharing and Training Environment (IMCITE) จาก CDWGซึ่งเป็นหลักสูตรทางไซเบอร์แบบออนไลน์ เป็นต้น

เป้าหมายที่ ๔ People ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติมผู้เชี่ยวชาญด้าน Network, Website, Mobile, Malware เพิ่มเติมหลักสูตรการพัฒนาช่องโหว่ (Exploit) การพัฒนา Malware และเพิ่มเติมการฝึก การฝึกร่วมผสมทางไซเบอร์ระดับกองบัญชาการกองทัพไทย, กองทัพไทย และนานาชาติ

Process ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติมกรอบแนวคิด National Institute of Standards and Technology (NIST) 800-115, SANS' Red Team Framework and Methodology (RTFM) และ Open Web Application Security Project (OWASP) ในยุทธศาสตร์ หลักนิยมฯ และการดำเนินการตามคู่มือการปฏิบัติการแบบ Red Team

Technology ➔ ใช้วิธีการเดียวกับเป้าหมายที่ ๑ เพิ่มเติม ในส่วนโรงเรียนฯ ระบบฝึกทักษะป้องปรามทางไซเบอร์ เพิ่มส่วนสนับสนุนการปฏิบัติการ การเตรียม Platform เชิงป้องปรามที่เกี่ยวข้อง

๓.๓ ทรัพยากร: Means การขับเคลื่อนสู่เป้าหมายทั้ง ๔ ต้องอาศัยทรัพยากรที่หลากหลาย ประกอบด้วย

๑). หน่วยงาน ประกอบด้วยทั้งภาครัฐและเอกชนที่จะสนับสนุนหนทางปฏิบัติ

- ภาครัฐ ได้แก่ กระทรวงกลาโหม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงศึกษาธิการกองทัพไทย กองบัญชาการกองทัพไทย หน่วยบัญชาการไซเบอร์ทหาร ศูนย์ปฏิบัติการร่วมทางไซเบอร์ โรงเรียน ไซเบอร์ทหาร ศูนย์ไซเบอร์ของเหล่าทัพ และสำนักงานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- ภาคเอกชน ได้แก่ บริษัทด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) บริษัทด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในและต่างประเทศ สถาบันการศึกษาของเอกชน สถาบันการศึกษาของต่างประเทศ สถาบันฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์

๒). ทรัพยากรบุคลากร เป็นหัวใจสำคัญ เช่น ผู้บังคับบัญชาระดับต่าง ๆ ที่มีความเข้าใจและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ ข้าราชการทหารทุกระดับในกองทัพไทย (ทท.), กองบัญชาการกองทัพไทย (บก.ทท.) และเหล่าทัพที่เป็นเจ้าหน้าที่ปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในส่วนต่างๆ พันธกิจของหน่วยบัญชาการไซเบอร์ ที่ปรึกษาจากเอกชนที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์

๓). ทรัพยากรด้านเทคโนโลยี ได้แก่ระบบต่าง ๆ ที่มีความจำเป็นในการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์เช่น ระบบตรวจจับภัยคุกคามขั้นสูง (Intrusion Detection Systems และ SIEM) ซอฟต์แวร์ป้องกันมัลแวร์ ระบบวิเคราะห์ข้อมูลข่าวกรอง และเครื่องมือสำหรับการเจาะระบบและจำลองสถานการณ์ (Penetration Testing Tools) เป็นต้น

๔). งบประมาณและการลงทุน ในการพัฒนาโครงสร้างพื้นฐาน เช่น ศูนย์ข่าวกรองไซเบอร์ ศูนย์ฝึกซ้อม (Cyber Range) และห้องสมุดดิจิทัล เป็นสิ่งสำคัญสำหรับสร้างความมั่นคงระยะยาว

๕). ความร่วมมือระหว่างประเทศและองค์กรในประเทศ เช่น หน่วยงาน

ภาครัฐ ภาคเอกชน และพันธมิตรระหว่างประเทศที่ช่วยเสริมการแบ่งปันข้อมูลและพัฒนามาตรฐานร่วมกัน

๖). นโยบายและกฎหมาย ที่สนับสนุนการทำงาน เช่น การคุ้มครองข้อมูลและความปลอดภัยในระบบไซเบอร์ เพื่อช่วยเพิ่มความน่าเชื่อถือในการปฏิบัติการ

๗). โครงสร้างพื้นฐานดิจิทัลที่ปลอดภัย เช่น เครือข่ายสื่อสารที่เข้ารหัสและการจัดเก็บข้อมูลสำรองเพื่อป้องกันเหตุการณ์ฉุกเฉิน รวมถึงการสร้างความตระหนักรู้แก่ประชาชนและบุคลากรในทุกระดับ เพื่อเสริมสร้างภูมิคุ้มกันทางไซเบอร์ที่ยั่งยืน

๔. ขีดความสามารถที่ต้องการทางไซเบอร์ตามกรอบยุทธศาสตร์

การเสริมสร้างขีดความสามารถทางไซเบอร์เป็นสิ่งจำเป็นอย่างยิ่งและเป็นหัวใจสำคัญในการบรรลุเป้าหมาย (Ends) ของกองทัพไทย ขีดความสามารถทางไซเบอร์ที่ต้องการประกอบด้วยส่วนต่าง ๆ ดังนี้

๔.๑ ทรัพยากรบุคคล (People)

๔.๑.๑ บุคลากร

๑) ผู้บังคับบัญชา และฝ่ายอำนวยการ สามารถบริหารงาน วางแผนปฏิบัติการทางไซเบอร์ มีความเข้าใจในยุทธศาสตร์ หลักนิยม และเทคโนโลยีเกี่ยวกับการปฏิบัติการทางไซเบอร์ เพื่อให้การสั่งการหรือการให้แนวทางปฏิบัติมีประสิทธิภาพ

๒) ชุดปฏิบัติการป้องกันทางไซเบอร์ (Cyber Protection Team: CPT) สามารถปกป้องเครือข่ายข้อมูล โครงสร้างสารสนเทศของกองทัพไทย หน่วยงานราชการ และเอกชน รวมถึงการสนับสนุนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๓) ชุดปฏิบัติการทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CNMT) มีขีดความสามารถเช่นเดียวกับ ชุดปฏิบัติการป้องกันทางไซเบอร์ (CPT) และมุ่งเน้นการป้องกันระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT) ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศ

๔) ชุดปฏิบัติการข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence: CTI) สามารถรวบรวมข้อมูล วิเคราะห์แหล่งที่มา ติดตาม คาดการณ์ภัยคุกคามในอนาคต ประเมินความเสี่ยง และผลกระทบ รวมถึงการสร้างกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์เชิงป้องปราม

๕) ชุดปฏิบัติการด้านการวิเคราะห์ทางไซเบอร์ (Analyst Support Team: AST) สามารถรวบรวมข้อมูลภัยคุกคามและมัลแวร์ วิเคราะห์พฤติกรรม ช่องโหว่ในระบบ ข้อมูลย้อนกลับการแพร่กระจายของมัลแวร์ และประเมินผลกระทบจากการโจมตี เพื่อวางแผนการป้องกันอย่างมีประสิทธิภาพ

๖) ชุดตรวจประเมินทางไซเบอร์ (Cyber Audit Team: CAT) สามารถประเมินความเสี่ยงทางไซเบอร์ ตรวจสอบและวิเคราะห์ข้อมูลในเครือข่าย ประเมินความปลอดภัยของแอปพลิเคชัน ตรวจสอบระบบควบคุมการเข้าถึง ตรวจสอบการตั้งค่าความปลอดภัยของระบบปฏิบัติการ การประเมินผลกระทบของเหตุการณ์ทางไซเบอร์ ตลอดจนการตรวจสอบความพร้อมของแผนรับมือเหตุการณ์ฉุกเฉิน

๗) ชุดสนับสนุนการช่วยปฏิบัติการทางไซเบอร์ (Mission Support Team: MST) สามารถแก้ไขปัญหาซอฟต์แวร์ฮาร์ดแวร์ อุปกรณ์เครือข่าย เซิร์ฟเวอร์และระบบคลาวด์ ตรวจสอบ แก้ไขปัญหาการเชื่อมต่อเครือข่าย และโครงสร้างสายสัญญาณ

๔.๑.๒ การพัฒนาบุคลากร โรงเรียนไซเบอร์ทหารสามารถออกแบบหลักสูตรทางไซเบอร์ขั้นพื้นฐาน ขั้นกลาง ขั้นสูงและด้านฝ่ายอำนวยการ เพื่อผลิตบุคลากรในข้อ ๔.๑.๑ รวมถึงสามารถประเมินผลหลักสูตร ตามแนวทางการประกันคุณภาพการศึกษาที่กองบัญชาการกองทัพไทย (บก.ทท.) กำหนด

๔.๑.๓ ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ เป็นแกนนำในการสร้างเครือข่ายบุคลากรทางไซเบอร์ดำเนินกิจกรรมทางวิชาการและงานวิจัยทางไซเบอร์ ประชาสัมพันธ์สร้างความตระหนักรู้ทางไซเบอร์ รวมถึงพัฒนาบุคลากรผ่านหลักสูตรที่มีสถาบันรับรองมาตรฐานทั้งในและต่างประเทศ

๔.๑.๔ การฝึกฝนความชำนาญให้กับบุคลากร หน่วยบัญชาการไซเบอร์ทหาร (นซบ.ทหาร) สามารถนำบุคลากรทางไซเบอร์ในกลุ่มงานต่าง ๆ เข้ารับการฝึกร่วมของกองทัพไทย การฝึกเป็นหน่วย การฝึกตามหน้าที่ การจัดการฝึกบริหารวิกฤตการณ์ระดับชาติ (National Crisis Management Exercise: C-MEX)ร่วมกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) การฝึกรับมือเหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) การฝึกกับศูนย์ปฏิบัติการต่อต้านการก่อการร้ายสากล การฝึกร่วม/ผสม กับเหล่าทัพและกองกำลังต่างชาติทั้งแบบ Bilateral; US UK AUS Singapore Malaysia, Indonesia และ Multilateral; Cobra Gold, Cyber Flag, Cyber Marvel, Talisman Sabre รวมถึงการฝึกปฏิบัติการร่วมทางไซเบอร์ขั้นสูง

๔.๑.๕ มีระบบ Recruit and Talent Management สามารถคัดเลือกบุคลากรที่มีประสิทธิภาพเข้าประจำการ และบริหารจัดการกลุ่มคนเหล่านั้นได้อย่างเหมาะสม ผ่านการจัดการแข่งขันทักษะทางไซเบอร์ (ระดับกองทัพไทย หน่วยงานรัฐ เอกชน และหน่วยงานต่างประเทศ ระดับโรงเรียนทหาร-ตำรวจ ระดับนักเรียนทหาร และมัธยมศึกษา) จัดกิจกรรม Cyber Bootcamp ระดับมัธยมศึกษา เพื่อประชาสัมพันธ์และสร้างฐานข้อมูลบุคลากรที่มีความสามารถทางไซเบอร์เพื่อเลือกใช้งาน รวมถึงสามารถคัดเลือกแนวร่วมนักรบอาสาทางไซเบอร์ พันธมิตรในการปฏิบัติการร่วม พนักงานราชการเชี่ยวชาญพิเศษ รวมถึงผู้เชี่ยวชาญด้าน Network, Website, Mobile, Malware มาเสริมกำลังทั้งการป้องกันโจมตีป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และงานด้านการสนับสนุนการปฏิบัติการ ฯ

๔.๒ กระบวนการ (Process)

๔.๒.๑ กรอบแนวคิด สามารถพัฒนา White Paper (เอกสารปกขาว) หรือเอกสารรายงานเชิงลึกหลักนิยมการปฏิบัติการร่วมทางไซเบอร์ที่สนับสนุนแนวคิด Multi-Domain Operations (MDO), National Institute of Standards and Technology (NIST 800-115), SANS' Red Team Framework and Methodology (RTFM) และ Open Web Application Security Project (OWASP) รวมถึงการพัฒนานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์รัฐมนตรีกระทรวงกลาโหม (รมว.กห.) และ ผู้บัญชาการทหารสูงสุด (ผบ.ทสส.) แผนรับมือภัยคุกคามทางไซเบอร์ กองทัพไทย (ทท.) สนับสนุนสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) การปฏิบัติการทางไซเบอร์ ประกอบแผนป้องกันประเทศ กฎหมาย, พระราชบัญญัติ, กฎกระทรวง กฎการใช้กำลัง (Rules of Engagement: ROE) ที่เกี่ยวข้อง และมาตรฐานขั้นตอนการทำงาน (Standard Operating Procedure: SOP) ในบริบทที่สัมพันธ์กันกับยุทธศาสตร์และหลักนิยม ฯ

๔.๒.๒ การดำเนินการต่าง ๆ สามารถดำเนินการประเมินความเสี่ยง ตรวจประเมินทางไซเบอร์ที่เป็นมาตรฐาน ปฏิบัติการด้านการข่าวไซเบอร์ที่มีประสิทธิภาพ สร้างความร่วมมือด้านข่าวสารข้อมูลกับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานอื่นทั้งในและนอกประเทศ ดำเนินงานประชาคมไซเบอร์กองทัพไทย ประสานความร่วมมือกับต่างประเทศ ได้แก่ CDWG SSCI ADMM (Cyber) ปฏิบัติตามคู่มือการปฏิบัติการแบบ Red Team รวมถึงการปฏิบัติการ Joint Cyberspace Operations Task Force Deployment และ CTI Sharing

๔.๓ เทคโนโลยี (Technology)

๔.๓.๑ โรงเรียนไซเบอร์ทหาร มีห้องปฏิบัติการคอมพิวเตอร์สำหรับการเรียนและฝึกฝนอย่างพอเพียง มีระบบ Online Course ที่สามารถสนับสนุนการศึกษาด้วยตนเองสำหรับบุคลากรในข้อ ๔.๑.๑ รวมถึงระบบ Online Course ที่ได้รับการสนับสนุนจากต่างประเทศเช่น ระบบ IMCITE เป็นต้น มีระบบ Cyber Range & Simulation, Training Center, Training Labs ทางไซเบอร์ที่ต้องการอย่างครบถ้วน มีห้องปฏิบัติการเทคโนโลยีปฏิบัติการ (Operational Technology Lab: OT Lab) ที่เป็นห้องจำลองการฝึกเฝ้าระวังเหตุการณ์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๔.๓.๒ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ มีเครื่องมือที่จำเป็นในการปฏิบัติงานได้แก่ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ (Joint Cyber Operations Center: JCOC) และเทคโนโลยีการบังคับบัญชา และควบคุมทางไซเบอร์ (Cyber Command and Control Technology: Cyber-C2 Technology) ใช้วางแผน ควบคุม และประสานงาน Protect & Detect Response ใช้ป้องกันและตอบสนองต่อภัยคุกคาม Cyber Threat Intelligence ใช้วิเคราะห์ภัยคุกคามและให้ข้อมูลเชิงลึก Cloud & Edge Computing รองรับการจัดเก็บและประมวลผลข้อมูลจำนวนมาก Post Quantum Cryptography Technology ใช้การเข้ารหัสที่ป้องกันการโจมตีจากคอมพิวเตอร์ควอนตัมในอนาคต Zero Trusted Architecture Technology ปฏิบัติการบนหลักการ “ไม่เชื่อถือใคร” โดยตรวจสอบทุกการเข้าถึง

๔.๓.๓ เทคโนโลยีในการสนับสนุนทีมปฏิบัติการ มีเครื่องมือที่จำเป็นสำหรับการสนับสนุนการปฏิบัติงานได้แก่ Cyber Deployment Platform Technologies, Forensic, Big DATA, AI, GIS และการเตรียม Platform อื่น ๆ ที่จำเป็นสำหรับการปฏิบัติการ

๕. แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของ นซบ.ทหาร

นซบ.ทหาร มีสมรรถนะเฉพาะตำแหน่ง (Job-Specific Competencies) เพื่อให้เกิดความรู้ (Knowledge), ทักษะ (Skills), และความสามารถ (Abilities) ที่จำเป็นและเฉพาะเจาะจงสำหรับการปฏิบัติงานในตำแหน่งงานอย่างมีประสิทธิภาพซึ่งสมรรถนะดังกล่าวจะแตกต่างกันไปตามบทบาท หน้าที่และความรับผิดชอบ รวมไปถึงเพื่อให้องค์กรสามารถใช้สมรรถนะเฉพาะตัวแทนดังกล่าวเป็นกรอบในการคัดเลือก พัฒนาและประเมินผลกำลังพลได้อย่างเหมาะสมเพื่อความสอดคล้องกับภารกิจและเป้าหมายเชิงยุทธศาสตร์ขององค์กร

ทั้งนี้ ระบบการประเมินและพัฒนาบุคลากรของ นซบ.ทหาร ให้ความสำคัญกับ ๓ แกนหลักของสมรรถนะ ได้แก่ **๑). ความรู้ (Knowledge)** คือชุดข้อมูลและความเข้าใจที่บุคคลสั่งสมมาไม่ว่าจะผ่านการศึกษาหรือประสบการณ์ตรง เช่น ความรู้ด้านการขาย การเขียนโค้ด (Code) หรือความเชี่ยวชาญเฉพาะทางในวิชาชีพต่าง ๆ **๒). ทักษะ (Skills)** คือความเชี่ยวชาญที่เกิดจากการฝึกฝนและลงมือปฏิบัติจริง ซึ่งสามารถพัฒนาให้เกิดความชำนาญได้ เช่น ทักษะการสื่อสาร การแก้ปัญหาหรือการนำเสนอ และ **๓). ความสามารถ (Abilities)** คือคุณสมบัติภายในที่เป็นนามธรรม เช่น ทัศนคติที่ดี ในการทำงาน มนุษย์สัมพันธ์ ความกระตือรือร้น ความคิดสร้างสรรค์ หรือความยืดหยุ่น แม้สิ่งเหล่านี้จะจับต้องได้ยาก แต่ทุกคนสามารถเรียนรู้และพัฒนาได้ผ่านกระบวนการดังนี้

- การประเมินช่องว่าง (Gap Assessment) ตรวจสอบว่ากำลังพลในตำแหน่งต่าง ๆ มีทักษะอย่างไร

- หลักสูตรเฉพาะทาง (Micro Module) จัดการฝึกอบรมแบบย่อยที่เน้นแก้ปัญหาเฉพาะจุด เช่น การรับมือเหตุการณ์ละเมิด (Incident Handling) และ

- การสะสมประสบการณ์ พัฒนาจากระดับพื้นฐานจนถึงระดับผู้เชี่ยวชาญ (Expert) ที่สามารถตัดสินใจเชิงยุทธศาสตร์ในสถานการณ์วิกฤตได้

นอกจากนี้ นซบ.ทหาร ยังมียุทธศาสตร์การพัฒนากำลังพลด้านไซเบอร์ผ่านการใช้โมเดล Ends, Ways และ Means ในการดำเนินงานเพื่อให้สามารถระบุ **“คนที่ใช่สำหรับงานที่ใช่”** มีรายละเอียด ดังนี้

Ends (เป้าหมาย) คือการสร้างระบบสรรหาและพัฒนาบุคลากรที่อิงตามสมรรถนะ (Competency) เพื่อลดช่องว่างความรู้ (Gap Analysis) รวมถึงการสร้างเครื่องมือสำหรับการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทย ที่สามารถสรรหากำลังพลไซเบอร์ที่มีขีดความสามารถเฉพาะตำแหน่งทางไซเบอร์ รวมถึงสามารถ “ปิด” ช่องว่าง (Gap) ของสมรรถนะของชุดปฏิบัติการทางไซเบอร์ได้

Ways (วิธีการ) คือการกำหนดตำแหน่ง/บทบาทหน้าที่ ทางไซเบอร์, กำหนดชุดปฏิบัติการทางไซเบอร์กำหนดสมรรถนะเฉพาะตำแหน่ง และสมรรถนะของชุดปฏิบัติการทางไซเบอร์ เพื่อสร้างชุดการประเมินที่สามารถหาช่องว่าง (Gap) ของสมรรถนะเฉพาะตำแหน่งและสมรรถนะของชุดปฏิบัติการทาง ไซเบอร์ รวมถึงกำหนดหน่วยย่อยของการฝึกอบรม (Micro Module) เพื่อปิดช่องว่างดังกล่าว นซบ. ทหาร

ทั้งนี้ นซบ.ทหาร จะใช้ระบบการประเมินช่องว่างสมรรถนะ ๕ ระดับ เพื่อใช้ในการประเมิน และวางแผนการฝึกอบรม ได้แก่ **๑. Entry** รู้จักเหตุการณ์ไซเบอร์เบื้องต้นและรายงานตามขั้นตอนได้ **๒. Beginner** คัดกรองเหตุการณ์เบื้องต้นและดำเนินการกักกันภายใต้การกำกับดูแลได้ **๓. Intermediate** วิเคราะห์ความเชื่อมโยงของข้อมูลเพื่อหาต้นตอ (Root Causes) ได้ **๔. Advanced** พัฒนาและปรับปรุง Playbooks สำหรับตอบโต้ภัยคุกคามที่เกิดขึ้นซ้ำได้ และ **๕. Expert** บริหารจัดการเหตุการณ์วิกฤตและนำการตอบโต้ภัยคุกคามระดับสูงได้

Means (ทรัพยากร) ใช้ระบบ IMCITE สำหรับการฝึกอบรมเสมือนจริง (Cyber Range) ทั้งนี้ นซบ. ทหารได้จัดทำสมุดปกขาว (ยุทธศาสตร์ฉบับย่อ) ซึ่งได้กำหนดทิศทางการทำงานของหน่วยบัญชาการ ไซเบอร์ทหาร ดังนี้

- ทรัพยากรบุคคล นซบ. ทหาร พร้อมเข้าสู่กระบวนการพัฒนารวมถึงการจัดทำสมรรถนะ การประเมินและการอบรม นอกจากนี้ยังมีความร่วมมือกับหน่วยงานอุดมศึกษาและภาคเอกชนในการจัดทำสมรรถนะการประเมินและการอบรมอีกด้วย

- เทคโนโลยี นซบ. ทหาร ใช้ระบบ Server Cloud และระบบ IMCITE ที่ได้รับการสนับสนุนจากสหรัฐฯ ในการฝึกอบรม มีระบบ Server Cloud ของหน่วยบัญชาการไซเบอร์ทหาร ระบบ Server Cloud ของกรมการสื่อสารทหาร และมีระบบ IMCITE ที่ได้รับการสนับสนุนจากสหรัฐฯ สำหรับจัดทำระบบการฝึกอบรมรวมถึงมีแผนงาน ในการจัดหาเทคโนโลยีที่ทันสมัยมาสนับสนุนเครื่องมือสำหรับการฝึกอบรม

- งบประมาณ นซบ. ทหาร ได้รับงบประมาณสนับสนุนจากภาครัฐในการจัดทำสมรรถนะ และมีความร่วมมือระหว่างประเทศ (USA) ผ่าน Cyber Defense Working Group

อนึ่ง ปัจจัยสู่ความสำเร็จ ของ นซบ.ทหาร ได้แก่ การมีสมุดปกขาว (White Paper) ที่กำหนดยุทธศาสตร์ที่ชัดเจน โครงสร้างพื้นฐาน (ระบบ Server Cloud) และเครื่องมือที่ทันสมัยที่สามารถสนับสนุนการปฏิบัติงานรวมถึงเครือข่ายความร่วมมือได้รับการสนับสนุนจากกองทัพไทยและพันธมิตรนานาชาติ เพื่อก้าวให้ทันเทคโนโลยีไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว

ส่วนที่ ๓
การสรรหาและพัฒนากำลังพล ด้านไซเบอร์ในอนาคต



ส่วนที่ ๓ การสรรหาและพัฒนากำลังพลด้านไซเบอร์ในอนาคต

จากการสัมมนาปัญหายุทธศาสตร์ ครั้งที่ ๑/๒๕๖๙ หัวข้อ “แนวทางการสรรหาและพัฒนากำลงพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่” เมื่อวันที่ ๑๕ มกราคม พ.ศ. ๒๕๖๙ ผู้ร่วมการสัมมนา ประกอบด้วยผู้แทนหน่วยงานด้านไซเบอร์จากเหล่าทัพ หน่วยงานภาคพลเรือน และภาคเอกชน ในระดับนโยบาย ระดับอำนวยการ และระดับปฏิบัติการ รวมทั้งส่วนงานด้านกำลังพล ยุทธการ และวิชาการ รวมทั้งสิ้น ๔๐ ท่าน ทั้งนี้ ภายหลังการสัมมนามีการแบ่งกลุ่มย่อยเพื่อให้ผู้เข้าร่วมได้ระดมความคิด โดยแบ่งออกเป็น ๓ กลุ่ม ดังนี้ ๑) กลุ่มนโยบาย/ฝ่ายบริหาร ๒) กลุ่มอำนวยการ และ ๓) กลุ่มปฏิบัติการ เพื่อจัดทำภาพอนาคต (Scenario) ในหัวข้อ (Focal Question) **“การคาดการณ์ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่”** ซึ่งกำหนดตัวแปรผลักดัน (Driving Forces: DF) ที่จะส่งผลกระทบต่อการสรรหาและพัฒนากำลังพลด้านไซเบอร์ไว้ ๒ ตัว คือ (๑) ความรู้และความภาคภูมิใจในอาชีพ และ (๒) เงินเดือน ค่าตอบแทนและสวัสดิการ เพื่อใช้เป็นแกน X และ Y ในการวิเคราะห์ โดยการเลือก DF ทั้ง ๒ ตัว ได้ผ่านการพิจารณาด้วยกรอบแนวคิดด้านการบริหารทุนมนุษย์ (Human Capital Management) และทฤษฎีแรงจูงใจ (Motivation Theory) ดังนี้

- **ตัวแปรผลักดัน (DF) ที่ ๑: ความรู้และความภาคภูมิใจในอาชีพ**

ในมิติแรงจูงใจภายในและศักยภาพทุนมนุษย์ ตัวแปรนี้สะท้อนถึง **แรงจูงใจภายใน (Intrinsic Motivation)** และขีดความสามารถทางปัญญา ซึ่งเป็นรากฐานสำคัญของวิชาชีพทหารในยุคสงครามข้อมูลข่าวสาร (Information Warfare)

ในสมรภูมิไซเบอร์ อาวุธที่ทรงอานุภาพที่สุดคือ “สติปัญญา ความรู้ และทักษะ” ของบุคลากร เทคโนโลยีมีการเปลี่ยนแปลงในอัตราเร่ง ความรู้ของกำลังพลจึงเป็นตัวแปรที่มีความไม่แน่นอนสูง หากกองทัพไม่สามารถรักษาระดับความรู้ให้ทันต่อภัยคุกคามรูปแบบใหม่ (Zero-day exploits, AI-driven attacks) ศักยภาพในการป้องกันประเทศจะถดถอยลงทันที

ขณะที่ความภาคภูมิใจและอุดมการณ์ในองค์กรทางทหารมีลักษณะเฉพาะที่แตกต่างจากองค์กรธุรกิจ คือ การขับเคลื่อนด้วยอุดมการณ์ความรักชาติและเกียรติภูมิ ความภาคภูมิใจในอาชีพทำหน้าที่เป็น “พันธะทางจิตใจ” ที่ช่วยยึดเหนี่ยวให้บุคลากรที่มีความสามารถสูงยังคงปฏิบัติงานรับใช้ชาติ แม้จะต้องเผชิญกับสภาวะการทำงานที่มีความกดดันสูง ปัจจัยนี้จึงเป็นจุดแข็งเชิงเปรียบเทียบ (Comparative Advantage) เพียงประการเดียวที่กองทัพมีเหนือกว่าภาคเอกชน

➢ **ตัวแปรผลักดัน (DF) ที่ ๒: เงินเดือน ค่าตอบแทนและสวัสดิการ**

ในมิติแรงจูงใจภายนอกและพลวัตตลาดแรงงาน ปัจจัยนี้สะท้อนถึง **แรงจูงใจภายนอก (Extrinsic Motivation)** และสภาพแวดล้อมการแข่งขันทางเศรษฐศาสตร์ ซึ่งเป็นข้อจำกัดเชิงโครงสร้างที่สำคัญที่สุดของหน่วยงานภาครัฐ

ในสภาวะความขาดแคลนและสงครามแย่งชิงบุคลากร ผู้เชี่ยวชาญด้านไซเบอร์เป็นทรัพยากรบุคคลที่มีมูลค่าทางเศรษฐกิจสูงมาก และมีความต้องการในตลาดแรงงานโลกอย่างมหาศาล ภาคเอกชนสามารถใช้กลไกราคา ในการดึงดูดบุคลากรเหล่านี้ได้อย่างไร้ขีดจำกัด ขณะที่ความเปราะบางของโครงสร้างระบบราชการไทยมีความตายตัวและขาดความยืดหยุ่นในการปรับอัตราค่าตอบแทนให้สอดคล้องกับกลไกตลาด ความสามารถในการบริหารจัดการทรัพยากร เพื่อสร้างระบบสวัสดิการที่แข่งขันได้ (Competitive Benefits) จึงเป็นความไม่แน่นอนเชิงนโยบายระดับมหภาคที่ส่งผลโดยตรงต่อการตัดสินใจเข้าสู่ระบบ และการคงอยู่ของกำลังพล การไหลออกของสมอง (Brain Drain) ไปสู่ภาคเอกชนจึงเป็นความเสี่ยงเชิงยุทธศาสตร์ที่รุนแรงที่สุด

➢ เมื่อพิจารณาผ่าน **ทฤษฎีสองปัจจัยของเฮิร์ซเบิร์ก (Herzberg's Two-Factor Theory)** การนำสองแกนนี้มาตัดกันถือเป็นการจำลองสถานการณ์ที่ครอบคลุมมิติของพฤติกรรมมนุษย์อย่างสมบูรณ์ กล่าวคือ

(๑) แกน X มาจาก DF ความรู้และความภาคภูมิใจ ที่ทำหน้าที่เป็น ปัจจัยจูงใจ (Motivator Factors) หากกองทัพสามารถสร้างคุณค่าในงานและพัฒนาทักษะได้ จะก่อให้เกิดความผูกพันต่อองค์กรอย่างยั่งยืน

(๒) แกน Y มาจาก DF เงินเดือน ค่าตอบแทนและสวัสดิการ ที่ทำหน้าที่เป็นปัจจัยค้ำจุน (Maintenance Factors) หากกองทัพไม่สามารถตอบสนองความต้องการพื้นฐานทางเศรษฐกิจได้ กำลังพลจะเกิดความไม่พึงพอใจและลาออก

ดังนั้น การใช้พลวัตของการประสานกันระหว่าง "คุณค่าทางจิตใจ/อุดมการณ์" และ "ความมั่นคงทางกายภาพ/เศรษฐกิจ" จึงเป็นกรอบการวิเคราะห์ที่มีความสมเหตุสมผลเชิงวิชาการ และสามารถฉายภาพให้เห็นถึงความท้าทายเชิงโครงสร้างที่กองทัพไทยต้องเผชิญในการทำสงครามสมัยใหม่ได้อย่างเป็นรูปธรรม

จาก Driving Force (DF) ข้างต้น คณะนักวิชาการของศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ จึงทำการพิจารณาผ่านข้อมูลจากการศึกษางานวิจัยที่ผ่านมา ร่วมกับ

การใช้กระบวนการคาดการณ์อนาคตเชิงยุทธศาสตร์ตาม Focal Question ที่กำหนดที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อการตัดสินใจของกำลังพลด้านไซเบอร์ เพื่อกำหนด Future Events และจุดปลาย (Extremes) ของแกน X,Y ทั้ง ๒ แกน เพื่อจัดทำภาพอนาคต (Scenario) โดยมีรายละเอียดของการตัดทำแกน ดังนี้

Focal Question

"ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า"

- **แกน X**
  - **Driving Forces: ความรู้และความภาคภูมิใจในอาชีพ**
  - **Future Event: กำลังพลมีความเชี่ยวชาญในวิชาชีพเฉพาะและภาคภูมิใจในความเป็นทหาร** แกนนี้สะท้อนถึงปัจจัยด้านจิตใจ อุดมการณ์ และขีดความสามารถทางวิชาชีพของกำลังพลไซเบอร์
  - **จุดปลายด้านบวก X (+)**
    - ชื่อจุด: "อัจฉริยะไซเบอร์เปี่ยมเกียรติ" (Cyber Elite & Pride)
      คำอธิบาย: กำลังพลมีระดับความรู้และทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ล้ำสมัย เท่าทันภัยคุกคามรูปแบบใหม่ตลอดเวลา มีอุดมการณ์ความรักชาติและภาคภูมิใจอย่างสูงสุดที่ได้เป็น "นักรบไซเบอร์" ของกองทัพ รู้สึกว่างานที่ทำมีเกียรติ มีคุณค่า และเป็นฟันเฟืองสำคัญในการปกป้องอธิปไตยของชาติ
  - **จุดปลายด้านลบ X (-)**
    - ชื่อจุด: "ช่องว่างทักษะและศรัทธา" (Skill & Faith Gap)
      คำอธิบาย: กำลังพลขาดแรงจูงใจในการพัฒนาตนเอง ทำให้ความรู้และทักษะตามไม่ทันเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เกิดความรู้สึกหมดไฟ (Burnout) มองไม่เห็นคุณค่าหรือเกียรติภูมิในงานที่ทำ มองว่าเป็นเพียงงานธุรการหรืองานประจำวันทั่วไป ขาดอุดมการณ์ในการปกป้องชาติทางไซเบอร์

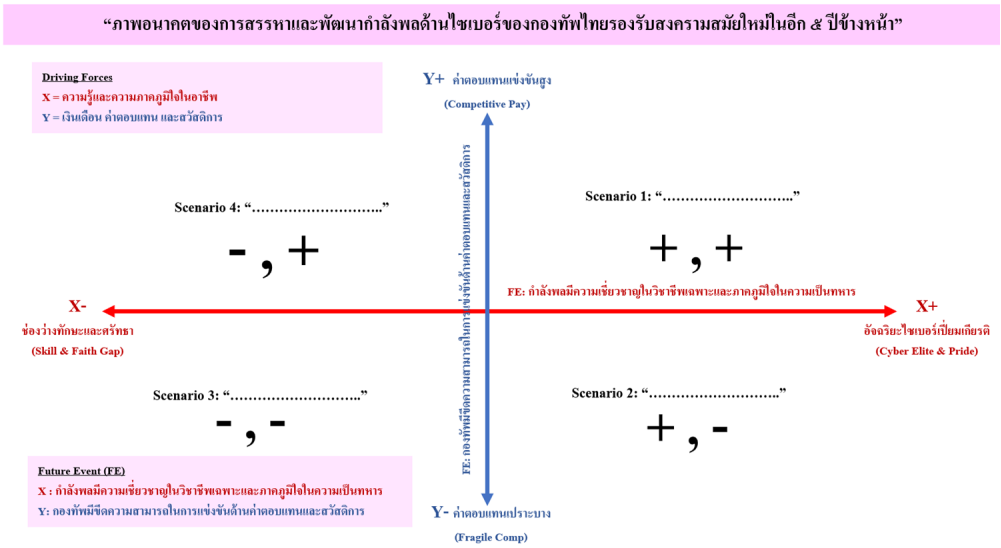
➢ **แกน Y**

- **Driving Forces: เงินเดือน ค่าตอบแทน และสวัสดิการ**
- **Future Event: กองทัพมีขีดความสามารถในการแข่งขันด้านค่าตอบแทนและสวัสดิการ** แกนนี้สะท้อนถึง แรงจูงใจภายนอก (Extrinsic Motivation) และสภาพแวดล้อมการแข่งขันทางเศรษฐศาสตร์ ซึ่งเป็นข้อจำกัดเชิงโครงสร้างที่สำคัญที่สุดของหน่วยงานภาครัฐและกองทัพ
- **จุดปลายด้านบวก Y (+)**
  - ชื่อจุด: “ค่าตอบแทนแข่งขันสูง” (Competitive Pay)
    คำอธิบาย: กองทัพมีงบประมาณและกลไกพิเศษที่สามารถจ่ายค่าตอบแทนเงินประจำตำแหน่ง และสวัสดิการ เช่น ที่พัก ทุนการศึกษา หรืออุปกรณ์เทคโนโลยี ให้กับผู้เชี่ยวชาญด้านไซเบอร์ในระดับที่ใกล้เคียง หรือสามารถแข่งขันกับบริษัทเทคโนโลยีในภาคเอกชนได้อย่างสูสี ทำให้ไม่มีปัญหาเรื่องสมองไหล (Brain Drain)
- **จุดปลายด้านลบ Y (-)**
  - ชื่อจุด: “ค่าตอบแทนเปราะบาง” (Fragile Comp)
  - **คำอธิบาย:** โครงสร้างเงินเดือนติดขัดด้วยระเบียบราชการและติดกรอบราชการแบบดั้งเดิม ไม่ดึงดูดใจ ทำให้ค่าตอบแทนและสวัสดิการต่ำกว่ามาตรฐานตลาดแรงงานด้านเทคโนโลยีในภาคเอกชนอย่างมาก ขาดแคลนทรัพยากรหรือกลไกพิเศษในการดึงดูดคนเก่ง สร้างความเหลื่อมล้ำทางรายได้จนเป็นอุปสรรคต่อการดำรงชีพของผู้เชี่ยวชาญ และเสี่ยงต่อปัญหาการไหลออกของบุคลากร (Brain Drain)

จัดทำเป็นแกน X, Y เพื่อใช้ในการจัดทำภาพอนาคต ดังนี้

๓.๑ การคาดการณ์ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์

จากการประชุมเชิงปฏิบัติการเพื่อวิเคราะห์ฉากทัศน์ (Scenario) ในมุมมองของกลุ่มทั้ง ๓ กลุ่ม คือ กลุ่มระดับนโยบาย/บริหาร, กลุ่มระดับอำนวยการ และกลุ่มระดับปฏิบัติการ เพื่อกำหนดทิศทาง เชิงยุทธศาสตร์ในอีก ๕ ปีข้างหน้า การตัดกันของแกน X และ แกน Y ทั้ง ๒ แกน จะทำให้เกิดภาพอนาคตหรือฉากทัศน์ (Scenario) ขึ้น ๔ ฉากทัศน์ ดังนี้



ภาพที่ ๓ แสดงการตัดกันของแกน X และ แกน Y ในการสร้างภาพอนาคต

จากภาพ กำหนดให้แกน X มี Future Event คือ กำลังพลมีความเชี่ยวชาญในวิชาชีพเฉพาะและภาคภูมิใจในความเป็นทหาร มาจาก Driving Force (DF) คือ ความรู้และความภาคภูมิใจในอาชีพ ขณะที่ แกน Y มี Future Event คือ กองทัพมีขีดความสามารถในการแข่งขันด้านค่าตอบแทนและสวัสดิการ ที่มาจากDriving Force (DF) คือ เงินเดือน, ค่าตอบแทน และสวัสดิการ จุดปลายของแกน X และ Y ที่เป็นบวกที่สุด (+) และจุดที่เป็นลบที่สุด (-) สามารถสร้างภาพอนาคตของการสรรหากำลังพลด้านไซเบอร์ของกองทัพรองรับสงครามสมัยใหม่ ตามตัวแปรผลักดัน (Driving Forces) และภาพเหตุการณ์ในอนาคต (Future Event) ที่ต้องการเพื่อคาดการณ์ภาพอนาคต โดยฉากทัศน์ทั้ง ๔ ฉากทัศน์มีรายละเอียด ดังนี้

ฉากทัศน์ที่ ๑: อัจฉริยะไซเบอร์เปี่ยมเกียรติ (X+) ควบคู่กับ ค่าตอบแทนแข่งขันสูง (Y+)

กองทัพไซเบอร์เกรียงไกร (The Cyber Vanguard)



ในบริบททั่วไป ฉากทัศน์นี้เป็นภาพอนาคตของกองทัพไซเบอร์เกรียงไกรที่พึงประสงค์ที่สุด (Best-case Scenario) ท่ามกลางสถานการณ์ความมั่นคงในมิติใหม่ที่มีความซับซ้อนและทวีความรุนแรงขึ้น เพราะกองทัพไทยสามารถปลดล็อกข้อจำกัดทางราชการ สร้างโครงสร้างค่าตอบแทนพิเศษที่ดึงดูดคนเก่งระดับแนวหน้า ควบคู่ไปกับการปลูกฝังอุดมการณ์ความรักชาติได้อย่างสมบูรณ์

ด้านการสรรหาและพัฒนา กองทัพกลายเป็นหนึ่งในองค์กรเป้าหมาย (Employer of Choice) ที่นักศึกษาหัวกะทิด้าน IT อยากร่วมงานด้วย มีงบประมาณสนับสนุนการฝึกอบรมเทคโนโลยีขั้นสูง (เช่น AI-driven Cybersecurity, Quantum Cryptography) ในระดับนานาชาติ

ขณะที่ด้านขีดความสามารถรองรับสงครามสมัยใหม่ กองทัพมีขีดความสามารถเต็มรูปแบบทั้งเชิงรับ (Defensive) และเชิงรุก (Offensive) สามารถป้องปรามภัยคุกคามทางไซเบอร์ที่มุ่งเป้ามายังโครงสร้างพื้นฐานระดับชาติได้อย่างเบ็ดเสร็จ

มุมมองของระดับนโยบาย/บริหาร ท่ามกลางสถานการณ์ความมั่นคงในมิติใหม่ที่มีความซับซ้อนและทวีความรุนแรงขึ้น ส่งผลให้กองทัพมีความต้องการ **“นักรบไซเบอร์”**

ระดับสมรรถนะสูงอย่างเร่งด่วน เมื่อกองทัพสามารถปฏิรูประบบโครงสร้างเงินเดือน ค่าตอบแทน และสวัสดิการให้เทียบเท่าหรือแข่งขันกับภาคเอกชนได้ อีกทั้ง ควบคู่ไปกับการสร้างระบบองค์ความรู้ที่ทันสมัยและเชิดชูเกียรติภูมิในอาชีพอย่างเป็นรูปธรรม ซึ่งจะกลายเป็นแรงดึงดูดสำคัญที่ทำให้กลุ่มคนผู้มีความสามารถในระดับอัจฉริยะได้หลั่งไหลเข้ามาและพร้อมอุทิศตนทำงานให้แก่กองทัพ ทั้งนี้ จะทำให้เกิดกำลังพลที่มีความพร้อมรบสูงและมีแรงบันดาลใจในการปฏิบัติภารกิจ รวมถึงปกป้องอธิปไตยทางไซเบอร์ของชาติได้อย่างมีประสิทธิภาพสูงสุด

มุมมองของระดับอำนวยการ ซึ่งเน้นหนักไปที่ระบบการบริหารจัดการ (Administrative) และความยั่งยืนของอัตรากำลังพลรวมถึงความสัมพันธ์เชิงโครงสร้างที่ส่งผลต่อเสถียรภาพของกองทัพ ฉากทัศน์นี้ คือ สภาวะที่ระบบบริหารจัดการกำลังพลมีประสิทธิภาพสูงสุด โดยกองทัพจะมีจำนวนกำลังพลด้านไซเบอร์ ที่เพียงพอต่อความต้องการและมีฐานตัวเลือกในการคัดสรรบุคลากรที่มีคุณภาพสูงเข้าสู่หน่วยงานมากขึ้น ทั้งนี้ ปัจจัยด้านความมั่นคงในอาชีพและผลตอบแทนที่คุ้มค่าจะส่งผลให้อัตราการลาออกต่ำ เนื่องจากกำลังพลจะผูกพันและปฏิบัติงานกับองค์กรในระยะยาว (Retention) จึงช่วยลดภารกิจและงบประมาณในการสรรหากำลังพลใหม่เข้ามาทดแทน นอกจากนี้ สภาพแวดล้อมที่เอื้อต่อการเรียนรู้ยังกระตุ้นให้กำลังพลมีความกระตือรือร้นในการทำงาน มุ่งมั่นพัฒนาขีดความสามารถและสมรรถนะของตนเองอย่างต่อเนื่อง ส่งผลให้ขีดความสามารถโดยรวมของหน่วยงานพร้อมรับมือกับภัยคุกคามสมัยใหม่ได้อย่างเต็มที่

มุมมองของระดับปฏิบัติการ ซึ่งจะมุ่งเน้นไปที่หน้างานจริงและสภาพแวดล้อมในการทำงานรวมถึงพฤติกรรมของกำลังพลด้านไซเบอร์ อีกทั้ง ความเสียงทางเทคนิคที่เกิดขึ้นในสนามรบไซเบอร์ (Cyber Battlefield) เพื่อกำหนดทิศทางเชิงยุทธศาสตร์ ในระดับปฏิบัติการ ฉากทัศน์นี้ กองทัพจะกลายเป็นองค์กรชั้นนำที่มีโอกาสในคัดเลือกบุคลากรระดับเชี่ยวชาญเข้ามาปฏิบัติงาน ส่งผลให้หน่วยงานได้กำลังพลที่มีศักยภาพที่ตรงตามความต้องการของหน่วยงานและรองรับสถานการณ์ที่เปลี่ยนแปลงไป อย่างไรก็ตาม ความพร้อมของกำลังพลกลุ่มนี้จะทำให้เกิดการแข่งขันอย่างรุนแรงในการแย่งชิงตัวบุคลากรไซเบอร์ระหว่างกองทัพและหน่วยงานอื่น ๆ ของรัฐ รวมถึงภาคองค์กรเอกชน ซึ่งผลกระทบที่จะตามมา คือ อัตราการหมุนเวียนการเปลี่ยนงาน (Turn Over Rate) ที่อาจขยับสูงขึ้น ทั้งนี้ สภาวะดังกล่าวจะส่งผลกระทบโดยตรงต่อความมั่นคงในการปฏิบัติการ (Operations Security: OPSEC) โดยเฉพาะความเสี่ยงทางข้อมูลยุทธวิธีอาจรั่วไหลติดตัวไปกับกำลังพลเมื่อมีการย้ายสังกัด

ฉากทัศน์ที่ ๒: อัจฉริยะไซเบอร์เปี่ยมเกียรติ (X+) ควบคู่กับค่าตอบแทนเปราะบาง (Y-)

นักรบอุดมการณ์พลีชีพ (The Patriotic Martyrs)



ในบริบททั่วไป โครงสร้างเงินเดือนของกองทัพยังคงล้าหลังและสวัสดิการไม่เพียงพอต่อการดำรงชีพในเศรษฐกิจยุคใหม่ แต่กองทัพยังคงรักษาศักยภาพไว้ได้ด้วย “คนเก่งกลุ่มเล็กๆ” ที่ขับเคลื่อนด้วยอุดมการณ์ความเสียสละและความภักดีต่อสถาบันทหารอย่างแรงกล้า

ด้านการสรรหาและพัฒนาทำได้ยากมาก ต้องอาศัยเครือข่ายความสัมพันธ์ส่วนตัวหรือความผูกพันดั้งเดิม กำลังพลต้องขวนขวายพัฒนาทักษะด้วยตนเอง (Self-learning) ท่ามกลางข้อจำกัดทางทรัพยากร

ขณะที่ด้านขีดความสามารถรองรับสงครามสมัยใหม่ กองทัพสามารถป้องกันการโจมตีได้ในระดับที่น่าพอใจ แต่เป็นความมั่นคงที่ “เปราะบางอย่างยิ่ง” เนื่องจากพึ่งพิงความสามารถของบุคลากรระดับคีย์แมนเพียงไม่กี่คน (Single Point of Failure) หากกลุ่มอุดมการณ์เหล่านี้รับภาระไม่ไหว เกิดภาวะหมดไฟ (Burnout) หรือปัญหาทางการเงินส่วนตัวจนต้องลาออก ระบบป้องกันทั้งหมดจะล่มสลายทันที

มุมมองของระดับนโยบาย/บริหาร ในสภาวะที่กองทัพมีข้อจำกัดด้านงบประมาณ จึงทำให้ไม่สามารถยกระดับค่าตอบแทนให้สูงตามกลไกของตลาดทางเศรษฐกิจได้ แต่อย่างไรก็ตาม

กองทัพยังคงโดดเด่นในแง่ของการเป็นศูนย์รวมขององค์ความรู้และสามารถสร้างวัฒนธรรมองค์กรที่หล่อหลอมในความภาคภูมิใจและเกียรติยศในการเป็นผู้ปกป้องความมั่นคงของชาติได้ กระนั้น กำลังพลในกลุ่มนี้จะมีลักษณะของการ**ทำงานเพื่อสังคมและอุดมการณ์**เป็นหลัก และยังมีความจงรักภักดีและภาคภูมิใจในองค์กร แม้จะได้รับผลตอบแทนในระดับต่ำ ทั้งนี้ สถานะในฉากทัศน์ที่ ๒ จะทำให้กองทัพมีความท้าทายด้วยความเสี่ยงในการสูญเสียกำลังพลในระยะยาว (Brain Drain) หากความกดดันทางเศรษฐกิจภายนอกมีมากกว่าแรงขับเคลื่อนทางอุดมการณ์

มุมมองของระดับอำนวยการ ในฉากทัศน์นี้จะยังคงขับเคลื่อนไปได้ด้วยกลุ่มกำลังพลที่มีหัวใจรักมั่นในองค์กรและพร้อมอุทิศตน เสียสละเพื่อส่วนรวมอย่างแท้จริง แต่ในทางปฏิบัติระดับอำนวยการจะต้องเผชิญกับภาวะ “สมองไหล” (Brain Drain) เนื่องจากบุคลากรที่มีความเชี่ยวชาญบางส่วนทนแรงเสียดทานทางเศรษฐกิจภายนอกไม่ไหว จึงอาจส่งผลให้หน่วยงานประสบปัญหาขาดแคลนกำลังพล อีกทั้ง อัตราบรรจุไม่เต็มตามความต้องการ และเกิดความเหลื่อมล้ำในการทำงาน นอกจากนี้ ยังพบปัญหาสำคัญคือกำลังพลที่เหลืออยู่จะไม่สามารถแสดงขีดความสามารถออกมาได้อย่างเต็มประสิทธิภาพ เนื่องจากต้องแบกรับภาระงานที่เกินกำลัง (Burnout) และขาดแคลนเครื่องมือหรือการสนับสนุนที่เหมาะสมอันเนื่องมาจากข้อจำกัดทางงบประมาณ

มุมมองของระดับปฏิบัติการ เมื่อมีการปฏิบัติงานภายใต้เงื่อนไขที่ขาดแคลนด้านงบประมาณและการสนับสนุน แต่กำลังพลยังมีความรักและภาคภูมิใจในอาชีพสูง ทั้งนี้ ภาพที่เกิดขึ้นในระดับปฏิบัติการ คือ กำลังพลต้องยอมเสียสละค่าใช่จ่ายส่วนตัวเพื่อซื้ออุปกรณ์คอมพิวเตอร์หรือเครื่องมือไอทีที่มีประสิทธิภาพสูงมาใช้ในการทำงานให้แก่ภาครัฐ เพื่อให้ภารกิจสำเร็จลุล่วง แต่อย่างไรก็ตาม ความเสียสละนี้กลับกลายเป็นดาบสองคมที่ทำให้ผู้บังคับบัญชาหรือองค์กรมองไม่เห็นถึงปัญหาที่แท้จริงที่ควรได้รับการแก้ไขโดยเฉพาะปัญหาด้านงบประมาณที่ไม่สอดรับกับสภาวการณ์จริง และยิ่งไปกว่านั้นคือการขาดงบการสนับสนุนนี้ยังทำให้กำลังพลขาดโอกาสในการเข้าถึงการฝึกอบรมเพื่อพัฒนาทักษะใหม่ ๆ ให้เท่าทันต่อเทคโนโลยีที่เปลี่ยนไปอย่างรวดเร็ว ซึ่งจะทำให้กำลังพลในระดับปฏิบัติการเกิดภาวะหมดไฟ (Burnout) และสูญเสียแรงจูงใจในการทำงานไปอย่างน่าเสียดายจากการที่ต้องแบกรับระบบด้วยอุดมการณ์เพียงอย่างเดียว

ฉากทัศน์ที่ ๓: ช่องว่างทักษะและศรัทธา (X-) ควบคู่กับ ค่าตอบแทนเปราะบาง (Y-)

ปราการไซเบอร์ล่มสลาย (The Defenseless Frontier)



ในบริบททั่วไป ฉากทัศน์นี้เป็นภาพอนาคตที่เลวร้ายที่สุด (Worst-case Scenario) กองทัพเผชิญกับวิกฤตขีดความสามารถอย่างรุนแรง ระบบราชการไม่สามารถปรับอัตราเงินเดือนให้แข่งขันได้ และสภาพแวดล้อมการทำงานเต็มไปด้วยระบบอุปถัมภ์ที่ทำลายเกียรติภูมิในวิชาชีพ

ด้านการสรรหาและพัฒนา เกิดภาวะ “สมองไหล” (Brain Drain) อย่างหนัก คนเก่งลาออกไปอยู่ภาคเอกชนทั้งหมด การสรรหาได้เพียงบุคลากรที่ไม่มีทางเลือกอื่นหรือขาดคุณสมบัติที่เหมาะสม โครงการพัฒนาบุคลากรหยุดชะงักเพราะขาดงบประมาณและผู้นำที่มีวิสัยทัศน์

ขณะที่ด้านขีดความสามารถรองรับสงครามสมัยใหม่ กองทัพสูญเสียอธิปไตยทางไซเบอร์โดยสิ้นเชิง ไม่สามารถตรวจจับหรือป้องกันการโจมตีทางไซเบอร์ระดับชาติได้โครงสร้างพื้นฐานทางยุทธศาสตร์ถูกเจาะทำลายอย่างง่ายดาย

มุมมองของระดับนโยบาย/บริหาร ฉากทัศน์นี้เป็นภาพที่เสี่ยงมากที่สุด เมื่อโครงสร้างค่าตอบแทนและสวัสดิการของกองทัพอยู่ในเกณฑ์ต่ำ ไม่จูงใจ อีกทั้งองค์กรยังขาดระบบการพัฒนาองค์ความรู้ที่ชัดเจน และขาดการสร้างคุณค่าหรือความภาคภูมิใจในสายงานด้านไซเบอร์

ดังนั้น สิ่งที่จะเกิดขึ้นก็คือ กองทัพจะดึงดูดได้เพียงกลุ่มคนที่เข้ามาเพื่อแสวงหาความมั่นคงขั้นพื้นฐานหรือสวัสดิการขั้นต้นเท่านั้น แต่จะขาดความรักในองค์กร ความภาคภูมิใจ และแรงผลักดันในการพัฒนาตนเอง ซึ่งจะส่งผลให้กองทัพตกอยู่ในภาวะวิกฤต ที่ขาดแคลนขีดความสามารถในการเผชิญหน้ากับสงครามไซเบอร์สมัยใหม่โดยสิ้นเชิง

มุมมองของระดับอำนวยการ ฉากทัศน์นี้ ขั้นวิกฤตที่ระดับอำนวยการจะสูญเสียการควบคุมระบบการทำงานอย่างสิ้นเชิง กองทัพจะประสบภาวะขาดแคลนกำลังพลขั้นรุนแรงจนไม่มีบุคลากรเพียงพอในการปฏิบัติภารกิจหลักด้านไซเบอร์ นอกจากนี้กำลังพลที่หลงเหลืออยู่จะปฏิบัติงานด้วยความเพิกเฉย ไร้ความภาคภูมิใจในเกียรติยศของทหารไซเบอร์และมีความตื่นตัวพร้อมที่จะโยกย้ายหน่วยงานหรือลาออกทันทีที่มีโอกาส ทั้งนี้ สิ่งที่น่ากังวลที่สุดในเชิงการบริหารความเสี่ยง คือ กำลังพลบางส่วนอาจใช้ช่องโหว่จากความรู้และสิทธิ์การเข้าถึงระบบไซเบอร์แสวงหาผลประโยชน์ในทางมิชอบ หรือเกิดการทุจริตคอร์รัปชัน ซึ่งถือเป็นภัยคุกคามร้ายแรงต่อความมั่นคงของกองทัพ

มุมมองของระดับปฏิบัติการ ฉากทัศน์นี้จะเป็นฝันร้ายของกำลังพลในระดับปฏิบัติการ เนื่องจากกองทัพจะได้บุคลากรที่ขาดประสิทธิภาพและไม่มีขีดความสามารถที่เหมาะสม ซึ่งถือว่าไม่คุ้มค่ากับอัตราตำแหน่งที่เสียไป อีกทั้ง ปัญหาการขาดแคลนกำลังพลที่มีความเชี่ยวชาญจะบีบให้หน่วยงานต้องเสียงบประมาณซ้ำซ้อนไปกับการจ้างงานบุคคล (Outsource) หรือบุคลากรภายนอกเข้ามาดูแลระบบความมั่นคงซึ่งจะทำให้ป้องกันการรั่วไหลของข้อมูลได้ยาก อย่างไรก็ตาม ปัจจัยความเสี่ยงที่ร้ายแรงที่สุดในทางปฏิบัติ คือ เมื่อกำลังพลที่ปฏิบัติงานขาดความภาคภูมิใจและพร้อมที่จะลาออกตลอดเวลา นอกจากนั้น ยังต้องเผชิญกับความฝืดเคืองทางรายได้ที่อาจนำไปสู่ปัญหาการรั่วไหลของข้อมูลความมั่นคงจากกำลังพลภายในองค์กรเอง ทั้งนี้ ไม่ว่าจะเกิดจากความหละหลวม, ความประชดประชันต่อองค์กร หรือการจงใจขายข้อมูลเพื่อความอยู่รอดก็ตาม

ฉากทัศน์ที่ ๔: ช่องว่างทักษะและศรัทธา (X-) ควบคู่กับ ค่าตอบแทนแข่งขันสูง (Y+)

กรงทองของนักรบไร้ใจ (The Gilded Cage)



ในบริบททั่วไป รัฐบาลทุ่มงบประมาณมหาศาลในการเพิ่มเงินเดือนและสวัสดิการ แต่ล้มเหลวในการสร้างแรงจูงใจภายใน (Intrinsic Motivation) หรือไม่สามารถพัฒนาระบบนิเวศการทำงานที่ท้าทาย

การสรรหาและพัฒนาสามารถดึงดูดคนเข้ามาร่วมงานได้มากเพราะผลตอบแทนดี แต่กลายเป็น “ที่พักพิง” ของบุคลากรที่หมดไฟ (Deadwood) หรือคนที่แสวงหาความสบาย กำลังพลขาดแรงขับเคลื่อนในการเรียนรู้สิ่งใหม่ มองงานเป็นเพียงกิจวัตร ไม่มีความยึดโยงกับอุดมการณ์ทหาร

ขณะที่ในด้านขีดความสามารถรองรับสงครามสมัยใหม่ กองทัพมีเทคโนโลยีและซอฟต์แวร์ราคาแพง แต่ขาดบุคลากรที่มีไหวพริบในการประยุกต์ใช้ เมื่อเผชิญการโจมตีทางไซเบอร์รูปแบบใหม่ที่ซับซ้อน จะมีปฏิกิริยาตอบสนองที่ล่าช้าและล้มเหลวในการปกป้องข้อมูลความมั่นคง

มุมมองของระดับนโยบาย/บริหาร เมื่อกองทัพทุ่มงบประมาณไปกับการปรับระดับค่าตอบแทน และสวัสดิการที่สูง พร้อมการสร้างแรงจูงใจด้วยทุนการศึกษาและสวัสดิการที่ดีเยี่ยมเพื่อดึงดูดคนที่มีความสามารถแต่กลับล้มเหลวในการสร้างระบบองค์ความรู้ที่ยั่งยืน และไม่สามารถสร้างความภาคภูมิใจในอาชีพทหารได้ ดังนั้น ผลลัพธ์ที่ได้ คือ กลุ่มกำลังพล

ที่มีความสามารถสูง แต่อุดมการณ์ต่ำจะมองงานด้านไซเบอร์ของกองทัพเป็นเพียงงานประจำ หรือเป็น “ทางผ่าน” (Stepping Stone) เพื่อสร้างโปรไฟล์ด้วยการพัฒนาทักษะชั่วคราว ก่อนที่จะลาออกไปสู่ภาคเอกชนที่ให้ผลตอบแทนสูงกว่า นอกจากนี้ กำลังพลจะไม่เห็นความสำคัญเชิงยุทธศาสตร์ของภารกิจและมุ่งเน้นประโยชน์ส่วนตนมากกว่าความมั่นคงของชาติ

มุมมองของระดับอำนวยการ ในด้านการบริหารจัดการระดับอำนวยการจะพบกับกลุ่มกำลังพลที่เข้ามาทำงานและคงอยู่เพียงเพื่อหวังเงินเดือน, ผลตอบแทนและสวัสดิการเท่านั้น ซึ่งการปฏิบัติงานจะเป็นไปในลักษณะทำตามหน้าที่ไปวัน ๆ ขาดจิตวิญญาณความทุ่มเทและความเสียสละหรือการคิดค้นนวัตกรรมใหม่ ๆ ให้แก่กองทัพ ทั้งนี้ จึงทำให้กลุ่มระดับอำนวยการไม่สามารถดึงขีดความสามารถที่แท้จริงของกำลังพลมาใช้ในภารกิจสงครามไซเบอร์ได้อย่างเต็มที่ และยิ่งไปกว่านั้นการที่ตำแหน่งนี้มีผลตอบแทนที่สูงแต่ขาดเกณฑ์การวัดที่พิจารณาคุณค่าด้านความรู้และความสามารถที่แท้จริงของบุคคลก็จะนำไปสู่การทุจริตวิ่งเต้น รวมถึงวัฏจักรของ **“ระบบอุปถัมภ์”** ซึ่งจะทำลายระบบคุณธรรม (Merit System) ของสายงานไซเบอร์ลงในที่สุด

มุมมองของระดับปฏิบัติการ ฉากทัศน์นี้ แม้ว่ากองทัพจะจ่ายค่าตอบแทนและสวัสดิการที่สูง อย่างไรก็ตาม การขาดความรู้และความภาคภูมิใจในองค์กรต่ำจะส่งผลให้กำลังพลในระดับปฏิบัติการมองกองทัพเป็นเพียง “สถานที่ชุบตัว” หรือเป็นทางผ่านเพื่อเก็บเกี่ยวประสบการณ์ ก่อนที่จะลาออกไปทำงานในบริษัทเอกชน หรือแม้กระทั่งองค์กรต่างชาติที่มีข้อเสนอที่ดีกว่า ทั้งนี้ จึงทำให้เกิดปัญหาสมองไหลที่พ่วงเอาองค์ความรู้ภายในของกองทัพออกไปด้วยและยิ่งไปกว่านั้น ด้านพฤติกรรมที่พบได้บ่อยในการปฏิบัติงานคือ การปฏิบัติงานราชการแบบเช้าชามเย็นชาม ไม่คุ้มค่ากับค่าตอบแทนที่ได้รับ แต่ในทางกลับกันกลับเลือกให้เวลาและทุ่มเทความสามารถกับงานเสริม (Moonlighting) มากกว่า ส่งผลให้ประสิทธิภาพในการเฝ้าระวังภัยคุกคามของกองทัพลดลงและเกิดผลประโยชน์ทับซ้อนที่ยากจะตรวจสอบได้

กล่าวโดยสรุป การจัดการกำลังพลเชิงรุกโดยมุ่งเน้นไปที่ปัจจัยใดปัจจัยหนึ่งเพียงอย่างเดียวไม่สามารถสร้างกองทัพไซเบอร์ที่เข้มแข็งได้จากการอัดฉีดเงินเดือนสูงเพียงอย่างเดียว ซึ่งจะได้เพียงคนเก่งที่ไม่มีความภาคภูมิใจในองค์กรหรือการใช้เพียงอุดมการณ์ขับเคลื่อนก็อาจไม่เพียงพอในยุคเศรษฐกิจดิจิทัล ดังนั้น เป้าหมายสูงสุดที่จะต้องขับเคลื่อนให้เกิดขึ้นในอีก ๕ ปีข้างหน้า

ในมุมมองของกลุ่มผู้บังคับบัญชาในระดับนโยบาย/บริหาร คือ การพาองค์กรไปสู่**ฉากทัศน์ที่ ๑ กองทัพไซเบอร์เกรียงไกร (The Cyber Vanguard)** ซึ่งต้องอาศัยแนวทางคู่ขนาน คือ **๑). Hard Factors:** การปฏิรูปโครงสร้างสิทธิประโยชน์ ค่าตอบแทนพิเศษตามทักษะ (Skill-Based Pay) และสวัสดิการให้แข่งขันได้จริง **๒). Soft Factors:** การออกแบบเส้นทางความก้าวหน้า (Career Path) ที่ชัดเจน รวมถึงการติดอาวุธทางปัญญาด้วยเทคโนโลยีเปลี่ยนโลก (Disruptive Technology) และการสถาปนาเกียรติภูมิของนักรบไซเบอร์ทหารให้เป็นที่ประจักษ์ เพื่อให้ได้กำลังพลที่ **“เก่ง กล้า ศรัทธา และยั่งยืน”** พร้อมรับมือสงครามสมัยใหม่อย่างแท้จริง

ขณะที่ในมุมมองของระดับอำนวยการ ชี้ให้เห็นอย่างชัดเจนว่า ความล้มเหลวในการสร้างความสมดุลระหว่างโครงสร้างของผลตอบแทนและการสร้างคุณค่าในอาชีพจะนำไปสู่วิกฤตเชิงโครงสร้างและการปฏิบัติงานที่ไม่อาจแก้ไขได้ ทั้งนี้ หากกลุ่มระดับอำนวยการแก้ปัญหาเฉพาะหน้าด้วยการอัดฉีดงบประมาณเพียงอย่างเดียว อาจจะทำให้หน่วยงานเต็มไปด้วยกำลังพลที่ไร้ประสิทธิภาพและเกิดปัญหาการเมืองภายในองค์กร นอกจากนี้ หากพึ่งพาเพียงระบบอุดมการณ์และความรักชาติ อาจส่งผลให้หน่วยงานต้องแบกรับความเสี่ยงจากอัตรากำลังพลที่โหว่และไร้เสถียรภาพ ดังนั้น ในระดับอำนวยการ **กลไกสำคัญที่จะต้องเร่งดำเนินการเพื่อผลักดันองค์กรเข้าสู่ฉากทัศน์ที่ ๑ คือ การวางระบบที่เชื่อมโยงระหว่างผลตอบแทนและคุณธรรมเข้าด้วยกัน** ซึ่งผ่านการออกแบบระบบประเมินผลงานตามขีดความสามารถจริง รวมถึงการจัดทำเส้นทางเติบโตที่โปร่งใสและการสร้างสภาพแวดล้อมการทำงานที่สนับสนุนคนที่มีความสามารถเพื่อให้มั่นใจว่าเงินงบประมาณที่จ่ายไป และสามารถแปรเปลี่ยนเป็นความพร้อมรบที่จับต้องได้ในสงครามสมัยใหม่อย่างแท้จริง

และในมุมมองของระดับปฏิบัติการ สิ่งที่สะท้อนออกมาอย่างชัดเจนคือกำลังพลหน้างานด้านไซเบอร์ไม่สามารถขับเคลื่อนได้ด้วยเงินหรือด้วยใจเพียงอย่างใดอย่างหนึ่ง เพราะในโลกของเทคโนโลยีและสงครามสมัยใหม่ ปัจจัยทั้งสองส่งผลกระทบต่อพฤติกรรมและความปลอดภัยของข้อมูลอย่างมีนัยสำคัญ ทั้งนี้การให้ผลตอบแทนสูงแต่ไม่มีความภาคภูมิใจในอาชีพจะทำให้กองทัพกลายเป็นศูนย์ฝึกอบรมฟรีเพื่อส่งต่อให้เอกชน และเสี่ยงต่อการที่กำลังพลไปรับงานนอกจนเสียงานหลวง นอกจากนี้ การใช้แต่อุดมการณ์โดยไม่ดูแลคุณภาพชีวิตก็จะนำไปสู่ภาวะหมดไฟและการแก้ปัญหาแบบซุกไว้ใต้พรมจากการที่กำลังพลต้องแบกรับค่าใช้จ่ายเอง ดังนั้น ในมุมมองของระดับปฏิบัติการ **สิ่งที่ควรต้องเร่งสร้างคือ กลไกการควบคุมและจูงใจที่สมดุล เพื่อมุ่งสู่ฉากทัศน์ที่ ๑** ซึ่งจะเป็นสนามการแข่งขันของมืออาชีพและความท้าทาย

ด้านความมั่นคงข้อมูลต้องมีมาตรการรองรับที่จับต้องได้ เช่น การกำหนดข้อตกลงรักษาความลับ (NDA) และระยะเวลาการทำงานที่เหมาะสม เพื่อควบคุมอัตราการหมุนเวียนของคน (Turn Over Rate) รวมถึงควบคู่ไปกับการจัดหาเครื่องมือ อุปกรณ์คอมพิวเตอร์ และซอฟต์แวร์ที่ทันสมัยให้พร้อมรบ โดยไม่ปล่อยให้เป็นภาระของกำลังพล เพื่อแปรเปลี่ยน **“คนเก่ง”** ให้กลายเป็น **“นักรบไซเบอร์”** ที่มีประสิทธิภาพและมีธรรมาภิบาลในสมรภูมิ



แผนภาพที่ ๔ แสดง ภาพอนาคตของการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า

แกน X: Driving Forces: ความรู้และความภาคภูมิใจในอาชีพ

Future Event: กำลังพลมีความเชี่ยวชาญในวิชาชีพเฉพาะและภาคภูมิใจในความเป็นทหาร

แกน Y: Driving Forces: เงินเดือน ค่าตอบแทน และสวัสดิการ

Future Event: กองทัพมีขีดความสามารถในการแข่งขันด้านค่าตอบแทนและสวัสดิการ

๓.๒ แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่

มุมมองระดับนโยบาย/บริหาร: เน้นความภาคภูมิใจและอิสระในการบริหาร

แนวทางการเตรียมความพร้อมของกองทัพไทยสำหรับการสรรหาและพัฒนากำลังพลด้านไซเบอร์รองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า ตามมุมมองของกลุ่มระดับนโยบาย/บริหาร สามารถสรุปได้เป็น ๒ แนวทาง ดังนี้

๑). การสร้างมาตรฐานใหม่ในการสรรหา (New Recruitment Standards) เน้นการพัฒนาระบบการคัดเลือกให้มีความยืดหยุ่นและดึงดูดผู้มีศักยภาพสูง ผ่านการคัดเลือกด้วยคุณวุฒิวิชาชีพด้านความมั่นคงไซเบอร์ (Certificates) เป็นเกณฑ์สำคัญในการพิจารณา ลดขั้นตอนและอุปสรรคผ่านการปรับลดกฎระเบียบที่ซ้ำซ้อนเพื่อให้กระบวนการสรรหาคล่องตัวและรวดเร็วยิ่งขึ้น อีกทั้ง จัดสรรงบประมาณด้านทุนการศึกษาในสาขาที่ตรงความต้องการโดยเฉพาะเพื่อสร้างบุคลากรที่มีคุณสมบัติตรงความต้องการของกองทัพ รวมถึงมีมาตรการผูกพันและสร้างแรงจูงใจด้วยการปรับเพิ่มเงินเดือนตามระยะเวลาการทำงานและทักษะ มีสัญญาข้อผูกพันการทำงานที่ชัดเจนพร้อมบทลงโทษหากผิดสัญญา และจัดทำบัญชีรายชื่อกำลังพลด้านไซเบอร์ (Cyber Reserve) ในรูปแบบเดียวกับกำลังพลสำรอง นอกจากนี้ ยังมีการใช้โมเดล “ยืมตัวบุคลากร” พร้อมผลตอบแทนคู่ขนาน ทั้งนี้ รัฐบาลอนุญาตให้กำลังพลไซเบอร์สามารถรับงานหรือรับผลตอบแทนเพิ่มเติมจากหน่วยงานเอกชนที่เป็นพันธมิตรทางยุทธศาสตร์ของกองทัพได้

๒). การสร้างมาตรฐานใหม่ในการรักษากำลังพล (New Retention Standards) เน้นการพัฒนาเส้นทางอาชีพและสวัสดิการที่ยั่งยืน เพื่อให้กำลังพลสามารถเติบโตได้ในสายงานเทคนิคโดยตรง และมีกฎหมายรองรับกำลังพลสำรอง ผ่านการตรากฎหมายคุ้มครองและกำหนดค่าตอบแทนที่เหมาะสมสำหรับกำลังพลสำรองด้านไซเบอร์ นอกจากนี้ กำหนดค่าตอบแทนที่เหมาะสม ด้วยการตรากฎหมายเกี่ยวกับ “อัตราเงินเดือนพิเศษบุคลากรด้านความมั่นคงไซเบอร์” โดยปลดล็อกเพดานเงินเดือนจากระบบราชการปกติแล้วกำหนดฐานเงินเดือนและค่าตอบแทนพิเศษ (Hazard Pay/Skill Pay) ให้เทียบเท่าภาคเอกชนชั้นนำ อีกทั้งการพัฒนาและประเมินผลต่อเนื่องโดยการเพิ่มหลักสูตรอบรมด้านไซเบอร์ให้ทันสมัยอยู่เสมอพร้อมกับการวางระบบประเมินคุณภาพเพื่อคัดกรองและรักษาบุคลากรที่มีประสิทธิภาพไว้กับหน่วยงาน ทั้งนี้ ระบบดังกล่าวต้องประสานสอดคล้องระหว่างงานด้านเทคนิคและการบังคับใช้กฎหมายเพื่อให้การปฏิบัติงานมีประสิทธิภาพและก้าวหน้าไปพร้อมกัน

โดยสรุป ในมุมมองระดับนโยบาย/บริหาร นโยบายในอนาคตมุ่งเน้นการเปลี่ยนผ่านสู่ระบบคุณธรรมและความเชี่ยวชาญ โดยใช้แรงจูงใจด้านค่าตอบแทนและเส้นทางอาชีพที่เป็นสากลเพื่อให้กองทัพสามารถแข่งขันกับตลาดแรงงานภายนอกและรักษาบุคลากรที่มีความเชี่ยวชาญไว้ได้

มุมมองระดับอำนวยการ: เน้นการการสร้างแรงจูงใจและการพัฒนาขีดความสามารถในวิชาชีพ

แนวทางการเตรียมความพร้อมของกองทัพไทยสำหรับการสรรหาและพัฒนากำลังพลด้านไซเบอร์รองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า ตามมุมมองของกลุ่มระดับอำนวยการมุ่งเน้นการใช้เครื่องมือบริหารจัดการเพื่อแก้ปัญหาและส่งเสริมศักยภาพตามสภาวะของทรัพยากรมนุษย์ สามารถสรุปได้ เป็น ๔ แนวทาง ดังนี้

๑). แนวทางเมื่อมีสภาวะค่าตอบแทนและสวัสดิการที่สูง ให้ความสำคัญกับการใช้ทรัพยากรเพื่อสร้างความยั่งยืนและความเป็นเลิศยกระดับวิชาชีพส่งเสริมความเจริญก้าวหน้าในสายงาน (Career Path) และสร้างกำลังพลให้เป็นบุคคลต้นแบบขององค์กร รวมถึงรักษากำลังพลที่มีขีดความสามารถไว้กับหน่วยงาน/องค์กร โดยใช้ค่าตอบแทนเป็นฐานในการพิจารณาและพัฒนาขีดความสามารถด้วยการเพิ่มพูนทักษะของกำลังพลในหน่วยให้สูงขึ้นอย่างต่อเนื่อง พร้อมทั้ง เสริมสร้างภาพลักษณ์ ยกย่อง เชิดชูเกียรติยศของทหารให้กำลังพลมีความภาคภูมิใจในเกียรติภูมิและศักดิ์ศรีของทหารไซเบอร์

๒). แนวทางเมื่อมีสภาวะค่าตอบแทนและสวัสดิการที่ต่ำ เน้นการปรับปรุงระบบและการบริหารจัดการเชิงรุกเพื่อแก้ปัญหากำลังพลขาดแคลน โดยปฏิรูปการสรรหาปรับระเบียบให้เอื้อต่อการคัดสรรคนเก่งแบบเชิงรุก เช่น การแข่งขันทักษะ (Cyber Contest) การรับพลเรือนพาร์ทไทม์และการให้ทุนการศึกษา โดยใช้โมเดลการจ้างงานแบบยืดหยุ่น เช่น ระบบการจ้างบุคคล (Outsource) หรือการจ้างงานรายภารกิจ นอกจากนี้ ยังมีการบูรณาการความร่วมมือกับหน่วยงานภายนอก อีกทั้งการทดแทนด้วยเทคโนโลยี โดยการนำเทคโนโลยีสมัยใหม่มาปฏิบัติการแทนในส่วนที่ขาดแคลนกำลังพล พร้อมทั้งเพิ่มแรงจูงใจทางอ้อมกำหนดเครื่องหมายความสามารถและสิทธิประโยชน์อื่นที่ไม่ใช่เงินเดือน และมีระบบลงโทษที่ชัดเจนเพื่อรักษามาตรฐาน

๓). แนวทางแก้ไขเมื่อกำลังพลขาดความรู้และความภาคภูมิใจในอาชีพต่ำ เน้นการสร้างตัวตนและการยอมรับด้วยการเชิดชูผลงานมีระบบคัดสรรข้าราชการดีเด่น อีกทั้งมอบโล่ประกาศเกียรติคุณอย่างเป็นรูปธรรมและสร้างคุณค่าในงานโดยมอบหมายงานที่ได้รับ

การยอมรับจากสังคมและมีความสำคัญต่อประเทศชาติ รวมถึงมีการปรับภาพลักษณ์ขององค์กรด้วยการประชาสัมพันธ์ให้ความสำคัญของมิติไซเบอร์ให้เทียบเท่ากับมิติการรบอื่น ๆ เพื่อให้กำลังพลรู้สึกถึงความสำคัญของตนเอง

๔). แนวทางส่งเสริมเมื่อกำลังพลมีความรู้และความภาคภูมิใจในอาชีพสูง เน้นการขยายขีดความสามารถและสร้างประสบการณ์ระดับสากล โดยการเปิดโอกาสสู่ภายนอกด้วยการส่งเสริมให้ปฏิบัติงานร่วมกับองค์กรระหว่างประเทศหรือบริษัทเอกชนชั้นนำทั้งในและต่างประเทศ และมีการสร้างรายได้เสริมที่ถูกต้องด้วยการสนับสนุนการรับงานนอกผ่านระบบกองทุนที่กระทรวงการคลังรับรอง รวมทั้งเส้นทางเติบโตพิเศษที่สนับสนุนคนเก่งให้เติบโตในระบบราชการอย่างรวดเร็ว

โดยสรุป ในมุมมองกลุ่มระดับอำนวยการเน้นการยืดหยุ่นตามสถานการณ์ ซึ่งหากงบประมาณมีจำกัด จะต้องเน้นการปรับระเบียบและดึงภาคเอกชนมาช่วย แต่หากงบประมาณมีพร้อมต้องเน้นการสร้างบุคคลต้นแบบและขยายโอกาสไปสู่ระดับสากลเพื่อรักษาความภาคภูมิใจไว้อย่างยั่งยืน

มุมมองระดับปฏิบัติการ: ให้ความสำคัญกับค่าตอบแทนและการเรียนรู้อย่างยั่งยืน

แนวทางการเตรียมความพร้อมของกองทัพไทยสำหรับการสรรหาและพัฒนากำลังพลด้านไซเบอร์รองรับสงครามสมัยใหม่ในอีก ๕ ปีข้างหน้า ตามมุมมองของกลุ่มระดับปฏิบัติการสามารถสรุปได้เป็น ๓ แนวทาง ดังนี้

๑). การปฏิรูปกระบวนการคัดสรรและมาตรฐานความปลอดภัย มีการคัดกรองอย่างเข้มข้นเพิ่มความเข้มงวดในกระบวนการคัดสรรกำลังพลเพื่อให้ได้ผู้ที่มีความเชี่ยวชาญจริงและรักษาชั้นความลับโดยวางระบบการคัดกรองบุคคลที่สอดคล้องกับนโยบายการรักษาความลับทางราชการ เพื่อป้องกันความเสี่ยงในด้านความมั่นคงตั้งแต่ต้นทาง พร้อมทั้งการเตรียมความพร้อมผ่านการทำบันทึกข้อตกลง (MOU) กับหน่วยงานภายนอกเพื่อขยายฐานการสรรหาบุคลากร

๒). การยกระดับขีดความสามารถและระบบนิเวศแห่งการเรียนรู้ ด้วยการเสริมรากฐานโดยการวางหลักสูตรปรับพื้นฐานสำหรับกำลังพลเพื่อให้มีมาตรฐานเดียวกัน พร้อมจัดตั้งพื้นที่สำหรับแลกเปลี่ยนความรู้ (Knowledge Sharing Community) เพื่อให้เกิดการถ่ายทอดทักษะระหว่างกันอย่างต่อเนื่อง นอกจากนี้ ยังเพิ่มงบประมาณด้าน (R&D) เพื่อสร้างอาวุธและเครื่องมือทางไซเบอร์ที่ทันสมัย ให้กำลังพลมีขีดความสามารถในการต่อสู้ในสงครามรูปแบบใหม่

๓). การสร้างแรงจูงใจและการบริหารจัดการเชิงรุก การเพิ่มคุณค่าและสวัสดิการที่ให้ความสำคัญกับกำลังพลในฐานะฟันเฟืองหลัก เพื่อสร้างแรงจูงใจที่ตอบโจทย์ความต้องการอย่างแท้จริง เพื่อเพิ่มความภาคภูมิใจและคุณค่าในสายงาน นอกจากนั้น มีการจัดตั้งทีมผู้เชี่ยวชาญเฉพาะทางที่สามารถรับงานภายนอกเพื่อนำรายได้มาเป็นเงินปันผลเข้าส่วนกองกลางและพัฒนาหน่วยงาน อีกทั้งมีระบบแบ่งปันผลประโยชน์ที่ชัดเจนเพื่อสร้างแรงจูงใจให้กำลังพลทุ่มเทความสามารถได้อย่างเต็มที่

โดยสรุป ในมุมมองระดับปฏิบัติการ หน่วยงานควรเน้นไปที่การพัฒนาคนควบคู่กับการพัฒนาอาวุธโดยจะต้องมีระบบสวัสดิการและรายได้เสริมที่จูงใจ พร้อมกับการสร้างสังคมแห่งการเรียนรู้ เพื่อให้กำลังพลมีทั้งฝีมือและกำลังใจที่พร้อมจะทำงานในระยะยาว

ประเด็นท้าทายและข้อควรระวัง (Key Risks & Mitigation Strategies)

การปฏิรูปการสรรหาและพัฒนากำลังพลด้านไซเบอร์ แม้จะส่งผลดีต่อขีดความสามารถของกองทัพ ในอนาคตแต่หากขาดมาตรการควบคุมที่รัดกุม อาจนำไปสู่ความเสี่ยงใน ๓ มิติหลัก ดังนี้

๑). ความมั่นคงของข้อมูลและภัยคุกคามจากภายใน ความเสี่ยงที่เกิดจากกำลังพลซึ่งเข้าถึงข้อมูลความลับอ่อนไหวของชาติ ซึ่งหากบุคคลดังกล่าวขาดความตระหนักรู้อาจทำให้ข้อมูลที่เป็นความลับเสี่ยงต่อการรั่วไหลไปถึงตรงข้ามหรือองค์กรที่ไม่มีธรรมาภิบาลจนกลายเป็นภัยคุกคามระดับยุทธศาสตร์

<u>แนวทางแก้ไข</u> การทำสัญญา NDA ที่เข้มงวดรวมถึงการมีระบบตรวจสอบความปลอดภัยอย่างต่อเนื่อง พร้อมกับการสร้างกระบวนการถ่ายทอด ที่เพื่อสร้างความตระหนักรู้ให้กับกำลังพล

๒). ธรรมาภิบาลในระบบการสรรหา ในกระบวนการคัดเลือกที่ไม่โปร่งใสอาจนำไปสู่ข้อครหาเรื่องผลประโยชน์ และความเหลื่อมล้ำ หากระบบการให้ค่าตอบแทนสูงขึ้นแต่กระบวนการคัดเลือกยังอิงกับระบบอุปถัมภ์ (Connection) แทนที่จะเป็นระบบคุณธรรม (Meritocracy) กองทัพจะสูญเสียบุคลากรที่เชี่ยวชาญไปพร้อมกับการได้บุคลากรที่ไม่สามารถปฏิบัติงานได้จริงเข้ามาแทน ขณะเดียวกันหากการให้สิทธิประโยชน์พิเศษแก่กำลังพลด้านไซเบอร์ แต่ไม่มีการอธิบายถึงเหตุผลและความจำเป็นให้กำลังพลในสายงานอื่นๆเข้าใจด้วย อาจสร้างความรู้สึกไม่เท่าเทียมและส่งผลต่อความสามัคคีและขวัญกำลังใจในภาพรวมของกองทัพ

<u>แนวทางแก้ไข</u> การพิจารณาแต่งตั้งคณะกรรมการที่เป็นธรรมสำหรับการคัดเลือกกำลังพลรวมถึงการวัดผลการปฏิบัติงานด้วย (KPI) ที่เป็นรูปธรรมและการสร้างมาตรฐานความโปร่งใส

๓). ช่องว่างและความล้าสมัยทางเทคโนโลยี ความเสี่ยงด้านขีดความสามารถในการแข่งขันเมื่อเทียบกับภัยคุกคามระดับโลก หากกองทัพมีกำลังพลที่เชี่ยวชาญแต่ขาดเครื่องมือที่ทันสมัย เนื่องจากกระบวนการจัดซื้อจัดจ้างที่ใช้เวลาค่อนข้างมาก รวมถึงงบประมาณด้าน R&D ที่จำกัดอาจทำให้กำลังพลขาดการพัฒนาขีดความสามารถสำหรับการป้องกันภัยคุกคามที่มีเทคโนโลยีสูงกว่าได้ ทั้งนี้การพึ่งพาเทคโนโลยีต่างชาติเกินความจำเป็น หากขาดการวิจัยและพัฒนาเครื่องมือเอง กองทัพอาจจะต้องตัดกำลังจนขาดการพัฒนาจากภายใน

<u>แนวทางแก้ไข</u> การพิจารณาจัดสรรงบประมาณด้าน R&D อย่างต่อเนื่อง รวมถึงการสนับสนุนการพัฒนา Software ภายในหน่วยงานและการสร้าง Sandboxing เพื่อทดสอบเทคโนโลยีใหม่ ๆ อย่างเหมาะสม

กล่าวสรุป ความเสี่ยงเหล่านี้ไม่ใช่สิ่งที่ป้องกันไม่ได้ แต่หากต้องใช้การวางแผนและการบริหารจัดการที่มีประสิทธิภาพ ทั้งนี้ กองทัพต้องเปลี่ยนผ่านจากระบบความปลอดภัยที่เน้นกฎระเบียบ ไปสู่ระบบความปลอดภัยที่เน้นความไว้วางใจและการตรวจสอบได้ เพื่อให้การปฏิรูปกำลังพลครั้งนี้ยั่งยืนและปลอดภัยต่อความมั่นคงของชาติอย่างแท้จริง

ส่วนที่ ๔
บทสรุปและข้อเสนอแนะ



ส่วนที่ ๔ บทสรุปและข้อเสนอแนะ

๔.๑ บทสรุป

จากการวิเคราะห์ความคิดเห็นของกลุ่มสัมมนา Work shop ทั้ง ๓ กลุ่ม ได้แก่ กลุ่มระดับนโยบาย/บริหาร, กลุ่มระดับอำนวยการ และกลุ่มระดับปฏิบัติการ สามารถสรุปผลการวิเคราะห์สำหรับการสรรหาและพัฒนากำลังพลไซเบอร์รองรับสงครามสมัยใหม่ โดยแบ่งฉากทัศน์ของกองทัพในมิติไซเบอร์ตามปัจจัยหลัก ๒ ประการ คือ ๑). เงินเดือน ,ค่าตอบแทน และสวัสดิการ และ ๒). ความรู้และความภาคภูมิใจในอาชีพ ผ่านการวิเคราะห์ฉากทัศน์ในห้วงเวลา ๕ ปีข้างหน้า ทั้งนี้สามารถคาดการณ์สภาวะที่อาจจะเกิดขึ้น ซึ่งส่งผลกระทบต่อกองทัพไทยในเชิงยุทธศาสตร์ สรุปได้ดังนี้

๑. ฉากทัศน์พึงปรารถนา / ภาพอนาคตที่ควรเป็น “Q1 : กองทัพไซเบอร์เกรียงไกร” (The Cyber Vanguard) ในฉากทัศน์นี้ กองทัพสามารถปรับตัวเข้าสู่สถานการณ์ในยุคดิจิทัลได้อย่างสมบูรณ์ ทั้งในแง่โครงสร้างงบประมาณและวัฒนธรรมองค์กร โดยกองทัพไทยมีสถานะเป็นตัวเลือกแรก (Employer of Choice) ของบุคลากรด้านไอทีมีที่มีความสามารถอีกทั้งพฤติกรรมของกำลังพลมีแรงจูงใจสูง พร้อมทุ่มเทให้กับการวิจัยและพัฒนาด้านไซเบอร์ที่มีความจงรักภักดีต่อองค์กรเพราะเห็น **“อนาคต”** ในอาชีพที่ชัดเจน

<u>ผลกระทบต่อกองทัพ</u> เกิดการสร้างนวัตกรรมภายใน (In-house Innovation) และลดการพึ่งพาเทคโนโลยีต่างชาติ ทำให้มีความมั่นคงปลอดภัยของข้อมูลในระดับสูง เนื่องจากกำลังพลมีความตระหนักรู้ รวมถึงการมีภาพลักษณ์ของกองที่ทันสมัย สามารถดึงดูดความร่วมมือจากพันธมิตรนานาชาติได้

๒. ฉากทัศน์วิกฤต / ภาพอนาคตที่วิกฤต “Q3 : ปราการไซเบอร์ล่มสลาย” (The Defenseless Frontier) เป็นสถานการณ์ที่อันตรายที่สุด เมื่อกองทัพไม่สามารถปรับตัวตามตลาดแรงงานไซเบอร์และยังคงยึดติดกับระบบราชการแบบดั้งเดิม ทำให้เกิดสภาวะขาดแคลนบุคลากรที่มีความเชี่ยวชาญ (Critical Talent Shortage) ตำแหน่งงานว่างลงหรือถูกเติมเต็มด้วยบุคลากรที่ขาดทักษะ อีกทั้งพฤติกรรมกำลังพล เกิดภาวะ **“สมองไหล”** เนื่องจากคนเก่งลาออก และคนที่ยังอยู่รู้สึกจำใจและมีภาวะ (Burn out) สูงเนื่องจากภาระงานล้นมือแต่ผลตอบแทนไม่คุ้มค่า

<u>ผลกระทบต่อกองทัพ</u> กองทัพสั่นคลอน เสี่ยงต่อการถูกโจมตีทางไซเบอร์จากฝ่ายตรงข้าม เนื่องจากระบบป้องกันอ่อนแอ รวมถึงความลับรั่วไหลจากกำลังพลที่อาจนำความรู้ไปใช้

ในทางที่ผิดส่งผลต่อความลับทางทหาร นอกจากนี้อาจทำให้กองทัพสูญเสียอำนาจการต่อรองในมิติสงครามสมัยใหม่

๓. ฉากทัศน์ก้ำกึ่ง / ภาพอนาคต ๒ ทาง คือ "Q2 : นักรบอุดมการณ์พลีชีพ" (The Patriotic Martyrs) และ "Q4 : กรงทองของนักรบไร้ใจ" (The Gilded Cage) ฉากทัศน์นี้มักเกิดขึ้นในช่วงเปลี่ยนผ่าน โดยสามารถแบ่งออกเป็น ๒ กรณี มีรายละเอียดดังนี้

๓.๑ กรณีค่าตอบแทนและสวัสดิการสูง แต่ความรู้และความภาคภูมิใจในอาชีพของกำลังพลต่ำ โดยกองทัพทุ่มงบประมาณจ้างคนเก่งแต่โครงสร้างองค์กรยังไม่เอื้อต่อการพัฒนากำลังพลด้านไซเบอร์ หรือมีระบบอุปถัมภ์ อีกทั้งพฤติกรรมกำลังพลทำงานแบบนักรบรับจ้าง (Mercenary) มององค์กรเป็นเพียงทางผ่านไปสายงานอาชีพ **ผลกระทบต่อกองทัพ** กองทัพมีเสถียรภาพด้านกำลังพลในระดับต่ำ จากการเปลี่ยนผ่านกำลังพล (High Turnover) ทำให้งานนโยบายขาดความต่อเนื่อง และสิ้นเปลืองงบประมาณในการฝึกอบรมกำลังพลบรรจุใหม่

๓.๒ กรณีกำลังพลมีความรู้และความภาคภูมิใจในอาชีพสูง แต่ได้รับค่าตอบแทนและสวัสดิการต่ำ กำลังพลมีใจรักและภาคภูมิใจในอาชีพแต่ระบบสวัสดิการและเครื่องมือในการทำงานล้าหลังทำให้กำลังพลต้องแบกรับความเสี่ยงส่วนตัว เนื่องจากพยายามทำงานเต็มที่แต่ยังขาดแรงสนับสนุน **ผลกระทบต่อกองทัพ** ในระยะยาวกำลังพลจะเผชิญกับภาวะล้มละลายทางแรงใจ (Moral Injury) และสุดท้ายจะถูกบีบให้ต้องลาออกเพื่อความอยู่รอดทำให้กองทัพสูญเสียกำลังพลที่มีความสามารถไป

กล่าวโดยสรุป จากการวิเคราะห์ฉากทัศน์ทั้ง ๓ กรณีกองทัพควรพิจารณาเพื่อมุ่งไปสู่ **"ฉากทัศน์พึงปรารถนา"** โดยใช้กลยุทธ์แบบผสมผสาน คือ การพัฒนาระบบค่าตอบแทนที่แข่งขันได้เพื่อตรงตามความต้องการของบุคลากรที่มีความสามารถ และระบบนิเวศการทำงานที่พร้อมสนับสนุนกำลังพลเพื่อรักษาความภาคภูมิใจในองค์กร มิเช่นนั้นกองทัพอาจจะติดอยู่ในฉากทัศน์ก้ำกึ่งซึ่งไม่มีเสถียรภาพในระยะยาว

๔.๒ ข้อเสนอแนะและแนวทางในการสรรหาและพัฒนากำลังพลด้านไซเบอร์

การพัฒนากำลังพลด้านไซเบอร์ในโลกยุคใหม่ไม่ได้สิ้นสุดที่การฝึกอบรม แต่คือการสร้างสภาพแวดล้อมที่เอื้อต่อการแสดงศักยภาพและความก้าวหน้าอย่างต่อเนื่อง เพื่อป้องกันภาวะสมองไหลรวมถึงเพื่อสร้างแรงจูงใจผ่านการสรรหาและพัฒนากำลังพล มีแนวทางดังนี้

๑. เส้นทางอาชีพที่ชัดเจน (Career Path) กองทัพพิจารณากำหนดโครงสร้างองค์กรทางไซเบอร์ พร้อมกำหนดตำแหน่งผู้เชี่ยวชาญเฉพาะทางให้มีสิทธิประโยชน์ต่างๆ

เพื่อเป็นแรงจูงใจ เพื่อให้คนที่มีทักษะเทคนิคสูงสามารถอุทิศตนให้กับงานด้านเทคโนโลยีได้ตลอดชีวิตราชการ รวมถึงกำหนดเกณฑ์การเลื่อนตำแหน่งที่อิงกับความสามารถมากกว่าอายุราชการ เพื่อให้คนเก่งรุ่นใหม่มีโอกาสก้าวหน้าได้อย่างรวดเร็ว รวมถึง**การปฏิรูปมาตรฐานการคัดเลือกเชิงรุก** ผ่านการปรับลดกฎระเบียบบางประการเพื่อให้สามารถสรรหากำลังพลที่มีศักยภาพ อีกทั้ง พิจารณาการจัดการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ เช่น Capture The Flag – CTF เพิ่มขึ้นเพื่อใช้เป็นช่องทางหลักในการคัดสรรกำลังพลแทนการสอบข้อเขียนแบบเดิม โดยผู้ที่แสดงทักษะการแก้ปัญหาเชิงเทคนิคได้โดดเด่นควรได้รับสิทธิในการบรรจุเข้าทำงานทันที นอกจากนี้ยังกำหนดมาตรฐานการรับรอง (Certificates) ระดับสากลเพื่อเป็นเกณฑ์พิจารณาสำคัญ เช่น CISSP, OSCP หรือ GSEC ทั้งนี้ ผู้ที่มีใบรับรองเหล่านี้ควรได้รับการยกเว้นการสอบภาคทฤษฎีบางขั้นตอนเพื่อลดระยะเวลาในกระบวนการสรรหา อีกทั้งการพิจารณาให้ทุนการศึกษาในสาขาที่ขาดแคลน เช่น AI, Cryptography หรือ Digital Forensics พร้อมระบุเงื่อนไขการใช้ทุนที่ชัดเจนและให้สิทธิประโยชน์ที่จูงใจ เพื่อสร้างฐานกำลังพลที่เชี่ยวชาญในอนาคต

๒. การพัฒนารูปแบบการจ้างงานที่ยืดหยุ่น ทั้งนี้ สงครามสมัยใหม่ต้องการความเร็วและความเชี่ยวชาญเฉพาะด้าน ดังนั้นระบบการจ้างงานแบบข้าราชการดั้งเดิมอาจไม่ตอบโจทย์ ทำให้กองทัพอาจพิจารณานำรูปแบบการจ้างงานที่ยืดหยุ่นมาใช้ เช่น การจ้างผู้เชี่ยวชาญภายนอกสำหรับภารกิจเร่งด่วนหรือการพัฒนาระบบเฉพาะทางแบบ “เจอ-จ่าย-จบ” ว่าจ้างบริษัทพันธมิตรด้านความปลอดภัยไซเบอร์ในการดูแลงานที่เป็นโครงสร้างพื้นฐานที่ไม่กระทบต่อชั้นความลับ รวมถึงการพัฒนาระบบกำลังพลสำรองด้านไซเบอร์และนักรบไซเบอร์อาสาเพื่อดึงคนเก่งจากภาคเอกชนผ่านการสนับสนุนค่าตอบแทนและสวัสดิการที่จูงใจ ทั้งนี้เพื่อเป็นการเพิ่มขีดความสามารถของกองทัพโดยไม่ต้องเพิ่มจำนวนกำลังพลประจำการ

๓. การยกระดับขีดความสามารถและระบบเศรษฐกิจภายในหน่วย (CoP & Internal Ventures) การสร้างบรรยากาศแห่งการเรียนรู้ โดยการจัดตั้งแพลตฟอร์มหรือพื้นที่เรียนรู้ร่วมกันสำหรับกำลังพลในทุกระดับ เพื่อให้เกิดการแลกเปลี่ยนเทคนิคระหว่างกำลังพล รวมถึงการจัดทำฐานข้อมูลความรู้ของหน่วยเพื่อประโยชน์สำหรับการพัฒนาขีดความสามารถของกำลังพลทุกระดับ

๔. การสร้างเกียรติภูมิและภาพลักษณ์ในโลกดิจิทัล (Digital Prestige & Identity) โดยการพิจารณามอบรางวัลเชิดชูเกียรติ ในแบบเครื่องหมายความสามารถ (Badge) ลักษณะเช่นเดียวกับเครื่องหมายจู่โจมหรือปีกร่ม เพื่อเป็นสัญลักษณ์แห่งความภาคภูมิใจ

รวมทั้งการส่งเสริมให้กำลังพลเข้าร่วมเวทีสัมมนาระดับโลกในฐานะตัวแทนกองทัพ เพื่อสร้างชื่อเสียงและภาพลักษณ์ความเป็นผู้เชี่ยวชาญ ซึ่งจะช่วยเสริมสร้างความภาคภูมิใจของกำลังพลอีกด้วย อีกทั้ง **การสร้างแรงจูงใจเชิงโครงสร้าง** โดยการสร้างสมดุลระหว่างผลตอบแทนที่คุ้มค่ากับความรับผิดชอบที่เหมาะสมเพื่อรักษากำลังพลที่มีความเชี่ยวชาญและการพิจารณาปฏิรูปโครงสร้างเงินเดือนโดยแยกค่าตอบแทนวิชาชีพพิเศษ ออกจากเงินเดือนตามชั้นยศ โดยใช้ระดับทักษะ (Skill Level) และผลสัมฤทธิ์ของงานเป็นตัวกำหนด รวมถึงการพิจารณากำหนดเส้นทางการเติบโตในอาชีพราชการของกำลังพลสายเทคนิค (Technical Track) ให้ชัดเจนเพื่อเป็นแรงจูงใจด้านกำลังพลสายไซเบอร์

๕. การบูรณาการความร่วมมือและโครงการแลกเปลี่ยน (Strategic Partnerships & Rotational Programs) เพื่อเพิ่มพูนประสบการณ์ผ่านความร่วมมือกับองค์กรภายนอก รวมถึงการพิจารณาจัดทำข้อตกลง MOU กับภาคเอกชนและองค์กรระหว่างประเทศเพื่อส่งกำลังพลสำหรับการแลกเปลี่ยนการทำงานเป็นระยะเวลา ๖-๑๒ เดือน เพื่อเรียนรู้วัฒนธรรมการทำงานและเทคโนโลยีใหม่ๆ เพื่อนำความรู้กลับมาพัฒนาหน่วยรวมถึงสนับสนุนการเข้าฝึกร่วมกับกองทัพมิตรประเทศในระดับนานาชาติอย่างต่อเนื่อง เพื่อสร้างเครือข่ายความสัมพันธ์กับผู้เชี่ยวชาญจากทั่วโลก ทั้งนี้ เพื่อเป็นทั้งการพัฒนาทักษะและการสร้างประสบการณ์ที่อาจหาไม่ได้จากการทำงานในภาคเอกชนทั่วไป

๖. การสร้างกลไกกองหนุนไซเบอร์ (Cyber Reserves) ดึงผู้เชี่ยวชาญจากภาคเอกชนและพลเรือนมาเป็นกำลังพลสำรอง เพื่อเสริมภารกิจความมั่นคงในยามวิกฤต และจัดตั้งศูนย์จำลองยุทธการไซเบอร์ (Cyber Range) ประจำเหล่าทัพเพื่อฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ในสถานการณ์เสมือนจริงทุกระดับ นอกจากนี้ ยังมี**ระบบการเรียกกำลังพลสำรอง** และฝึกทบทวนเฉพาะทาง ออกแบบวงรอบการฝึกอบรมภาคปฏิบัติตามมาตรฐานสากล เช่น Cyber Flag ให้แก่กำลังพลสำรองอย่างต่อเนื่อง อีกทั้ง เสริมสร้างทักษะ Upskill และ Reskill ให้แก่กำลังพลประจำการและทหารกองประจำการที่มีศักยภาพด้านเทคโนโลยีสารสนเทศ ทั้งนี้ ควรมีการผลักดันให้รัฐบาลสนับสนุนงบประมาณระยะยาวในการสร้างผู้เชี่ยวชาญด้านไซเบอร์ให้เทียบเท่ากับการจัดซื้ออุทโธปกรณ์ และการพัฒนาขีดความสามารถข้ามมิติด้วยการเร่งบ่มเพาะกำลังพลให้เข้าใจเครื่องมือด้านไซเบอร์ที่แฝงอยู่ในทุกมิติการรบ เช่น บก ทะเล อากาศ และอวกาศ รวมถึง **การถอดบทเรียนโมเดลต่างประเทศ** การศึกษารูปแบบความสำเร็จจากต่างประเทศ เช่น แนวทางของอิสราเอลหรือสหรัฐฯ ในการบูรณาการไซเบอร์เข้ากับระบบกำลังพลทหาร อีกทั้ง **การพัฒนาระบบ Geo System** เพื่อการบริหารกำลังพล

ด้วยการสร้างระบบสารสนเทศภูมิศาสตร์ไซเบอร์ในการติดตาม จำแนก และจัดทำฐานข้อมูลทักษะกำลังพลทั่วประเทศอีกด้วย

โดยสรุป การเตรียมความพร้อมกำลังพลด้านไซเบอร์ไม่ใช่เพียงการเพิ่มจำนวนบุคลากร แต่คือการปฏิรูปเชิงโครงสร้างเพื่อเปลี่ยนคนเก่ง ให้เป็นนักรบไซเบอร์ ที่มีความเชี่ยวชาญ มีอุดมการณ์ และมีคุณภาพชีวิตที่ดี พร้อมตอบสนองและรับมือกับสงครามสมัยใหม่ได้ทันสถานการณ์

****

บรรณานุกรม

ภาษาไทย

กรมยุทธศึกษาทหารบก. (2563). *หลักนิยมกองทัพบกด้านไซเบอร์*. โรงพิมพ์กองสงเคราะห์ทหารผ่านศึก.

กระทรวงกลาโหม. (2560). *ยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม พ.ศ. 2560–2579*. สำนักงานนโยบายและแผนกลาโหม.

กระทรวงกลาโหม. (2568). *สมุดปกขาว หน่วยบัญชาการไซเบอร์ทหาร กองบัญชาการกองทัพไทย พ.ศ. 2568*. หน่วยบัญชาการไซเบอร์ทหาร.

กฤษฎา มณีวงศ์. (2565). *ความก้าวหน้าทางเทคโนโลยีกับการปรับตัวของกองทัพในศตวรรษที่ 21*. สำนักพิมพ์มหาวิทยาลัยป้องกันประเทศ.

จินดา สระสมบูรณ์. (2558). ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย. *รัฏฐาภิรักษ์*, *57*(2), 57–69.

ชัยชนะ จารุศิลาวงศ์. (2566). ยุทธศาสตร์การพัฒนากำลังพลไซเบอร์: แนวคิดและการปฏิบัติ. *วารสารความมั่นคงปลอดภัยไซเบอร์แห่งชาติ*, *4*(2), 45–60.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก, หน้า 20–52.

ศูนย์ไซเบอร์กองทัพบก. (2558). *แนวทางการปฏิบัติการและความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพบก*. เอกสารเผยแพร่ทางวิชาการการทหาร.

สถาบันเทคโนโลยีป้องกันประเทศ. (2565). *แนวโน้มเทคโนโลยีป้องกันประเทศและสงครามในอนาคต*.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2565). *นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565–2570)*. https://www.ncsa.or.th

สำนักงานสภาความมั่นคงแห่งชาติ. (2560). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560–2564)*. สำนักนายกรัฐมนตรี.

ภาษาอังกฤษ

Arquilla, J., & Ronfeldt, D. (2020). *The emergence of noopolitik: Toward an American information strategy*. RAND Corporation.

Biddle, S. (2021). The future of warfare: Non-state actors and high-tech weapons. *International Security*, *45*(3), 7–48.

Cyber Security Agency of Singapore. (2025, November 12). *AI-enabled capabilities and collaboration with industry elevate defence of critical infrastructure at national cyber defence exercise*. https://www.csa.gov.sg/news-events/press-releases/ai-enabled-capabilities-and-collaboration-with-industry-elevate-defence-of-critical-infrastructure-at-national-cyber-defence-exercise/

Defense Innovation Marketplace. (n.d.). *Cyber Vision 2025 - USAF cyberspace science and technology vision 2012-2025*. https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/12/Cyber-Vision-2025-USAF-Cyberspace-Science-and-Technology-Vision-2012-2025.pdf

Executive Office of the President. (2026). *President Trump's cyber strategy 2026: Deter and disrupt*. The White House. https://www.whitehouse.gov/

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Galeotti, M. (2019). (Re)Defining Hybrid Warfare. *The RUSI Journal*, *164*(4), 20–27. https://doi.org/10.1080/03071847.2019.1643265

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

International Committee of the Red Cross. (2024). *Modern warfare and its impact on civilians*.

Jensen, B., & Valeriano, B. (2024). The future of cyber power: Lessons from the integration of cyber operations in modern theater. *Journal of Strategic Studies*, *47*(2), 145–168. https://doi.org/10.1080/01402390.2024.xxxxxx

Jones, S. G. (2018). *The gray zone: Understanding the contemporary security environment*. Center for Strategic and International Studies (CSIS).

Luckenbaugh, J. (2026, March 10). ALGORITHMIC WARFARE: Cyber ops increasingly melding with kinetic conflict. *National DefenseMagazine*. https://www.nationaldefensemagazine.org/articles/2026/3/10/cyber-ops-increasingly-melding-with-kinetic-conflict

Ministry of Defence, Singapore. (2025a, March 3). *Fact sheet: Defence Cyber Command and SAF C4 & digitalisation command*. https://www.mindef.gov.sg/news-and-events/latest-releases/03mar25_fs/

Ministry of Defence, Singapore. (2025b, November 28). *SAF expands cybersecurity student talent development programme to include AI skills in 2026*. https://www.mindef.gov.sg/news-and-events/latest-releases/28nov25-nr2/

Ministry of Defence, Singapore. (2026a, February 11). *Singapore's Digital and Intelligence Service participates in multilateral cyber defence exercise*. https://www.mindef.gov.sg/news-and-events/latest-releases/11feb26-nr/

Ministry of Defence, Singapore. (2026b, February 27). *Fact sheet: Cyber Defence Test and Experimentation Centre (CyTEC) and sectoral cyber defence teams (SCDTs)*. https://www.mindef.gov.sg/news-and-events/latest-releases/27feb26-fs2/

NATO. (2022). *NATO's approach to hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO Cooperative Cyber Defence Centre of Excellence. (2024). *Locked Shields 2024: Cyber defence exercise reports and strategic takeaways*. CCDCOE Publications. https://ccdcoe.org/library/publications/

Rosner, Y., & Siman-Tov, D. (2018). *Cognitive warfare: The rise of the sixth domain*. Institute for National Security Studies (INSS).

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

SOCRadar. (2026, January 23). *The U.S. 2026 National Defense Strategy: A cybersecurity perspective*. https://socradar.io/blog/us-2026-national-defense-strategy-cybersecurity/

Synergia Foundation. (2026). *Global futures 2035: Scaling cyber resilience in an era of quantum computing*. Proceedings of the Synergia Conclave 2026.

Thales. (2026, January 6). *AI, Quantum, and the cybersecurity threats defining 2026*. https://cpl.thalesgroup.com/blog/data-security/ai-quantum-cybersecurity-threats-2026

Townsend, S. J. (2018). Multi-domain operations: Preparing for future war. *Military Review*, *98*(3), 4–11.

United Nations Institute for Disarmament Research. (2021). *The role of technological advancement in modern warfare: Challenges and opportunities*. https://unidir.org/publication/role-technological-advancement-modern-warfare

U.S. Army. (2024). *Army digital transformation strategy 2024-2028: Integrating artificial intelligence and cyber resilience*. Department of the Army.

U.S. Department of Defense. (2023a, May 26). *Fact sheet: 2023 DoD cyber strategy*. https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

U.S. Department of Defense. (2023b). *Summary of the 2023 Department of Defense cyber strategy*. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023-DOD-CYBER-STRATEGY-SUMMARY.PDF

ภาคผนวก

ภาคผนวก ก

ภาพการสัมมนาปัญหายุทธศาสตร์ ครั้งที่ ๑/๒๕๖๙ เรื่อง “แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่”

ภาคผนวก ข

ภาพการแถลงและวิพากษ์ผลงานทางวิชาการ ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ



ภาคผนวก ก

ภาพประกอบการสัมมนาฯ

๑. พิธีเปิด-ปิดการจัดสัมมนาฯ

พล.ต. นิรุจ ดวงปัญญา ผอ.ศศย.สปท. เป็นประธานในการสัมมนาฯ กล่าวเปิด-ปิดการจัดสัมมนาฯ











วิทยากรและผู้เข้าร่วมการสัมมนาฯ

วิทยากรผู้ทรงคุณวุฒิประกอบด้วย (๑) พลโท ดร.ชาติชาย ชัยเกษม ผู้บัญชาการหน่วยบัญชาการ ไซเบอร์ทหารกองบัญชาการกองทัพไทย (๒) นาวาอากาศเอก ดร.นที ปั้นทอง รองผู้อำนวยการศูนย์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อความเป็นเลิศ หน่วยบัญชาการไซเบอร์ทหาร และปฏิบัติหน้าที่ผู้อำนวยการโรงเรียนไซเบอร์ทหาร หน่วยบัญชาการไซเบอร์ทหาร (๓) พันเอก สรรพชัยย์ หุวะนันทน์ กรรมการผู้จัดการใหญ่ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) และ (๔) ดร.ปริญญา หอมอเนก กรรมการผู้ทรงคุณวุฒิ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีผู้เข้าร่วมประชุมฯ จำนวน ๔๐ คน จากหน่วยงานด้านไซเบอร์ทั้งภาครัฐ เอกชน กองทัพ และนักวิชาการจากสถาบันการศึกษา

ดำเนินรายการโดย พันเอกหญิง ธนิตา วงษ์จินดา ผู้เชี่ยวชาญด้านการฝึกอบรม ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ





บรรยากาศในการสัมมนาฯ

การสัมมนาฯแบ่งออกเป็น ๒ ช่วง รายละเอียดดังนี้ **ช่วงที่ ๑** การสัมมนาปัญหายุทธศาสตร์ ครั้งที่ ๑/๒๕๖๙ การบรรยายพิเศษ เรื่อง **“Cyber Workforce เพื่อความมั่นคงของชาติ”** และเวทีเสวนา หัวข้อ **“แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่”** และ **ช่วงที่ ๒** การสัมมนาฯแบ่งกลุ่มย่อย ในหัวข้อ “แนวทางการสรรหาและพัฒนากำลังพลด้านไซเบอร์ของกองทัพไทยรองรับสงครามสมัยใหม่”







ภาคผนวก ข

ภาพประกอบการแถลงและวิพากษ์ผลงานทางวิชาการฯ

๑) พิธีเปิด-ปิด การแถลงและวิพากษ์ผลงานทางวิชาการฯ พลตรี สุเทพ เขียวภักดี รองเสนาธิการ สถาบันวิชาการป้องกันประเทศ เป็นประธานเปิดการแถลงและวิพากษ์ผลงานวิชาการ โดยมีพลอากาศตรี ไชยา ออกแดง ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ เป็นผู้กล่าวรายงาน พร้อมถ่ายรูปร่วมกับนักวิจัยและผู้เข้าร่วมการแถลงผลงานฯ

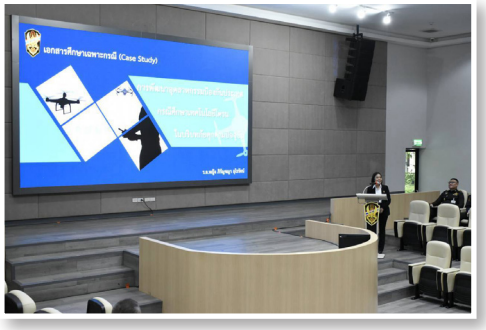






๒) การนำเสนองานเอกสารศึกษาเฉพาะกรณี เรื่อง “การพัฒนาอุตสาหกรรมป้องกันประเทศ กรณีศึกษาเทคโนโลยีโดรนในบริบทภัยคุกคามปัจจุบัน” โดย เรืออากาศเอกหญิง ภิรัญชญา อุไรรัตน์ นักวิจัยประจำกองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ











๓) การนำเสนองานวิจัย เรื่อง “การบูรณาการข่าวกรองเพื่อรับมือกับภัยคุกคามความมั่นคงชายแดนด้านตะวันออก” โดย เรือโทหญิง ปาณิสรา เทียนอ่อน นักวิจัยประจำกองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ











๔) การนำเสนองานเอกสารศึกษาเฉพาะกรณี เรื่อง “มิติไซเบอร์ : การสรรหาและพัฒนากำลังพลรองรับสงครามสมัยใหม่” โดย นางสาว กาญจนา เพิ่มพูน นักวิจัยประจำกองศึกษาวิจัยทางยุทธศาสตร์และ ความมั่นคง ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ







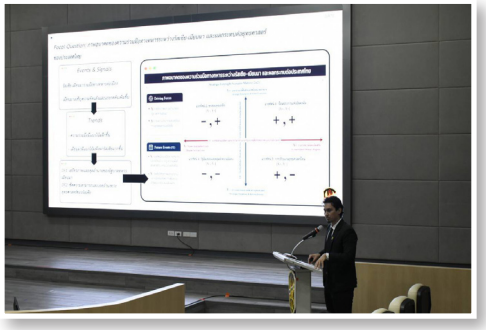




๕) การนำเสนองานเอกสารศึกษาเฉพาะกรณี **เรื่อง “ความสัมพันธ์เชิงยุทธศาสตร์ระหว่าง รัสเซีย – เมียนมา: จากความร่วมมือทางทหารสู่ความร่วมมือด้านพลังงานนิวเคลียร์ และนัยต่อประเทศไทย”** โดย **นายนิโคลัส อาเลคเซเยพว บุญหนุน** นักศึกษาจาก Moscow State Institute of International Relations (Russian Ministry of Foreign Affairs) นักศึกษาฝึกงานของศูนย์ศึกษายุทธศาสตร์







๖) กล่าวสรุปผลการนำเสนองานวิชาการ โดย พลอากาศตรี ไชยา ออกแดง ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ และกล่าวปิดการแถลงผลฯ โดย พลตรี สุเทพ เขียวภักดี รองเสนาธิการ สถาบันวิชาการป้องกันประเทศ





๗) ภาพรวมบรรยากาศการแถลงผลงานฯ


















ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๔๐๐
โทร ๐ ๒๕๗๒ ๒๙๓๒ เว็บไซต์ www.sscthailand.org