

แนวทางการขับเคลื่อนขีดความสามารถ การปฏิบัติการร่วมของกองทัพไทยด้วยระบบสื่อสารเชื่อมโยง Unleashing the Thai Military's Joint Operations Capabilities through an Integrated Communications Nexus

บทความวิชาการ

นภาพรรณ จันทรวัดน์,¹ อรณิชา คงวุฒิ,² พัทสนศรีญ์ เลหาไพบุลย์³ และ วุฒิรงค์ คงวุฒิ⁴

Napawan Juntawat, Ornnicha Kongwut, Phatsaran Laohhapaibon and Wuttirong Kongwut

สำนักงานสนับสนุน สำนักงานปลัดกระทรวงกลาโหม กรุงเทพฯ ประเทศไทย 10800¹

Office of Defence Logistics, Bangkok, Thailand 10800

สาขาวิชาฟิสิกส์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏกาญจนบุรี กาญจนบุรี ประเทศไทย 71190²

Department of Physics Faculty of Science and Technology,

Kanchanaburi Rajabhat University, Kanchanaburi, Thailand 71190

หจก.บุญพาวาสนาสง กรุงเทพฯ ประเทศไทย 10160³

Boonpawassanasong Partnership, Bangkok, Thailand 10160

กองบิน 2 กองทัพอากาศไทย ลพบุรี ประเทศไทย 15160⁴

Wing 2 Royal Thai Air Force, Lopburi, Thailand 15160

E-mail: napawan.wawaa@gmail.com¹, ornnicha.k@kru.ac.th²,

wirinwinu4289@gmail.com³ and wuttirong_k@rtaf.mi.th⁴

บทคัดย่อ

การศึกษาตัวอย่างการพัฒนาระบบสื่อสารรวมเหล่าทัพของประเทศชั้นนำเมื่อนำมาทำ Gap Analysis เปรียบเทียบกับสภาพปัจจุบันของกองทัพไทยพบว่า ยังมีช่องว่าง (Gaps) ที่ต้องพัฒนาในหลายด้าน ได้แก่ การบูรณาการเครือข่ายระหว่างเหล่าทัพ, การจัดโครงสร้างระบบให้สอดคล้องกับระดับบังคับบัญชา, การเพิ่มความยืดหยุ่นและความสามารถในการฟื้นฟูระบบ, การประยุกต์ใช้เทคโนโลยีสมัยใหม่ และการเพิ่มความสามารถในการทำงานร่วมกับหน่วยงานอื่น การวิเคราะห์ SWOT ระบุจุดแข็งของกองทัพไทย ได้แก่ โครงสร้างพื้นฐานและบุคลากรที่มีประสิทธิภาพ แต่ยังมีจุดอ่อนคือการขาดการบูรณาการระหว่างเหล่าทัพและข้อจำกัดด้านงบประมาณ นอกจากนี้ยังมีโอกาสจากความก้าวหน้าทางเทคโนโลยีและความร่วมมือระหว่างประเทศ แต่ต้องเผชิญอุปสรรคจากภัยคุกคามไซเบอร์และข้อจำกัดด้านกฎระเบียบ ผลจาก Gap Analysis และการวิเคราะห์ SWOT นำไปสู่ข้อเสนอแนะในการพัฒนาในหลายมิติ ทั้งด้านเทคโนโลยีและมาตรฐานการฝึกบุคลากร โครงสร้างการบังคับบัญชา และงบประมาณการจัดหา พร้อมทั้งต้องให้ความสำคัญกับการรับมือความท้าทาย เช่น การสร้างความร่วมมือระหว่างเหล่าทัพ, การรักษาความมั่นคงไซเบอร์, การจัดการการเปลี่ยนแปลง และการบริหารความเสี่ยง เพื่อให้การดำเนินงานบรรลุผลสำเร็จและเสริมสร้างขีดความสามารถของกองทัพไทยในการปฏิบัติภารกิจด้านความมั่นคง

คำสำคัญ : กองทัพไทย, กองบังคับบัญชา, เทคโนโลยีสื่อสาร

Abstract

By studying examples of joint forces communication system development from leading military nations, and conducting a Gap Analysis comparing them with the current state of the Thai military, several gaps were identified that require improvement. These include integrating networks across forces, aligning system structures with command levels, enhancing system flexibility and recoverability, leveraging modern technologies, and increasing interoperability with other agencies. A SWOT analysis highlighted the strengths of the Thai military, such as existing infrastructure and experienced personnel, but also weaknesses like the lack of integration across forces and budget

constraints. Additionally, opportunities arise from technological advancements and international cooperation, though threats from cyber threats and regulatory limitations exist. The Gap Analysis and SWOT findings led to recommendations for development across multiple dimensions, spanning technology and standards, personnel training, command structures, and procurement budgets. Simultaneously, addressing key challenges such as fostering inter-force collaboration, maintaining cybersecurity, managing change, and mitigating risks is crucial for successful implementation and enhancing the Thai military's capability in executing security missions effectively.

Keywords : Thai Military, Command and Control, Communications Technology

บทนำ

ความสำคัญของระบบสื่อสารต่อการปฏิบัติการทางทหาร

ในยุคปัจจุบันที่สภาพแวดล้อมด้านความมั่นคงมีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว การปฏิบัติการร่วมระหว่างเหล่าทัพต่าง ๆ กลายเป็นปัจจัยสำคัญต่อความสำเร็จของภารกิจทางทหาร ระบบสื่อสารที่เชื่อมโยงและบูรณาการข้อมูลข่าวสารจากแหล่งต่าง ๆ ได้อย่างราบรื่น จึงมีบทบาทสำคัญในการช่วยให้การประสานการปฏิบัติ การควบคุมกำลัง และการส่งกำลังบำรุงเป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง นำไปสู่ความได้เปรียบเชิงยุทธศาสตร์และการลดการสูญเสีย (Cossart, 2021)

อย่างไรก็ดีระบบสื่อสารของกองทัพไทยในปัจจุบันยังคงมีลักษณะแยกส่วนตามเหล่าทัพ ซึ่งก่อให้เกิดปัญหาความไม่สอดคล้องของเทคโนโลยีและมาตรฐาน ตลอดจนความซ้ำซ้อนในการลงทุนและการบริหารจัดการ ส่งผลให้

ขาดการบูรณาการขีดความสามารถอย่างแท้จริง และเกิดข้อจำกัดในการปฏิบัติการร่วมกันอย่างมีประสิทธิภาพ (Wilmelius, 2007)

ด้วยเหตุนี้บทความชิ้นนี้จึงมีวัตถุประสงค์เพื่อนำเสนอแนวทางการพัฒนา “ระบบสื่อสารโครงข่ายรวมเหล่าทัพ” ของกองทัพไทย ที่จะช่วยเพิ่มขีดความสามารถในการปฏิบัติการร่วมกันให้สอดคล้องกับแนวโน้มของสงครามยุคใหม่และเทียบเท่ามาตรฐานสากล โดยได้ทำการศึกษาตัวอย่างความสำเร็จจากประเทศชั้นนำ วิเคราะห์สภาพแวดล้อมและศักยภาพของกองทัพไทย และนำเสนอข้อเสนอแนะในด้านต่าง ๆ ทั้งเทคโนโลยี บุคลากร โครงสร้างงบประมาณ ตลอดจนแนวทางการรับมือกับความท้าทายที่อาจเกิดขึ้น (Coticchia et al., 2023; Ökten, 2022)

ปัญหาของระบบสื่อสารแยกส่วนในปัจจุบันของกองทัพไทย

สำหรับกองทัพไทยในปัจจุบันนั้น แม้จะมีการปรับปรุงพัฒนาระบบสื่อสารมาอย่างต่อเนื่อง แต่ก็ยังมีลักษณะที่แยกส่วนกันไปตามเหล่าทัพ กล่าวคือ กองทัพบก กองทัพเรือ และกองทัพอากาศ ต่างก็มีการพัฒนาระบบสื่อสารของตนเองขึ้นมาแยกจากกัน ทำให้เกิดปัญหาและข้อจำกัดหลายประการที่ส่งผลกระทบต่อขีดความสามารถโดยรวมในการปฏิบัติการร่วมทางทหาร (สุทัศน์ จารุมณี, 2561)

ประการแรกการแยกส่วนของระบบสื่อสารของเหล่าทัพ มีผลทำให้เกิดความเหลื่อมล้ำ ไม่สอดคล้องกันของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือ ICT (Information and Communications Technology) ไม่ว่าจะเป็นในด้านของอุปกรณ์ ช่างงาน ซอฟต์แวร์ และระบบรักษาความปลอดภัย ที่มีหลากหลายมาตรฐานและระดับเทคโนโลยี ก่อให้เกิดปัญหาในการเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลระหว่างกัน ทำให้การส่งเคราะห์ข้อมูลข่าวสารที่หลากหลายเพื่อประกอบการตัดสินใจของผู้บังคับบัญชาทำได้ยาก ไม่ครบถ้วน ล่าช้า และมีความคลาดเคลื่อนสูง

วัตถุประสงค์และขอบเขตของบทความ

ด้วยตระหนักถึงความสำคัญของการมีระบบสื่อสารที่เชื่อมโยงและบูรณาการขีดความสามารถของเหล่าทัพเข้าด้วยกัน บทความชิ้นนี้จึงมีวัตถุประสงค์ที่จะนำเสนอแนวทางในการพัฒนา “ระบบสื่อสารโครงข่ายร่วมเหล่าทัพ” หรือ “Joint Forces Network” ของกองทัพไทย ที่มุ่งไปสู่การปรับปรุงขีดความสามารถในการปฏิบัติการร่วมกัน (Joint Operations) ระหว่างกองทัพบก กองทัพเรือ และกองทัพอากาศ ให้สอดคล้องกับแนวโน้มของสงครามยุคใหม่ และทัดเทียมกับประเทศชั้นนำทางการทหารของโลก

ในการนี้ผู้เขียนจะได้ทำการศึกษาเปรียบเทียบตัวอย่างความสำเร็จของการพัฒนาระบบสื่อสารรวมเหล่าทัพของกองทัพต่างประเทศ โดยเฉพาะสหรัฐอเมริกา จีน และรัสเซีย เพื่อถอดบทเรียนและแนวปฏิบัติที่ดีมาปรับใช้ให้เหมาะสมกับบริบทของประเทศไทย นอกจากนี้จะได้มี

(สุทัศน์ ครำในเมือง และ มนวดี ตั้งตรงฤทัย, 2559; เนรมิต อัครมณีนันท์, 2561)

ยิ่งไปกว่านั้นปัญหาความไม่เข้ากันได้ของมาตรฐานและขั้นตอนการปฏิบัติ หรือ Standard Operating Procedures (SOPs) ที่แตกต่างกันไปของแต่ละเหล่าทัพ ยังเป็นอุปสรรคสำคัญต่อการพัฒนาการฝึกซ้อมและการฝึกกำลังเพื่อการปฏิบัติการในยามสงครามและในยามปกติ ไม่ว่าจะเป็นในการกิจการป้องกันประเทศ การต่อต้านการก่อการร้าย หรือการให้ความช่วยเหลือด้านมนุษยธรรมที่เหล่าทัพไม่สามารถประสานการปฏิบัติได้อย่างเป็นเอกภาพ นอกจากนี้ การที่ต่างเหล่าทัพต่างพัฒนาระบบสื่อสารของตนเอง ยังนำมาซึ่งความซ้ำซ้อน สิ้นเปลืองงบประมาณในการจัดหาอุปกรณ์ การพัฒนาบุคลากร ตลอดจนงานวิจัยและพัฒนาด้านวิทยาการสื่อสารและสารสนเทศที่ต่างก็ลงทุนลงแรงกันไปคนละทางทั้ง ๆ ที่หากมีการบูรณาการการพัฒนาเข้าด้วยกันก็จะช่วยประหยัดทรัพยากรได้มหาศาล (Killcross, 2021, p.155-164 ; Feng et al., 2021)

การวิเคราะห์สภาพแวดล้อมเชิงยุทธศาสตร์ ทั้งจุดแข็ง จุดอ่อน โอกาส และความท้าทายต่าง ๆ ของกองทัพไทย ในการพัฒนาระบบสื่อสารดังกล่าว เพื่อนำมาสรุปเป็นแนวทาง เป้าหมาย และยุทธศาสตร์การพัฒนาในด้านต่าง ๆ ไม่ว่าจะเป็นด้านโครงสร้างพื้นฐานทางเทคนิค การปรับมาตรฐานการปฏิบัติ การฝึกอบรมและพัฒนากำลังพล โครงสร้างการบังคับบัญชา การบูรณาการด้านงบประมาณ การจัดหาและวิจัยพัฒนา

ทั้งนี้ในการเสนอแนวทางพัฒนาข้างต้น ผู้เขียนได้คำนึงถึงความท้าทายหรืออุปสรรคสำคัญที่อาจเกิดขึ้นทั้งในด้านการสร้างความร่วมมือระหว่างเหล่าทัพ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ การบริหารการเปลี่ยนแปลงและการต้านทานจากผู้มีส่วนได้ส่วนเสีย อันจะนำไปสู่การกำหนดกลยุทธ์ในการรับมือที่เหมาะสมกับภูมิทัศน์ความมั่นคงในยุคปัจจุบันและอนาคต

กรณีศึกษาระบบสื่อสารรวมกองทัพของต่างประเทศ

สหรัฐอเมริกา

สหรัฐอเมริกาถือเป็นประเทศผู้นำในการพัฒนาระบบสื่อสารรวมเหล่าทัพ หรือที่เรียกว่า Joint Communications System (JCS) มาอย่างต่อเนื่องยาวนาน โดยมีจุดมุ่งหมายเพื่อสนับสนุนการปฏิบัติการร่วมระหว่างกองทัพบก กองทัพเรือ กองทัพอากาศ และหน่วยงานความมั่นคงอื่น ๆ ให้เป็นไปอย่างไร้รอยต่อและมีประสิทธิภาพสูงสุด

โครงสร้างและสถาปัตยกรรมของระบบ

โครงสร้างพื้นฐานของระบบ JCS ของสหรัฐประกอบด้วยเครือข่ายสื่อสารหลัก 2 ส่วน ได้แก่ เครือข่ายข้อมูลร่วม (Joint Data Network - JDN) ซึ่งเป็นโครงข่ายแกนหลักความเร็วสูงที่เชื่อมโยงศูนย์บัญชาการและหน่วยทหารทั่วโลกเข้าด้วยกัน โดยอาศัยเทคโนโลยีการสื่อสารผ่านดาวเทียม (SATCOM) เป็นหลัก และเครือข่ายแทคติกอล (Tactical Network) ซึ่งเป็นโครงข่ายสำหรับเชื่อมต่อกำลังพลและยุทธโศปกรณ์ในพื้นที่ปฏิบัติการแบบเคลื่อนที่ โดยใช้เทคโนโลยีสื่อสารแบบ Ad Hoc เช่น Mobile Ad Hoc Network (MANET) และ Airborne Network เป็นต้น โดยทั้งสองเครือข่ายจะถูกเชื่อมโยงเข้าด้วยกันผ่านอุปกรณ์เกตเวย์ (Gateway) ที่ทำหน้าที่แปลงสัญญาณและโปรโตคอลให้สามารถสื่อสารกันได้ (Start & McMillan, 2013)

สถาปัตยกรรมของระบบ JCS จะเป็นแบบ Service Oriented Architecture (SOA) กล่าวคือ จะมี

การจัดบริการด้านสื่อสารและสารสนเทศต่าง ๆ เป็นชุดของบริการมาตรฐาน (Standard Services) ที่จะถูกนำมาประกอบกันขึ้นเป็นแอปพลิเคชันเฉพาะงานตามความต้องการของผู้ใช้ เช่น บริการด้านการสนทนา (Voice Service) บริการด้านข้อความ (Messaging Service) บริการด้านภาพและวิดีโอ (Imaging/Video Service) บริการด้านแผนที่และภูมิสารสนเทศ (Mapping/GIS Service) เป็นต้น ซึ่งบริการเหล่านี้สามารถทำงานร่วมกันได้ผ่านมาตรฐานเปิด เช่น XML, SOAP และ Web Services เป็นต้น ทำให้ทุกเหล่าทัพสามารถพัฒนาแอปพลิเคชันของตนเองโดยอาศัยบริการพื้นฐานที่มีอยู่ร่วมกัน ไม่ต้องลงทุนสร้างใหม่ ประหยัดเวลาและงบประมาณ (Wang et al., 2023, p.1-7)

นอกจากนี้ ระบบ JCS ยังประกอบด้วยชุดเครื่องมือช่วยสนับสนุนการทำงานร่วมกัน (Collaboration Tools) เพื่ออำนวยความสะดวกในการสื่อสาร ประชุม และทำงานข้ามหน่วยงาน โดยใช้เทคโนโลยีการประชุมทางไกลผ่านจอภาพ (Video Tele-Conference) การใช้งานเอกสารร่วมกัน (Document Collaboration) และระบบสารบรรณอิเล็กทรอนิกส์ (Electronic Document Management) เป็นต้น ซึ่งช่วยให้ผู้บังคับบัญชาและฝ่ายอำนาจการในระดับต่าง ๆ สามารถสั่งการ วางแผน และติดตามการปฏิบัติการร่วมกันได้อย่างมีประสิทธิภาพ

ข้อดีและข้อจำกัดของระบบ

ระบบ JCS ของสหรัฐ มีทั้งข้อดีและข้อจำกัด ซึ่งส่งผลต่อประสิทธิภาพการปฏิบัติการร่วมและความท้าทายในการนำไปใช้ ดังตารางที่ 1 (Ashour et al., 2018, p.42-51; Upadhyay et al., 2022, p.1-6)

ตารางที่ 1 แสดงข้อดีและข้อจำกัดของระบบ JCS ของสหรัฐอเมริกา

ข้อดี	ข้อจำกัด
การบูรณาการและแลกเปลี่ยนข้อมูลระหว่างเหล่าทัพอย่างไร้รอยต่อ	ต้นทุนสูงในการจัดหาและดูแลรักษาเทคโนโลยีที่หลากหลายและซับซ้อน
ความรวดเร็ว แม่นยำ และมีประสิทธิภาพในการปฏิบัติการร่วม	การกำหนดมาตรฐานกลางที่เข้มงวดและใช้เวลาในการปรับเปลี่ยน
ความยืดหยุ่นในการพัฒนาแอปพลิเคชันตามมาตรฐานเดียวกัน	อาจไม่ครอบคลุมทุกกรณีการใช้งานจริงในสนามรบ
เครื่องมือช่วยการทำงานร่วมกันลดความผิดพลาดในการสื่อสารและสั่งการ	ความเสี่ยงสูงต่อการถูกโจมตีทางไซเบอร์และการรบกวนทางอิเล็กทรอนิกส์

สาธารณรัฐประชาชนจีน

สาธารณรัฐประชาชนจีนเป็นอีกประเทศหนึ่งที่ทำให้ความสำคัญกับการพัฒนาระบบสื่อสารรวมเหล่าทัพ หรือที่เรียกว่า Integrated Command Platform (ICP) เพื่อเพิ่มขีดความสามารถในการปฏิบัติการร่วมและการบัญชาการและควบคุมเชิงรุก (Active Command and Control) ของกองทัพปลดปล่อยประชาชนจีน (People's Liberation Army - PLA) โดยเฉพาะในบริบทของการทำสงครามข้อมูลข่าวสาร (Information Warfare) (Zhen, 2020)

โครงสร้างและสถาปัตยกรรมของระบบ

โครงสร้างของระบบ ICP ของจีนจะประกอบด้วย 3 ส่วนหลัก ๆ ได้แก่ 1) ระบบเครือข่ายแกนหลัก (Backbone Network) ซึ่งเป็นโครงข่ายสื่อสารความเร็วสูงที่เชื่อมโยงระหว่างศูนย์บัญชาการระดับภูมิภาค (Theater Command) และระดับยุทธบริเวณ (Strategic Region) เข้าด้วยกัน โดยอาศัยเครือข่ายเคเบิลใต้น้ำ (Submarine Cable Network) และเครือข่ายไฟเบอร์ออปติก (Fiber Optic Network) ที่ครอบคลุมทั่วประเทศเป็นหลัก 2) ระบบเครือข่ายยุทธวิธี (Tactical Network) ซึ่งเชื่อมโยงหน่วยรบและอาวุธยุทธโปกรณ์ต่าง ๆ ในระดับกองพันและกองร้อยเข้ากับระบบแกนหลัก ผ่านเครือข่ายสื่อสารวิทยุและดาวเทียมเคลื่อนที่แบบอัจฉริยะ (Cognitive Radio SATCOM) ที่สามารถปรับเปลี่ยนความถี่และรูปแบบการมอดูเลตได้เองตามสภาพแวดล้อมและการรบกวน และ 3) ศูนย์ปฏิบัติการเครือข่าย (Network Operations Center: NOC) ซึ่งทำหน้าที่ควบคุมดูแลและบริหารจัดการทรัพยากรเครือข่ายทั้งหมดแบบรวมศูนย์ รวมถึงการป้องกันการโจมตีทางไซเบอร์ด้วย

ในส่วนของสถาปัตยกรรมของระบบนั้น จีนเลือกใช้สถาปัตยกรรมเครือข่ายหลายชั้น (Multi-Tiered Network Architecture) กล่าวคือ มีการแบ่งระบบออกเป็นชั้นต่าง ๆ ตามหน้าที่และความสำคัญ เช่น ชั้นเครือข่ายแกนหลัก ชั้นเครือข่ายบริการ ชั้นเครือข่ายยุทธวิธี และชั้นเครือข่ายเซ็นเซอร์ เป็นต้น โดยแต่ละชั้นจะมีโปรโตคอลการสื่อสารและการรักษาความปลอดภัยแตกต่างกันไป นอกจากนี้ จีนยังใช้หลักการออกแบบเครือข่ายที่เน้นความยืดหยุ่น (Resilience) ความอยู่รอด (Survivability) และความสามารถในการฟื้นฟู (Recoverability) กล่าวคือ หากเครือข่ายส่วนใดถูกโจมตีหรือชำรุดเสียหาย ก็สามารถเบี่ยงเบนทราฟฟิกไปใช้เส้นทางสำรองได้ทันที โดยเฉพาะอย่างยิ่งในระดับยุทธวิธีที่มีการใช้เทคโนโลยีเครือข่ายแบบกระจาย (Distributed Network) ที่ไม่มีจุดล้มเหลวที่เดียว (No Single Point of Failure)

นอกจากเทคโนโลยีการสื่อสารแล้ว ระบบ ICP ของจีนยังมีความโดดเด่นในแง่ของการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการสนับสนุนการตัดสินใจของผู้บังคับบัญชา ผ่านการใช้ซอฟต์แวร์ช่วยวิเคราะห์และคาดการณ์สถานการณ์ การหาทางเลือกที่เหมาะสม และการจำลองผลลัพธ์ทางยุทธศาสตร์และยุทธวิธี เรียกว่า Decision Support System (DSS) ซึ่งจะเชื่อมโยงกับระบบบัญชาการและควบคุมอัตโนมัติ (Automated Command and Control System) ทำให้การประเมินสถานการณ์ การออกคำสั่ง และการกำกับควบคุมสามารถทำได้อย่างรวดเร็ว แม่นยำ และทันการณ์ยิ่งขึ้น (Li, 2015)

ข้อดีและข้อจำกัดของระบบ

ระบบ ICP ของจีนมีจุดเด่นและข้อจำกัดที่สำคัญ ซึ่งส่งผลต่อประสิทธิภาพและความท้าทายในการใช้งาน ดังตารางที่ 2 (Institute of Electrical and Electronics Engineer [IEEE], 2018, 2023; Chang et al., 2021)

ตารางที่ 2 แสดงข้อดีและข้อจำกัดของระบบ ICP ของจีน

ข้อดี	ข้อจำกัด
เครือข่ายที่มีความยืดหยุ่นและฟื้นฟูได้ เหมาะกับสภาพแวดล้อมที่มีการโจมตีทางอิเล็กทรอนิกส์และไซเบอร์	ต้องพึ่งพาเครือข่ายสื่อสารที่ครอบคลุมพื้นที่กว้างและหนาแน่น ทำให้ต้องลงทุนสูงทั้งงบประมาณและกำลังพล
ใช้ AI สนับสนุนการตัดสินใจ เพิ่มความสามารถในการคาดการณ์และความได้เปรียบในการรบเชิงรุก	ซอฟต์แวร์ AI ซับซ้อน มีความเสี่ยงต่อความผิดพลาด หากออกแบบหรือทดสอบไม่รัดกุม
เชื่อมโยงกับระบบอาวุธอัตโนมัติ เช่น โดรนติดอาวุธ และหุ่นยนต์สนามรบ	ต้องการนักปฏิบัติการที่มีความเชี่ยวชาญสูงในการควบคุมดูแลระบบ
	ใช้มาตรฐานเทคนิคเฉพาะของตนเอง ทำให้เกิดปัญหาความเข้ากันไม่ได้กับระบบสื่อสารของประเทศอื่น

สหพันธรัฐรัสเซีย

สหพันธรัฐรัสเซียเป็นอีกประเทศที่ให้ความสำคัญกับการพัฒนาระบบสื่อสารรวมเหล่าทัพ โดยเฉพาะอย่างยิ่งภายหลังจากการปฏิรูปกองทัพครั้งใหญ่ในปี ค.ศ. 2008 ที่มุ่งเน้นการเพิ่มขีดความสามารถในการปฏิบัติการร่วมและการบูรณาการระบบบัญชาการและควบคุม (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance : C4ISR) ของหน่วยงานความมั่นคงทั้งหมดเข้าด้วยกัน ภายใต้ชื่อ Integrated Military Communications System (IMCS) (Arifin et al., 2018, p.90-95)

โครงสร้างและสถาปัตยกรรมของระบบ

โครงสร้างของระบบ IMCS แบ่งออกเป็น 4 ระดับ ได้แก่ 1) ระดับยุทธศาสตร์ (Strategic Level) ซึ่งเชื่อมโยงศูนย์บัญชาการส่วนกลางของกระทรวงกลาโหมและหน่วยข่าวกรองเข้าด้วยกัน ผ่านเครือข่ายสื่อสารผสมผสาน (Hybrid Network) ที่รวมการสื่อสารผ่านดาวเทียม เคเบิลใยแก้วนำแสง และการสื่อสารไร้สาย 2) ระดับปฏิบัติการ (Operational Level) ซึ่งเชื่อมโยงกองบัญชาการยุทธบริวาร (Regional Commands) 4 แห่ง ได้แก่ ทิศตะวันตก ทิศใต้ ทิศกลาง และทิศตะวันออก เข้ากับหน่วยเหนือและหน่วยรอง ผ่านเครือข่ายไมโครเวฟและดาวเทียม 3) ระดับ

ยุทธวิธี (Tactical Level) ซึ่งเชื่อมโยงกำลังพลและยุทธโธปกรณ์ในสนามรบเข้ากับโครงข่ายใหญ่ โดยใช้เครือข่ายวิทยุสื่อสารแบบ Frequency-Hopping Spread Spectrum (FHSS) ที่ทนทานต่อการรบกวนและดักฟัง และ 4) ระดับสนับสนุน (Supporting Level) ซึ่งเชื่อมโยงฐานทัพคลังสรรพาวุธ และสถานีสนับสนุนต่าง ๆ เข้ากับระบบหลักผ่านเครือข่ายภาคพื้นดินและเครือข่ายเฉพาะงาน (Dedicated Networks)

ในแง่ของสถาปัตยกรรมระบบ IMCS ของรัสเซียเน้นไปที่การสร้างเครือข่ายที่มีความยืดหยุ่นและปรับขนาดได้ (Scalable Network) กล่าวคือ สามารถปรับเพิ่มหรือลดจำนวนโหนดและทรัพยากรเครือข่ายได้ตามความจำเป็นของการปฏิบัติการ โดยใช้สถาปัตยกรรมแบบ Modular Architecture ที่ประกอบขึ้นจากส่วนย่อยต่าง ๆ ที่เชื่อมต่อกันได้อย่างอิสระ ผ่านอุปกรณ์สลับสัญญาณ (Switches) และเกตเวย์แบบอัจฉริยะ (Intelligent Gateways) นอกจากนี้ยังมีการใช้การสื่อสารแบบ Asynchronous Transfer Mode (ATM) และ Multiprotocol Label Switching (MPLS) ในการจัดการทราฟฟิกที่หนาแน่น ให้สามารถส่งข้อมูลได้หลายชนิด หลายระดับความสำคัญ ผ่านช่องสัญญาณเดียวกันได้อย่างมีประสิทธิภาพ (Packer & Reeves, 2020, p.109-123)

จุดเด่นอีกประการของระบบ IMCS คือการบูรณาการระบบสงครามอิเล็กทรอนิกส์ (Electronic Warfare System) เข้ามาเป็นส่วนหนึ่งของการปฏิบัติการ ทำให้สามารถรบกวน ปิดกั้น หรือทำลายเครือข่ายสื่อสารของฝ่ายตรงข้ามได้โดยตรง ในขณะที่ยังสามารถป้องกันตนเองจากการโจมตีทางอิเล็กทรอนิกส์ได้ด้วยเทคนิค Frequency

Agility กล่าวคือ สามารถปรับเปลี่ยนช่วงความถี่และรูปแบบการส่งสัญญาณได้อย่างต่อเนื่อง เพื่อหลบหลีกการถูกรบกวนหรือสกัดกั้น นอกจากนี้ ในเครือข่ายภาคพื้นดินบางส่วนยังได้นำเทคโนโลยีสื่อสารควอนตัม (Quantum Communication) มาใช้ในการเข้ารหัส เพื่อป้องกันการดักฟังแบบสมบูรณ์อีกด้วย (Medhi & Ramasamy, 2018, p.734-764)

ข้อดีและข้อจำกัดของระบบ

ระบบ IMCS ของรัสเซียมีข้อดีและข้อจำกัดที่สำคัญ ซึ่งส่งผลต่อประสิทธิภาพและความท้าทายในการใช้งาน ดังตารางที่ 3 (Fathurrahmad & Yusuf, 2019, p.6504-6517; Chen et al., 2023)

ตารางที่ 3 แสดงข้อดีและข้อจำกัดของระบบ IMCS ของ สหพันธรัฐรัสเซีย

ข้อดี	ข้อจำกัด
ออกแบบเฉพาะสำหรับการปฏิบัติการทางทหาร โครงสร้างหลายระดับสอดคล้องกับการบังคับบัญชา	ความซับซ้อนสูงของเทคโนโลยี ต้องการผู้เชี่ยวชาญเฉพาะทางในการติดตั้งและดูแลรักษา
สถาปัตยกรรมแบบโมดูลาร์ปรับขยายได้ง่าย	มาตรฐานเทคนิคไม่เป็นสากล อาจมีปัญหาความเข้ากันได้กับระบบอื่น
เชื่อมโยงกับระบบสงครามอิเล็กทรอนิกส์ มีเทคนิคป้องกันการรบกวนหลากหลาย	เทคโนโลยีล้ำสมัยมีราคาแพง ต้องนำเข้า ทำให้มีข้อจำกัดในการจัดหาและซ่อมบำรุง
ใช้เทคโนโลยีควอนตัมในการเข้ารหัส ปลอดภัยสูงสำหรับข้อมูลยุทธศาสตร์	การพึ่งพาเทคโนโลยีมากเกินไปอาจส่งผลเสียหากเกิดเหตุขัดข้องที่ควบคุมไม่ได้

สรุปบทเรียนและแนวปฏิบัติที่ดี

จากการศึกษาเปรียบเทียบระบบสื่อสารรวม เหล่าทัพของสหรัฐอเมริกา จีน และรัสเซีย สามารถสรุป (Current State) ของกองทัพไทย และนำไปสู่การระบุคุณลักษณะที่พึงประสงค์ (Desired Characteristics) ช่องว่าง (Gap) ที่ต้องดำเนินการพัฒนา ดังตารางต่อไปนี้

ตารางที่ 4 แสดงการวิเคราะห์ช่องว่างที่สมควรพัฒนาของกองทัพไทย

คุณลักษณะที่พึงประสงค์	สภาพปัจจุบันของกองทัพไทย	ช่องว่างที่ต้องพัฒนา
การบูรณาการเครือข่ายเหล่าทัพให้ทำงานร่วมกันได้ไร้รอยต่อ	ระบบสื่อสารของเหล่าทัพยังแยกส่วนและขาดมาตรฐานกลาง	- พัฒนามาตรฐานกลางด้านเทคนิคและขั้นตอนปฏิบัติ - จัดหาเทคโนโลยีที่ทำงานข้ามแพลตฟอร์มได้
การแบ่งโครงสร้างระบบเป็นระดับชั้นตามความสำคัญ	โครงสร้างระบบไม่ชัดเจนและไม่สอดคล้องกับระดับการบังคับบัญชา	- ออกแบบสถาปัตยกรรมระบบแบบลำดับชั้น - กำหนดนโยบายรักษาความปลอดภัยตามระดับชั้นข้อมูล
ความยืดหยุ่น ความสามารถฟื้นฟู และความอยู่รอดของเครือข่าย	ขาดมาตรการป้องกันการโจมตีทางไซเบอร์ที่เพียงพอ	- ใช้เทคโนโลยีเครือข่ายที่ปรับขนาดและกำหนดเส้นทางได้ - วางมาตรการด้านการทำให้กลับมาใช้งานได้และการสำรองข้อมูล

การประยุกต์ใช้เทคโนโลยีสมัยใหม่เพื่อเพิ่มประสิทธิภาพ	ยังไม่มีเมื่อนำเทคโนโลยี AI และคอมพิวเตอร์มาใช้อย่างจริงจัง	- วิจัยและพัฒนาการประยุกต์ใช้ AI ในระบบสื่อสารและบัญชาการ - ศึกษาความเป็นไปได้ในการใช้เทคโนโลยีคอมพิวเตอร์เพื่อการเข้ารหัส
ความเข้ากันได้กับหน่วยงานอื่น ๆ ทั้งในและต่างประเทศ	ยังไม่มีความร่วมมือกับเหล่าทัพอื่น ๆ ในการพัฒนาระบบสื่อสารร่วม	- เลือกใช้มาตรฐานเปิดที่เป็นสากลเป็นหลัก - เสริมสร้างความร่วมมือกับมิตรประเทศในการพัฒนาขีดความสามารถ

นอกจากนี้บทเรียนสำคัญจากกรณีศึกษาข้างชี้ให้เห็นถึงความจำเป็นในการบริหารจัดการทรัพยากร ทั้งด้านงบประมาณ เทคโนโลยี และบุคลากรอย่างเหมาะสม โดยต้องวางแผนในระยะยาว จัดลำดับความสำคัญ ตลอดจนเลือกรูปแบบการพัฒนาให้สอดคล้องกับบริบทและข้อจำกัดของประเทศ เช่น การสร้างขีดความสามารถในการพัฒนา

เทคโนโลยีด้วยตนเองในบางส่วน ควบคู่ไปกับการจัดหาจากต่างประเทศ หรือการให้ความสำคัญกับการฝึกอบรมกำลังพลเพื่อให้ใช้ประโยชน์จากเทคโนโลยีได้เต็มประสิทธิภาพ เป็นต้น ซึ่งกองทัพไทยจะต้องนำมาพิจารณาอย่างรอบคอบในการกำหนดแนวทางการพัฒนาระบบสื่อสารร่วมเหล่าทัพต่อไป

การวิเคราะห์ SWOT ระบบสื่อสารปัจจุบันของกองทัพไทย

ในการวิเคราะห์สภาพแวดล้อมของระบบสื่อสารปัจจุบันของกองทัพไทย สามารถสรุปจุดแข็ง จุดอ่อน โอกาส และอุปสรรค ได้ดังตารางต่อไปนี้

ตารางที่ 5 การวิเคราะห์ SWOT ของระบบกองทัพไทย

จุดแข็ง (Strengths)	จุดอ่อน (Weaknesses)
- มีโครงสร้างพื้นฐานด้านการสื่อสารที่ครอบคลุมทั่วประเทศ - กำลังพลมีความเชี่ยวชาญและประสบการณ์ในการใช้งานระบบ - มีหน่วยงานวิจัยและพัฒนาด้านเทคโนโลยีสื่อสารในกองทัพ - ผู้บังคับบัญชาระดับสูงให้ความสำคัญและสนับสนุนการพัฒนาระบบ	- ขาดการบูรณาการและมาตรฐานกลางระหว่างเหล่าทัพ - อุปกรณ์และเทคโนโลยีบางส่วนล้าสมัยและเสื่อมสภาพ - ขาดแคลนกำลังพลที่มีความเชี่ยวชาญด้านเทคโนโลยีสมัยใหม่ - งบประมาณในการจัดหาและพัฒนาระบบมีจำกัด
โอกาส (Opportunities)	อุปสรรค (Threats)
- ความก้าวหน้าทางเทคโนโลยีสื่อสารและสารสนเทศในปัจจุบัน - แนวโน้มราคาอุปกรณ์และบริการสื่อสารที่ถูกลง - ความร่วมมือด้านความมั่นคงและการฝึก ร่วมกับมิตรประเทศ - นโยบายรัฐบาลที่ส่งเสริมการพัฒนาเทคโนโลยีและนวัตกรรม	- ภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากขึ้น - การพึ่งพาเทคโนโลยีและอุปกรณ์จากต่างประเทศ - ข้อจำกัดด้านกฎหมายและข้อบังคับในการจัดหาและใช้งานเทคโนโลยี - การเปลี่ยนแปลงที่รวดเร็วของสภาพแวดล้อมด้านความมั่นคง

สรุปผลการวิเคราะห์ SWOT

จากการวิเคราะห์ SWOT ข้างต้น สามารถสรุปได้ว่า ระบบสื่อสารของกองทัพไทยในปัจจุบันมีจุดแข็งที่สำคัญคือการมีโครงสร้างพื้นฐานและบุคลากรที่มีประสิทธิภาพ รวมถึงการมีหน่วยงานสนับสนุนการวิจัยและพัฒนาในกองทัพ ซึ่งเป็นรากฐานสำคัญในการต่อยอดเพื่อพัฒนาขีดความสามารถต่อไป

อย่างไรก็ดีจุดอ่อนที่สำคัญคือการขาดการบูรณาการและมาตรฐานกลางระหว่างเหล่าทัพ ตลอดจนข้อจำกัดด้านงบประมาณและความล้าสมัยของอุปกรณ์บางส่วน ซึ่งเป็นประเด็นท้าทายที่จำเป็นต้องได้รับการแก้ไขโดยเร่งด่วน

ในขณะเดียวกันการเปลี่ยนแปลงทางเทคโนโลยีและความร่วมมือระหว่างประเทศก็นับเป็นโอกาสสำคัญที่จะช่วยให้กองทัพไทยสามารถพัฒนาขีดความสามารถด้านการสื่อสารได้อย่างก้าวกระโดด ผ่านการเข้าถึงเทคโนโลยีที่ทันสมัยและมีราคาถูกลง ตลอดจนการแลกเปลี่ยนองค์ความรู้และประสบการณ์จากมิตรประเทศ

อย่างไรก็ตามภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรง ข้อจำกัดด้านกฎระเบียบ รวมถึงการเปลี่ยนแปลงอย่างรวดเร็วของสภาพแวดล้อมความมั่นคง ก็เป็นความท้าทายที่สำคัญซึ่งกองทัพไทยจำเป็นต้องให้ความสำคัญและเตรียมแนวทางในการรับมืออย่างเหมาะสม ผ่านการพัฒนาขีดความสามารถในการป้องกันทางไซเบอร์ การปรับปรุงกฎระเบียบให้ทันสมัย ตลอดจนการสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกประเทศ

โดยสรุปแม้ระบบสื่อสารของกองทัพไทยในปัจจุบันจะยังมีข้อจำกัดที่ต้องได้รับการแก้ไขอยู่บ้าง แต่ก็มีศักยภาพและโอกาสที่จะพัฒนาไปสู่ระบบสื่อสารรวมเหล่าทัพที่ทันสมัยและมีประสิทธิภาพได้ หากได้รับการสนับสนุนและการดำเนินการอย่างเป็นระบบและต่อเนื่อง ซึ่งจำเป็นต้องอาศัยการผนึกกำลังและความร่วมมือจากทุกภาคส่วนที่เกี่ยวข้อง

ข้อเสนอแนะทางการพัฒนาระบบสื่อสารรวมเหล่าทัพของกองทัพไทย

ด้านเทคโนโลยีและมาตรฐานเทคนิค

การกำหนดสถาปัตยกรรมและมาตรฐานกลาง

- พัฒนาสถาปัตยกรรมอ้างอิงของระบบสื่อสารรวมเหล่าทัพ (Joint Communications System Architecture - JCSA) ที่กำหนดองค์ประกอบ อินเทอร์เน็ต และมาตรฐานต่าง ๆ ให้สอดคล้องกัน

- กำหนดมาตรฐานข้อมูล (Data Standards) เพื่อให้สามารถแลกเปลี่ยนและประมวลผลข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ เช่น Tactical Data Link (TDL), Cursor on Target (CoT) เป็นต้น (Yang et al., 2020; Anca et al., 2016)

- เลือกใช้มาตรฐานเทคนิคที่เป็นสากล เช่น IP, ATM, MPLS เพื่อให้สามารถเชื่อมต่อกับระบบอื่น ๆ ได้ง่าย และลดความเสี่ยงจากการล็อกอินกับเทคโนโลยีใดเทคโนโลยีหนึ่ง

การปรับปรุงโครงสร้างพื้นฐานและอุปกรณ์

- ปรับปรุงและขยายโครงข่ายสื่อสารความเร็วสูงให้ครอบคลุมทุกพื้นที่ปฏิบัติการสำคัญ ทั้งระบบเคเบิลใยแก้วนำแสง ไมโครเวฟ ดาวเทียม และสื่อสารไร้สาย

- จัดหาอุปกรณ์สื่อสารที่ทันสมัย เช่น Software Defined Radios (SDR) ที่สามารถปรับเปลี่ยนความถี่และรูปแบบสัญญาณได้ตามความต้องการ เพื่อเพิ่มความยืดหยุ่นในการใช้งาน

- พัฒนาระบบสำรองและทำให้กลับมาใช้งานได้ (Backup & Recovery) สำหรับโครงสร้างพื้นฐานที่สำคัญ เพื่อให้สามารถทำงานได้อย่างต่อเนื่องแม้ในภาวะวิกฤต (Nelson, 2011)

ด้านการฝึกและพัฒนาบุคลากร

การจัดทำหลักสูตรการฝึกอบรมร่วม

- พัฒนาหลักสูตรฝึกอบรมระบบสื่อสารรวมเหล่าทัพ โดยเน้นการสร้างความรู้ความเข้าใจในสถาปัตยกรรม มาตรฐาน และขั้นตอนปฏิบัติที่เป็นแบบเดียวกัน

- จัดการฝึกอบรมเชิงปฏิบัติการอย่างสม่ำเสมอ เพื่อให้กำลังพลมีความคุ้นเคยกับการใช้งานอุปกรณ์และระบบต่าง ๆ รวมถึงการแก้ไขปัญหาเบื้องต้น

- บูรณาการหลักสูตรเข้ากับการฝึกผสมผสมผสานกำลัง (Joint Training) และการฝึกร่วม/ผสม (Combined/Multinational Training) เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงานจริง (Wood et al., 2017)

การแลกเปลี่ยนบุคลากรระหว่างเหล่าทัพ

- จัดให้มีการแลกเปลี่ยนบุคลากรระหว่างหน่วยสื่อสารของเหล่าทัพ เพื่อให้มีความเข้าใจในภารกิจ ซิตความ สามารถ และข้อจำกัดของกันและกัน
- ส่งเสริมการทำงานร่วมกันในลักษณะทีมข้ามสายงาน (Cross-Functional Team) ในการพัฒนา ทดสอบ และแก้ไขปัญหา ระบบสื่อสาร
- สร้างเครือข่ายผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและสื่อสารในกองทัพ เพื่อแลกเปลี่ยนความรู้และประสบการณ์อย่างต่อเนื่อง (อนันต์ ชูยิ่งสุภกิจ, 2561)

ด้านโครงสร้างการบังคับบัญชาและอำนาจหน้าที่

การจัดตั้งหน่วยงานกลางด้าน C4ISR (Ferris, 2019)

- จัดตั้งหน่วยงานกลางที่รับผิดชอบการวางแผนนโยบาย มาตรฐาน และกำกับดูแลการพัฒนาระบบ C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) ในภาพรวมของกองทัพ
- กำหนดโครงสร้างการบังคับบัญชาและการประสานงานที่ชัดเจน ระหว่างหน่วยงานกลาง หน่วยเหล่าทัพ และหน่วยงานวิจัยและพัฒนาต่าง ๆ
- จัดสรรอำนาจหน้าที่ในการจัดหา ติดตั้ง ดูแลรักษา และบริหารจัดการทรัพยากรสื่อสารให้มีความชัดเจน และลดความซ้ำซ้อน

การกำหนดกลไกประสานงานระหว่างเหล่าทัพ

- จัดทำ Joint Communications Doctrine ที่กำหนดแนวทางการใช้งานและประสานระบบสื่อสารร่วมระหว่างเหล่าทัพในการปฏิบัติการต่าง ๆ
- จัดตั้งศูนย์ปฏิบัติการสื่อสารร่วม (Joint Communications Operations Center - JCOC) เพื่อวางแผน อำนาจการ และกำกับดูแลการใช้งานระบบสื่อสารร่วมในการปฏิบัติการ
- พัฒนาระบบการและระบบสารสนเทศเพื่อสนับสนุนการแลกเปลี่ยนข้อมูลและการประสานงานด้านสื่อสารระหว่างเหล่าทัพ เช่น ฐานข้อมูลทรัพยากรสื่อสาร ระบบจัดการเหตุการณ์ เป็นต้น

ด้านงบประมาณและการจัดหาอุปกรณ์

การจัดทำแผนแม่บทและแผนปฏิบัติการ

- จัดทำแผนแม่บทการพัฒนาระบบสื่อสารรวมเหล่าทัพ 10 - 20 ปี ที่สอดคล้องกับยุทธศาสตร์ชาตินโยบายความมั่นคง และแผนพัฒนากองทัพในภาพรวม
- กำหนดแผนปฏิบัติการและโครงการย่อยตามลำดับความสำคัญและความเร่งด่วน โดยแบ่งเป็นระยะสั้น กลาง และยาว ที่สามารถวัดผลสำเร็จได้อย่างเป็นรูปธรรม
- วางแผนความต้องการงบประมาณและทรัพยากรให้สอดคล้องกับแผนการดำเนินงาน โดยพิจารณาสัดส่วนที่เหมาะสมระหว่างการจัดหา การวิจัยและพัฒนา และการบำรุงรักษาระบบ

การบูรณาการงบประมาณจัดหาอุปกรณ์

- จัดตั้งคณะกรรมการจัดหายุทธโศปกรณ์สื่อสารระดับกองทัพ เพื่อวิเคราะห์ความต้องการและจัดลำดับความสำคัญในการจัดหาอุปกรณ์ของเหล่าทัพต่าง ๆ
- จัดทำแผนการจัดซื้อจัดจ้างร่วม (Joint Procurement) เพื่อให้ได้ประโยชน์จากการประหยัดต่อขนาด และการบำรุงรักษาที่มีประสิทธิภาพ
- กำหนดแผนการผลิตหรือจัดหาอะไหล่และชิ้นส่วนภายในประเทศ เพื่อลดการพึ่งพาการนำเข้า และสร้างขีดความสามารถในการซ่อมบำรุงระยะยาว

กรอบระยะเวลาการดำเนินการ

- ระยะเร่งด่วน (1-2 ปี) : จัดทำสถาปัตยกรรมอ้างอิงและมาตรฐานระบบ, จัดตั้งหน่วยงานกลาง, เริ่มโครงการนำร่อง, ปรับปรุงโครงสร้างพื้นฐานที่มีอยู่
 - ระยะกลาง (3-5 ปี) : ขยายผลการพัฒนาในโครงการนำร่อง, ปรับปรุงกฎระเบียบและมาตรฐานปฏิบัติ, จัดทำหลักสูตรฝึกอบรม, เพิ่มอัตรากำลังพลที่มีความเชี่ยวชาญ
 - ระยะยาว (5-10 ปี) : บูรณาการระบบเข้าด้วยกันอย่างสมบูรณ์, พัฒนาขีดความสามารถในการวิจัยและสร้างนวัตกรรม, สร้างเครือข่ายความร่วมมือกับภาคส่วนต่าง ๆ
- โดยสรุปการพัฒนา ระบบสื่อสารรวมเหล่าทัพของกองทัพไทย จำเป็นต้องดำเนินการในหลายมิติอย่างบูรณาการ ทั้งด้านเทคโนโลยี กำลังพล กระบวนการทำงาน และการบริหารจัดการ โดยเน้นการสร้างความร่วมมือระหว่างเหล่าทัพ และการแสวงหาความร่วมมือจากภาคส่วนอื่น ๆ

ทั้งนี้การดำเนินการควรยึดตามกรอบยุทธศาสตร์และแผนปฏิบัติการที่ชัดเจน และมีการทบทวนปรับปรุงตามสถานการณ์อย่างต่อเนื่อง เพื่อให้การพัฒนาเป็นไปอย่างเป็น

ขั้นตอน มีความยั่งยืน และเกิดประสิทธิผลสูงสุดต่อขีดความสามารถของกองทัพไทยในการปฏิบัติการกิจด้านความมั่นคงของชาติต่อไป

ความท้าทายและข้อเสนอแนะในการดำเนินการ

การสร้างความร่วมมือระหว่างเหล่าทัพ (Ferreyra & Soeters, 2024)

ความท้าทาย

- ความแตกต่างของวัฒนธรรมองค์กรและกระบวนการทำงานของแต่ละเหล่าทัพ ทำให้การประสานงานและบูรณาการเป็นไปได้ยาก
- การแข่งขันชิงอำนาจและอิทธิพลระหว่างเหล่าทัพ อาจส่งผลต่อการยอมรับการเปลี่ยนแปลงและการแบ่งปันข้อมูลและทรัพยากร
- ความเสี่ยงต่อการรั่วไหลของข้อมูลสำคัญระหว่างเหล่าทัพ ซึ่งอาจกระทบต่อประสิทธิภาพและความปลอดภัยในการปฏิบัติการ (Dan-ly & Ozgur, 2022)

ข้อเสนอแนะ

- พัฒนากลไกการกำกับดูแลและประสานงานในระดับยุทธศาสตร์ เพื่อให้เกิดการกำหนดทิศทางและความรับผิดชอบที่ชัดเจนร่วมกัน
- สร้างความไว้วางใจผ่านการฝึกซ้อม/ผสมและกิจกรรมเสริมสร้างความสัมพันธ์ เพื่อส่งเสริมความเข้าใจและการยอมรับซึ่งกันและกัน
- กำหนดมาตรการรักษาความปลอดภัยข้อมูลที่รัดกุม และสร้างความตระหนักรู้แก่กำลังพลในการปฏิบัติตามอย่างเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบ (Siegel & Sweeney, 2020)

ความท้าทาย

- ภัยคุกคามทางไซเบอร์ในปัจจุบันมีความซับซ้อนและรุนแรงมากขึ้น ยากต่อการป้องกันและตรวจจับด้วยมาตรการแบบดั้งเดิม
- ข้อจำกัดด้านบุคลากรและเครื่องมือในการรับมือภัยคุกคามทางไซเบอร์ ทำให้มีความเสี่ยงต่อการถูกโจมตีและเจาะระบบ
- การเชื่อมโยงระบบเข้าด้วยกันอาจสร้างช่องโหว่ใหม่ๆ และเพิ่มผลกระทบจากการโจมตีให้ขยายวงกว้างมากขึ้น

ข้อเสนอแนะ

- กำหนดนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่เข้มงวด ครอบคลุมด้านกายภาพ เทคนิค และการบริหารจัดการ
- พัฒนาบุคลากร เครื่องมือ และกระบวนการเฝ้าระวัง ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านไซเบอร์ที่ทันสมัยและพร้อมปฏิบัติงานได้ตลอด 24 ชม.
- จัดให้มีการซักซ้อมและทดสอบระบบอย่างสม่ำเสมอ รวมถึงการประเมินความเสี่ยงและจัดทำแผนความพร้อมใช้งานอย่างต่อเนื่อง

การจัดการความเปลี่ยนแปลงและการต้านทาน (Hughes, 2018)

ความท้าทาย

- การต้านทานการเปลี่ยนแปลงโดยเฉพาะจากผู้ที่มีส่วนได้เสีย เช่น ผู้ใช้งานเดิม ผู้พัฒนาระบบ ผู้บริหารระดับกลาง เป็นต้น
- ความยุ่งยากในการปรับเปลี่ยนกระบวนการทำงาน การฝึกอบรม และการใช้เทคโนโลยีใหม่ ๆ ซึ่งต้องใช้เวลาและงบประมาณจำนวนมาก
- ความท้าทายในการสื่อสารและสร้างความเข้าใจให้กับกำลังพลในทุกระดับ ถึงความจำเป็นในการเปลี่ยนแปลงและ ‘ภาพใหญ่’ ของการพัฒนาาระบบ

ข้อเสนอแนะ

- จัดทำแผนการสื่อสารเพื่อสร้างความตระหนักรู้ถึงประโยชน์และความจำเป็นของการเปลี่ยนแปลงให้กับผู้มีส่วนได้เสียทุกกลุ่ม
- สร้างการมีส่วนร่วมของผู้บังคับบัญชาทุกระดับในการผลักดันและสนับสนุนการเปลี่ยนแปลง
- จัดทำโครงการนำร่องขนาดเล็กที่มีผลสัมฤทธิ์ชัดเจน เพื่อสร้างความเชื่อมั่นก่อนขยายผลในวงกว้าง พร้อมทั้งรับฟังข้อเสนอแนะเพื่อนำมาปรับปรุง

แนวทางการบริหารความเสี่ยง

ประเภทของความเสี่ยง (Yilmaz & Flouris, 2019)

- ความเสี่ยงด้านกลยุทธ์ : การกำหนดทิศทางที่ไม่สอดคล้องกับสถานการณ์ การขาดการสนับสนุนทางการเมือง
- ความเสี่ยงด้านปฏิบัติการ : การออกแบบระบบที่ไม่ตอบสนองต่อความต้องการผู้ใช้ การขาดการบำรุงรักษาที่เหมาะสม
- ความเสี่ยงด้านการเงิน : การจัดสรรงบประมาณไม่เพียงพอ การบริหารสัญญาจัดหาไม่มีประสิทธิภาพ
- ความเสี่ยงด้านกฎหมาย : การละเมิดกฎหมายและกฎระเบียบ การใช้งานระบบในทางที่ผิด
- ความเสี่ยงด้านเทคโนโลยี : การเลือกใช้เทคโนโลยีที่ไม่เหมาะสม การพึ่งพาผู้ให้บริการรายเดียว
- ความเสี่ยงของระบบสื่อสารเชื่อมโยง : การถูกโจมตีทางไซเบอร์ ทำให้ระบบล่มหรือข้อมูลรั่วไหล

กลยุทธ์การบริหารความเสี่ยง

- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) : การปรับยุทธศาสตร์ การยกเลิก/เลื่อนโครงการที่มีความเสี่ยงสูง

- การลดความเสี่ยง (Risk Reduction) : การลดโอกาสเกิดหรือผลกระทบ เช่น การพัฒนาระบบอย่างค่อยเป็นค่อยไป การใช้ระบบสำรอง

- การถ่ายโอนความเสี่ยง (Risk Sharing) : การแบ่งความรับผิดชอบกับหน่วยงานอื่น เช่น การทำประกันภัย การจ้างที่ปรึกษา

- การยอมรับความเสี่ยง (Risk Acceptance) : การตระหนักและเตรียมแผนรับมือหากเกิดความเสี่ยงที่สามารถจัดการได้

ทั้งนี้การบริหารความเสี่ยงที่มีประสิทธิภาพนั้น จำเป็นต้องมีการระบุความเสี่ยงอย่างรอบด้าน พร้อมทั้งจัดลำดับความสำคัญตามโอกาสและผลกระทบ รวมถึงการกำหนดตัวชี้วัดที่ชัดเจนในการติดตามและควบคุมความเสี่ยง และการทบทวนแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับสถานการณ์และปัจจัยเสี่ยงที่เปลี่ยนแปลงไป อันจะช่วยให้การพัฒนาระบบสื่อสารรวมเหล่าทัพเป็นไปอย่างราบรื่น และบรรลุเป้าหมายที่วางไว้ได้ในที่สุด (Wang, 2023)

บทสรุป

การพัฒนาระบบสื่อสารรวมเหล่าทัพถือเป็นความจำเป็นเร่งด่วนสำหรับกองทัพไทย หากต้องการเพิ่มขีดความสามารถในการปฏิบัติการร่วมให้มีประสิทธิภาพและทัดเทียมมาตรฐานสากล จากการศึกษาพบว่าระบบสื่อสารปัจจุบันยังขาดการบูรณาการระหว่างเหล่าทัพ มีข้อจำกัดด้านงบประมาณและเทคโนโลยี ตลอดจนขาดนโยบายและแนวทางนำที่ชัดเจน

นอกจากการวิเคราะห์สภาพปัจจุบันแล้ว บทความนี้ยังได้นำเสนอข้อเสนอแนะเชิงนโยบายและแนวทางปฏิบัติสำหรับการพัฒนาระบบสื่อสารให้มีประสิทธิภาพมากยิ่งขึ้น โดยเน้นไปที่การกำหนดสถาปัตยกรรมและมาตรฐานกลาง การให้ความสำคัญกับการฝึกอบรมและพัฒนาบุคลากร การปรับโครงสร้างองค์กรและอำนาจการบังคับบัญชา

ตลอดจนการจัดสรรงบประมาณและดำเนินการจัดท้าวอย่างมีประสิทธิภาพและคุ้มค่า

ทั้งนี้การนำเสนอแนะดังกล่าวไปปฏิบัติย่อมต้องเผชิญกับความท้าทายอย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเป็นประเด็นการสร้างความร่วมมือระหว่างเหล่าทัพ การรักษาความปลอดภัยด้านไซเบอร์ การบริหารจัดการ การเปลี่ยนแปลง รวมถึงข้อจำกัดด้านงบประมาณและกฎระเบียบ ดังนั้นการดำเนินการอย่างเป็นระบบและต่อเนื่อง โดยได้รับการสนับสนุนจากทุกภาคส่วนที่เกี่ยวข้องอย่างจริงจังและนำแนวปฏิบัติที่ดีจากนานาประเทศมาประยุกต์ใช้จะเป็นกุญแจสู่ความสำเร็จ เพื่อให้เกิดประโยชน์สูงสุดต่อขีดความสามารถการปฏิบัติการร่วมของกองทัพไทย ในยุคปัจจุบันและอนาคต

เอกสารอ้างอิง

- เนรมิตร อัมมอภินันท์. (2561). *การพัฒนาซอฟต์แวร์ตรวจสอบประวัติข้าราชการบนอุปกรณ์สื่อสารเคลื่อนที่ของกองบัญชาการกองทัพไทย (ระบบปฏิบัติการแอนดรอยด์)* [วิทยานิพนธ์มหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ]. คลังทรัพยากรสารสนเทศดิจิทัล มหาวิทยาลัยรังสิต. <https://rsuir-library.rsu.ac.th/bitstream/123456789/891/1/Neramit%20Archaapinun.pdf>
- สุทัศน์ ครำในเมือง และ มนวิดี ตั้งตรงฤทัย. (2559). การพัฒนาแนวทางการสื่อสารทางยุทธศาสตร์ (Strategic Communication: STRATCOM) ของกองบัญชาการกองทัพไทย. *วารสารสถาบันวิชาการป้องกันประเทศ*. 7(2), 62-74.
- สุทัศน์ จารุมณี. (2561). *การฝึกทักษะเพื่อปรับเปลี่ยนและพลิกแพลงเพื่อเอาชนะ* (พิมพ์ครั้งที่ 2). ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์ กรมยุทธศึกษาทหารบก.
- อนันต์ ชูยิ่งสุกุลทิพย์. (2561). *ระบบการพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อความมั่นคงปลอดภัยของสารสนเทศ* [วิทยานิพนธ์ปริญญาโทสาขาเทคโนโลยีสารสนเทศ]. คลังปัญญา มหาวิทยาลัยบูรพา. <https://buuir.buu.ac.th/xmlui/handle/1234567890/8714>
- Anca, S., Diana, M., Dan, M., & Alina, P. (2016). Tactical Data Link - from Link 1 to Link 22. *Scientific Bulletin "Mircecel Batran" Naval Academy; Constanta*. 19(2). 346.
- Arifin, M. S., Widyotriatmo, A., Sumari, A. D. W., & Julostuti, E. (2018). Opinion Formation for Decision Making Process in Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. In *2018 5th Asian Conference on Defense Technology (ACDT)*. pp. 90-95. IEEE. <https://doi.org/10.1109/ACDT.2018.8592979>
- Ashour, O., St-Hilaire, M., & Kunz, T. (2018). Multicasting in Tactical Networks: Forwarding Versus Network Coding. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*. pp. 42-51. <https://doi.org/10.5220/0006907902080217>
- Chang, Z., Piurkowsky, S., Huang, S., & Kirschbaum, M., (2021). Applications of triple quadrupole ICP-MS (ICP-MS/MS, or ICP-MS QQQ) in economic geology. In *Proceeding Article published 2021 in Goldschmidt 2021 abstracts*. Goldschmidt <https://doi.org/10.7185/gold2021.8289>
- Chen, X., Feng, Z., Wei, Z., Yuan, X., & Zhang, P. (2023). Multiple signal classification based joint communication and sensing system. *IEEE Transactions on Wireless Communications*, 22(10), 6504-6517, <https://doi.org/10.1109/TWC.2023.3244195>
- Cossart, B. (2021). Transformation of military technology in Portugal. In H. Carvalhal, A. Murteira, & R. Lee de Jesus (Eds.). *The First World Empire: Portugal, War and Military Revolution*. Routledge.
- Coticchia, F., Dian, M., & Moro, F. N. (2023). *Reluctant Remilitarisation: Transforming the Armed Forces in Germany, Italy and Japan After the Cold War*. Edinburgh University Press. <https://doi.org/10.3366/edinburgh/9781474467278.003.0003>
- Dan-lya, B. I., & Ozgur, C. (2022). Efficiency vs Inefficiency in Operations Management: The Singapore Armed Forces (SAF) vs. the Malaysian Armed Forces (MAF) in Southeast Asia?. In *Conference: Efficiencies and Inefficiencies in Operations Management Resiliency*.

- Fathurrahmad, F., & Yusuf, S. (2019). Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). *Jurnal JTik (Jurnal Teknologi Informasi dan Komunikasi)*, 3(1), 29-33. <https://doi.org/10.35870/jtik.v3i1.83>
- Feng, Z., Wei, Z., Chen, X., Yang, H., Zhang, Q., & Zhang, P. (2021). Joint Communication, Sensing, and Computation Enabled 6G Intelligent Machine System. *IEEE Network*, 35(6), 34-42. <https://doi.org/10.1109/MNET.121.2100320>
- Ferreya, M., & Soeters, J. (2024). Multinational Military Cooperation in the Global South. *Armed Forces & Society*, 50(1), 25-54. <https://doi.org/10.1177/0095327X221114928>
- Ferris, J. (2019). *Netcentric warfare, C4ISR and information operations Towards a revolution in military intelligence?* (2nd ed.). Routledge.
- Hughes, M. (2018). *Resistance and organizational change readiness*. Routledge.
- Institute of Electrical and Electronics Engineers. (2018). *2018 IEEE 7th International Conference on Photonics (ICP)*. IEEE. <https://doi.org/10.1109/ICP41633.2018>
- Institute of Electrical and Electronics Engineers. (2023). *2023 Seminar on Information Computing and Processing (ICP)*. IEEE. <https://doi.org/10.1109/ICP60417.2023>
- Killcross, M. (2021). 18-Develop Standard Operating Procedures (SOPs). In *Chemical and Process Plant Commissioning Handbook* (pp.155-164). Butterworth-Heinemann. <https://doi.org/10.1016/B978-0-12-824049-6.00007-X>
- Li, H. Y. (2015). Design and management of intelligent transportation integrated command platform. In *Information, Computer and Application Engineering*. CRC Press.
- Medhi, D., & Ramasamy, K. (2018). Chapter 22 - MultiProtocol Label Switching (MPLS). In *Network Routing* (pp. 734-764). Morgan Kaufmann. <https://doi.org/10.1016/B978-0-12-800737-2.00026-0>
- Nelson, S. (2011). *Pro Data Backup and Recovery*. Apress.
- Ökten, T. (2022). *The Transformation of the Turkish Armed Forces*. Routledge.
- Packer, J., & Reeves, J. (2020). 5. Intelligence, Surveillance, and Reconnaissance (DoD). In *Killer Apps: War, Media, Machine* (pp. 109-123). Duke University Press. <https://doi.org/10.1515/9781478007272-008>
- Siegel, C. A., & Sweeney, M. (2020). *The 6 STEPs in Developing and Maintaining a Cybersecurity and Cyber Resiliency Strategy*. Auerbach Publications.
- Start, A., & McMilian, G. (2013). The critical role of tactical Satcom in deployed operations. In *IET Seminar on Military Satellite Communications 2013 (Milsatcoms 2013)*. IET. <https://doi.org/10.1049/ic.2013.0105>
- Upadhyay, D., Mohd, N., Tiwari, P., & Singh, A. (2022). Methodology for SNR Improvement on SatCom Network From orbiting Satellites. In *Proceeding of the 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*. pp. 1-6. IEEE. <https://doi.org/10.1109/otcon56053.2023.10113993>
- Wang, J., Richards, T., & Narula-Tam, A. (2023). Application of recent reliable transport layer advancements to DoD SATCOM network challenges. In *2023 IEEE Aerospace Conference*. pp 1-7. IEEE. <https://doi.org/10.1109/aero55745.2023.10115799>

- Wang, W. (2023). Leverage effect in options trading risk management strategy research. *Financial Engineering and Risk Management*, 6(10), 87-91. <https://dx.doi.org/10.23977/ferm.2023.061012>
- Wilmelius, M. E. (2007). The Future of Military Interventions in International Relations. In H. Edström & Å. Wiss (Eds.). *International Trends Analysis: Yearbook 2007 with an Introduction to the ART Model* (pp.117-138). Swedish Defence Research Agency. <https://doi.org/10.21557/mth.82119910>
- Wood, P. S., Grant, C. C., Toit, P. J., & Fletcher, L. (2017). Effect of Mixed Basic Military Training on the Physical Fitness of Male and Female Soldiers. *Military Medicine*, 182(7), pp. e1771-e1779. <https://doi.org/10.7205/MILMED-D-16-00218>
- Yang, X., Li, Y., Chen, L., Feng, W., & Yan, Z. (2020). TDL-Chain: An Intelligent Data Transmission Control System in Tactical Data Link Based on Blockchain. In *Proceeding article in 2020 IEEE International Conference on Blockchain (Blockchain)*. pp. 305-312. <https://doi.org/10.1109/Blockchain50366.2020.00045>
- Yilmaz, A. K., & Flouris, T. G. (2019). Enterprise Risk Management in Aviation Management and Strategy. In *Values, Ergonomics and Risk Management in Aviation Business Strategy*. Springer. https://doi.org/10.1007/978-981-15-1006-9_4
- Zhen, Z. (2020). Research on Army and Local Government Integrated Joint Command Information Platform. *Journal of Physics: Conference Series*. 1607(1), Article 012117. <https://doi.org/10.1088/1742-6596/1607/1/012117>