



นวิกสารปิตยสาร

Naval Strategic Studies Journal

วารสารยุทธศาสตร์และความมั่นคงทางทะเล กองทัพเรือ

เทคโนโลยีและแนวคิด การทำสงครามทางเรือในอนาคต

USV



Ambush



UUV for Anti-submarine Patrol



Anti-submarine Patrol

Tracking
Sub

ฉบับที่ ๑๐๖
ปีที่ ๕๕ เล่มที่ ๒
(มกราคม - กันยายน ๒๕๖๕)

ภาพหน้าปก

AI

ที่มา: <https://positioningmag.com/1235760>

“ปฏิบัติการทางทะเลแบบกระจาย (DMO)”

ที่มา: IDSTCH.com

สงครามไซเบอร์ (Cyberwarfare)

ที่มา: <https://patrioutfitthailand.com/blog/>

ระบบการเดินเรือไร้คนขับ

ที่มา: https://www.hanwhasystems.com/m/en/business/defense/naval/marine_index.do

ภาพปกใน

อากาศยานไร้คนขับ รุ่น MARCUS B

ที่มา : <https://aagtj1.blogspot.com/2021/11/marcus-b.html>





นāvīkāri pīdīyāsār

Naval Strategic Studies Journal

วารสารยุทธศาสตร์และความเป็นคองทางทะเล กองทัพเรือ



ศูนย์ศึกษายุทธศาสตร์ทหารเรือ
Naval Strategic Studies Center



**"A WORLD CLASS STRATEGIC
AND NAVAL WARFARE
THINK TANK 2036"**

เป็นคลังสมองด้านยุทธศาสตร์และการสงครามทางเรือระดับโลกในปีพ.ศ. ๒๕๖๙



วัตถุประสงค์

Naval Strategic Studies Journal

นับจากปี พ.ศ.๒๕๒๐ วารสารนาวิกาธิปไตยสาร ฉบับที่ ๑ ได้เริ่มตีพิมพ์สู่สายตาผู้อ่านจนถึงวันนี้ พ.ศ.๒๕๖๔ วารสารนาวิกาธิปไตยสาร ได้นำเสนอองค์ความรู้ทางทะเลมาแล้วถึง ๑๐๒ ฉบับ ประสบการณ์และช่วงเวลาที่ผ่านมาวารสารนาวิกาธิปไตยสารได้ทำหน้าที่อย่างเจียบ ๆ ในการเป็นคลังสมอง เผยแพร่วิทยาการ สร้างทฤษฎี องค์ความรู้ใหม่ ๆ จากผู้เชี่ยวชาญด้านต่าง ๆ ของกองทัพเรือให้แก่ทหารเรือ คณาจารย์ และผู้ที่เกี่ยวข้องกับทะเล รวมทั้งผู้ที่สนใจทั้งในด้านยุทธศาสตร์ ความมั่นคงทางทะเล การสงคราม เศรษฐกิจ เทคโนโลยี และสิ่งแวดล้อม อันเกี่ยวข้องกับทะเลทั้งปวง

นับตั้งแต่วารสารนาวิกาธิปไตยสารเล่มแรกที่จัดทำโดยโรงเรียนนายทหารเรือในยุคนุยกเบิก และได้ปรับปรุงไปสู่สถาบันวิชาการทหารเรือชั้นสูง เมื่อมีการปรับโครงสร้างหน่วยงานในกองทัพเรือและเปลี่ยนชื่อหน่วย จวบจนปัจจุบัน ศูนย์ศึกษายุทธศาสตร์ทหารเรือ กรมยุทธศึกษาทหารเรือ เป็นหน่วยงานรับผิดชอบ ก็ถือได้ว่าวารสารนาวิกาธิปไตยสารเล่มนี้ได้ผ่านห้วงเวลาต่าง ๆ ไปพร้อม ๆ กับสถานการณ์ของประเทศไทยและของโลกที่เปลี่ยนแปลงไป แต่สิ่งหนึ่งที่ไม่เปลี่ยนแปลงคือการทำหน้าที่ติดต่ออาวุธทางปัญญาให้แก่ผู้อ่านให้สามารถรับมือกับผลกระทบจากสภาวะแวดล้อมความมั่นคงทางทะเลที่เปลี่ยนแปลงไปได้อย่างรู้เท่าทัน

นาวิกาธิปไตยสาร หรือ Naval Strategic Studies Journal เป็นวารสารยุทธศาสตร์และความมั่นคงทางทะเลของกองทัพเรือ ซึ่งมีวัตถุประสงค์ในการเผยแพร่ผลงาน การค้นคว้าวิจัย ยกระดับผลงานทางวิชาการสู่ระดับสากล และเป็นเวทีแลกเปลี่ยนความคิดเห็นและพัฒนางองค์ความรู้ โดยเน้นที่ระดับผู้บริหาร รวมทั้งเผยแพร่กิจกรรมทางวิชาการของกองทัพเรือให้แก่หน่วยต่าง ๆ ทั้งในสังกัดกระทรวงกลาโหม และหน่วยงานหรือสถาบันทางวิชาการอื่น ๆ

บทความ แนวคิด หรือข้อคิดเห็นที่นำลงนาวิกาธิปไตยสารเป็นของผู้เขียนมิใช่ข้อคิดเห็นของศูนย์ศึกษายุทธศาสตร์ทหารเรือ กรมยุทธศึกษาทหารเรือ การคัดลอก ทำซ้ำหรือดัดแปลงส่วนใดส่วนหนึ่งทั้งหมดของวารสารฯ นี้เป็นไปตาม พ.ร.บ.ลิขสิทธิ์ พ.ศ.๒๕๓๙ ผู้ที่สนใจหรือหน่วยงานที่ต้องการจะนำบทความหรือข้อมูลที่ลงตีพิมพ์ในวารสารฯ นี้ไปเผยแพร่ซ้ำ สามารถติดต่อได้ที่กองบรรณาธิการนาวิกาธิปไตยสาร

วารสารฯ ยินดีรับบทความทางวิชาการที่เกี่ยวข้องกับความมั่นคงและกิจการทางทะเลเพื่อพิจารณาลงตีพิมพ์ในวารสารฯ โดยสามารถส่งต้นฉบับหรือติดต่อได้ที่กองบรรณาธิการฯ เมื่อได้รับการตีพิมพ์ลงในวารสารฯ จะมีค่าตอบแทนที่เหมาะสมให้แก่เจ้าของบทความ ทั้งนี้ กองบรรณาธิการฯ ขอสงวนสิทธิ์ที่จะรับหรือปฏิเสธบทความ ตามที่พิจารณาเห็นสมควร

กองบรรณาธิการนาวิกาธิปไตยสาร ศูนย์ศึกษายุทธศาสตร์ทหารเรือ
กรมยุทธศึกษาทหารเรือ ต.ศาลายา อ.พุทธมณฑล จ.นครปฐม ๗๓๑๗๐

โทร. ๐ ๒๕๗๕ ๓๔๕๘ หรือ ๐ ๒๕๗๕ ๓๔๗๖

www.tnssc.navy.mi.th/journal

Email : tnssc.journal@gmail.com



กองบรรณาธิการ

ประธานคณะที่ปรึกษา

พลเรือโท เคารพ ไหลมคม

รองประธานคณะที่ปรึกษา

พลเรือตรี จิรวล ว่องวิทย์

พลเรือตรี กิตติ ยศไทร

คณะที่ปรึกษา

พลเรือตรี เพติมชัย สุคนธรัต

พลเรือตรี สุพพัต ยุทธวงษ์

พลเรือตรี พิเศษ ชันแข็ง

พลเรือตรี สุภชิต นาวีสุรพล

นาวาเอก รศ.นเรศ เพ็ชรนิ้น

นาวาเอก กุญเงิน จงรักชอบ

นาวาเอก นพดล บงกชภาณจน

นาวาเอก เขียว เกตุวัฒนกิจ

ผู้อำนวยความสะดวก

พลเรือตรี สนิท โนนินา

รองผู้อำนวยความสะดวก

นาวาเอก กระแสร์ แม่อำพัน

บรรณาธิการ

นาวาเอก กระแสร์ แม่อำพัน

ผู้ช่วยบรรณาธิการ

นาวาเอก สกาทพร วาจรัตน์

นาวาเอก วริษ วัจยีน

นาวาเอก บุณย์ กาโน

นาวาเอก ทิวา อ่อนละออ

ประจำกองบรรณาธิการ

นาวาเอก ปราโมทย์ นงศ์ทอง

นาวาเอก ดุสิต ยมจินดา

นาวาเอก ณตฐพล ชุ่มธี

นาวาเอก เอนกพงศ์ แจ่มกระจ่าง

ว่าที่ นาวาเอก ณัฐกร ไทศรีกุล

นาวาโท สำราญ มรรจ

นาวาโท อนุรักษย์ เจริญศรี

พันจ่าเอก สุริโย ชันทองดี

ฝ่ายบทความและวิชาการ

นาวาเอก รัชภูมิ อินม่วง

นาวาเอก สกาทพร วาจรัตน์

นาวาเอก ปราโมทย์ นงศ์ทอง

นาวาเอก เอนกพงศ์ แจ่มกระจ่าง

พันจ่าเอก พิธวิวัฒน์ ศรีประชาสวัสดิ์

ฝ่ายจัดหารายได้ สมาชิกสัมพันธ์

จ่าหน้าย และแจกจ่าย

นาวาเอก วริษ วัจยีน

นาวาเอก ดุสิต ยมจินดา

นาวาเอก มนต์ชัย มีสวัสดิ์

พันจ่าเอก ทองเจือ พุฒศรี

ฝ่ายการเงิน

นาวาเอก ทิวา อ่อนละออ

นาวาเอก ณตฐพล ชุ่มธี

นาวาโท สำราญ มรรจ

นาวาโทหญิง กฤษณา หอมกลิ่น

เรือโท ขจรศักดิ์ กระทุบแก้ว

9

Drone Warfare From The Past to the Future:
สงครามโดรนจากอดีตสู่นาคต

โดย นาวาเอก นาวี ฤทัยทัณญ

37

สงครามไซเบอร์และพัฒนาการปฏิบัติการไซเบอร์
ในอนาคต

โดย นาวาเอก ดร. กรกช วิไลลักษณ์

63

การใช้ AI ในสงครามอนาคต

โดย นาวาโท ดร. มนต์ชัย บุญยกิจตานนท์

83

เทคโนโลยีเรือดำน้ำกับสงครามในอนาคต

โดย นาวาโท สุระ บรรจงจิตร

105

Unmanned Surface Vehicle for RTN's Future
Warfare : Conceptual Design of Suitable Platform
เรือผิวน้ำไร้คนขับ สำหรับสงครามอนาคตของกองทัพเรือไทย
: การออกแบบตัวเรือและระบบขับเคลื่อนในระดับเบื้องต้น

โดย ว่าที่ นาวาโท ปริญญ์ กันอยู่

133

การพัฒนาระบบควบคุมบังคับบัญชา

โดย นาวาเอก วิทยา ปัญญวรญาณ

155

แนวคิด “Informatized Distributed Maritime
Operation: IDMO” ในการปฏิบัติการทางเรือในอนาคต
(FNOC)

โดย นาวาเอก ศิลป์ พันธุ์รังษี

185

ผู้บัญชา ๔.๐ : คุณสมบัติที่จำเป็นต้องมี

โดย พลเรือเอก ไพโรจน์ แก่นสาร

บรรณาธิการแถลง

Editor Talk

สวัสดีครับท่านผู้อ่านที่เคารพครับ เป็นที่ทราบกันโดยทั่วไปแล้วนะครับว่าทุกวันนี้ เทคโนโลยีต่าง ๆ รวมถึงเทคโนโลยีทางทหารล้วนพัฒนาไปเร็วมาก จึงมีความจำเป็นอย่างยิ่งที่นักการทหารเรือจะต้องศึกษาแนวโน้มการใช้เทคโนโลยีในการทำสงครามทางเรือในอนาคต เพื่อจะนำมาใช้ในการกำหนดเป็นแนวความคิดในทางปฏิบัติ (Operational Concepts) ที่เหมาะสมกับภารกิจของกองทัพเรือและสภาวะแวดล้อมที่เกี่ยวข้อง ดังนั้น วารสารนาวิกาธิปไตยสาร ฉบับที่ ๑๐๒ นี้ ขออนุญาตนำเสนอในธีม (Theme) ที่มีชื่อว่า “เทคโนโลยีและแนวความคิดการทำสงครามทางเรือในอนาคต หรือ “The Future Technologies and Concepts of Naval Warfare” โดยมีบทความทั้งสิ้น ๘ บทความ มีผู้เขียนและโครงเรื่อง ดังนี้

บทความเรื่องแรก “สงครามโดรนจากอดีตสู่อนาคต” โดย นาวาเอก นาวี ฤทัยทัตญญ ได้เขียนบรรยายถึงความหมาย และวัตถุประสงค์ของการ “โดรน” ตลอดจนการนำไปใช้และบทบาทที่มากขึ้นในอนาคต

บทความเรื่องที่สอง “สงครามไซเบอร์และพัฒนาการปฏิบัติการไซเบอร์ในอนาคต” โดย นาวาเอก ดร.กรกช วิไลลักษณ์ ได้นำเสนอหลักการพื้นฐานที่เกี่ยวข้องกับสงครามไซเบอร์ การศึกษาและวิเคราะห์ การปฏิบัติการไซเบอร์ที่ผ่านมา การป้องกันและรักษาความมั่นคงปลอดภัยของทรัพยากรและโครงสร้างพื้นฐานที่เกี่ยวข้องกับกองทัพเรือ รวมทั้งการเตรียมความพร้อมรองรับกับภัยคุกคามทางไซเบอร์ในอนาคต

บทความเรื่องที่สาม “การใช้ AI ในสงครามอนาคต” โดย นาวาโท ดร.มนต์ชัย บุญยกิจตานนท์ ได้ชี้ให้เห็นถึงแนวโน้มของสงครามในอนาคตว่า

จะมีการปฏิบัติการที่หลากหลายมิติ โดยอาศัยระบบอัตโนมัติ ระบบเครือข่าย และระบบเทคโนโลยีปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) เป็นปัจจัยสำคัญ การเสริมสร้างความรู้ความเข้าใจในเทคโนโลยี AI ที่กำลังเข้ามา มีบทบาทและจะเปลี่ยนแปลงรูปแบบการปฏิบัติงานของกองทัพในทุกส่วนอย่างหลีกเลี่ยงมิได้

บทความเรื่องที่ว่า “เทคโนโลยีเรือดำน้ำกับสงครามในอนาคต” โดย นาวาโท สุระ บรรจงจิตร ได้กล่าวถึงขีดความสามารถของเรือดำน้ำ การพัฒนาเทคโนโลยีที่เกี่ยวข้องในอนาคตซึ่งส่งผลให้กำลังรบใต้น้ำจะยังคงมีบทบาทสำคัญต่อไปอีกนาน

บทความเรื่องที่ว่า “เทคโนโลยีการออกแบบเรือเพื่อสงครามอนาคต” โดย นาวาโท ดร.ปริญญา กันอยู่ ได้นำเสนอการออกแบบตัวเรือตามหลักการนาวาสถาปัตยกรรม ผสมผสานกันเทคนิคการออกแบบเรือสมัยใหม่เพื่อพัฒนาการไปสู่การเป็นเรือผิวน้ำไร้คนขับ (Unmanned Surface Vessels: USVs) ที่สามารถใช้ในราชการกองทัพเรือได้

บทความเรื่องที่หก “การพัฒนาระบบควบคุมบังคับบัญชา” โดย นาวาเอก วิทยา ปัญญาวรรณ ได้นำเสนอแนวทางการพัฒนาระบบควบคุมบังคับบัญชา ซึ่งเป็นหัวใจสำคัญที่จะนำไปสู่การตัดสินใจอย่างชาญฉลาด ทำให้กำลังรบในภาคส่วนต่าง ๆ ปฏิบัติหน้าที่สอดประสานกัน และเป็นการเพิ่มโอกาสในการใช้อาวุธในมิติต่าง ๆ อีกด้วย

บทความเรื่องที่เจ็ด “แนวคิด Informatized Distributed Maritime Operation : IDMO” ในการปฏิบัติการทางเรือในอนาคต (FNOC) โดย นาวาเอก ศิลป์ พันธุ์รังสี ได้นำเสนอที่มาและแนวคิดการปฏิบัติการทางทะเลแบบกระจายศูนย์ด้วยความเป็นเลิศด้านข้อมูลข่าวสาร (IDMO) ที่บูรณาการข้อดีจากหลากหลายทฤษฎียุทธศาสตร์สมัยใหม่

และส่งท้ายด้วยบทความเรื่องที่แปด “ผู้นำยุค ๔.๐ : คุณสมบัติที่จำเป็นต้องมี” โดย คุณครูพลเรือเอก ไพโรจน์ แก่นสาร ซึ่งคุณครูท่านได้กรุณาเขียนบรรยายถึงคุณสมบัติสำคัญที่ผู้นำในยุค ๔.๐ พึงมี

หลังจากที่ทุกคนอ่านบทความแล้ว จะพบว่าเทคโนโลยีในอนาคต โดยเฉพาะเทคโนโลยี AI จะทำให้การปฏิบัติในภารกิจต่าง ๆ ตั้งแต่ยามสงบ ไปจนถึงยามสงครามของกองทัพเรือ บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ และประสิทธิผลมากยิ่งขึ้น จะสูญเสียชีวิตและทรัพย์สินน้อยลง รวมทั้งมีโอกาส เป็นไปตามที่ขุนวูได้กล่าวไว้แล้วว่า “การชนะทั้งร้อย มิใช่วิธีการอันประเสริฐแท้ แต่การชนะโดยไม่ต้องรบเลย จึงถือว่าเป็นวิธีการอันวิเศษยิ่ง” ได้มากยิ่งขึ้น ตลอดจนจะมีความเป็นไปได้เพิ่มขึ้นถ้านำเทคโนโลยีควอนตัม (Quantum Technologies) มาใช้กับเทคโนโลยีทางทหารดังกล่าวได้อย่างเหมาะสม

สุดท้ายนี้ กองบรรณาธิการ ขอกราบขอบพระคุณผู้ที่ให้การสนับสนุน ท่านผู้เขียนและท่านผู้อ่านที่เคารพทุกท่าน โดยหวังว่านวิกาสปดธ์สารเล่มนี้ จะเป็นประโยชน์ต่อนายทหารที่กำลังศึกษาในหลักสูตรต่าง ๆ และประชาชน ที่สนใจในเชิงวิชาการด้านการใช้เทคโนโลยีในการทำสงครามทางเรือในอนาคต และนำไปประยุกต์ใช้ได้ ทั้งนี้ หากมีความคิดเห็นรวมทั้งข้อเสนอแนะสามารถ ส่งได้ที่ nssc.journal@gmail.com หรือที่กองบรรณาธิการ ครับ

นาวาเอก กระแสร์ เม่งอำพัน
บรรณาธิการ

**DRONE WARFARE FROM THE
PAST TO THE FUTURE :
สงครามโดรนจากอดีตสู่อนาคต**

**นางสาวเอก นานี ฤทธิยวาทินญญ
ประจำกรมกำลังพลทหารเรือ**

“

การพัฒนาโทรคมนาคม
จะส่งผลกระทบต่อแนวทางการปฏิบัติการทางทหาร
ในอนาคตอย่างมาก

”

บทคัดย่อ

สามารถกล่าวได้ว่าโทรคมนาคมเกิดขึ้นมาตั้งแต่ยุคคริสต์ศตวรรษที่ ๑๙ ด้วยวัตถุประสงค์ที่จะสร้างรายได้เปรียบทางการและความปลอดภัยให้กับกำลังทหาร ด้วยการดำรงอยู่ของแนวความคิดดังกล่าว โทรคมนาคมจึงได้รับการพัฒนาให้มีขีดความสามารถที่สูงขึ้น จากที่เคยเป็นเพียงอาวุธบินเข้าทำลายเป้าหมายโดยตรง พัฒนาไปสู่การเป็นเป้าฝึกอาวุธ เป็นเครื่องมือหาข่าวในพื้นที่เสี่ยง มีขีดความสามารถด้านสงครามอิเล็กทรอนิกส์ จนกระทั่งสามารถโจมตีเป้าหมายได้เช่นเดียวกับอากาศยานที่มีนักบินควบคุม บทบาททั้งจากอดีตและปัจจุบันได้พิสูจน์ให้เห็นถึงศักยภาพของโทรคมนาคมต่อการทหาร จึงไม่ใช่เรื่องแปลกที่ทุกชาติจะเร่งการพัฒนาและวางแผนการใช้งานโทรคมนาคมที่เหมาะสมในอนาคต

บทนำ

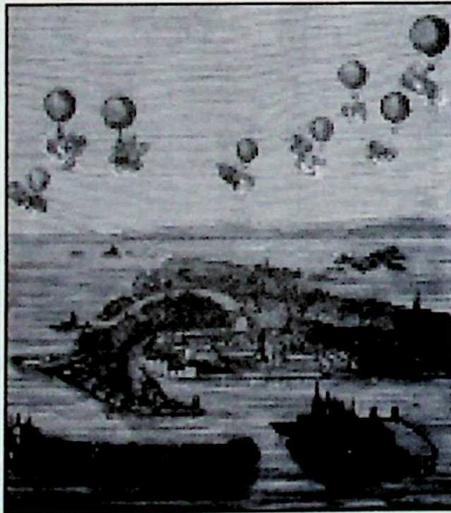
มีการพูดถึงโดรน (Drone) มากขึ้นอย่างต่อเนื่องในยุคปัจจุบัน ทั้งนี้ เนื่องจากการใช้งานโดรนในด้านต่าง ๆ มากมาย เช่น ด้านการขนส่ง ด้านการสำรวจ ด้านอุตสาหกรรมบันเทิง ด้านการแพทย์ ด้านการเกษตร ด้านการรักษากฎหมาย และโดยเฉพาะอย่างยิ่งด้านปฏิบัติการทางทหาร ซึ่งถือว่าเป็นการใช้งานด้านแรกที่มีผลกระตุ้นให้เกิดการพัฒนา และการใช้งานโดรนอย่างแพร่หลายในปัจจุบัน สำหรับบทความนี้จะได้กล่าวถึงนิยามของโดรน ซึ่งอาจมีใจความบางส่วนแตกต่างกันระหว่างคำนิยามทางการทหารและพลเรือน การกำเนิดและพัฒนาการของโดรน ตั้งแต่ยุคคริสต์ศตวรรษที่ ๑๙ จนถึงยุคคริสต์ศตวรรษที่ ๒๐ บทบาทที่สำคัญของโดรนในการปฏิบัติการทางทหาร ในปัจจุบัน การแบ่งประเภทและส่วนประกอบที่สำคัญของโดรน อากาศ และระบบต่อต้านโดรน ข้อดีและข้อเสียเมื่อเปรียบเทียบกับอากาศยานแบบมีนักบิน แนวโน้มการพัฒนาและใช้งานโดรน รวมไปถึงบทบาทของโดรนต่อกองทัพเรือในอนาคต

เมื่อกล่าวถึงความหมายของ “โดรน” โดยทั่วไปในปัจจุบันมักจะหมายถึงอากาศยานไร้คนขับ หรือ Unmanned Aerial Vehicle (UAV) ความหมายนี้สามารถเห็นได้จากคำนิยามตามพจนานุกรมที่ได้รับการยอมรับ เช่น Cambridge Dictionary ได้ให้ความหมายว่า โดรนเป็นอากาศยานที่ไม่มีนักบิน ถูกควบคุมด้วยคนที่ประจำอยู่ภาคพื้นและถูกใช้ทั้งระเบิดหรือลาดตระเวน^๑ Collins Dictionary ได้ให้ความหมายใกล้เคียงกันว่า โดรนเป็นอากาศยานที่ไม่มีนักบิน ถูกควบคุมโดยสัญญาณวิทยุ^๒ Oxford Dictionary ก็ได้ให้ความหมายไปในทางเดียวกันคือ โดรนเป็นอากาศยานไร้คนขับ สามารถควบคุมจากภาคพื้น ใช้งานเพื่อการถ่ายรูป การทิ้งระเบิด และการขนส่งของอย่างใดก็ตาม เมื่อดูคำนิยามของกระทรวงกลาโหมสหรัฐฯ ซึ่งเป็นหน่วยงานทางทหารที่มีการใช้งานโดรนมากที่สุดในปัจจุบัน ความหมายของโดรนจะครอบคลุมไปถึงยานอัตโนมัติทั้งทางบก ทางทะเล และทางอากาศ ที่ถูกบังคับจากระยะไกลหรือทำงานด้วยตัวเอง^๓ หมายความว่ากองทัพสหรัฐฯ เรียกยานไร้คนขับในทุกมิติว่าโดรน ยานไร้คนขับเหล่านี้ได้แก่ Unmanned Aerial Vehicle (UAV) Unmanned Ground Vehicle (UGV) Unmanned Surface

Vehicle (USV) และ Unmanned Underwater Vehicle (UUV) อย่างไรก็ตาม ด้วยข้อจำกัดในด้านเนื้อหา บทความนี้จะกล่าวถึงโดรนเฉพาะในมิติของ อากาศยานไร้คนขับ หรือ UAV เท่านั้น

๑. การกำเนิดของโดรน

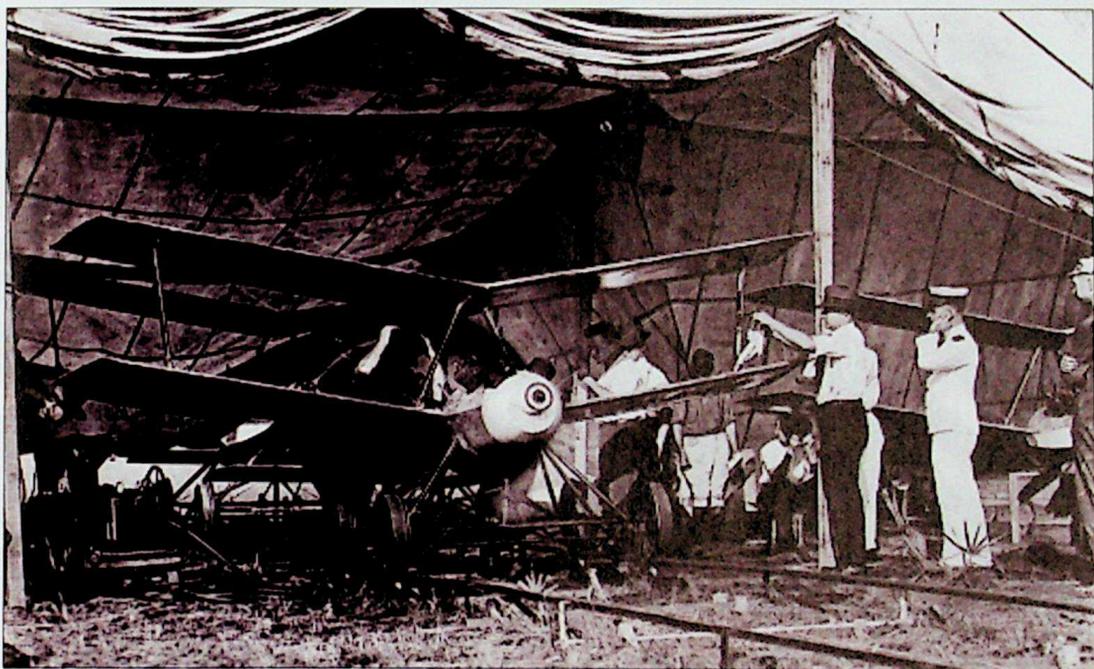
การใช้โดรนครั้งแรกในประวัติศาสตร์สามารถย้อนหลังไปได้ถึง เหตุการณ์ในปี ค.ศ.๑๘๔๙ ซึ่งเป็นการรบกันระหว่าง Austria และ Venice โดยฝ่าย Austria พยายามใช้กำลังเข้ายึดครองเมือง Venice ด้วยการโจมตี แบบต่าง ๆ แต่ไม่ประสบความสำเร็จ จึงมีความคิดที่จะใช้บอลลูนจำนวนกว่า ๒๐๐ ลูก ซึ่งไม่มีคนบังคับบรรทุกวัตถุระเบิดจำนวนประมาณ ๑๑ - ๑๔ กิโลกรัม ลอยตามลมไปจนถึงตำแหน่งที่วางแผนไว้ หลังจากนั้นกลไกอัตโนมัติจะปล่อย วัตถุระเบิดจากบอลลูนลงทำลายเป้าหมายที่อยู่ในเมืองด้านล่าง แต่ผลการโจมตี จากบอลลูนในครั้งนั้นไม่เป็นไปตามที่วางแผน มีการเปลี่ยนแปลงกระแสลม อย่างกะทันหันทำให้ท้ายที่สุดแล้ว มีบอลลูนเพียง ๑ ลูกเท่านั้น ที่สามารถ ปล่อยระเบิดลงสู่พื้นที่เป้าหมายได้ จากเหตุการณ์ดังกล่าวถึงแม้ว่าท้ายที่สุดแล้ว การใช้บอลลูนไร้คนบังคับของ Austria ไม่สามารถสร้างผลลัพธ์ตามที่ได้ วางแผนไว้ แต่ก็ถือว่าเป็นจุดเริ่มต้นของการใช้อากาศยานไร้คนขับ เพื่อการทหารในเวลาต่อมา



ภาพวาดบอลลูนติดระเบิดลอยบริเวณเมือง Venice ในปี ค.ศ.๑๘๔๙

๒. การพัฒนาโดรนในคริสต์ศตวรรษที่ ๒๐

ในช่วงสงครามโลกครั้งที่ ๑ เพื่อที่จะเอาชนะสงครามสนามเพลาะที่ต่างฝ่ายไม่สามารถรุกคืบเข้าหาอีกฝ่ายได้ และกินเวลายืดเยื้อกว่า ๔ ปี กระทั่งกลางโหมสหรัฐฯ จึงได้ผลักดันให้เกิดการพัฒนาโดรน ภายใต้โครงการ Kettering Bug^๖ โดยมีวัตถุประสงค์ที่จะสร้างอากาศยานไร้คนบินตามระยะทางและเวลาที่กำหนดเพื่อเข้าถึงตำบลเป้าหมาย หลังจากนั้นโดรนพร้อมด้วยวัตถุระเบิด จำนวน ๓๐๐ ปอนด์ จะพุ่งเข้าชนและระเบิดเป้าหมายที่สำคัญต่าง ๆ ของฝ่ายเยอรมัน Kettering Bug ได้ถูกนำไปทดลองบินครั้งแรกในช่วงปลายปี ค.ศ.๑๙๑๘ ซึ่งเป็นเวลาเพียง ๑ เดือน ก่อนการยอมจำนนของฝ่ายเยอรมัน จึงส่งผลให้ไม่ได้ถูกนำไปใช้ปฏิบัติการจริงตามที่ตั้งใจเอาไว้^๗ อย่างไรก็ตาม ผลของโครงการ Kettering Bug ได้สะท้อนให้เห็นแนวความคิดในการใช้โดรนเพื่อเปลี่ยนยุทธวิธีการรบ สร้างความได้เปรียบให้กับฝ่ายตนเอง และในขณะเดียวกันยังเป็นการลดความเสี่ยงการสูญเสียของกำลังพลด้วย



ภาพโดรน Kettering Bug^๖

ที่มา : <https://www.tatreviewmagazine.com/article/game-of-drone/>

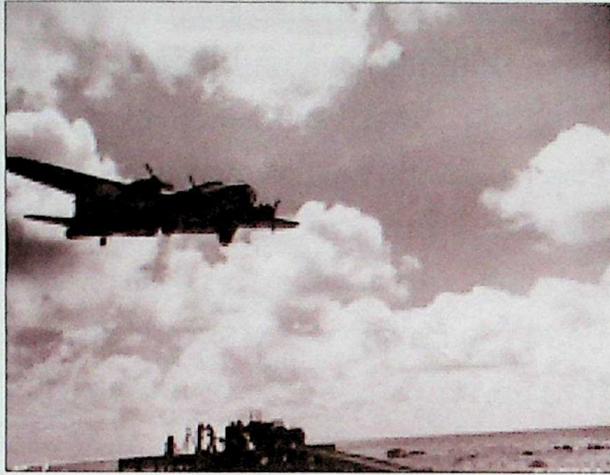
หลังจากสงครามโลกครั้งที่ ๑ ความพยายามในการพัฒนาโดรน เพื่อใช้ในการทหารยังคงมีอยู่อย่างต่อเนื่อง ในปี ค.ศ.๑๙๓๕ กองทัพอังกฤษ ได้พัฒนาโดรนบังคับด้วยคลื่นวิทยุ ชื่อ Queen Bee เพื่อใช้เป็นเป้าสำหรับการฝึกใช้อาวุธต่อต้านอากาศยาน โดรนดังกล่าวมีขนาดเท่ากับอากาศยานทั่วไป ส่วนประกอบบางส่วนของ Queen Bee ทำจากผ้าและไม้ ซึ่งทำให้โดรนมีราคาถูกและหากไม่ถูกทำลายด้วยอาวุธที่ถูกใช้ฝึก โดรนดังกล่าวยังสามารถถูกนำกลับมาใช้งานได้อีก^๑ ในช่วงเวลาเดียวกันบริษัทเอกชนชื่อ Radioplane Company ในสหรัฐฯ ได้สร้างโดรนขนาดเล็กที่มีชื่อว่า Raidoplane OQ ให้กับกองทัพบกและกองทัพเรือของสหรัฐฯ เพื่อใช้เป็นเป้าฝึกอาวุธ โดรนดังกล่าวถูกสร้างขึ้นถึงเกือบ ๑,๐๐๐ ลำ ภายหลังจากที่สหรัฐฯ เข้าสู่สงครามโลกครั้งที่ ๒^{๑๐}



ภาพโดรน Radioplane OQ-2 (TDD) ถูกปล่อยจากเรือ USS New York ในปี ค.ศ.๑๙๔๓ เพื่อใช้เป็นเป้าซ้อมการฝึกใช้อาวุธบนเรือ^{๑๑}

ในช่วงสงครามโลกครั้งที่ ๒ ความพยายามสร้างความได้เปรียบในสงคราม และลดการเสียชีวิตของนักบินยังคงผลักดันให้ชาติต่าง ๆ เดินหน้าโครงการพัฒนาโดรน ตัวอย่างเช่น ในช่วงปี ค.ศ.๑๙๔๒ สหรัฐฯ ได้ปรับปรุงโดรนจากโครงการ Kettering Bug เพิ่มขีดความสามารถด้านต่าง ๆ ได้แก่ ความเร็ว จากเดิม ๕๐ ไมล์ต่อชั่วโมง เป็น ๒๐๐ ไมล์ต่อชั่วโมง ระยะเวลาปฏิบัติการจากเดิม ๔๐๐ ไมล์เป็น ๑,๐๐๐ ไมล์ความสามารถในการบรรทุกระเบิดจากเดิม ๓๐๐ ปอนด์ เป็น ๒,๐๐๐ ปอนด์^{๑๖} อย่างไรก็ตาม โดรนดังกล่าวยังมีข้อจำกัดหลายจุดในการนำไปปฏิบัติงานจริง ได้แก่ ระบบนำร่องอัตโนมัติยังไม่มีคามแม่นยำเพียงพอต่อการทำลายเป้าหมายและไม่สร้างความเสียหายต่อประชาชนที่ไม่เกี่ยวข้องกับสงคราม การบินขึ้นของโดรนยังต้องใช้เครื่องดีดตัว ซึ่งทำให้เกิดข้อจำกัดในการปฏิบัติการจากพื้นที่ส่วนหน้า ระยะทางที่ได้รับการปรับปรุงเพิ่มขึ้นยังไม่สามารถครอบคลุมพื้นที่เป้าหมายการโจมตีทางอากาศต่าง ๆ ในเยอรมันได้ และประสิทธิภาพของเครื่องทิ้งระเบิดก็ยังไม่สามารถชดเชยการทำงานของเครื่องบินทิ้งระเบิดแบบปกติ ดังนั้น โดรนที่กล่าวถึงจึงไม่ได้ถูกนำมาใช้งานจริงในช่วงสงครามโลกครั้งที่ ๒

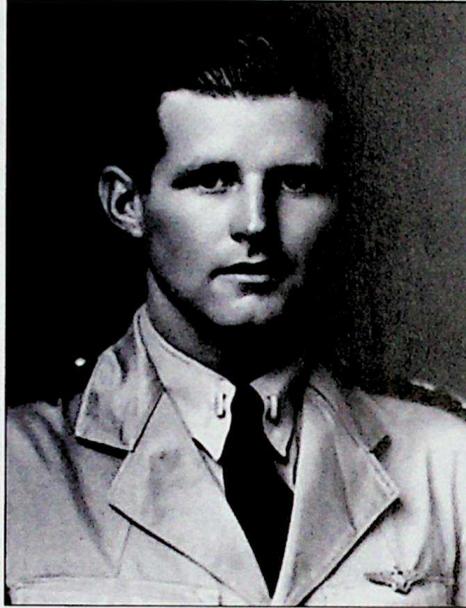
โครงการพัฒนาโดรนชื่อ Aphrodite และ Anvil ของกองทัพบก และกองทัพเรือสหรัฐฯ ในช่วงปี ค.ศ.๑๙๔๔ เป็นอีกตัวอย่างของความพยายามนำโดรนมาสร้างความได้เปรียบ และลดการเสียชีวิตของนักบินในช่วงสงครามโลกครั้งที่ ๒ โครงการโดรนดังกล่าวเป็นการนำเอาเครื่องบินทิ้งระเบิดที่ถูกปลดประจำการแล้ว เช่น B-17 และ B-24 ของกองทัพบก และ PB4Y-1 ของกองทัพเรือ มาเปลี่ยนสภาพจากอากาศยานธรรมดาเป็นโดรนด้วยการนำเกราะ อาวุธ และอุปกรณ์ภายในที่ไม่จำเป็นต่อการบินออก แล้วแทนที่ด้วยระบบควบคุมพร้อมวัตถุระเบิด จากหลักการนี้โดรนสามารถปฏิบัติการได้ไกลเหมือนเครื่องบินทั่วไป อีกทั้งยังสามารถบรรทุกระเบิดได้ถึง ๑๔,๐๐๐ - ๑๘,๕๐๐ ปอนด์ ซึ่งเป็นจำนวนมากถึง ๒ เท่าของอัตราการบรรทุกปกติของเครื่องบินทิ้งระเบิดบังคับด้วยนักบิน โดรนเหล่านี้ถูกเรียกว่า Weary Willies^{๑๗} การทำงานของ Weary Willies จะเริ่มต้นด้วยการใช้นักบินควบคุมในช่วงการบินขึ้นเหมือนอากาศยานทั่วไป หลังจากสามารถทำความสูงที่ ๒,๐๐๐ ฟุต นักบินจะกระโดดร่มออกจากตัวอากาศยานดังกล่าว การควบคุมโดรนชนิดนี้ในเวลา



ภาพโดรน Weary Willies ขณะขึ้นบินจากเรือบรรทุกเครื่องบิน^{๑๖}

ที่เหลือจะถูกกระทำผ่านอากาศยานแม่ซึ่งบินตามอยู่ด้านหลัง อากาศยานแม่จะบังคับโดรนด้วยสัญญาณวิทยุเข้าชนและระเบิดเป้าหมาย การทำงานของ Weary Willies จึงมีความคล้ายคลึงกับเครื่องบิน Kamikaze ของญี่ปุ่น หากแต่มีความได้เปรียบอย่างมากตรงที่ไม่ต้องสละชีวิตนักบินอันสำคัญยิ่งเพื่อทำลายเป้าหมาย อย่างไรก็ตาม Weary Willies ก็ยังคงมีข้อจำกัดหลายประการ เมื่อเปรียบเทียบกับอากาศยานที่มีนักบินควบคุมในสมัยนั้น ประการแรก การถูกควบคุมด้วยสัญญาณวิทยุจากเครื่องบินที่ตามมาด้านหลังทำให้การเคลื่อนไหวเพื่อหลบเลี่ยงการโจมตีจากเครื่องบินข้าศึกเป็นไปได้อย่างจำกัด ประการที่สอง Weary Willies ไม่มีเกราะป้องกันเหมือนเครื่องบินทั่วไปซึ่งทำให้สามารถถูกทำลายได้อย่างง่ายดายตายก่อนจะสามารถเข้าชนเป้าหมาย และ ประการที่สาม ถึงแม้จะใช้ นักบินเพียงขั้นตอนการนำโดรนขึ้นเท่านั้น แต่ก็ยังคงสร้างความเสี่ยงให้เกิดขึ้น เช่น ในการปฏิบัติครั้งหนึ่งของกองทัพเรือ โดรนเกิดการระเบิดขึ้นในขณะที่นักบินที่ชื่อ เรือเอก Joseph P. Kennedy Jr ซึ่งเป็นพี่ชายของประธานาธิบดี John F. Kennedy ยังคงบังคับเครื่องในขณะที่บินขึ้น ทำให้นักบินดังกล่าวเสียชีวิต โดยสาเหตุการระเบิดที่เกิดขึ้นก่อนเวลาถึงเป้าหมายในครั้งนี้น่าจะมาจากความบกพร่องของกลไกการตั้งเวลาระเบิด^{๑๗} จากข้อจำกัดต่าง ๆ ที่ได้กล่าวในเบื้องต้น ทำให้โดรนในโครงการนี้ไม่ประสบ

ความสำเร็จในการทำลายเป้าหมาย อากาศยานหลายลำเสียการควบคุมจาก ยานแม่ หลายลำถูกยิงตกก่อนเข้าถึงเป้าหมาย มีเพียงไม่กี่ลำที่สามารถระเบิด ใกล้กับเป้าหมาย โดยอากาศยานในโครงการมีโอกาสออกปฏิบัติการทั้งหมด ๑๙ ครั้ง ตั้งแต่ปลายปี ค.ศ.๑๙๔๔ จนถึงช่วงต้นปี ค.ศ.๑๙๔๕ ที่โครงการถูก ยกเลิก^{๑๕}



ภาพ เรือเอก Joseph P.Kennedy Jr^{๑๖}

ที่มา : <https://www.nps.gov/articles/000/joseph-patrick-kennedy-jr-a-dream-unfulfilled.htm>

ยุคสงครามเย็นถือเป็นช่วงเวลาที่สำคัญยิ่งสำหรับการพัฒนาโดรน เพื่อปฏิบัติการทางทหาร อากาศยานสอดแนมของสหรัฐฯ ถูกยิงตกสร้างความ สูญเสียกำลังพลในหลายเหตุการณ์ เช่น เหตุการณ์ เครื่องบิน U-2 ถูกยิงตก ในเหนือน่านฟ้าสหภาพโซเวียต ในปี ค.ศ.๑๙๖๐ เครื่องบิน U-2 ถูกยิงตกอีกครั้ง เหนือน่านฟ้าคิวบา ในปี ค.ศ.๑๙๖๒ และเครื่องบิน Lockheed EC-121M Warning Star ถูกยิงตกด้วยเครื่องบิน MiG-21 ของเกาหลีเหนือ บริเวณ ทะเลญี่ปุ่น ในปี ค.ศ.๑๙๖๙ โดยรวมแล้วสหรัฐฯ สูญเสียเครื่องบินกว่า ๒๐ ลำ นักบินเสียชีวิตเกือบ ๒๐๐ คน เหตุการณ์การสูญเสียนักบินและกำลังพล บนเครื่องบินเหล่านี้สร้างความไม่พอใจให้กับประชาชน รวมทั้งความยาก ลำบากในการดำเนินนโยบายต่างประเทศเป็นอย่างยิ่ง ความพยายามหลีกเลี่ยง

ความสูญเสียกำลังพลจึงเป็นแรงผลักดันสำคัญให้เกิดโครงการพัฒนาโดรน เพื่อใช้ในการปฏิบัติการทางทหาร เน้นภารกิจการหาข่าวในพื้นที่ที่มีอันตรายสูง โครงการพัฒนาที่ประสบความสำเร็จในช่วงเวลานั้น ได้แก่ โครงการ Lighting Bug ซึ่งเริ่มต้นในปี ค.ศ.๑๙๖๒ ได้ผลิต Ryan Model 147 รุ่นต่าง ๆ ออกมาปฏิบัติการ ในพื้นที่ต่าง ๆ โดยเฉพาะในเอเชียตะวันออกเฉียงใต้

โดรนแบบ Ryan Model 147 เป็นโดรนที่ขับเคลื่อนด้วยเครื่องยนต์เจ็ท สามารถถูกควบคุมระยะไกลหรือโปรแกรมให้บินด้วยระบบอัตโนมัติ ขึ้นบินได้จากพื้นดินหรือถูกปล่อยจากอากาศยานลำอื่น ใช้การลงสู่พื้นเมื่อเสร็จสิ้นภารกิจ มีขีดความสามารถในการถ่ายภาพ ทั้งในเขตแดนบินระดับต่ำและสูง ทำสงครามอิเล็กทรอนิกส์ทำหน้าที่เป็นเป้าลวงการโจมตี รวบรวมข้อมูลทางอิเล็กทรอนิกส์ ปฏิบัติการด้านจิตวิทยา และลาดตระเวนเผ่าตรวจพื้นที่ โดยตั้งแต่ปี ค.ศ.๑๙๖๔ ถึง ๑๙๗๕ โดรนในโครงการนี้ผลิตออกมาเพื่อปฏิบัติการกิจในพื้นที่ภูมิภาค เอเชียตะวันออกเฉียงใต้ ช่วงสงครามเวียดนาม ถึงกว่า ๓,๔๓๕ เทียวบิน^{๑๓} อย่างไรก็ตาม โดรน Ryan Model 147 ยังมีข้อจำกัดในเรื่องของการถ่ายภาพ ที่ยังไม่คมชัด ไม่สามารถให้รายละเอียดได้เท่ากับเครื่องบินสอดแนมแบบมีนักบิน การลงสู่พื้นด้วยร่มที่มักทำให้เกิดความเสียหายกับตัวโดรนและอุปกรณ์เก็บข้อมูล ราคาในการผลิตและบำรุงรักษาที่ยังสูง อีกทั้งทัศนคติของทหารในระดับต่าง ๆ ที่ยังเชื่อมั่นต่อประสิทธิภาพของอากาศยานแบบมีนักบินควบคุมมากกว่าโดรน



ภาพ Ryan Model 147 Lightning Bug ถูกปล่อยจากเรือ USS Ranger^{๑๓}

ในช่วงสงครามเย็นนั้น การพัฒนาโดรนไม่ได้ถูกจำกัดแค่ในสหรัฐฯ หากแต่หลายชาติก็ได้ให้ความสนใจในการพัฒนาด้านนี้ ดังเช่น อิสราเอล ที่ได้พัฒนาโดรน ที่ชื่อ IAI Scout ในช่วงคริสต์ทศวรรษที่ ๑๙๗๐ โดยนำไปใช้ลาดตระเวนหาข่าว ทำสงครามอิเล็กทรอนิกส์ และถ่ายทอดภาพสถานการณ์ในสนามรบได้อย่างมีประสิทธิภาพ จนอิสราเอลมีชัยชนะในสงครามเลบานอน รวมถึงไปถึงการเผชิญหน้ากับซีเรีย ในช่วงปี ค.ศ.๑๙๘๒ ความสำเร็จของอิสราเอล ในครั้งนี้ได้กระตุ้นให้สหรัฐฯ ร่วมกับอิสราเอลเร่งการพัฒนาโดรนเพื่อการทหาร ซึ่งก็ได้นำไปสู่การผลิตโดรนที่ชื่อว่า RQ-2 Pioneer ถูกใช้สำหรับลาดตระเวนหาข่าว ฝ้าตรวจ ถ่ายทอดภาพสถานการณ์ ค้นหา และชี้เป้าให้กับอาวุธ โดยประจำการในกองทัพบก กองทัพเรือ และหน่วยนาวิกโยธินของสหรัฐฯ ในช่วงปี ค.ศ.๑๙๘๖ - ๒๐๐๗ โดรนดังกล่าวสามารถบินขึ้นจากสนามบิน ดาดฟ้าเรือ (ติดตั้งจรวดขับดัน) และเครื่องติดตัว โดรนแบบ RQ-2 Pioneer สามารถปฏิบัติการได้ทั้งเวลากลางวันและกลางคืน ด้วยการติดตั้งอุปกรณ์ตรวจจับ Electro-Optical (EO)/Infrared (IR) มีพิสัยการบิน ๑๘๕ กิโลเมตร โดรนแบบ RQ-2 Pioneer ได้ปฏิบัติหน้าที่ในภารกิจจำนวนมากในหลายพื้นที่ เช่น สงครามอ่าว Persian Gulf การปฏิบัติการเพื่อสันติภาพในโซมาเลีย (UNOSOM II) การปฏิบัติการในบอสเนีย โคโซโว และอิรัก



ภาพขั้นตอนการลงสู่พื้นของ RQ-2 Pioneer บนเรือ USS Iowa ในปี ค.ศ.๑๙๘๖ ^{๒๐}

การพัฒนาโดรนของสหรัฐฯ ยังเกิดขึ้นอย่างต่อเนื่อง ในต้นคริสต์ทศวรรษ
ที่ ๑๙๙๐ อากาศยานที่มีชื่อว่า MQ-1 Predator ได้ถูกสร้างขึ้นเพื่อวัตถุประสงค์
คล้ายคลึงกับ RQ-2 Pioneer หากแต่ต่อมาได้รับการพัฒนาให้สามารถใช้อาวุธ
AGM-114 Hellfire missiles ทำลายเป้าหมายได้ นอกจากนั้นยังติดตั้งอุปกรณ์
ตรวจจับหลายประเภท ได้แก่ กล้องโทรทัศน์ (Digital Video Camera) และ
กล้องถ่ายภาพความร้อน (Thermal Imaging System: TIS) และเรดาร์
(Synthetic Aperture Radar) ที่สามารถทำให้ตรวจจับเป้าหมายผ่านเมฆ หมอก
และควัน โดรนชนิดนี้มีพิสัยการบิน ๗๔๐ กิโลเมตร ปฏิบัติการได้ต่อเนื่อง
ถึง ๑๔ ชั่วโมง ในช่วงแรกต้องควบคุมการบินเครื่องโดยชุดควบคุมในระยะใกล้
กับโดรนที่บินขึ้น ต่อมาได้รับการเพิ่มประสิทธิภาพให้สามารถควบคุมการบิน
ขึ้นลงและปฏิบัติการทั้งหมดจากฐานควบคุมซึ่งอาจอยู่ไกลจากโดรนผ่านระบบ
ดาวเทียม หลังจากเข้าประจำการในปี ค.ศ. ๑๙๙๕ จนถึงปัจจุบัน MQ-1 Predator
ถูกใช้ในภารกิจจำนวนมากในหลายพื้นที่ เช่น การปฏิบัติการในบอสเนีย
ยูโกสลาเวีย และเป็นเครื่องมือสำคัญสำหรับสงครามต่อต้านการก่อการร้าย
(War on Terror) หลังเหตุการณ์ 9/11 โดยปฏิบัติงานในพื้นที่ อัฟกานิสถาน
ปากีสถาน อิรัก เยเมน ลิเบีย ซีเรีย และโซมาเลีย นอกจากประจำการในกองทัพ
สหรัฐฯ อากาศยานประเภทนี้ยังใช้ในหน่วยงานภาครัฐอื่น ๆ เพื่อบังคับ
ใช้กฎหมายตามแนวชายแดน บรรเทาภัยพิบัติทางธรรมชาติ ฝ้าตรวจสอบสภาพ
อากาศ และงานวิจัยทางวิทยาศาสตร์



ภาพ MQ-1 Predator ปฏิบัติการทางยุทธวิธีโดยการควบคุมจากเรือบรรทุกเครื่องบิน
USS Carl Vinson

๓. การพัฒนาโดรนในปัจจุบัน

การพัฒนาโดรนหลังปี ค.ศ.๒๐๐๐ มีมากขึ้นอย่างต่อเนื่อง หลายชาติให้ความสนใจในการพัฒนาและสร้างโดรนเพื่อกิจการทางการทหาร ดังจะเห็นจากโดรนที่ถูกเพิ่มขีดความสามารถในการโจมตีเป้าหมายด้วยตัวเอง และการออกแบบที่ทำให้สามารถลดการถูกตรวจจับจากเรดาร์ ตัวอย่างเช่น Bayraktar TAI Aksungur ของตุรกี Sukhoi S-70 ของรัสเซีย Hongdu GJ-11 ของจีน EADS Barracuda ของเยอรมัน และสเปน BAE Systems Taranis ของอังกฤษ และ MQ-9 Reaper (Predator B) ของสหรัฐฯ โดย MQ-9 Reaper นั้น เป็นโดรนที่ปัจจุบันมีบทบาทสำคัญในการปฏิบัติการทางการทหารในพื้นที่ตะวันออกกลาง MQ-9 Reaper เป็นโดรนที่ถูกพัฒนาต่อเนื่องจากโครงการ Predator ในคริสต์ทศวรรษที่ ๑๙๙๐ ด้วยวัตถุประสงค์สำหรับเป็นอากาศยานที่สามารถใช้อาวุธทำลายเป้าหมายได้อย่างแม่นยำ โดรนชนิดนี้มีอุปกรณ์ตรวจจับที่ทันสมัยหลายชนิด เช่น ระบบเซ็นเซอร์อินฟราเรด กล้องถ่ายภาพสีและขาวดำ และเครื่องค้นหาระยะเลเซอร์ รวมทั้งอุปกรณ์การกำหนดเป้าหมายสำหรับการโจมตีที่มีความแม่นยำสูง Reaper ยังสามารถติดตั้งอาวุธได้ถึง ๗ จุด ซึ่งรองรับอาวุธปล่อยนำวิถีอากาศสู่พื้น AGM-144 Hellfire อาวุธปล่อยนำวิถีอากาศสู่อากาศ AIM-92 Stinger ระเบิดนำวิถีด้วยเลเซอร์ GBU-12 Paveway II และ GBU-38 Jdam อากาศยานดังกล่าวมีระยะปฏิบัติการไกลถึงกว่า ๑,๘๕๐ กิโลเมตร ปฏิบัติการได้ต่อเนื่องกว่า ๓๐ ชั่วโมง นับตั้งแต่ปี ค.ศ.๒๐๐๗ Reaper ได้ปฏิบัติการในพื้นที่ต่าง ๆ เช่น อัฟกานิสถาน อิรัก เยเมน และลิเบีย โดยประสิทธิภาพและความสำเร็จในปฏิบัติการที่ผ่านมา MQ-9 Reaper ได้ถูกนำเข้าประจำการในหน่วยงานภาครัฐอื่น ๆ เช่น U.S. Customs and Border Protection และกองทัพของหลายชาติ



ภาพ MQ-9 Reaper ขณะใช้อาวุธ^{๒๒}

ที่มา : <https://twitter.com/Amitraaz/status/1282683866583449602/photo/1>

Russia's Okhotnik stealth drone

The Sukhoi S-70 Okhotnik (Hunter) is Russia's first heavy unmanned aerial vehicle (UAV), designed to perform reconnaissance and strike missions using high speed and fully autonomous flight

SUKHOI S-70 OKHOTNIK-B (HUNTER-B)

Airframe: Reportedly made of composite materials and treated with radiation-absorbent (stealth) coating

Dorsal-mounted engine air intake

Powerplant: Single turbofan, likely AL-31/41 series

Weapons bay

SPECIFICATIONS (estimated)

Wingspan 19 metres

Take-off weight 20 tonnes

Maximum speed 1,000km/h

Range 4,000km

Payload Up to two tonnes

Armament

Air to surface missiles and array of bombs carried inside ventral bay or bays to reduce drone's visibility on enemy radar

"Fully robotized" vehicle capable of making independent combat decisions – only requiring human operator to deploy weapons

Flat "flying wing" design similar to U.S. Air Force's B-2 stealth bomber

Possible hypersonic weapon

Weapons bays: Should be able to carry most, if not all, missiles and munitions being developed for Russia's Su-57 multirole aircraft, including hypersonic missile with characteristics similar to Kh-47M2 Kinzhal

ภาพโดรน ชื่อ Sukhoi S-70 Okhotnik ของรัสเซีย^{๒๓}

ที่มา : <https://www.graphicnews.com/en/pages/39179/military-russian-s-70-stealth-drone>

๔. การแบ่งประเภทของโดรน

การแบ่งประเภทของโดรนสามารถกระทำได้หลายแบบขึ้นอยู่กับ ขนาด ลักษณะขีดความสามารถ และวัตถุประสงค์การใช้งาน โดยตัวอย่างการแบ่งประเภทของโดรน มีรายละเอียดดังนี้

๔.๑ การแบ่งตามขนาดของโดรน สามารถแบ่งได้ ๔ ขนาด ดังนี้

๔.๑.๑ ขนาดจิ๋ว (Micro) เป็นโดรนที่มีน้ำหนักน้อยกว่า ๑๑ ปอนด์

๔.๑.๒ ขนาดเล็ก (Small) เป็นโดรนที่มีน้ำหนักน้อยกว่า ๕๐๐ ปอนด์

๔.๑.๓ ขนาดกลาง (Medium) เป็นโดรนที่มีน้ำหนักระหว่าง ๕๐๐ ปอนด์ ถึง ๑,๕๐๐ ปอนด์

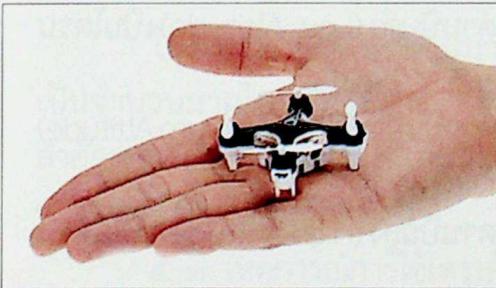
๔.๑.๔ ขนาดใหญ่ (Large) เป็นโดรนที่มีน้ำหนักมากกว่า ๑,๕๐๐ ปอนด์

๔.๒ การแบ่งประเภทตามลักษณะของโดรน สามารถแบ่งได้ ๓ ประเภท ดังนี้

๔.๒.๑ ประเภทปีกติดลำตัว (Fixed Wing) เป็นโดรนที่ใช้ปีก ในการสร้างแรงยกตัวและขับเคลื่อน

๔.๒.๒ ประเภทปีกหมุน (Rotary Wing or Helicopter) เป็นโดรน ที่ใช้การหมุนใบพัด (Rotor) เพื่อกำเนิดทั้งแรงยกตัวและแรงขับเคลื่อน

๔.๒.๓ ประเภทผสม (Tilt Rotor or Shrouded Rotor) เป็นโดรน ที่มีลักษณะผสมของเครื่องบินและเฮลิคอปเตอร์ เพื่อขจัดข้อจำกัดต่าง ๆ ของทั้งแบบปีกติดลำตัวและแบบปีกหมุน



ภาพโดรนขนาดเล็ก

ที่มา : <https://www.sanook.com/men/11693/>



ภาพโดรนปีกหมุน (และโดรนต้นแบบ ชื่อ VSR700 VTOL ของฝรั่งเศส)

ที่มา : <https://www.navalnews.com/>

๔.๓ การแบ่งประเภทตามขีดความสามารถ อาจสามารถแบ่งย่อยได้ ตามพิสัยการบิน (Endurance) รัศมีปฏิบัติการ (Mission Radius or Range) และเพดานความสูงในการบิน (Altitude) ดังนี้

๔.๓.๑ การแบ่งประเภทตามพิสัยบิน สามารถแบ่งได้ ๓ ประเภท คือ

๔.๓.๑.๑ ประเภทพิสัยสั้น (Short Endurance) เป็นโดรน ที่มีพิสัยบินน้อยกว่า ๔ ชม.

๔.๓.๑.๒ ประเภทพิสัยปานกลาง (Medium Endurance) เป็นโดรนที่มีพิสัยบินระหว่าง ๖ ชม. ถึง ๑๐ ชม.

๔.๓.๑.๓ ประเภทพิสัยนาน (Long Endurance) เป็นโดรนที่มีพิสัยบินเกินกว่า ๒๔ ชม.

๔.๓.๒ การแบ่งประเภทตามรัศมีปฏิบัติการ สามารถแบ่งได้ ๓ ประเภท คือ

๔.๓.๒.๑ ประเภทรัศมีปฏิบัติการใกล้ (Short Mission Radius or Range) เป็นโดรนที่มีรัศมีทำการไม่เกิน ๗๐ กิโลเมตร

๔.๓.๒.๒ ประเภทรัศมีปฏิบัติการปานกลาง (Medium Mission Radius or Range) เป็นโดรนที่มีรัศมีทำการระหว่าง ๗๐ - ๕๐๐ กิโลเมตร

๔.๓.๒.๓ ประเภทรัศมีปฏิบัติการไกล (Long Mission Radius or Range) เป็นโดรนที่มีรัศมีทำการเกิน ๑,๐๐๐ กิโลเมตร

๔.๓.๓ การแบ่งประเภทตามเพดานความสูงในการบิน สามารถแบ่งได้ ๓ ประเภท คือ

๔.๓.๓.๑ ประเภทเพดานบินต่ำ (Low Altitude) เป็นโดรนที่เพดานบินไม่เกิน ๓,๐๐๐ ฟุต

๔.๓.๓.๒ ประเภทเพดานบินปานกลาง (Medium Altitude) เป็นโดรนที่เพดานบินระหว่าง ๓,๐๐๐ - ๒๐,๐๐๐ ฟุต

๔.๓.๓.๓ ประเภทเพดานบินสูง (High Altitude) เป็นโดรนที่เพดานบินเกิน ๒๐,๐๐๐ ฟุต

๔.๔ การแบ่งประเภทตามวัตถุประสงค์ทางการทหาร เพื่อความสะดวก อาจสามารถแบ่งออกเป็น ๒ ประเภทหลัก ดังนี้

๔.๔.๑ ประเภทติดอาวุธ (Lethal) หรืออาจถูกเรียกว่า UCAV (Unmanned Combat Aerial Vehicle) เป็น UAV ที่สร้างขึ้นให้สามารถติดตั้งอาวุธประเภทต่าง ๆ และใช้อาวุธต่อเป้าหมายที่ได้รับมอบ

๔.๔.๒ ประเภทไม่ติดอาวุธ (Non-Lethal) เป็น UAV ที่สร้างขึ้นโดยมีวัตถุประสงค์หลักอื่น ๆ เช่น เป็นเป้าลวงการโจมตีหรือซุ่มใช้อาวุธสนับสนุนการลาดตระเวนหาข่าวและเฝ้าตรวจในพื้นที่ ถ่ายทอดสัญญาณการสื่อสาร สงครามอิเล็กทรอนิกส์ สนับสนุนการวิจัยและพัฒนา และส่งกำลังบำรุง เป็นต้น



ภาพโดรนกำลังขนอาหารให้กับกำลังพลของจีนในทิเบต
ซึ่งอยู่สูงกว่าระดับน้ำทะเลถึง ๔,๕๐๐ เมตร^{๒๖}

๕. บทบาทที่สำคัญของโดรนในปัจจุบัน

ในช่วงเวลา ๓ ปีที่ผ่านมา มีการใช้งานโดรนในปฏิบัติการทางทหารเป็นจำนวนมากในภูมิภาคต่าง ๆ ของโลก ในจำนวนนี้มี ๓ ตัวอย่างเหตุการณ์สำคัญของโลก ซึ่งสะท้อนให้เห็นถึงขีดความสามารถของโดรนในการปฏิบัติการทางทหาร มีรายละเอียดดังนี้

๕.๑ เหตุการณ์การใช้โดรนโจมตีโรงกลั่นน้ำมัน ๒ แห่ง ในเมืองอัชคาอิก และคูราฮิส ประเทศซาอุดีอาระเบีย เมื่อ ๑๔ ก.ย.๑๙ โดยกลุ่มกบฏฮูตี ในเยเมนได้อ้างความรับผิดชอบในการส่งโดรนจำนวนหลายลำเข้าโจมตีโรงกลั่นน้ำมันดังกล่าว^{๒๗} โดรนสามารถรุดพ้นการตรวจจับของระบบป้องกันภัยทางอากาศของกองทัพซาอุดีอาระเบียได้ เนื่องจากมีขนาดเล็กและเพดานบินต่ำแตกต่างจากอากาศยานรบที่มีนักบิน ความเสียหายครั้งนี้ส่งผลให้ทางการซาอุดีอาระเบียต้องใช้จ่ายเงินหลายร้อยล้านในการซ่อมแซมโรงกลั่น กำลังการผลิตของประเทศลดลงประมาณครึ่งหนึ่งของปกติ กระทบต่อกำลังการผลิตของโลกประมาณ ๕% ทำให้ราคาน้ำมันโลกดีดตัวสูงขึ้นอย่างรวดเร็ว หลังจากเหตุการณ์โจมตีในครั้งนี้สะท้อนให้เห็นความสามารถของโดรนในการหลบหลีกการตรวจจับของระบบป้องกันภัยทางอากาศ รวมทั้งความเสียหายอันมหาศาลทางเศรษฐกิจ ซึ่งเป็นผลมาจากการโจมตีครั้งนี้^{๒๘}

๕.๒ เหตุการณ์การลอบสังหาร พลตรี คาเซม โซเลมานี ผู้บัญชาการกองกำลังคุดส์ (Quds Forces) ซึ่งเป็นส่วนหนึ่งของกองกำลังพิทักษ์การปฏิวัติอิสลามอิหร่าน เมื่อ ๓ ม.ค.๒๐ โดยสหรัฐฯ ยืนยันว่า การปฏิบัติการครั้งนี้กระทำโดยการใช้โดรนติดอาวุธ MQ-9 Reaper เพียง ๑ ลำ โจมตีขบวนรถของ พลตรี คาเซม ขณะเดินทางใกล้กับสนามบินนานาชาติแบกแดด การโจมตีครั้งนี้ ยังทำให้ อาบู มาร์ที อัล มุฮันดิส รองผู้บัญชาการกองกำลังฮัซด์ของอิรัก ซึ่งมีความใกล้ชิดกับรัฐบาลอิหร่านเสียชีวิตด้วย เหตุการณ์นี้ชี้ให้เห็นศักยภาพของโดรนในการโจมตีเป้าหมายบุคคลสำคัญ ซึ่งน่าจะได้รับการรักษาความปลอดภัยและคุ้มกันแน่นหนา^{๒๔}

๕.๓ เหตุการณ์การต่อสู้ระหว่างอาร์เมเนียกับอาเซอร์ไบจานจากประเด็นความขัดแย้งในพื้นที่นากอร์โน-คาราบัค ในช่วงเดือนกันยายน ปี ค.ศ.๒๐๒๐ โดยอาเซอร์ไบจานได้ประยุกต์ใช้โดรนที่จัดหาจากประเทศอิสราเอลและตุรกีในการลาดตระเวนหาข่าว ตรวจการณ์ การรวบรวมข้อมูลและภาพสถานการณ์ รวมถึงโจมตีเป้าหมายกำลังของฝ่ายอาร์เมเนีย ส่งผลให้ท้ายที่สุดฝ่ายอาเซอร์ไบจานได้รับชัยชนะ โดยประธานาธิบดีอาเซอร์ไบจานได้กล่าวว่า การปฏิบัติของโดรนเพียงอย่างเดียวสามารถทำลายยุทธโศภกรณ์ของฝ่ายอาร์เมเนีย รวมมูลค่ากว่า ๑ พันล้านเหรียญสหรัฐฯ โดยโดรน Bayraktar TB2 ของตุรกีมีบทบาทอย่างมากในการใช้อาวุธโจมตีเป้าหมายต่าง ๆ ในการปะทะกันครั้งนี้ เหตุการณ์ครั้งนี้แสดงให้เห็นบทบาทที่สำคัญของโดรนต่อการใช้กำลังทางทหารปะทะกันอย่างเต็มรูปแบบ

๖. การพัฒนาโดรนในอนาคต

จากการที่กองทัพต่าง ๆ ทั่วโลกได้เห็นถึงขีดความสามารถและความสำเร็จของการใช้งานโดรนจากเหตุการณ์ต่าง ๆ ตั้งแต่อดีตถึงปัจจุบัน การพัฒนาโดรนเพื่อการทหารจะเพิ่มขึ้นและแพร่หลายไปทุก ๆ ที่ แนวทางการพัฒนาจะเป็นการเพิ่มศักยภาพให้ดีกว่าอากาศยานที่มีใช้อยู่ในปัจจุบันซึ่งครอบคลุมหัวข้อดังต่อไปนี้

๖.๑ พัฒนาความแม่นยำในการใช้อาวุธ รวมทั้งระบบยืนยันและระบบชี้เป้าหมาย เพื่อขจัดข้อกังวลในการโจมตีของโดรนต่อผลกระทบต่อประชาชนหรือผู้บริสุทธิ์ที่ไม่ใช่เป้าหมาย

๖.๒ พัฒนาขีดความสามารถในการใช้อาวุธให้สามารถใช้อาวุธได้หลากหลายประเภท เพื่อที่จะสามารถใช้ทดแทนการใช้งานอากาศยานที่ใช้นักบินควบคุม ลดความเสี่ยงของกำลังพล โดยเฉพาะในพื้นที่ที่มีระบบป้องกันภัยทางอากาศอย่างหนาแน่น

๖.๓ พัฒนาขีดความสามารถในการลดการถูกตรวจจับโดยเซ็นเซอร์แบบต่าง ๆ ทั้งในรูปการแผ่กระจายหรือการสะท้อนคลื่นเรดาร์ ความร้อน เสียง และภาพ เพื่อลดการถูกต่อต้านจากระบบป้องกันทางอากาศ หรือแม้แต่วาระบบต่อต้านโดรน

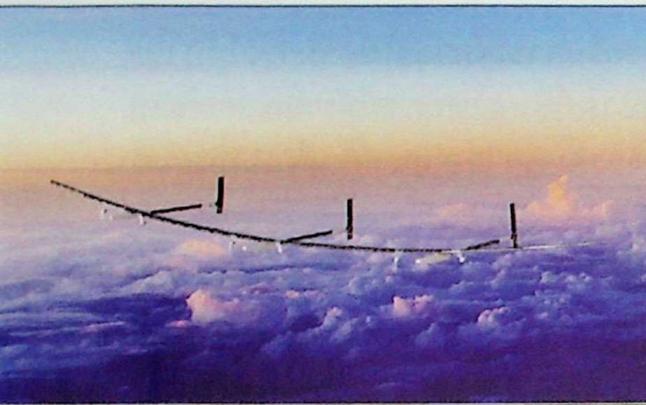
๖.๔ พัฒนาระบบขับเคลื่อน และระบบควบคุม เพื่อให้โดรนมีรัศมีปฏิบัติการไกลครอบคลุมพื้นที่เป้าหมายได้ทั้งหมด และสามารถถูกควบคุมได้จากกองบัญชาการหรือสถานที่อื่นที่มีความปลอดภัยสูงซึ่งอาจอยู่ห่างไกลจากพื้นที่ปฏิบัติการ

๖.๕ พัฒนาขีดความสามารถในการปฏิบัติงานร่วมกันในลักษณะเป็นกลุ่มโดรน หรือทำงานร่วมกับยานรบมิติต่าง ๆ ที่ควบคุมด้วยมนุษย์ เพื่อตอบสนองต่อแนวทางการใช้กำลังในลักษณะปฏิบัติการร่วม

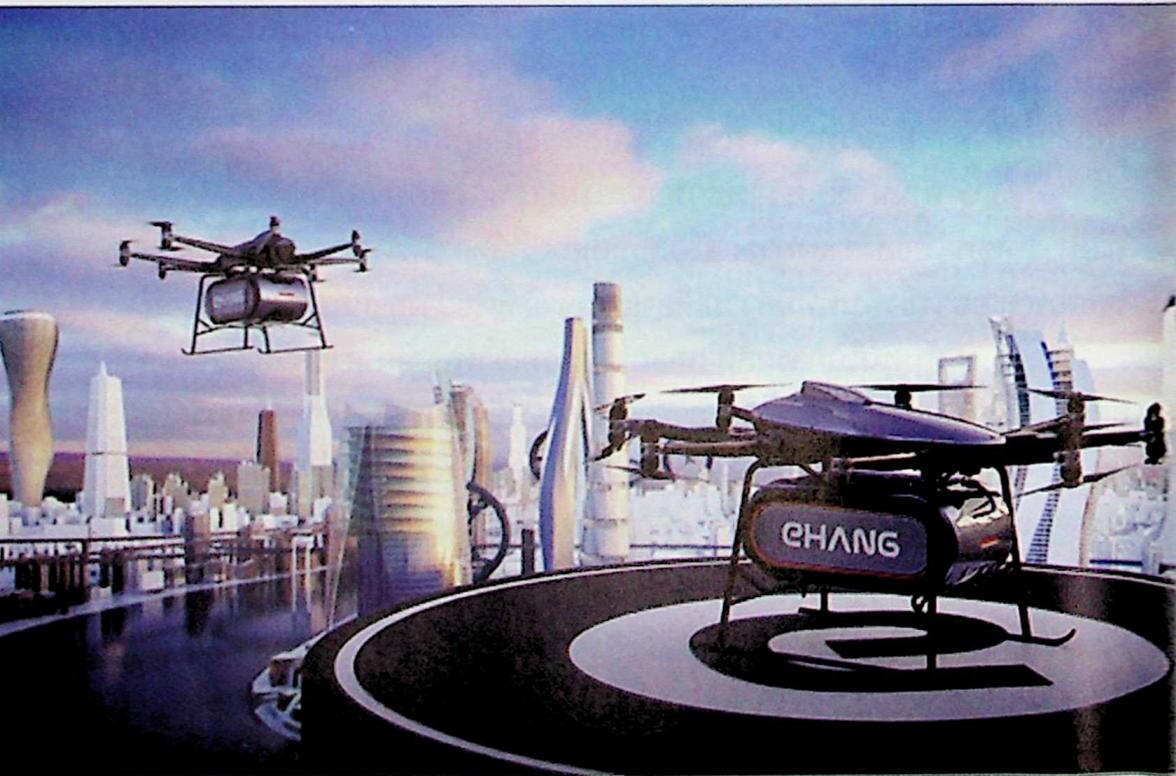
๖.๖ พัฒนาขีดความสามารถในการบรรทุกสิ่งของหรืออุปกรณ์ทางการทหาร เพื่อส่งกำลังบำรุง หรือสนับสนุนปฏิบัติการทางทหารในพื้นที่ต่าง ๆ โดยเฉพาะอย่างยิ่งพื้นที่ที่มีความเสี่ยงและเข้าถึงได้อย่างยากลำบาก

๖.๗ ต้นทุนในการผลิต และการอบรมเจ้าหน้าที่ในการควบคุมจะถูก

ลดลง เพื่อลดงบประมาณที่ใช้ในการจัดการปฏิบัติการ และการบำรุงรักษา การพัฒนาโดรนในอนาคตตามที่ได้กล่าวในเบื้องต้นจะส่งผลต่อแนวทางการปฏิบัติการทางทหารในอนาคตอย่างมาก โดยรูปแบบการปฏิบัติการทางทหารตั้งแต่ขั้นตอนหาข่าวทั้งในและนอกพื้นที่ปฏิบัติการ จัดทำแผนปฏิบัติการ การปฏิบัติการต่อเป้าหมาย และตรวจสอบผลการปฏิบัติ จะมีโดรนเข้าไปเกี่ยวข้องทั้งหมด อากาศยานหรือแม้กระทั่งยานรบในมิติอื่นที่ถูกควบคุมมีมนุษย์ควบคุมบนตัวยานจำนวนมากจะถูกแทนที่ด้วยโดรน จำนวนของกำลังพลที่มีความเสี่ยงจากการปฏิบัติงานในพื้นที่อันตรายสามารถถูกลดจำนวนลง โดยการทำงานของโดรน ความร่วมมือและบูรณาการทั้งในระดับเหล่าทัพ และระดับนานาชาติในการใช้โดรนปฏิบัติการร่วมกันจะมีมากขึ้น



ภาพโดรน High Altitude Long Endurance ใช้พลังงานแสงอาทิตย์เป็นหลักในการขับเคลื่อน
กลุ่มโดรนถูกควบคุมให้เก็บข้อมูลจากจุดต่าง ๆ ในพื้นที่เป้าหมาย
ที่มา : <https://www.unmannedsystemstechnology.com/2018/11/high-altitude-solar-powered-unmanned-aircraft-features-ultra-long-endurance/>



ภาพโดรนขณะขนส่งพัสดุน้ำหนัก ๒๐๐ กก.^{๓๑}
ที่มา : <https://thaibizchina.com/ehang20201014/>

๗. แนวทางการใช้โดรนในการปฏิบัติการทางเรือของกองทัพเรือ

การกำหนดแนวทางการใช้งานโดรนของกองทัพเรือจะต้องเข้าใจความสามารถของโดรนในแบบต่าง ๆ แล้วนำมาพิจารณาการใช้งานเพื่อตอบสนองต่อภารกิจของกองทัพ นอกจากนี้ยังต้องระมัดระวังถึงข้อจำกัดตลอดจนผลกระทบที่อาจเกิดขึ้นจากการใช้งานโดรน

จากบทความข้างต้นพบว่า โดรนมีข้อดีหลายอย่าง ได้แก่ ไม่เกิดความเสียหายต่อกำลังพล แม้จะปฏิบัติงานในพื้นที่อันตราย ทำงานได้ในระยะเวลานาน และต่อเนื่อง หลายแบบมีน้ำหนักเบาทำให้สามารถขนย้ายไปที่ต่าง ๆ ได้ง่าย มีขนาดเล็กสามารถแทรกซึมและหลบหลีกการตรวจจับได้ง่ายกว่าอากาศยานทั่วไป นอกจากนี้ยังพบว่า โดรนสามารถปฏิบัติการทางทหารได้หลายรูปแบบ เช่น เป็นเป้าลวงการโจมตีหรือซุ่มใช้อาวุธ สนับสนุนการลาดตระเวนหาข่าว และเฝ้าตรวจในพื้นที่ ถ่ายทอดสัญญาณการสื่อสาร สงครามอิเล็กทรอนิกส์ ส่งกำลังบำรุง และสนับสนุนการวิจัยและพัฒนา แม้กระทั่งใช้อาวุธทำลายเป้าหมาย อย่างไรก็ตาม ประสิทธิภาพของปฏิบัติการทางทหารเหล่านี้ยังขึ้นอยู่กับหลายปัจจัย ได้แก่ ชนิด ขนาด อุปกรณ์ที่เกี่ยวข้อง ความชำนาญของเจ้าหน้าที่ประจำเครื่อง และหลักนิยมในการใช้

เมื่อพิจารณาถึงข้อดีและความสามารถในการปฏิบัติการของโดรนตามที่ได้กล่าวข้างต้นควบคู่กับภารกิจงานที่กองทัพเรือต้องดำเนินการในระยะ ๒๐ ปีข้างหน้าตามที่ได้ระบุไว้ในยุทธศาสตร์กองทัพเรือ นั้น พบว่า โดรนสามารถเป็นเครื่องมืออย่างหนึ่งที่จะทำให้กองทัพเรือปฏิบัติการกิจได้ลู่ลวงอย่างมีประสิทธิภาพ จากแนวความคิดของผู้เขียนเองสามารถสรุปได้ ดังนี้

๗.๑ ภารกิจป้องกันราชอาณาจักรและรักษาสีหิทธิธิปไตยเหนืออาณาเขตทางทะเลของไทย: โดรนเป็นเครื่องมือสำคัญยิ่งที่เพิ่มขีดความสามารถของกองทัพเรือในภารกิจหลักนี้ เช่นเดียวกับกองทัพชาติอื่น ๆ ดังที่ได้เห็นจากตัวอย่างข้างต้น โดรนติดอาวุธสามารถปฏิบัติการรบทางทะเลโดยตรง ส่วนโดรนแบบอื่น ๆ สามารถใช้สนับสนุนหน่วยกำลังทางเรือต่าง ๆ หลากหลายภารกิจ เช่น การข่าว การส่งกำลังบำรุง การปฏิบัติการจิตวิทยา และการฝึก เป็นต้น โดยภาพรวมของการใช้งานโดรนกับปฏิบัติการทางทหารจะเพิ่มขีดความสามารถของกองทัพอย่างชัดเจน ความเร็วและคล่องตัวของโดรนจะทำให้กองทัพเรือ

สามารถตอบสนองได้อย่างรวดเร็วต่อภัยคุกคาม (Quick Response) ความสามารถในการรวบรวมข้อมูลข่าวสารของโดรนจะสร้างความรู้เท่าทันสถานการณ์ทางทะเล (Maritime Situation Awareness) ขีดความสามารถของโดรนติดอาวุธจะทำให้หน่วยกำลังมีอำนาจเหนือพื้นที่การรบ (Battlespace Dominance) และพิสัยการบินยาวของโดรนจะทำให้สามารถดำรงความต่อเนื่องในการปฏิบัติการ (Sustained Operations) ไว้ได้จนบรรลุภารกิจ

๗.๒ ภารกิจคุ้มครองและรักษาเส้นทางคมนาคมทางทะเลของไทย: สามารถใช้โดรนในการลาดตระเวนหาข่าวและเฝ้าตรวจในทะเลตามพื้นที่หรือเส้นทางคมนาคมที่สำคัญได้ในระยะเวลาอันยาวนานและต่อเนื่อง หากพบภัยคุกคาม เช่น โจรสลัด (Piracy) และการปล้นเรือ (Armed Robbery) ก็สามารถใช้โดรนสนับสนุนการพิสูจน์ทราบ ไล่ติดตามและจับกุม รวมทั้งหากอยู่ในสถานการณ์จำเป็นเร่งด่วน โดรนติดอาวุธอาจเป็นทางเลือกที่ใช้ในการป้องกันหรือยับยั้งภัยคุกคามนั้นได้

๗.๓ ภารกิจสนับสนุนการป้องกันพื้นที่ทางบกและตามลำน้ำที่ได้รับมอบหมาย: เนื่องจากระดับน้ำในลำน้ำโขงที่ลดลงส่งผลกระทบต่อปฏิบัติการของ นรข. โดยเฉพาะอย่างยิ่งการลาดตระเวนตามลำน้ำ นรข. จึงจำเป็นต้องปรับเปลี่ยนวิธีลาดตระเวน การใช้งานโดรนในการลาดตระเวนเป็นทางเลือกที่เหมาะสม สามารถชดเชยการลาดตระเวนทางน้ำที่ถูกจำกัดด้วยสภาพของลำน้ำในปัจจุบันได้

๗.๔ ภารกิจสนับสนุนการป้องกันและปราบปรามการกระทำผิดกฎหมายในทะเล: สามารถใช้งานโดรนเป็นเครื่องมือในการรวบรวมข้อมูลข่าวสารทางทะเล เพื่อพัฒนาการรับรู้เท่าทันสถานการณ์ทางทะเล (Maritime Domain Awareness) ร่วมกับส่วนราชการอื่น ๆ อีกทั้งยังสามารถใช้โดรนที่มีพิสัยนาน (Long Endurance) ติดตามสถานการณ์ครอบคลุมพื้นที่สำคัญหรือมีความเสี่ยงต่อการกระทำผิดกฎหมายต่าง ๆ เช่น การประมงผิดกฎหมาย การค้ามนุษย์ การลักลอบขนของผิดกฎหมาย และการก่อการร้ายทางทะเล

๗.๕ ภารกิจสนับสนุนการบรรเทาสาธารณภัยประชาชนในทะเลชายฝั่ง และพื้นที่ที่ได้รับมอบหมาย: การเข้าถึง และได้ภาพของพื้นที่ประสบสาธารณภัยอย่างละเอียดชัดเจนเป็นสิ่งที่กระทำได้ยาก หากแต่การใช้งานโดรน

รวบรวมข้อมูลหรือถ่ายภาพสถานการณ์ในพื้นที่ก็สามารถทำได้อย่างมีประสิทธิภาพ นอกจากนี้การใช้โดรนขนส่งสิ่งของจำเป็นเข้าสู่พื้นที่ประสบภัย เช่น อาหาร เครื่องนุ่งห่ม หรือยานั้น เป็นสิ่งที่สามารถกระทำได้ในปัจจุบัน และน่าจะมีความมากขึ้นในอนาคต

ถึงแม้ว่าจะมีความเป็นไปได้ในการใช้งานโดรนในภารกิจต่าง ๆ ตามที่ได้กล่าวไปข้างต้น กองทัพเรือยังคงต้องตระหนักถึงข้อจำกัดตลอดจนผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานโดรน เช่น ความกังวลใจเกี่ยวกับความแม่นยำในการโจมตีที่อาจทำให้พลเรือนซึ่งไม่เกี่ยวข้องต้องได้รับบาดเจ็บหรือเสียชีวิต ความชอบธรรมในการใช้งานโดรนในการสังหารเป้าหมาย การไม่ยอมรับในการใช้ระบบอัตโนมัติทำสงครามแทนมนุษย์ นอกจากนี้ โดรนยังอาจถูกระบบต่อต้าน (Anti-Drone System) ลดทอนหรือทำลายขีดความสามารถได้ และที่สำคัญ โดรนยังไม่สามารถทดแทนการใช้กำลังทหารปฏิบัติงานในพื้นที่ได้ทั้งหมด ตัวอย่างเช่น ปฏิบัติการต่อต้านการก่อการร้ายและการปราบปรามความไม่สงบในพื้นที่เป้าหมาย ซึ่งจำเป็นต้องมีกำลังทหารเข้าไปปฏิบัติงานในพื้นที่เพื่อเอาชนะใจของคนในพื้นที่ดังกล่าว (Winning hearts and Minds) ถึงจะสามารถบรรลุภารกิจเหล่านั้นได้

บทสรุป

ด้วยวัตถุประสงค์ที่จะสร้างความได้เปรียบทางการทหาร และความปลอดภัยให้กับกำลังทหาร การใช้งานโดรนครั้งแรกได้กำเนิดขึ้นในยุคคริสต์ศตวรรษที่ ๑๙ แม้ว่าจะไม่ประสบความสำเร็จในการใช้งาน แนวความคิดในการพัฒนาโดรนเพื่อการทหารยังคงมีต่อเนื่อง การพัฒนาที่เด่นชัดเกิดขึ้นอีกครั้งในสมัยสงครามโลกครั้งที่ ๑ โดรนถูกพัฒนาให้เป็นอาวุธบินเข้าทำลายเป้าหมายโดยตรง เพื่อเอาชนะสงครามสนามเพลาะที่ต่างฝ่าย

ไม่สามารถรुकึบเข้าหาอีกฝ่ายได้ ต่อมาโดรนถูกนำไปใช้เพื่อการฝึกการใช้อาวุธ และเมื่อสงครามโลกครั้งที่ ๒ เกิดขึ้น แนวความคิดการพัฒนาโดรนเพื่อใช้เป็นอาวุธ ทำลายได้กลับมาอีกครั้ง หลังจากสงครามโลกทั้งสองครั้ง โลกก้าวเข้าสู่ยุคสงครามเย็น ความต้องการข้อมูลข่าวสารในพื้นที่ฝ่ายตรงข้ามได้ผลักดันให้เกิดการพัฒนาโดรนเพื่อเป็นเครื่องมือในการรวบรวมข้อมูลในพื้นที่ที่มีความเสี่ยงสูงต่ออากาศยานแบบมีนักบินควบคุม บทบาทของโดรนในสงครามเลบานอน รวมไปถึงการเผชิญหน้ากับซีเรีย ช่วงปี ค.ศ.๑๙๘๒ ได้แสดงให้เห็นศักยภาพของโดรนในการรวบรวมข้อมูลด้านการข่าว สงครามอิเล็กทรอนิกส์ และการแสดงภาพสถานการณ์ เหตุการณ์เหล่านี้ได้กระตุ้นให้เกิดความร่วมมือในการเร่งพัฒนาโดรนในหลายประเทศ ในยุคคาบเกี่ยวระหว่างคริสต์ศตวรรษที่ ๒๐ และ ๒๑ โดรนได้ถูกพัฒนาให้มีขีดความสามารถในการปฏิบัติการทางทหารที่หลากหลาย เช่น ลาดตระเวนหาข่าวและเฝ้าตรวจในพื้นที่ ถ่ายทอดสัญญาณการสื่อสาร สงครามอิเล็กทรอนิกส์ สนับสนุนการวิจัยและพัฒนาส่งกำลังบำรุง และโดยเฉพาะอย่างยิ่งโจมตีเป้าหมายต่าง ๆ ด้วยความสามารถและลักษณะที่หลากหลาย ทำให้การแบ่งประเภทของโดรนสามารถกระทำได้หลายแบบ ขึ้นอยู่กับ ขนาด ลักษณะ ขีดความสามารถ และวัตถุประสงค์ของการใช้งาน จากความสำเร็จทั้งในอดีตและปัจจุบันทำให้สามารถเชื่อได้ว่าการพัฒนาโดรนจะมีมากขึ้นอย่างต่อเนื่อง ทั้งนี้ การพัฒนาโดรนในอนาคตจะครอบคลุมหัวข้อต่าง ๆ ได้แก่ ความแม่นยำและความหลากหลายในการใช้อาวุธ การลดการถูกตรวจจับโดยเซ็นเซอร์แบบต่าง ๆ การเพิ่มประสิทธิภาพ

ระบบขับเคลื่อนและควบคุม การเพิ่มขีดความสามารถ
ในการปฏิบัติการร่วมและการส่งกำลังบำรุง รวมทั้ง
ลดต้นทุนในการผลิต ดังนั้น กองทัพต่าง ๆ รวมทั้ง
กองทัพเรือจำเป็นต้องศึกษาและติดตามการพัฒนา
เทคโนโลยีที่เกี่ยวข้องกับโดรนอย่างใกล้ชิด รวมทั้งเร่งวาง
แนวทางการใช้งานโดรนในอนาคตด้วย

เอกสารอ้างอิง

- ๑ Cambridge. (2021, 6 10). Dictionary.cambridge.org. Retrieved from <https://dictionary.cambridge.org/dictionary/english/drone>
- ๒ Collins. (2021, 6 11). collinsdictionary. Retrieved from <https://www.collinsdictionary.com/dictionary/english/drone>
- ๓ Philpott, D. (2010). Terms and Acronyms. In G. I. Press., A Guide to Federal Terms and Acronyms (p. 482). Maryland: Inc. Lanham.
- ๔ Kozera, C. A. (2018). Military Use of Unmanned Aerial Vehicles - A Historical Study. Scientific and Technical Journal, P 17-21.
- ๕ Ibid
- ๖ McKinnon, G. D. (2012). THE BIRTH OF A DRONE NATION: AMERICAN UNMANNED AERIAL. Louisiana State: Louisiana State University. Retrieved from Andreas Parsch, "Dayton Wright/Kettering Liberty Eagle "Bug," (May 12, 2005), Accessed April 01, 2013, <http://www.designation-systems.net/dusrm/app4/bug.html>.
- ๗ (U.S.), A. F. (2002). developing air power for the United States Air Force during the first century of powered flight. Washington, D.C.
- ๘ Sampaio, R. C. (2015). Novel Morphologies on Flying Robots: Design for Field. Sˆao Carlos: the University of Sˆao Paulo.

- ๙ Museum, D. H. (2021, 6 11). The Queen Bee. Retrieved from dehavillandmuseum.co.uk :[https://www. Dehavilland museum. co.uk/aircraft/de-havilland-dh82b-queen-bee](https://www.dehavillandmuseum.co.uk/aircraft/de-havilland-dh82b-queen-bee)
- ๑๐ Goebel, G. (2021, 6 11). Early US Target Drones. Retrieved from vectorsite.net: http://www.vectorsite.net/twuav_01.html
- ๑๑ H, R. D. (2021, 6 11). The pioneers. Retrieved from Righter Radioplane in the Navy,: [https://www.ctie.monash.edu.au /hargrave/radioplane_ navy.html](https://www.ctie.monash.edu.au/hargrave/radioplane_navy.html)
- ๑๒ McKinnon, G. D. (2012). THE BIRTH OF A DRONE NATION: AMERICAN UNMANNED AERIAL. Louisiana State: Louisiana State University.
- ๑๓ Magazine, A. F. (2021, 6 11). The Remote Control Bombers. Retrieved from Air Force Magazine: [https://www.airfor cemag .com/ article/11110bombers](https://www.airforcemag.com/article/11110bombers)
- ๑๔ Channel, H. (Director). (2006). Weird Weapons: The Allies [Motion Picture].
- ๑๕ Ibid
- ๑๖ Wikipedia. (2021, 6 1). Aphrodite-drone. Retrieved from Wikipedia: [http://en.wikipedia.org/wiki/File:Aphroditie_droneb17 .jpg](http://en.wikipedia.org/wiki/File:Aphroditie_droneb17.jpg).
- ๑๗ Fklibrary. (2021, 6 11). Joseph P. Kennedy Jr. Retrieved from Fklibrary: [http://www.jfklibrary.org/JFK/The-Kennedy-Family/Joseph-P-Ken nedy-Jr.aspx](http://www.jfklibrary.org/JFK/The-Kennedy-Family/Joseph-P-Kennedy-Jr.aspx).
- ๑๘ Vectorsite. (2021, 6 11). the Lightning Bug Reconnaissance Drones. Retrieved from Vectorsite: [http://www.vectorsite .net /twuav_03. html](http://www.vectorsite.net/twuav_03.html)
- ๑๙ Forbes. (2021, 6 11). The U.S. Navy Flew Drones From Flattops in 1969. Retrieved from Forbes: [www.forbes.com/sites /davidaxe/2020/ 05/13/the-us-navy-flew-drones-from-flattops-in-1969/?sh=68491461742e](http://www.forbes.com/sites/davidaxe/2020/05/13/the-us-navy-flew-drones-from-flattops-in-1969/?sh=68491461742e)
- ๒๐ Olive-drab. (2021, 6 11). RQ-2 Pioneer UAV. Retrieved from Olive-drab: [https://olive-drab.com/idphoto/id_photos_ uav _rq2.php](https://olive-drab.com/idphoto/id_photos_uav_rq2.php)
- ๒๑ Technology, N. (2021, 6 11). Predator RQ-1. Retrieved from Naval Technology: Predator RQ-1, Naval Technology, [https://www.naval- technology.com/projects/predator](https://www.naval-technology.com/projects/predator)

- ๒๒ Militaryimages. (2021, 6 11). Reaper. Retrieved from Militaryimages: <https://www.militaryimages.net/media/mq-9-reaper.88865/>
- ๒๓ Graphicnews. (2021, 6 11). Russian S-70 stealth drone. Retrieved from Pinterest: <https://www.pinterest.com/pin/520095456969597953/>
- ๒๔ Geagea. (2021, 6 11). World's Smallest Camera Drone. Retrieved from geagea.xyz: <https://www.geagea.xyz/Product.aspx?iid=Detail.49437587&pr=79.99>
- ๒๕ Navalnews. (2021, 6 11). France Speeds Up UAV Procurement for French Navy. Retrieved from Navalnews: www.navalnews.com/navalnews/2020/06/france-speeds-up-uav-procurement-for-french-navy-as-part-of-industry-recovery-plan/
- ๒๖ Theweek. (2021, 6 11). Swarm threat. Retrieved from Theweek: www.theweek.in/news/world/2020/09/12/swarm-threat-why-chinas-use-of-drones-for-food-delivery-is-no-laughing-matter.html
- ๒๗ Washingtonpost. (2011, 6 11). Why Iran is getting the blame for an attack on Saudi Arabia. Retrieved from Washingtonpost: <https://www.washingtonpost.com/world/2019/09/16/why-iran-is-getting-blame-an-attack-saudi-arabia-claimed-by-yemens-houthis/>
- ๒๘ Journal, T. W. (2019). Aramco's Repairs. The Wall Street Journal.
- ๒๙ Bangkokbiznews. (2021, 6 11). MQ-9' โดรนสังหารนายพลอิหร่าน. Retrieved from Bangkokbiznews: <https://www.bangkokbiznews.com/news/detail/860910>
- ๓๐ Technology, U. S. (2021, 6 11). Solar Powered UAV. Retrieved from Unmannedsystemstechnology: <https://www.unmannedsystemstechnology.com/category/supplier-directory/platforms/solar-powered-drones/>
- ๓๑ Engineering, I. (2021, 6 11). Logistics Drone. Retrieved from Interesting Engineering: <https://interestingengineering.com/this-logistics-drone-has-a-440-pound-payload-capacity>



MARSUN SHIP BUILDER & REPAIRER SINCE 1980

เรือตรวจการณ์ลำน้ำ ความยาว 10 ม.



เรือปฏิบัติการความเร็วสูง ความยาว 18 ม.



เรือตรวจการณ์ชายฝั่ง ความยาว 21 ม.



เรือตรวจการณ์ใกล้ฝั่ง ความยาว 36 ม.



เรือตรวจการณ์ใกล้ฝั่งพร้อมปืนเรดาร์ ความยาว 41.45 ม.



เรือตรวจการณ์ปืน ส.ส.ทะเลสีฟ้า ความยาว 58 ม.



เรือดำน้ำพร้อมขีปนาวุธ ความยาว 55 ม.



เรือลากจูงขนาด 70 ตัน ความยาว 37 ม.



บริษัท มาร์ซัน จำกัด (มหาชน) "ผู้ต่อเรือของคนไทย เพื่อสังคมไทย"

413 หมู่ 4 ซอยสิทธิไชย ถนนท้ายบ้าน อำเภอเมือง จังหวัดสมุทรปราการ 10280

โทร : +66(0)2 173-8942-48 แฟกซ์ : +66(0)2 1738949 อีเมล : contact@marsun.th.com

WWW.MARSUN.TH.COM



สบดรามไซเบอร์และพัฒนากการ ปฏิบัติกาไซเบอร์ในอนาคต

นางเอก ดร.กรภ วิไลลักษณ์
นักศึกษากการวิจัย กองเอกสารการวิจัย
ฝ่ายวิชาการ กรมยุทธศึกษาทหารเรือ

บทคัดย่อ

ไซเบอร์สเปซ คือ ขอบเขตพื้นที่เสมือนที่ถูกนำมาใช้ประโยชน์ด้านความมั่นคงและการทหารเพิ่มขึ้นอย่างต่อเนื่อง เห็นได้จากการพัฒนาเสริมสร้าง และการแสดงขีดความสามารถทางไซเบอร์ของรัฐต่าง ๆ ซึ่งปรากฏให้เห็นอย่างเด่นชัดในรอบ ๒ ทศวรรษที่ผ่านมา อย่างไรก็ตาม ภูมิปัญญา ความรู้ความเข้าใจในหลักการพื้นฐาน และหลักนิยามปฏิบัติการไซเบอร์ยังเป็นไปอย่างจำกัด จึงอาจส่งผลให้การดำเนินยุทธศาสตร์และนโยบายไม่สอดคล้องกับสภาพแวดล้อมด้านความมั่นคงบนไซเบอร์สเปซ ที่มีการเปลี่ยนแปลงไปอย่างรวดเร็วและต่อเนื่อง บทความนี้จะนำเสนอหลักการพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์และศึกษาวิเคราะห์ปฏิบัติการไซเบอร์ครั้งสำคัญ ๆ เพื่อเชื่อมโยงให้เห็นความสัมพันธ์ของการป้องกันไซเบอร์และการรักษาความมั่นคงปลอดภัยของทรัพยากรและโครงสร้างพื้นฐานที่เกี่ยวข้องของกองทัพเรือให้พร้อมรองรับต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

คำสำคัญ

สงครามไซเบอร์ ปฏิบัติการไซเบอร์ ไซเบอร์สเปซ ความมั่นคงปลอดภัยไซเบอร์ และความมั่นคงปลอดภัยระบบสารสนเทศ

บทนำ

บทความนี้จะนำเสนอหลักการพื้นฐานที่เกี่ยวข้องกับสงครามไซเบอร์เพื่อรายงานสภาพแวดล้อม หลักการทั่วไปของปฏิบัติการไซเบอร์และแนวโน้มการเปลี่ยนแปลงปฏิบัติการไซเบอร์ โดยมีวัตถุประสงค์หลักเพื่อให้ผู้อ่านมีความรู้และความตระหนักรู้เพียงพอที่จะเข้าใจภัยคุกคามทางไซเบอร์ สามารถคาดการณ์แนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนประกอบสำคัญของไซเบอร์ และกำหนดยุทธศาสตร์การป้องกันไซเบอร์สเปซ ได้อย่างเหมาะสม

๑. หลักการพื้นฐานสำคัญที่เกี่ยวข้องกับสงครามไซเบอร์

๑.๑ ไซเบอร์ หมายถึงอะไร

เครือข่ายอินเทอร์เน็ตซึ่งในระยะเริ่มแรกถูกพัฒนาขึ้นเพื่อตอบโต้ภัยเกี่ยวกับสงครามนิวเคลียร์จึงถูกออกแบบเป็นเครือข่ายที่มีความพร้อมใช้

มีความเข้ากันได้กับอุปกรณ์แตกต่างชนิดและสามารถทำงานได้แม้ว่าเครือข่ายส่วนหนึ่งจะถูกทำลายไปจากอาวุธนิวเคลียร์ ทั้งนี้ พัฒนาการของเครือข่ายอินเทอร์เน็ตและเทคโนโลยีอื่น ๆ ที่เกี่ยวข้อง ส่งผลให้มนุษยชาติสามารถเข้าถึงและใช้ประโยชน์โครงข่ายและเครือข่ายข้อมูลข่าวสารที่มีขนาดใหญ่ที่สุดในประวัติศาสตร์ของมนุษย์ ความสามารถในการเข้าถึงโครงข่ายและเครือข่ายข้อมูลข่าวสารส่งผลให้มนุษย์สัมผัสได้ถึง “การมีอยู่” เสมือนกับเป็นขอบเขตทางกายภาพอื่น ๆ ที่มนุษย์รู้จักและรับรู้ นั่นคือ บก ทะเล อากาศ และอวกาศ จึงกล่าวได้ว่า “ไซเบอร์สเปซ (Cyberspace)” คือขอบเขตที่เกิดขึ้นจากการประยุกต์ใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารในการสร้าง ประมวลผล แลกเปลี่ยนและจัดเก็บข้อมูลข่าวสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ ทั้งนี้ ขอบเขตดังกล่าวหมายรวมถึงมนุษย์ที่ปฏิสัมพันธ์กับโครงสร้างพื้นฐานฯ อีกด้วย

ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารได้ปรับเปลี่ยนแนวคิดและการปฏิบัติที่เกี่ยวข้องกับการปฏิบัติการทางทหารในยุคปัจจุบันเป็นอย่างมาก เราสามารถพบเห็นการใช้ประโยชน์จากไซเบอร์สเปซเพื่อความมั่นคงจากการประยุกต์ใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและระบบเครือข่าย ในการปฏิบัติการทางทหารเพื่อความมั่นคงในหลากหลายมิติ โดยเฉพาะอย่างยิ่งในประเทศมหาอำนาจขนาดกลาง และประเทศมหาอำนาจ เช่น การผนวกรวมระบบควบคุมบังคับบัญชา (C2, C4I, C4ISR) ระบบค้นหา (Surveillance Systems) วิเคราะห์และประเมินค่าการปฏิบัติการทางทหาร (Operational Analysis and Simulations) เข้าเป็นโครงสร้างพื้นฐานสำหรับปฏิบัติการทางทหาร ด้วยเหตุที่ว่าเทคโนโลยีสารสนเทศและการสื่อสารช่วยให้วงรอบการตัดสินใจของผู้บังคับบัญชารวดเร็วและตอบสนองต่อสถานการณ์ที่เปลี่ยนแปลงไปได้อย่างแม่นยำ จนกล่าวได้ว่า การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารได้อย่างเหมาะสมย่อมเพิ่มโอกาสที่หน่วยจะบรรลุภารกิจ เนื่องจากการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารสามารถลดวงรอบการตัดสินใจของการปฏิบัติในทุกๆระดับ ตั้งแต่หน่วยในระดับยุทธวิธี ยุทธการและยุทธศาสตร์

อย่างไรก็ดี เครือข่ายอินเทอร์เน็ตตลอดจนเทคโนโลยีส่วนควบอื่น ๆ ที่เป็นโครงสร้างพื้นฐานที่สำคัญของไซเบอร์สเปซอาจถูกใช้ประโยชน์จาก

ผู้ไม่ประสงค์ดี ทั้งในระดับปัจเจกบุคคล องค์กรการก่อการร้าย และรัฐ เพื่อช่วงชิงผลประโยชน์ให้กับตน โดยเห็นได้จากหลากหลายเหตุการณ์ เช่น การใช้บริการต่าง ๆ ที่มีบนอินเทอร์เน็ตในการล่อลวงบุคคล การปฏิบัติการข่าวสารเพื่อเผยแพร่อุดมการณ์และแนวคิดการก่อการร้าย การปฏิบัติการเครือข่ายคอมพิวเตอร์เชิงรุกต่อโครงสร้างพื้นฐานระบบสารสนเทศและระบบเศรษฐกิจของประเทศเป้าหมาย จนกล่าวได้ว่าไซเบอร์สเปซซึ่งเป็นโดเมนที่ถือกำเนิดขึ้นใหม่และถูกใช้ประโยชน์ด้านความมั่นคงแห่งชาติอย่างต่อเนื่องในระยะเวลาราว ๒๐ ปีที่ผ่านมา โดยสามารถพบเห็นพัฒนาการของภัยคุกคามบนไซเบอร์สเปซที่มีความก้าวหน้าและมีศักยภาพในการลดขีดความสามารถการปฏิบัติการของกองกำลังทางบก ทางทะเล และทางอากาศ ตลอดจนขีดความสามารถด้านข้อมูลข่าวสารของฝ่ายตรงข้ามซึ่งเป็นหนึ่งในพลังอำนาจแห่งชาติที่สำคัญ

๑.๒ ภัยคุกคามทางไซเบอร์

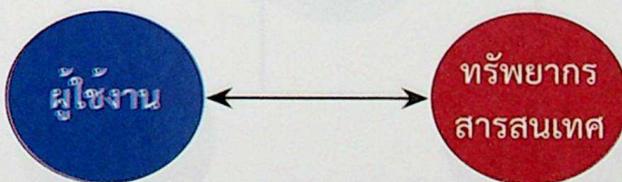
ภัยคุกคาม (Threats) หมายถึง บุคคล หรือเหตุการณ์ใด ๆ ก็ตามที่เป็นสาเหตุของการลดทอนความมั่นคงปลอดภัยของทรัพยากรสารสนเทศซึ่งประกอบด้วยโครงสร้างพื้นฐานฯ อันประกอบกันเป็นไซเบอร์สเปซ ตลอดจนข้อมูลข่าวสารที่รับ-ส่ง ผ่านช่องทางการสื่อสาร โดยภัยคุกคามดังกล่าวรวมไปถึงเหตุการณ์ที่เกิดขึ้นจากภัยธรรมชาติและอุบัติเหตุ โดยปกติบุคคลที่ทำการโจมตีนิยมเรียกว่า “ผู้ไม่ประสงค์ดี” “ผู้บุกรุก” หรือ “แฮกเกอร์” ทั้งนี้ ผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารที่แตกต่างกันออกไป ได้แก่ ความเชื่อพื้นฐานทางศาสนา ลัทธิการเมือง แรงจูงใจทางการเงิน ชื่อเสียง ความอยากรู้อยากเห็น เป็นต้น และเมื่อพิจารณาถึงแหล่งที่มาของการโจมตีจะสามารถจำแนกแหล่งที่มาของการโจมตีได้ ๒ ลักษณะ ได้แก่ ผู้บุกรุกจากภายนอก ซึ่งหมายถึงผู้บุกรุกที่ทำการโจมตีต่อทรัพยากรสารสนเทศจากภายนอกขอบเขตที่เราสนใจ เช่น ภายนอกโครงสร้างพื้นฐานฯ ของกองทัพ และผู้บุกรุกจากภายใน อันหมายถึงผู้บุกรุกที่ทำการโจมตีต่อทรัพยากรสารสนเทศจากภายในขอบเขตที่เราสนใจ เช่น ภายในเครือข่ายคอมพิวเตอร์ของกองทัพ

รายงานการโจมตีต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารถูกเปิดเผยเป็นครั้งแรกในช่วงคริสต์ทศวรรษที่ ๑๙๙๐ โดยมีเหตุการณ์สำคัญ ๆ เช่น ในปี ค.ศ.๑๙๙๙ กระทรวงกลาโหมสหรัฐฯ รายงานการถูกโจมตีจาก

ระบบเครือข่ายที่มีต้นทางจากสหภาพโซเวียต และส่งผลให้ข้อมูลสำคัญเกี่ยวกับเทคโนโลยีทางทหารถูกโจรกรรม และเชื่อกันว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยทางเครือข่ายที่มีรัฐเป็นตัวแสดงครั้งแรก อย่างไรก็ตาม สหภาพโซเวียตปฏิเสธความรับผิดชอบโดยสิ้นเชิงต่อเหตุการณ์ดังกล่าว ต่อมาในปี ค.ศ. ๒๐๐๗ กลุ่มแฮกเกอร์ที่เชื่อกันว่าได้รับการสนับสนุนจากรัฐบาลรัสเซียทำการโจมตีต่อเว็บไซต์ของหน่วยงานราชการเอสโตเนีย จนรัฐบาลเอสโตเนียต้องขอรับการสนับสนุนทรัพยากรจากประเทศในกลุ่ม NATO เข้ามาช่วยแก้ปัญหาและฟื้นคืนระบบ ซึ่งปรากฏรายงานเหตุการณ์ความมั่นคงปลอดภัยเกิดขึ้นอย่างต่อเนื่องจนถึงปัจจุบัน ทั้งนี้ หน่วยงานในรัฐบาลสหรัฐฯ นิยมเรียกเหตุการณ์ด้านความมั่นคงปลอดภัยที่มี “รัฐ” เป็นตัวแสดงว่า “Advance Persistent Threat: APT” โดยผลกระทบที่เกิดขึ้นจะส่งผลต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน ข้อมูลข่าวสารของรัฐที่ถูกโจมตีโดยขอบเขตความมั่นคงปลอดภัยจะครอบคลุมถึงการรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรสารสนเทศและการสื่อสาร ทั้งนี้ โครงสร้างพื้นฐานฯ เหล่านี้ จะถูกหลอมรวมเป็น “ข้อมูลข่าวสาร” องค์ประกอบหลักสำคัญของกำลังอำนาจแห่งชาติ (DIME)

๑.๓ ผลกระทบของภัยคุกคามทางไซเบอร์

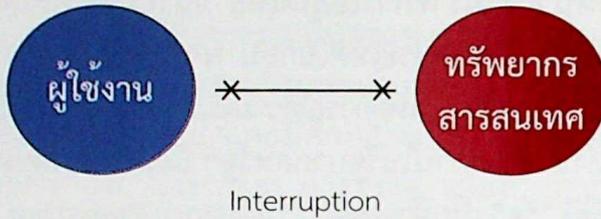
การเข้าถึงและใช้ประโยชน์จากทรัพยากรสารสนเทศและการสื่อสารของผู้ใช้งาน หากเป็นไปอย่างมั่นคงปลอดภัยสามารถแสดงได้ ดังภาพที่ ๑ โดยจะเห็นว่าผู้ใช้งานจะสามารถเข้าใช้งานทรัพยากรสารสนเทศได้โดยไม่มีบุคคลอื่นเข้าถึงทรัพยากรที่ผู้ใช้งานเข้าถึงอยู่โดยไม่มีสิทธิ์ ทั้งนี้ เมื่อจำแนกผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศ ไม่ว่าจะมีส่วนกำเนิดจากภายในหรือภายนอกองค์กร จะสามารถจำแนกได้ ๔ ประเภท ได้แก่



สภาวะการณ์ที่มั่นคงปลอดภัย

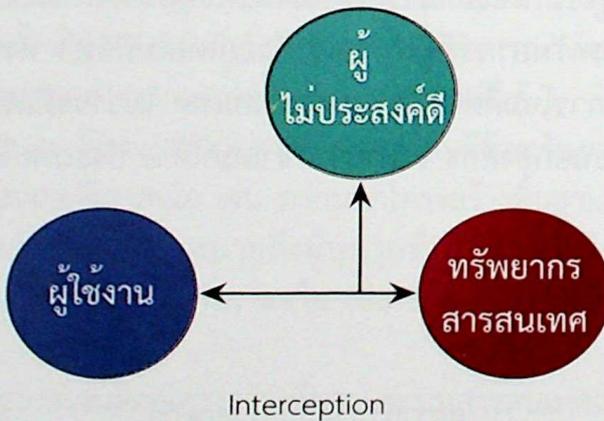
ภาพที่ ๑ สภาวะการณ์ที่มั่นคงปลอดภัย

๑.๓.๑ การสกัดขัดขวาง (Interruption) คือ การทำให้ทรัพยากรสารสนเทศไม่สามารถให้บริการได้ เช่น การเข้ารหัสไฟล์หรือฮาร์ดดิสก์โดยซอฟต์แวร์เรียกค่าไถ่ การโจมตีแบบกระจาย (Distributed Denial of Service: DDoS) การขโมยอุปกรณ์ ดังแสดงในภาพที่ ๒ ยกตัวอย่าง การขโมยอุปกรณ์ย่อมส่งผลให้ผู้ใช้งานไม่สามารถเข้าถึงทรัพยากรนั้น ๆ ได้



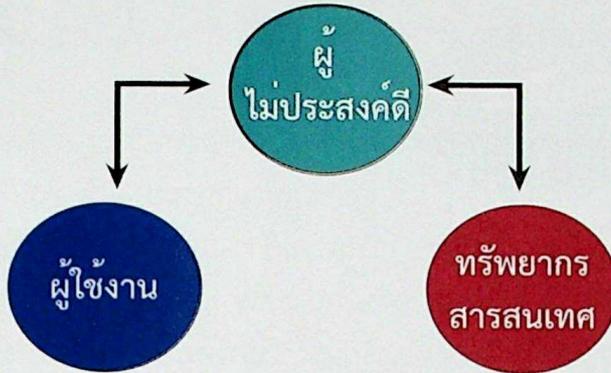
ภาพที่ ๒ การถูกสกัดขัดขวาง

๑.๓.๒ การดักจับดักฟัง (Interception) คือ การเข้าถึงทรัพยากรสารสนเทศระหว่างที่กำลังถูกส่งผ่านระบบการสื่อสารหรือระบบเครือข่าย เช่น การใช้โปรแกรม Sniffer ดักจับดักฟังเครือข่าย หรือการดักจับสัญญาณที่แพร่กระจาย การค้ายขยะเพื่อค้นหาข้อมูลสำหรับเข้าใช้งานระบบ ดังแสดงในภาพที่ ๓ จะเห็นว่าทรัพยากรสารสนเทศเหล่านั้นจะถูกเข้าถึงได้จากผู้ไม่ประสงค์ดี ซึ่งถ้าหากปราศจากมาตรการป้องกันที่เหมาะสมผู้ไม่ประสงค์ดีย่อมทำความเข้าใจและล่วงรู้ถึงข้อมูลที่ รับ-ส่ง นั้น ๆ ได้



ภาพที่ ๓ การถูกดักจับดักฟัง

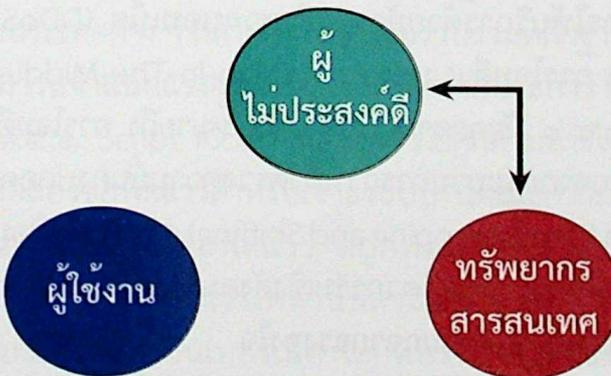
๑.๓.๓ การเปลี่ยนแปลงแก้ไข (Modification) คือ การทำให้ ทรัพยากรสารสนเทศและการสื่อสารถูกเปลี่ยนสภาพไปโดยไม่มีสิทธิ์ หรือไม่ได้ รับอนุญาต ดังแสดงในภาพที่ ๔ ยกตัวอย่างเช่น การเปลี่ยนแปลงแก้ไขข้อมูล เงินเดือนในระบบงานเงินเดือน การแก้ไขรายชื่อคำสั่งโดยไม่มีสิทธิ์ การแก้ไข หน้าเว็บโดยไม่ได้รับอนุญาต



Modification

ภาพที่ ๔ การเปลี่ยนแปลงแก้ไข

๑.๓.๔ การปลอมแปลง (Fabrication) คือ การสร้างทรัพยากร สารสนเทศและการสื่อสารเข้าสู่โครงสร้างพื้นฐานหรือระบบ เช่น การปลอมแปลง ข้อมูล หรือการปลอมแปลงตัวตน ดังแสดงในภาพที่ ๕ ซึ่งหมายรวมถึง การส่งข้อมูลข่าวสารที่เป็นเท็จ (Misinformation) เพื่อสร้างผลกระทบต่อ กระบวนการคิด การตัดสินใจ



Fabrication

ภาพที่ ๕ การปลอมแปลง

จะเห็นได้ว่า ผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารตามที่ได้กล่าวมา จะมีความเชื่อมโยงกับหลักการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสาร ซึ่งประกอบด้วย การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการรักษาความพร้อมใช้ (Availability) ของทรัพยากรสารสนเทศและการสื่อสารที่ผสมผสานเชื่อมต่อกันเป็นไซเบอร์สเปซ โดยปัจจัยสำคัญที่จะสร้างเสริมความมั่นคงปลอดภัยให้กับทรัพยากรจะเกี่ยวข้องกับมนุษย์ (People) ซึ่งมีปฏิสัมพันธ์กับทรัพยากร กระบวนการบริหารจัดการ การเข้าถึงทรัพยากรต่าง ๆ (Process) และเทคโนโลยี (Technology) ที่สามารถนำมาประยุกต์ใช้เสริมสร้างความมั่นคงปลอดภัยให้กับโครงสร้างพื้นฐาน กระบวนการ และทรัพยากรมนุษย์ที่ก่อปรเป็นไซเบอร์ ความเข้าใจถึงภัยคุกคามและผลกระทบที่เกิดขึ้นจะทำให้สามารถกำหนดขอบเขตและกำหนดมาตรการรับมือได้อย่างเหมาะสมสอดคล้องกับประเภทของภัยคุกคามนั้น ๆ

๑.๔ การจำแนกประเภทของภัยคุกคาม

เมื่อพิจารณาผลกระทบของภัยคุกคามที่ได้กล่าวมาแล้วจะพบว่า แนวทางการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารจะถูกแบ่งเป็น ๒ ลักษณะคือ ภัยคุกคามแบบแอคทีฟ (Active threats) และภัยคุกคามแบบพาสซีฟ (Passive threats)

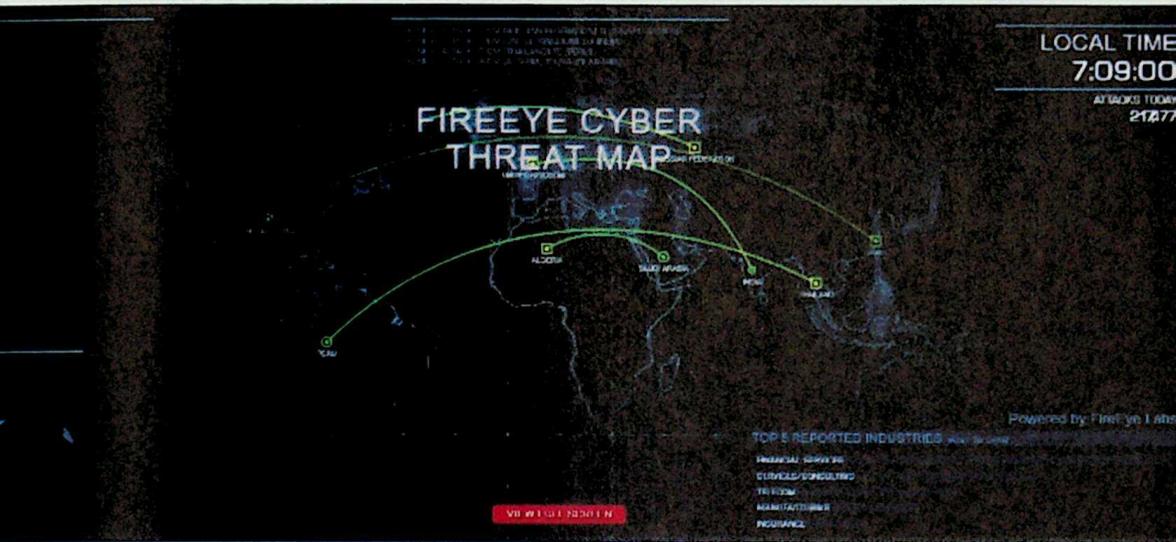
๑.๔.๑ ภัยคุกคามแบบแอคทีฟ หมายถึง การโจมตีที่ผู้ไม่ประสงค์ดี อาจถูกตรวจพบได้จากกระบวนการเฝ้าตรวจความมั่นคงปลอดภัย เช่น การทำให้ระบบปฏิเสธการให้บริการด้วยมัลแวร์จำพวกบอทเน็ต (DDoS via botnet) SQL Injection การโจมตีแบบคนกลาง (Man-In-The-Middle) เป็นต้น

๑.๔.๒ ภัยคุกคามแบบพาสซีฟ หมายถึง การโจมตีที่ผู้ไม่ประสงค์ดี จะไม่ถูกตรวจพบจากกระบวนการเฝ้าตรวจความมั่นคงปลอดภัย เช่น OSINT การดักจับดักฟัง (Eavesdropping and Sniffing) การสืบค้นข้อมูลจาก Search Engine การโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม (Social Engineering) เป็นต้น

๑.๕ ภัยคุกคามจำแนกจากแรงจูงใจ

แรงจูงใจที่ทำให้ผู้ไม่ประสงค์ดีตัดสินใจโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารแตกต่างกันในแต่ละบุคคลและกลุ่มบุคคล

และด้วยแรงจูงใจที่แตกต่างกันย่อมส่งผลกระทบต่อพลังอำนาจแห่งชาติในระดับที่แตกต่างกันออกไป ภาพที่ ๖ แสดงเหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของประเทศซึ่งเกิดขึ้นอย่างต่อเนื่อง



ภาพที่ ๖ การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่เคยเกิดขึ้นในประเทศต่าง ๆ

จากการรวบรวมหลักฐานจากเหตุการณ์ที่ผ่านมาจะสามารถจำแนกแรงจูงใจที่ทำให้ผู้ไม่ประสงค์ดีตัดสินใจโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารแตกต่างกันในแต่ละบุคคลและกลุ่มบุคคล เหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของประเทศต่าง ๆ หลายประเทศ เมื่อรวบรวมหลักฐานจากเหตุการณ์ที่ผ่านมาจะสามารถจำแนกแรงจูงใจเหล่านั้นได้หลายประการ ดังนี้

๑.๕.๑ Script Kiddy หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ที่ชอบศึกษาทดลองซอฟต์แวร์สำหรับเจาะระบบ แต่ไม่มีความสามารถในการพัฒนาซอฟต์แวร์จึงต้องใช้ซอฟต์แวร์ ที่ถูกพัฒนาขึ้นมาจากแฮกเกอร์ที่มีความสามารถสูง โดยซอฟต์แวร์เหล่านั้นสามารถดาวน์โหลดได้จากแหล่งซอฟต์แวร์เปิดบนเครือข่ายอินเทอร์เน็ต โดยพบว่าเหตุการณ์ด้านความมั่นคงปลอดภัย ส่วนใหญ่เป็นผลจากการโจมตีกลุ่มคนในกลุ่มนี้และพบว่าผลเสียหายที่เกิดขึ้นไม่มีนัยสำคัญอย่างไรต่อพลังอำนาจแห่งชาติ

๑.๕.๒ Criminal หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากแรงขับเคลื่อนขององค์กรอาชญากรรมที่มุ่งหาประโยชน์จากการโจมตีโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร จากสถิติพบว่าปริมาณการโจมตีที่เกิดขึ้นจากกลุ่มนี้มีจำนวนมากรองลงมาจากการโจมตีของกลุ่มสคริปคิตตี้

๑.๕.๓ Hacker Groups หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินกิจกรรมของกลุ่มแฮกเกอร์ที่มีฝีมือ และเป็นผู้พัฒนาเครื่องมือสำหรับใช้โจมตีต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร โดยพบว่าผลกระทบของภัยคุกคามจากกลุ่มนี้มีมากถึงร้อยละ ๘๐ ของผลเสียหายทั้งหมด ลักษณะเฉพาะของภัยคุกคามจากกลุ่มนี้คือการกระทำเพื่อหวังผลประโยชน์ในรูปของตัวเงิน และเศรษฐกิจ

๑.๕.๔ Insider หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลจากการดำเนินการของกลุ่มคนภายในองค์กร ซึ่งเป็นจุดที่ได้รับการปกป้องต่ำกว่าโครงสร้างพื้นฐานที่เชื่อมต่อกับเครือข่ายภายนอก โดยมีแรงจูงใจในการกระทำส่วนใหญ่เพื่อแก้แค้นองค์กร หรือได้รับการสนับสนุนทางการเงินจากองค์กรคู่แข่ง

๑.๕.๕ Political/Religious หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินการจากบุคคลที่มีความเชื่อทางการเมืองตรงข้ามกันกระทำต่อกันเพื่อล้มล้างหรือสร้างสถานะที่ฝ่ายตนต้องการ โดยมักไม่หวังผลความเสียหายต่อพลังอำนาจแห่งชาติ อย่างไรก็ตาม เมื่อพิจารณาขอบเขตการใช้ความเชื่อทางศาสนาเป็นเครื่องมือจะพบว่าแนวโน้มการใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารในการปลุกฝังและขยายจำนวนผู้ร่วมอุดมการณ์ของกลุ่มก่อการร้ายเพิ่มขึ้นอย่างมีนัยสำคัญ

๑.๕.๖ APT/Nation/State หมายถึง ภัยคุกคามทางไซเบอร์ที่มี “รัฐ” เป็นผู้ดำเนินการหรือเป็นผู้ให้การสนับสนุน ดังนั้น การโจมตีที่เกิดขึ้นจึงอาจเกิดขึ้นจากกองกำลังตามแบบหรือกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนทั้งทางตรงและทางอ้อม โดยปรากฏรายงานการจัดตั้งหน่วยงานสำหรับการปฏิบัติการไซเบอร์อย่างต่อเนื่อง เช่น The Tenth Fleet - The U.S. Fleet Cyber Command

๑.๖ กำลังอำนาจแห่งชาติ

การประเมินกำลังอำนาจแห่งชาติสามารถกระทำได้หลากหลาย ไม่ว่าจะเป็น DIME - Diplomatic, Information, Military, Economy หรือ MIDLIFE - Military, Intelligence, Diplomatic, Law Enforcement, Information, Finance, Economic หรือ PMESII - Political, Military, Economic, Social, Informational, Infrastructure โดยเมื่อพิจารณาอย่างถี่ถ้วนจะพบว่า องค์ประกอบของกำลังอำนาจแห่งชาติที่ได้ยกตัวอย่าง มีความเหลื่อมทับระหว่างกันอย่างเห็นได้ชัด โดยเฉพาะอย่างยิ่งข้อมูลข่าวสาร ซึ่งปรากฏอยู่ในทุก ๆ แนวคิด เนื่องจากข้อมูลข่าวสารเป็นปัจจัยอันดับต้น ๆ ที่ต้องคำนึงถึงในการทำสงครามทุก ๆ สมรภูมิ ประกอบกับความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารที่มีความก้าวหน้าแบบก้าวกระโดด ในช่วง ๒ - ๓ ทศวรรษที่ผ่านมา จึงทำให้การสร้าง การประมวลผล และการแพร่กระจายข้อมูลข่าวสารกระทำได้อย่างรวดเร็ว

หลักการพื้นฐานที่ได้กล่าวมานี้เป็นพื้นฐานที่สำคัญในการทำ ความเข้าใจคุณลักษณะของพื้นที่ปฏิบัติการแนวทางการใช้กำลัง คุณลักษณะ เฉพาะของปฏิบัติการไซเบอร์ และกรณีศึกษาได้อย่างถ่องแท้ในตอนถัดไป

๒. คุณลักษณะของสงครามไซเบอร์

ไซเบอร์สเปซเป็นพื้นที่เสมือนที่เกิดขึ้นจากความร่วมมือระหว่างกัน ในการพัฒนาเทคโนโลยีและบริการ ซึ่งผลักดันให้เกิดวิทยาการและความก้าวหน้า ทางวิทยาศาสตร์จากการใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลข่าวสาร ดำเนิน ธุรกิจ พัฒนาเศรษฐกิจและสังคมร่วมกัน อย่างไรก็ตาม เมื่อเกิดความขัดแย้งขึ้น ระหว่างกัน ไซเบอร์สเปซก็ถูกใช้พื้นที่สนามรบ (Battlespace) เช่นเดียวกับ โดเมนอื่น ๆ เพื่อดำรงรักษาไว้ซึ่งความมั่งคั่งประสงค์แห่งชาติทางกายภาพเสมือน เป็นอาณาเขตอีกอาณาเขตหนึ่งของรัฐ การเข้าใจถึงคุณลักษณะเฉพาะ และ แนวทางการใช้กำลังบนพื้นที่เสมือนแห่งนี้จึงมีความสำคัญอย่างยิ่งยวด

๒.๑ ลักษณะพื้นที่การรบและแนวทางการใช้กำลัง

หลักนิยมการใช้กำลังเป็นแนวคิดที่ใช้กำหนดทิศทางการใช้กำลังรบเพื่อ บรรลุความมั่งคั่งประสงค์ของชาติ (National Purpose) การพัฒนาหลักนิยม จึงต้องคำนึงถึงปัจจัยสำคัญ นับตั้งแต่ความมั่งคั่งประสงค์ของชาติ ผลประโยชน์ของชาติ

วัตถุประสงค์ของชาติ นโยบายของชาติ นโยบายทางทหาร ยุทธศาสตร์ทหาร หลักนิยมพื้นฐาน และยุทธวิธีของหน่วย ร่วมกับองค์ความรู้ในประวัติศาสตร์ การรบ บทเรียนจากการรบ ภัยคุกคาม ความเจริญก้าวหน้าด้านวิทยาศาสตร์และเทคโนโลยี และอาจกล่าวได้ว่า การใช้กำลังรบในแต่ละพื้นที่การรบ มีความต้องการและหลักนิยมการใช้กำลังที่แตกต่างกัน แม้ว่าจุดมุ่งหมายของการรบ ทางบก ทางทะเล และทางอากาศจะมีความคล้ายคลึงกัน โดยมีความต้องการหลัก ๆ เพื่อ ยึดพื้นที่ (Command) การควบคุมพื้นที่ (Control) หรือการปฏิเสธ การใช้ประโยชน์ของพื้นที่นั้น ๆ จากฝ่ายตรงข้าม (Denial) โดยการก้าวเข้าสู่ สภาวะสงครามในการรบทางบก ทางทะเล และทางอากาศมีความตรงไปตรงมา โดยมักเริ่มขึ้นเมื่อกำลังของแต่ละฝ่ายเคลื่อนเข้าหากัน เพื่อยึดครอง ควบคุม หรือปฏิเสธการใช้ประโยชน์เหนือพื้นที่นั้น ๆ จากฝ่ายตรงข้ามด้วยกองกำลัง ของตน บนหรือในยุทธบริเวณนั้น ๆ แต่สงครามไซเบอร์คุณลักษณะแตกต่าง จากพื้นที่การรบอื่น ๆ อย่างมีนัยสำคัญ

๒.๑.๑ สงครามทางบก การดำเนินกลยุทธ์บนพื้นที่ทางบกมีมาควบคู่ กับการวิวัฒนาการของมนุษย์ โดยอาวุธ ยุทธวิธี และการดำเนินกลยุทธ์ของ การทำการรบทางบกได้รับการพัฒนามาอย่างต่อเนื่อง นับตั้งแต่ การขว้างปาหิน พัฒนาเป็นหอก ธนู เครื่องยิง ระเบิด ปืน ปืนใหญ่ ปืนกล รถถัง และกล่าวได้ว่า การพัฒนาของอาวุธชนิดต่าง ๆ ส่งผลโดยตรงต่อหลักนิยม ยุทธวิธี และการจัด กำลัง ซึ่งจะต้องถูกพัฒนาให้เหมาะสมกับอาวุธในแต่ละแบบ โดยมีแนวคิดพื้นฐาน ในการแบ่งมอบการบังคับบัญชาให้หน่วยรองและควบคุมการปฏิบัติ (Chain of Command and Span of Control) สำหรับการรบในยุคปัจจุบันจะพบว่าการ ใช้กำลังเพื่อทำการรบทางบก จะมีลักษณะเป็นการจัดกำลังผสมเหล่า ที่ฝึกกำลังรบที่มีอำนาจการยิง และสามารถดำเนินกลยุทธ์ด้วยการจู่โจม รวดเร็ว รุนแรง สามารถเอาชนะกำลังรถถังและยานเกราะ มีส่วนยิงสนับสนุน จากอาวุธยิงสนับสนุน เช่น การจัดกองพันผสม ซึ่งประกอบด้วย กองร้อยรถถัง กองร้อยรถสายพาน กองร้อยรถสายพานลาดตระเวน และทหารราบ เพื่อปฏิบัติ การรบด้วยวิธีรุก รับ และร่นถอยได้อย่างอ่อนตัวและมีประสิทธิภาพ และ เมื่อพิจารณาประวัติศาสตร์สงครามที่ผ่านมาจะเห็นว่า การยุทธ์ในปัจจุบัน ต่างก็มีการใช้กองกำลังผสมเหล่าในการทำการรบ

๒.๑.๒ สงครามทางเรือ เมื่อพิจารณาพื้นที่ปฏิบัติการของการยุทธ์ทางเรือจะพบว่า พื้นที่การยุทธ์มีอาณาเขตกว้างขวางซึ่งเกื้อกูลต่อการเคลื่อนกำลังโดยมีอุปสรรคเกี่ยวกับภูมิประเทศน้อยกว่าการยุทธ์ทางบก มีความเร็วในการเคลื่อนกำลังมากกว่าการรบทางบก โดยในหนึ่งวันอาจเคลื่อนที่ได้หลายสิบล้านไมล์ ในขณะที่การรบทางบกอาจใช้ระยะเวลา นานกว่าในการรุกคืบเข้าไปในภูมิประเทศ หลักนियมการยุทธ์ทางเรือก็ได้รับอิทธิพลจากความก้าวหน้าของเทคโนโลยีเช่นเดียวกัน โดยเห็นได้จากการเปลี่ยนหลักนियม ยุทธวิธีของกำลังทางเรือ เมื่อมีการพัฒนาเรือบรรทุกเครื่องบิน และกล่าวได้ว่าการยุทธ์ทางเรือในปัจจุบันขึ้นอยู่กับ ยุทธศาสตร์ในการใช้กำลังรบทางเรือ ระบบอำนวยการรบ การควบคุมบังคับบัญชา อันเป็นผลจากความก้าวหน้าของเทคโนโลยีสารสนเทศ และการสื่อสารของอุปกรณ์ตรวจจับและระบบอาวุธ โดยมักมีแนวคิดการจัดกำลังเข้าทำการรบแบบตามความสามารถ (Capability-Based)

๒.๑.๓ สงครามทางอากาศ การยุทธ์ทางอากาศมีแนวคิดในการควบคุมเป็นสำคัญ โดยจะต้องมีการจัดกำลังและการบังคับบัญชาตามคุณลักษณะของอาวุธ และมอบความรับผิดชอบทางยุทธการให้กับผู้บังคับบัญชาเพียงคนเดียว เพื่อสนธิกำลังทางอากาศทั้งปวงไว้ด้วยกันในลักษณะของ Centralized Control และ Decentralized Execution เนื่องจากมูลค่าของกำลังรบสูงมากและมีจำนวนจำกัด การควบคุมบังคับบัญชาจึงต้องกระทำอย่างรัดกุม มีการจัดลำดับความสำคัญอย่างเหมาะสม เพื่อตอบสนองยุทธศาสตร์การใช้อากาศยานเพื่อการครองอากาศ การควบคุมห้วงอากาศ ซึ่งมีความคล้ายคลึงกับแนวคิดการใช้กำลังทางเรือ เนื่องจากมีสภาพทางกายภาพคล้ายคลึงกันคือ การไม่สามารถระบุขอบเขตพื้นที่ได้อย่างชัดเจนนั่นเอง

๒.๑.๔ สงครามไซเบอร์ มีความคล้ายคลึงกับสงครามทางเรือและสงครามทางอากาศ เนื่องจากการไม่สามารถระบุขอบเขตทางกายภาพได้อย่างแน่นอน และการเชื่อมต่อกันเสมือนไร้พรมแดน ซึ่งในสงครามทางเรือและทางอากาศคู่ขัดแย้งสามารถเคลื่อนย้ายกำลังเข้าปะทะกันได้เมื่อเกิดความขัดแย้ง อย่างไรก็ตาม ไซเบอร์ไม่ได้ถูกจำกัดที่ทรัพยากรทางทหารหรือทรัพยากรของรัฐคู่กรณีแต่เพียงอย่างเดียว เนื่องจากเป้าหมายที่ถูกโจมตีอาจเป็นโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารอื่น ๆ

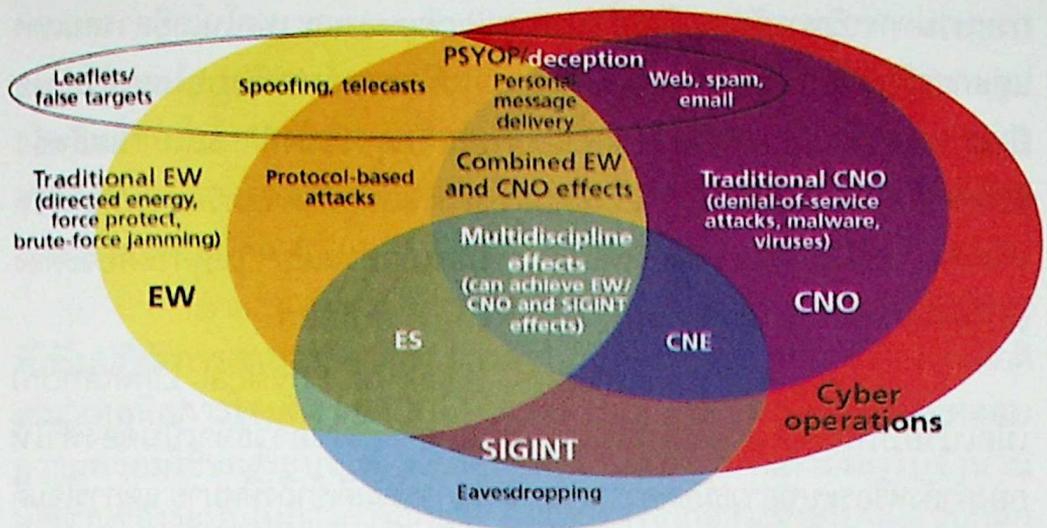
ที่อยู่นอกการควบคุมของหน่วยงานรัฐหรือกองทัพ อีกทั้งการระบุคู่ขัดแย้งในไซเบอร์สเปซก็กระทำได้อย่างไม่ชัดเจน ยกตัวอย่างเช่น โครงสร้างพื้นฐานของหน่วยงาน รัฐ B มีข้อบกพร่องด้านความมั่นคงปลอดภัยอย่างรุนแรง จึงถูกกองกำลังไซเบอร์รัฐ A โจมตีเพื่อใช้เป็นฐานสำหรับการโจมตีต่อโครงสร้างพื้นฐาน รัฐ C ซึ่งไม่มีความขัดแย้งใด ๆ กับรัฐ B การระบุตัวตนและการพิสูจน์ทราบกำลังทางกายภาพก็กระทำได้ยากเช่นเดียวกัน เนื่องจากผู้ที่ทำการโจมตีทางไซเบอร์อาจไม่ใช่กองกำลังจัดตั้งตามแบบ แต่กลับเป็นกลุ่มอาชญากรรมจัดตั้ง กลุ่มนักเคลื่อนไหวที่มีอุดมการณ์ร่วมต่อต้านรัฐซึ่งอาจได้รับข้อมูลที่ผิดเพี้ยนจากปฏิบัติการข่าวสารของรัฐคู่ขัดแย้งก็เป็นได้

๒.๒ คุณลักษณะของอาวุธที่ใช้ในสงครามไซเบอร์

ไซเบอร์สเปซเป็นพื้นที่เสมือนที่มนุษย์รับรู้ได้ โดยเป็นผลจากการเชื่อมต่อเข้ากันเป็นระบบของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งทำหน้าที่รับข้อมูลข่าวสารจากการนำเข้าสู่ระบบโดยมนุษย์หรือผลการคำนวณของระบบ จากนั้นอาจประมวลผล จัดเก็บ และกระจายข้อมูลข่าวสารเหล่านั้นไปยังโครงสร้างพื้นฐานอื่น ๆ ที่เชื่อมต่อกันผ่านอินเทอร์เน็ต ทั้งนี้ การโจมตีต่อเป้าหมายบนไซเบอร์สเปซทำได้โดยการใช้ประโยชน์ของช่องโหว่เกี่ยวกับการรักษาความมั่นคงปลอดภัยที่มีในโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารนั้น ๆ หากการโจมตีประสบผลสำเร็จจะส่งผลต่อการรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และความพร้อมใช้ของทรัพยากรนั้น ๆ นอกจากนี้ยังอาจส่งผลต่อ “การรับรู้” ของมนุษย์ที่ปฏิสัมพันธ์จากการปล่อยข่าวลวง การโจมตีด้วยเทคนิควิศวกรรมสังคม ดังนั้น อาวุธที่ใช้ในสงครามไซเบอร์จึงมีหลากหลายลักษณะ และครอบคลุมขีดความสามารถในหลายระดับ ตั้งแต่สัญญาณไฟฟ้า อุปกรณ์อิเล็กทรอนิกส์ ข่าวสาร ซอฟต์แวร์ เทคนิควิศวกรรมสังคม เป็นต้น

๒.๓ ปฏิบัติการไซเบอร์

ในปัจจุบันสหรัฐฯ ยังไม่มีการกำหนดหลักนิยามสงครามไซเบอร์อย่างเป็นทางการ แต่มีการประยุกต์ใช้แนวทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารจนกล่าวได้ว่า แนวทางดังกล่าวเป็นปฏิบัติการเชิงรับ โดยหากกระทำสำเร็จจะมั่นใจได้ว่าทรัพยากรที่เกี่ยวข้องกับข้อมูล



ภาพที่ ๗ ภาพรวมการปฏิบัติการข้อมูลข่าวสาร

ที่มา : Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World," p.51

ข่าวสารทั้งปวงถูกสร้าง รับ-ส่ง ผ่านโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารอย่างมั่นคงปลอดภัย และสามารถบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ สำหรับการปฏิบัติเชิงรุก สหรัฐฯ กำหนดแนวทางการปฏิบัติเกี่ยวกับสงครามไซเบอร์เป็นส่วนหนึ่งของปฏิบัติการข้อมูลข่าวสาร (IO) ดังแสดงในภาพที่ ๗ และเรียกปฏิบัติการที่เกี่ยวข้องกับสาขานี้ว่า "ปฏิบัติการด้านเครือข่ายคอมพิวเตอร์ (Computer Network Operation)" ครอบคลุมถึงปฏิบัติการสาขาย่อย ๆ ๓ สาขา ได้แก่ การเจาะระบบเครือข่าย (Computer Network Exploitation) การโจมตีระบบเครือข่าย (Computer Network Attack) การป้องกันระบบเครือข่าย (Computer Network Defense) ทั้งนี้ ปฏิบัติการไซเบอร์มีความครอบคลุมถึงการดักจับดักฟังสัญญาณและคลื่นแม่เหล็กไฟฟ้า การปฏิบัติการจิตวิทยาและการลวง การปลอมแปลงสัญญาณ ตลอดจนการโจมตีต่อโพรโทคอลทางการสื่อสาร ดังนั้น หากต้องการป้องกันการโจมตีทางไซเบอร์จึงมีความจำเป็นอย่างยิ่งที่จะต้องจัดการเสริมสร้างขีดความสามารถให้กับปัจจัยที่เกี่ยวข้องกับทรัพยากรสารสนเทศ ๓ ปัจจัยหลัก ได้แก่ ทรัพยากรมนุษย์ (People)

กระบวนการบริหารจัดการข้อมูลข่าวสาร (Process) และ เทคโนโลยีสารสนเทศ และการสื่อสาร (Technology) ทั้งนี้ ปฏิบัติการทางทหารบนไซเบอร์สเปซ มีแนวทางการปฏิบัติหลากหลายขึ้นอยู่กับ “วัตถุประสงค์” และ “ผลลัพธ์” ที่สอดคล้องกับความต้องการในระดับยุทธการและยุทธศาสตร์อย่างเห็นได้ชัด หากต้องการปฏิบัติการไซเบอร์ให้ได้ผล “ผู้มีส่วนได้ส่วนเสีย” ในทุกระดับจะต้อง เข้าใจคุณลักษณะสำคัญของปฏิบัติการไซเบอร์ อันได้แก่

๒.๓.๑ ความไร้พรมแดน (Lack of Physical Limitation) เมื่อเปรียบเทียบกับภารกิจในโดเมนอื่น ๆ การใช้อาวุธจำเป็นต้องทำให้ กองกำลังหรือระบบอาวุธมีขีดความสามารถในการโจมตีเข้าถึงที่หมาย แต่การโจมตี ทางไซเบอร์แทบจะไม่มีข้อจำกัดในลักษณะนั้น ตรวจจับการเชื่อมต่อของระบบ เครือข่ายสามารถติดต่อสื่อสารระหว่างกัน หรือมีช่องทางสามารถส่งผ่านการ โจมตีผ่านสื่อลักษณะอื่นได้ เช่น USB แฟลชไดรฟ์ หรือการแพร่กระจายของ มัลแวร์จากอุปกรณ์ที่ได้รับความเชื่อถือ ตามที่ปรากฏในกรณี Stuxnet เป็นต้น

๒.๓.๒ ผลทางกายภาพ (Kinetic Effect) ผลสัมฤทธิ์ที่ต้องการ สูงสุดของการปฏิบัติการไซเบอร์คือ การสร้างความเสียหายต่อโครงสร้างพื้นฐาน เทคโนโลยีสารสนเทศ แต่ส่งผลกระทบต่อทางกายภาพ^๓ ดังเห็นได้จากกรณีศึกษา การโจมตีด้วยมัลแวร์ Stuxnet และ Downadup

๒.๓.๓ พหุติกรรมลับ (Stealth) ปฏิบัติการไซเบอร์โดยเฉพาะ อย่างยิ่ง CNO จำเป็นต้องมีการซ่อนพรางการปฏิบัติอย่างเหมาะสม ดังกรณี การโจมตีศูนย์ข้อมูลกลาโหมสาธารณรัฐเกาหลี ซีเรีย Stuxnet และเหตุการณ์ อื่น ๆ จะเห็นได้ว่าการค้นหาตัวตนที่แท้จริงของผู้ทำการโจมตีบนไซเบอร์สเปซ กระทำได้อย่างจำกัด

๒.๓.๔ ความยืดหยุ่นสูง (Mutability and Inconsistency) จากกรณีศึกษาที่ได้กล่าวมาจะพบว่า ปฏิบัติการไซเบอร์ต้องการความอ่อนตัว และจะต้องปรับเปลี่ยนตนเองให้สอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงได้ ยกตัวอย่างเช่น การโจมตีด้วยเทคนิคหนึ่ง ๆ ต่อเป้าหมายที่แตกต่างกัน ผลลัพธ์ ที่ได้อาจแตกต่างกันเนื่องจากปัจจัยของซอฟต์แวร์และฮาร์ดแวร์ที่เกี่ยวข้อง เปลี่ยนไป

๒.๓.๕ การระบุตัวตนและสิทธิ (Identity and Privileges) ผลสำเร็จของปฏิบัติการไซเบอร์ขึ้นอยู่กับความสามารถในการได้รับฐานานุกรมและสิทธิของบุคคลหรือระบบที่เกี่ยวข้องกับเป้าหมายการโจมตี ซึ่งแตกต่างจากการปฏิบัติการทางทหารโดยปกติ ซึ่งการรับรู้ถึงตัวตนและสิทธินั้นไม่มีผลระหว่างการปฏิบัติการ

๒.๓.๖ ความเป็นอรรถประโยชน์ (Dual Use) เครื่องมือต่าง ๆ ที่ใช้ในปฏิบัติการไซเบอร์มีคุณประโยชน์ทั้งในปฏิบัติการทางทหาร และภาวะปกติ เช่น เทคนิคการโจมตีแบบ DDoS อาจนำมาใช้ประโยชน์ในการวัดทดสอบความพร้อมใช้ของระบบเพื่อทดสอบขีดความสามารถในการรองรับจำนวนผู้ใช้งานของระบบในภาวะการณปกติ ซึ่งแตกต่างจากอาวุธซึ่งใช้ประโยชน์หลักในการทำลายเป้าหมายฝั่งตรงข้ามในระหว่างปฏิบัติการทางทหาร

๒.๓.๗ การควบคุมโครงสร้างพื้นฐาน (Infrastructure Control) การควบคุมโครงสร้างพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์ได้อย่างเบ็ดเสร็จย่อมส่งผลดีต่อความสำเร็จของปฏิบัติการ คล้ายคลึงกับการเข้ายึดพื้นที่สำคัญทางทหารในการปฏิบัติทางทหารในโดเมนอื่น ๆ อย่างไรก็ตาม การควบคุมโครงสร้างพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์นั้น กระทำได้อย่างจำกัดในทางปฏิบัติ เนื่องจากคุณลักษณะเฉพาะของเครือข่ายอินเทอร์เน็ตที่การรับส่งข้อมูลไม่สามารถควบคุมเส้นทางได้อย่างสมบูรณ์ และการโจมตีอาจเกิดขึ้นกับช่องโหว่ด้านการบริหารจัดการทรัพยากรที่เชื่อมต่อกันบนโครงสร้างพื้นฐานนั้น ๆ

๒.๓.๘ ข่าวสารเป็นสภาพแวดล้อมในการปฏิบัติการ (Information as Operational Environment) ปฏิบัติการต่าง ๆ บนไซเบอร์สเปซเป็นปฏิบัติการข่าวสารโดยธรรมชาติ จึงมีความแตกต่างจากปฏิบัติการในโดเมนอื่น ๆ ที่กองทัพจะต้องบริหารจัดการทรัพยากรที่มีโดยเปลี่ยนเป็นข้อมูลข่าวสารเพื่อใช้ในการควบคุมบังคับบัญชาทรัพยากรเหล่านั้น ปฏิบัติการไซเบอร์ใช้ประโยชน์จากข้อมูลข่าวสารที่มีบนไซเบอร์เพื่อบรรลุวัตถุประสงค์ของปฏิบัติการ

๓. กรณีศึกษาจากปฏิบัติการไซเบอร์ในอดีต

พัฒนาการการโจมตีทางไซเบอร์ซึ่งสนับสนุนวัตถุประสงค์ทางทหารเกิดขึ้นอย่างต่อเนื่องนับตั้งแต่ปี ค.ศ.๒๐๐๓ เป็นที่รู้จักกันภายใต้ชื่อเหตุการณ์ “Titan Rain” เป็นการโจมตีทางไซเบอร์ต่อกลุ่มองค์กรที่มีสัญญาณกับกระทรวง

กลาโหมสหรัฐฯ เช่น บริษัทล็อกฮีด มาติน (Lockheed Martin) ศูนย์การทดลองแห่งชาติซานเดีย (Sandia National Laboratories) เรดสโตนอาร์เซนอล (Redstone Arsenal) เป็นต้น โดยผลพิสูจน์หลักฐานคอมพิวเตอร์ (Computer Forensic) บ่งชี้ว่าการโจมตีมีจุดกำเนิดมาจากมณฑลกว่างตุง (Guangdong) สาธารณรัฐประชาชนจีน โดยมีข้อมูลบ่งชี้ว่า การโจมตีทางไซเบอร์เหล่านั้นเกิดขึ้นภายใต้การสนับสนุนจากรัฐบาลสาธารณรัฐประชาชนจีนอย่างลับ ๆ การโจมตีทางไซเบอร์ขนาดใหญ่ครั้งต่อมาเกิดขึ้นระหว่างปี ค.ศ. ๒๐๐๗ - ๒๐๐๙

คู่ขัดแย้งในครั้งนี่คือ สาธารณรัฐเอสโตเนีย และสหภาพโซเวียต^๕ ซึ่งมีความขัดแย้งกันเนื่องจากสาธารณรัฐเอสโตเนียมีความต้องการเข้าร่วมกลุ่มสหภาพยุโรป เป้าหมายสำคัญของการโจมตีคือ โครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารขององค์การภาครัฐ เช่น รัฐสภา กระทรวง องค์การการเงิน การธนาคาร และองค์การสื่อต่าง ๆ ของสาธารณรัฐเอสโตเนีย ถูกโจมตีอย่างต่อเนื่องด้วยการโจมตีแบบกระจาย (DDoS) และการปรับเปลี่ยนหน้าเว็บเพจ (Web Defacement) ซึ่งเป็นการโจมตีแบบพื้นฐานและส่งผลเพียงเพื่อสกัดกั้นไม่ให้ผู้ใช้งานที่มีสิทธิ์สามารถเข้าใช้งานระบบที่ตกเป็นเป้าหมาย หรือเพียงเพื่อก่อกวน ไม่ได้สร้างความเสียหายให้กับโครงสร้างพื้นฐานอย่างหนักตั้งแต่วันที่ ๒๗ เมษายน ค.ศ. ๒๐๐๗ อย่างไรก็ดี ผลกระทบที่เกิดขึ้นอย่างเห็นได้ชัดจากการโจมตีดังกล่าวคือ ความสับสนวุ่นวายและการเสียความเชื่อมั่นจากประชาชนในการบริหารจัดการภาวะวิกฤต ทั้งนี้ จากกรณีดังกล่าวส่งผลให้รัฐสภาแห่งสหภาพยุโรปร่วมกับ NATO ทำการตรวจประเมินความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญในประเทศกลุ่มสมาชิกและพัฒนาต่อเนื่องเป็นศูนย์ความร่วมมือป้องกันไซเบอร์สเปซของนาโต้ พร้อมกับบังคับใช้คู่มือ Tallinn^๖ ซึ่งเป็นกฎหมายระหว่างประเทศที่ใช้ในกลุ่มประเทศสหภาพยุโรป แต่ถูกนำมาใช้เป็นบรรทัดฐานอ้างอิงในระดับนานาชาติเมื่อจำเป็นต้องอ้างอิงประเด็นกฎหมายระหว่างประเทศในบริบทของสงครามไซเบอร์

ในช่วงเวลาเดียวกัน สาธารณรัฐอิสราเอลปฏิบัติการ Orchard สำเร็จเป็นอย่างดีในการโจมตีต่อเตาปฏิกรณ์นิวเคลียร์ Al Kibar ของสาธารณรัฐอิรักซึ่งสำเร็จ โดยที่ไม่มีการต่อต้านจากระบบป้องกันภัยทางอากาศอันเป็นผลจากมัลแวร์ที่ถูกติดตั้งในโครงสร้างพื้นฐานฯ ที่เกี่ยวข้อง^๗

ต่อมาในปี ค.ศ.๒๐๐๙ ระบบสารสนเทศและการสื่อสารขององค์กรการบินพลเรือนแห่งสหรัฐฯ ถูกโจมตี ส่งผลกระทบต่อการเดินอากาศของสายการบินและเที่ยวบินทางทหาร ในปีเดียวกันนั้น กองทัพเรือฝรั่งเศสจำเป็นต้องยกเลิกเที่ยวบินทางทหารของกองทัพเรือ โดยเป็นผลจากการแพร่ระบาดของมัลแวร์ Downadup^๙ ทั้งนี้ มัลแวร์ชนิดนี้ถูกปรับปรุงคุณสมบัติจากมัลแวร์ Conficker ที่แพร่ระบาดนับตั้งแต่ปี ค.ศ.๒๐๐๘ ให้มีขีดความสามารถในการซ่อนพรางและป้องกันตนเองได้เป็นอย่างดี โดยผลจากการวิเคราะห์ซอร์ซโค้ดบ่งชี้ว่ามัลแวร์มีต้นกำเนิดมาจากสาธารณรัฐยูเครนและสาธารณรัฐประชาชนจีน โดยการแพร่ระบาดของมัลแวร์ดังกล่าวเป็นไปอย่างต่อเนื่องจนถึงปี ค.ศ.๒๐๑๔ จะเห็นว่าพัฒนาการของรูปแบบการโจมตีนับตั้งแต่ปี ค.ศ.๒๐๐๓ จนถึงปี ค.ศ.๒๐๑๐ มีรูปแบบการโจมตีและเป้าหมายการโจมตีที่เปลี่ยนแปลงไป นอกจากนี้ยังแสดงให้เห็นถึงผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติของกองกำลังมากขึ้นอย่างเห็นได้ชัด

เป้าหมายการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานของรัฐเป็นการเฉพาะเริ่มเป็นรูปธรรมมากยิ่งขึ้นในเหตุการณ์ที่เตาปฏิกรณ์นิวเคลียร์ในเมือง Natanz สาธารณรัฐอิสลามอิหร่าน ซึ่งตกเป็นเป้าหมายของการโจมตีจากมัลแวร์ที่ถูกออกแบบมาสำหรับการโจมตีต่อระบบระบายความร้อนของเตาปฏิกรณ์ที่ควบคุมด้วยระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งเป็นระบบที่ใช้ในการตรวจสอบ เก็บข้อมูล และควบคุมกระบวนการผลิตต่าง ๆ จากระยะไกลที่ถูกใช้งานทั่วโลก มัลแวร์ Stuxnet^{๑๐} เป็นมัลแวร์ที่ถูกพัฒนาขึ้นสำหรับปฏิบัติการนี้ เป็นหนอนอินเทอร์เน็ตที่มีความซับซ้อนและออกแบบให้โจมตีต่อระบบควบคุมเตาปฏิกรณ์นี้เป็นการเฉพาะ โดยถูกออกแบบให้แพร่กระจายตัวเองผ่าน USB แฟลชไดรฟ์ และระบบเครือข่ายและสร้างผลกระทบต่อระบบควบคุมเฉพาะที่ติดตั้งในระบบที่เมือง Natanz เท่านั้น ปฏิบัติการนี้ส่งผลให้เกิดความเสียหายทางกายภาพแก่อุปกรณ์และระบบควบคุมระบบปฏิกรณ์นิวเคลียร์ทำให้อิหร่านจำเป็นต้องปิดระบบปฏิกรณ์นิวเคลียร์และชะลอโครงการพัฒนาขีดความสามารถทางนิวเคลียร์ไประยะหนึ่ง สหรัฐฯ และอิสราเอลตกเป็นผู้ต้องสงสัยที่เกี่ยวข้องกับการพัฒนาและใช้มัลแวร์ดังกล่าวในการโจมตีต่อระบบปฏิกรณ์นิวเคลียร์ ซึ่งทั้งสหรัฐฯ และอิสราเอลปฏิเสธข้อกล่าวหาดังกล่าวอย่างสิ้นเชิง

ในปี ค.ศ.๒๐๑๒ มีนักวิจัยด้านความมั่นคงปลอดภัยรายงานตรวจพบช่องโหว่ที่ซ่อนอยู่ในโปรเซสเซอร์ Microsemi ProASIC3^{๑๑} ซึ่งเป็นไมโครโปรเซสเซอร์สำคัญที่ถูกติดตั้งในอากาศยานหลากหลายชนิดนับตั้งแต่เครื่องบินขับไล่ของกองทัพอากาศสหรัฐฯ ไปจนถึงเครื่องบินโบอิง 777 ของสายการบินพาณิชย์ อย่างไรก็ตาม บริษัทผู้ผลิตปฏิเสธว่าช่องโหว่ดังกล่าวเป็นคุณสมบัติสำหรับการตรวจแก้ไขบักของโปรเซสเซอร์นั้นที่ไม่ได้รับการเผยแพร่ด้วยความตั้งใจ เหตุการณ์ดังกล่าวสร้างความเคลือบแคลงใจในการใช้งานผลิตภัณฑ์ที่มีความซับซ้อนสูงเช่นนี้ โดยเฉพาะอย่างยิ่งการประยุกต์ใช้ในอุตสาหกรรมทางทหาร เนื่องจากช่องโหว่ลักษณะนี้อาจถูกใช้เป็นช่องทางในการโจมตีต่อระบบได้นั่นเอง

สาธารณรัฐประชาธิปไตยประชาชนเกาหลีหรือเกาหลีเหนือ ทำการโจมตีต่อศูนย์ข้อมูลกระทรวงกลาโหมสาธารณรัฐเกาหลีสำเร็จ^{๑๒} สามารถเข้าถึงเอกสารที่มีชั้นความลับที่มีขนาดรวมถึง ๒๓๕ กิกะไบต์ ซึ่งในจำนวนนั้นมีข้อมูลการวางแผนร่วมทางทหารระหว่างกองกำลังสหรัฐอเมริกาและสาธารณรัฐเกาหลี เมื่อปี ค.ศ.๒๐๑๖ โดยผลของการโจมตีในครั้งนั้นเป็นผลสำเร็จครั้งใหญ่ครั้งหนึ่งที่เกิดขึ้นจากความพยายามโจมตีต่อเป้าหมายทางทหาร และหน่วยงานเอกชนสำคัญของเกาหลีได้อย่างต่อเนื่องนับตั้งแต่ปี ค.ศ.๒๐๐๙

จากกรณีศึกษาสำคัญ ๆ ที่กล่าวมาจะเห็นว่า ไซเบอร์สเปซถูกรัฐต่าง ๆ นำมาใช้ประโยชน์ด้านความมั่นคงเสมือนเป็นอาณาเขตหนึ่งของรัฐ ซึ่งผลสัมฤทธิ์ของปฏิบัติการไซเบอร์ที่ผ่าน ๆ มามีแนวโน้มที่จะส่งผลกระทบโดยตรงต่อยุทธศาสตร์ความมั่นคงและปฏิบัติการทางทหารในระดับยุทธการอย่างเห็นได้ชัด จึงส่งผลให้รัฐต่าง ๆ ดำเนินนโยบายเพิ่มขีดความสามารถในการควบคุมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานระบบสารสนเทศภายใน ตลอดจนความพยายามพัฒนาขีดความสามารถเชิงรุกเพื่อสร้างความได้เปรียบบนไซเบอร์สเปซ^{๑๓}

๔. แนวโน้มการเปลี่ยนแปลงปฏิบัติการไซเบอร์

จากการพิจารณารูปแบบการโจมตีต่อระบบสารสนเทศและการสื่อสารในช่วงระยะเวลา ๑๐ ปีที่ผ่านมา สามารถอนุมานแนวโน้มการเพิ่มขีดความสามารถของการประยุกต์ใช้รูปแบบการโจมตีลักษณะดังกล่าวในปฏิบัติการไซเบอร์ได้ ดังนี้

แม้ว่าพัฒนาการการโจมตีที่มีความซับซ้อนและยากจะสามารถกระทำได้ในทางปฏิบัติ เช่น การโจมตีทางเครือข่ายต่อ UAV RQ-๑๗๐^{๑๔} ของสหรัฐฯ ซึ่งบินเหนือ่านฟ้าสาธารณรัฐอิสลามอิหร่าน เพื่อเปลี่ยนเส้นทางและนำร่อนลงเพื่อทำการวิศวกรรมย้อนกลับ (Reverse Engineer) นั้น มีโอกาสเกิดขึ้นน้อยกว่าการโจมตีที่มีความซับซ้อนน้อยกว่า เช่น DDoS ที่หวังผลเพียงแค่ทำให้เป้าหมายไม่สามารถให้บริการต่อผู้ใช้งานได้ เช่นเดียวกับเทคนิคการโจมตีโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารผ่านมัลแวร์ซอฟต์แวร์เรียกค่าไถ่ซึ่งโจมตีต่อช่องโหว่ด้านความมั่นคงปลอดภัยที่ถูกเปิดเผยเป็นสาธารณะ เนื่องจากการโจมตีบรรลุดำเนินการเสร็จและสร้างผลกระทบได้เร็ว ทันท่องสถานการณ์มากกว่า

ทั้งนี้ รูปแบบปฏิบัติการไซเบอร์ที่ส่งผลต่อโครงสร้างพื้นฐานทางกายภาพและการรับรู้ของประชาชนในประเทศเป้าหมายมีแนวโน้มเพิ่มขึ้นอย่างเห็นได้ชัด โดยเป็นผลจากความสำเร็จของมัลแวร์ Stuxnet ติดตามด้วยเหตุการณ์ที่มีลักษณะคล้ายคลึงกันจากการโจมตีด้วยอีเมลฟิชซิง ซึ่งนำเข้ามัลแวร์ BlackEnergy3 เข้าสู่โครงสร้างพื้นฐานระบบ SCADA ซึ่งควบคุมระบบไฟฟ้าของสาธารณรัฐยูเครน มัลแวร์ดังกล่าวทำงานโดยไม่ถูกตรวจพบได้นานถึง ๖ เดือน และสร้างความเสียหายทางกายภาพด้วยการโจมตีต่อระบบควบคุมการจ่ายพลังงานไฟฟ้า ทั้งนี้ การโจมตีลักษณะนี้สามารถป้องกันและลดผลสำเร็จของการโจมตีได้ด้วยการสร้างความตระหนักรู้ให้กับผู้ที่เกี่ยวข้องและประยุกต์ใช้แนวทางการบริหารจัดการโครงสร้างพื้นฐานอย่างมั่นคงปลอดภัย

ความก้าวหน้าของเทคโนโลยีปัญญาประดิษฐ์ (AI) จะส่งผลต่อขีดความสามารถของปฏิบัติการไซเบอร์ เช่น การพัฒนามัลแวร์หรือซอฟต์แวร์อัตโนมัติที่สามารถค้นหาและวิเคราะห์ช่องโหว่ รวมถึงทำการโจมตีต่อช่องโหว่ที่มีในระบบควบคุมบังคับบัญชา หรือการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการสร้างและเผยแพร่ข้อมูลข่าวสารที่เป็นเท็จ เพื่อสร้างผลกระทบต่อบรรณการข่าวกรอง การลงทางการข่าว ด้วยการสร้างข้อความหรือมัลติมีเดียที่ไม่มีอยู่จริงแต่ดูมีความน่าเชื่อถือ เนื่องจากสามารถผลิตซ้ำชุดข้อมูลดังกล่าวได้ในรูปแบบที่หลากหลายและมีแหล่งที่มาต่างกัน^{๑๕}

ความก้าวหน้าด้านวิทยาศาสตร์และเทคโนโลยี โดยเฉพาะอย่างยิ่งเทคโนโลยี เช่น ควอนตัมคอมพิวเตอร์ จะพลิกโฉมหลักนิยามปฏิบัติการไซเบอร์ อันเป็นผลจากขีดความสามารถในการคำนวณที่ส่งผลให้ขั้นตอนวิธีที่ใช้ในการรักษาความมั่นคงในปัจจุบันไม่สามารถทำงานได้อย่างมีประสิทธิภาพ สำหรับกองทัพชาติมหาอำนาจและมหาอำนาจระดับกลางมีแนวโน้มที่จะประยุกต์ใช้หุ่นยนต์ และแนวคิด “Soldier 4.0” ดังแสดงในภาพที่ ๘ ซึ่งนำเทคโนโลยีเข้ามาช่วยเสริมสร้างสมรรถนะของกำลังรบผ่านโครงสร้างภายนอก (Exoskeletons) ซึ่งเชื่อมต่อกับกำลังรบข้างเคียงผ่านเครือข่ายเฉพาะบริเวณ จะสามารถเพิ่มขีดความสามารถทางกายภาพให้หน่วยรบ กำลังทางเรือ และอากาศยาน ให้มีศักยภาพในการปฏิบัติการร่วมโดยใช้เครือข่ายเป็นศูนย์กลางได้อย่างสมบูรณ์



ภาพที่ ๘ Soldier 4.0 Concept

ที่มา : <https://nerdreactor.com/wp-content/uploads/2010/09/xos-2-main.jpg>

๕. ขีดความสามารถที่พึงประสงค์สำหรับ Cyber Defense ของกองทัพเรือ

กองทัพเรือพัฒนาขีดความสามารถด้านไซเบอร์อย่างต่อเนื่องตามยุทธศาสตร์กองทัพเรือ พ.ศ.๒๕๕๘ – พ.ศ.๒๕๖๗ อย่างไรก็ตาม หากทำการประเมินความพร้อมของโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร การปฏิบัติตามมาตรการ

รักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสาร รวมถึงการประเมินความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของกำลังพลในทัศนะของผู้เขียนแล้วพบว่า มีระดับต่ำกว่าที่พึงประสงค์ในทางปฏิบัติ สังเกตได้จากโครงสร้างพื้นฐานที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสาร ซึ่งเป็นรากฐานสำคัญของการป้องกันไซเบอร์สเปซ เช่น โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ซึ่งมีความจำเป็นอย่างยิ่งยวดต่อการพิสูจน์ตัวตนจริงของผู้ใช้งานในระบบต่าง ๆ ได้รับการพิจารณาความเร่งด่วนน้อยกว่าที่พึงจะเป็น นอกจากนี้ ความตระหนักรู้ของกำลังพลต่อภัยคุกคามทางไซเบอร์และความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารยังคงอยู่ในระดับต่ำกว่าที่ควรจะเป็นด้วยเช่นกัน โดยการพิจารณาและตั้งข้อสังเกตที่วัฒนธรรมการทำงานและความเพียงพอของโครงสร้างพื้นฐานฯ ที่จำเป็นต่อการปฏิบัติงานและการป้องกันภัยคุกคามต่อทรัพยากรสารสนเทศและการสื่อสารของกองทัพเรือ ในปัจจุบันจะพบว่าการเชื่อมต่ออุปกรณ์เข้ากับระบบเครือข่ายภายในกองทัพเรือสามารถกระทำได้ค่อนข้างสะดวก เนื่องจากมาตรการควบคุมการเข้าถึงทรัพยากรในระบบเครือข่ายค่อนข้างหละหลวม นอกจากนี้ ยังสามารถพบเห็นเครือข่ายไร้สายที่หน่วยติดตั้งไว้เพื่อความสะดวกในการเข้าถึงเครือข่ายอินเทอร์เน็ตและมีการเชื่อมต่อกับเครือข่ายภายในจึงอนุมานได้ว่าการเชื่อมต่ออุปกรณ์ต่าง ๆ เข้ากับเครือข่ายภายในกองทัพเรือ ซึ่งมีที่ตั้งหน่วยกระจายอยู่ทั่วประเทศเป็นไปอย่างไม่มั่นคงปลอดภัย เนื่องจากการพิสูจน์ตัวตนจริงเป็นไปอย่างจำกัด จึงมีความเสี่ยงที่จะถูกโจมตีจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอก ดังนั้น เพื่อลดผลเสียหายที่อาจเกิดขึ้น กองทัพเรือมีความจำเป็นอย่างยิ่งที่จะต้องประยุกต์ใช้โครงสร้างพื้นฐานที่จำเป็นสำหรับการพิสูจน์ตัวตนจริง การกำหนดสิทธิ์ในการเข้าถึงและบริหารจัดการทรัพยากรสารสนเทศอย่างมั่นคงปลอดภัยไปพร้อม ๆ กับการเสริมสร้างความตระหนักรู้และทักษะที่จำเป็นให้กับบุคลากรในทุกระดับของกองทัพเรือ อันจะเป็นหลักประกันเดียวที่ทำให้มั่นใจได้ว่า “ไซเบอร์สเปซ” ที่กองทัพเรือสามารถบริหารจัดการได้นั้น ได้รับการป้องกันอย่างเหมาะสม

- ๑ Andress J., Winterfeld S. (2013), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners: Second Edition.*, Waltham, MA 02451, USA, ISBN 978-0-12-416672-1
- ๒ Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70–94. <https://doi.org/10.1016/j.cose.2014.11.007>
- ๓ Wilailux, Korakoch, (2019), *The Kinetic Effect of Cyberwar*,
- ๔ Elliott C.. (2010), Botnets: To what extent are they a threat to information security? *Information Security Technical Report*, 15 (3), pp.79–103. <https://doi.org/10.1016/j.istr.2010.11.003>
- ๕ Koch, R., & Golling, M. (2018). The cyber decade: Cyber defence at a X-ing point. 2018 10th International Conference on Cyber Conflict (CyCon), 2018-May, pp.159–186, <https://doi.org/10.23919/CYCON.2018.8405016>
- ๖ S, Michael N (Gen. ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, United States of America: Cambridge University Press.
- ๗ S. Adee.(2008) , “The hunt for the kill switch” , *IEEE Spectrum*, Vol.45 No.5, pp.34-39, <https://doi.org/10.1109/MSPEC.2008.4505310>
- ๘ Marks, P. (2011). “Air traffic system vulnerable to cyber-attack”. *New Scientist*. Vol. 211 No. 2829, pp. 22-23.
- ๙ D. Cenciotti (2009). “French Navy Rafales grounded by a computer viru”. *The Aviationist*. Available at <https://theaviationist.com/2009/02/13/french-navy-rafales-grounded-by-a-computer-virus/>
- ๑๐ Shin, J., Son, H., Khalil ur, R., & Heo, G. (2015). Development of a cyber-security risk model using Bayesian networks. *Reliability Engineering & System Safety*, 134, 208–217. <https://doi.org/10.1016/j.res.2014.10.006>

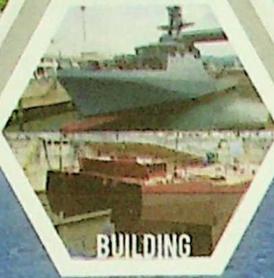
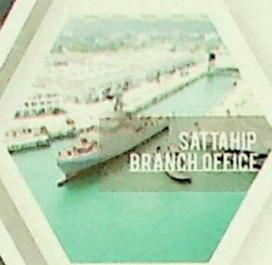
- ๑๑ Skorobogatov, S. and Woods, C. (2012). “Breakthrough silicon scanning discovers backdoor in military chip”. International Workshop on Cryptographic Hardware and Embedded Systems. Available
- ๑๒ Kshetri, N. (2014). Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses. *East Asia*, 31(3), 183–201. <https://doi.org/10.1007/s12140-014-9215-1>
- ๑๓ Darko Galinec, Darko Možnik & Boris Guberina (2017) Cybersecurity and cyber defence: national level strategic approach, *Automatika*, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022
- ๑๔ Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J.C.H.; and Carter, Candice, (2018), «Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA’s Advanced Air Assets» NPP Book
- ๑๕ Rod Thornton & Marina Miron (2020) Towards the ‘Third Revolution in Military Affairs’, *The RUSI Journal*, 165:3, 12-21, DOI:10.1080/03071847.2020.1765514





THE BANGKOK DOCK COMPANY (1957) LIMITED

A STATE-OWNED ENTERPRISE
UNDER THE OVERSIGHT OF THE MINISTRY OF
BY THE ROYAL THAI NAVY



รัฐวิสาหกิจในความควบคุมดูแลของกองทัพเรือ สังกัดกระทรวงกลาโหม
Stata Enterprise, Controlled by Royal Thai Navy, Ministry of Defense

ที่อยู่ : 174/1 ถนนเจริญกรุง แขวงยานนาวา เขตสาทร กรุงเทพฯ 1

โทร: 02-3078576 แฟกซ์ : 2-3078576

การใช้ AI ในสวดรามอนาคต

บทอาโท ดร.มนต์ชัย บุญยกิจตานนท์
หัวหน้านโยบายและยุทธศาสตร์
กองนโยบายและแผน สำนักนโยบายและแผน
กรมการสื่อสารและเทคโนโลยีสารสนเทศสหการเรือ

บทคัดย่อ

การรบในอนาคตมีแนวโน้มที่จะเป็นสงครามที่มีการปฏิบัติการหลากหลายมิติ (Multidomain Operations: MDO) ซึ่งเป็นปฏิบัติการทางทหารในยุคใหม่ที่มีความซับซ้อนและเปลี่ยนแปลงง่าย ต้องการความเร็วสูง และการเชื่อมต่ออุปกรณ์และระบบอำนาจการรบในหลากหลายมิติ ตั้งแต่พื้นดิน พื้นน้ำ ห้วงอากาศ ห้วงอวกาศ และห้วงไซเบอร์ ปฏิบัติการนี้จะอาศัยระบบอัตโนมัติและเครือข่าย รวมถึงเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นปัจจัยสำคัญสำหรับการนำ AI มาใช้ในทางทหารนี้ไม่ได้จำกัดอยู่แค่เพียงในสถานการณ์ฉุกเฉินหรือภาวะสงครามเท่านั้น แต่ยังสามารถนำมาใช้ประโยชน์ในด้านอื่น ๆ เนื่องจากหน่วยงานความมั่นคงของรัฐมีภารกิจทั้งในยามสงบและยามสงคราม ทั้งในเรื่องการเตรียมความพร้อม การบริหารจัดการ การวิจัยพัฒนา เป็นต้น นอกจากนี้ยังมีภารกิจอื่น ๆ เช่น การบรรเทาสาธารณภัย การควบคุมโรค ฯลฯ ที่สามารถนำ AI มาช่วยในการปฏิบัติได้ทั้งสิ้น อย่างไรก็ตาม AI ยังถือเป็นเรื่องใหม่ของกองทัพ ดังนั้น ในบทความนี้จะมุ่งเน้นการเสริมสร้างความเข้าใจในเทคโนโลยี AI โดยกล่าวถึงเทคโนโลยี AI ในปัจจุบัน แนวทางการนำมาใช้ในหน่วยงานความมั่นคง และการเปลี่ยนแปลงที่จะเกิดขึ้นเมื่อมีการนำ AI มาใช้ในการรบ

บทนำ

เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นเทคโนโลยีสำคัญที่จะช่วยเพิ่มความสามารถทางปัญญาของเครื่องจักรให้เลียนแบบมนุษย์ ทำให้เครื่องจักรสามารถ รับรู้ เรียนรู้ ใช้เหตุผล หรือตัดสินใจจากชุดข้อมูลที่มีอยู่ได้โดยปราศจากการแทรกแซงจากมนุษย์ ด้วยความสามารถทางปัญญาของเครื่องจักรนี้ ทำให้องค์กรต่าง ๆ ทั้งหน่วยงานของรัฐและภาคเอกชนต่างพยายามนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในองค์กรของตน เพื่อช่วยลดภาระงาน เพิ่มประสิทธิภาพในการทำงาน สร้างความพึงพอใจให้กับผู้มีส่วนได้ส่วนเสีย หรือสร้างความได้เปรียบทางธุรกิจ ซึ่งในปัจจุบันมี AI ที่ได้ถูกนำไปใช้

อย่างแพร่หลายในชีวิตประจำวันบ้างแล้ว โดยสามารถยกตัวอย่างการใช้งาน AI ที่ผู้คนต่างคุ้นเคยกันดี เช่น ระบบนำทาง ระบบแนะนำภาพยนตร์หรือสินค้า ระบบสแกนใบหน้า เป็นต้น อย่างไรก็ตาม การพัฒนา AI ในปัจจุบันนั้นยังอยู่ในช่วงเริ่มต้นที่ยังมีช่องว่างในการพัฒนา AI อีกมาก ซึ่งการพัฒนา AI มักมีวัตถุประสงค์เพื่อให้เครื่องจักรทำงานแทนมนุษย์ รวมทั้งเพื่อเพิ่มประสิทธิภาพให้กับงานบางอย่างเท่านั้น ซึ่งนับเป็นเพียง AI ในระดับต้น ที่ยังสามารถถูกพัฒนาให้มีขีดความสามารถในวางแผนเพื่อแก้ไขปัญหาต่าง ๆ สามารถเรียนรู้จากประสบการณ์ในอดีต และใช้เหตุผลได้ดีขึ้น นอกจากนี้เรายังสามารถนำ AI เฉพาะด้านต่าง ๆ เหล่านี้มาบูรณาการให้เป็นระบบที่สามารถทำงานแทนมนุษย์โดยสมบูรณ์

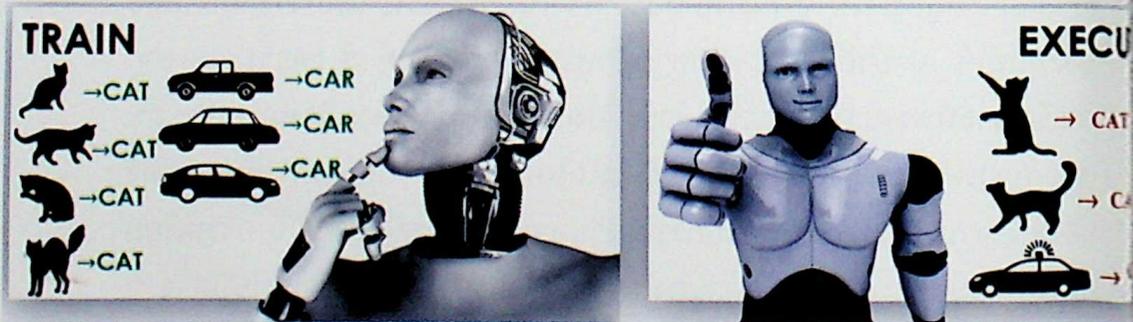
การนำ AI มาใช้งานด้านความมั่นคงนั้น สามารถนำมาประยุกต์ใช้ในกิจการทหารได้แทบทุกกิจกรรม ซึ่งครอบคลุมการปฏิบัติการทางทหารในทุกมิติ ทั้งทางบก ทางน้ำ ทางอากาศ ทางอวกาศ และไซเบอร์ สำหรับหน่วยใช้กำลังสามารถใช้ในการปฏิบัติการ เช่น การลาดตระเวนตรวจการณ์ การรักษาความปลอดภัยหน่วย ในส่วนฝ่ายอำนวยการรบ สามารถใช้ในการภารกิจ เช่น การวิเคราะห์พฤติกรรม และสำหรับหน่วยสนับสนุน สามารถใช้ในการคาดการณ์ยานพาหนะที่ต้องได้รับการบำรุงรักษา เป็นต้น นอกจากนี้ AI ยังสามารถนำมาใช้ในการบริหารจัดการ งานธุรการของหน่วยงานต่าง ๆ ได้เป็นอย่างดี เช่น การแปลงภาพเป็นตัวอักษร จากตัวอย่างข้างต้นจะเห็นได้ว่า AI สามารถถูกนำไปใช้ได้ในทุกส่วนอย่างเป็นรูปธรรม แต่การพัฒนาและประยุกต์ใช้ AI ยังถือเป็นโจทย์ยากสำหรับแทบทุกองค์กร เพราะนอกจากการวิเคราะห์หา AI ที่เหมาะสมแล้วยังต้องเผชิญความท้าทายอีกหลายประเด็น เช่น การเตรียมข้อมูล การกระตุ้นให้เกิดการยอมรับความเปลี่ยนแปลงของพนักงาน การปรับกระบวนการทำงานตามเทคโนโลยีที่นำมาใช้ การเตรียมความพร้อมของบุคลากรในด้านองค์ความรู้ การปรับหรือแก้ระเบียบต่าง ๆ ให้เหมาะสม ในบางองค์กรยังอาจรวมไปถึงการสร้างความร่วมมือ และการบูรณาการกับหน่วยงานหรือองค์กรอื่น ๆ ทั้งในและต่างประเทศ ถึงแม้

การพัฒนาและประยุกต์ใช้ AI จะมีปัญหาและอุปสรรคดังกล่าว องค์กรต่าง ๆ โดยเฉพาะอย่างยิ่งองค์กรด้านความมั่นคงก็ยังคงมีความจำเป็นที่จะต้องนำ AI มาใช้ เนื่องจากหากไม่เริ่มเรียนรู้หรือทำความเข้าใจ AI ในตอนนี้ อาจส่งผลเสียหายอย่างร้ายแรงในอนาคต

๑ AI คืออะไร

หนังสือเทคโนโลยีปัญญาประดิษฐ์สำหรับการบริหารงานและการบริการภาครัฐ ได้นิยามเทคโนโลยี AI ไว้ว่า “AI หรือ ปัญญาประดิษฐ์ (Artificial Intelligence) เป็นเทคโนโลยีการสร้างความสามารถให้แก่เครื่องจักรและคอมพิวเตอร์ด้วยอัลกอริทึมและกลุ่มเครื่องมือ ทางสถิติ เพื่อสร้างซอฟต์แวร์ทรงปัญญาที่สามารถเลียนแบบความสามารถของมนุษย์ที่ซับซ้อนได้ เช่น จดจำ แยกแยะ ให้เหตุผล ตัดสินใจ คาดการณ์ และสื่อสารกับมนุษย์ เป็นต้น ในบางกรณีอาจไปถึงขั้นเรียนรู้ได้ด้วยตนเอง”

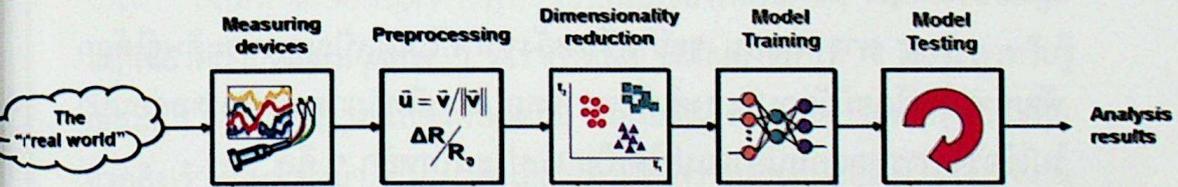
จากนิยามข้างต้นจะเห็นได้ว่า AI นั้นเปรียบเหมือนสมองของเครื่องจักรที่ถูกสอนให้เรียนรู้แบบมนุษย์นั่นเอง ยกตัวอย่างดังภาพที่ ๑ ที่แสดงทักษะทางด้านการมองเห็นนั้น มนุษย์จะมองเห็นแมวทางสายตา และสามารถจดจำแมวนั้นได้ ถึงแม้ว่าแมวจะเปลี่ยนจากทำนองเป็นยืน รวมทั้งสามารถจดจำลักษณะของแมวได้แม้ว่าจะเห็นแมวตัวอื่นก็ตาม แต่เครื่องจักรนั้นจะสามารถจดจำได้เฉพาะรูปแมวในนั้นเท่านั้น ไม่สามารถจดจำตัวแมวในรูปนั้นได้



ภาพที่ ๑ การเรียนรู้ทักษะการมองเห็นของเครื่อง

หากเปลี่ยนเอารูปแนวตัวเดียวกันในทำอื่นมาใช้ เครื่องจักรก็ไม่สามารถบอกว่า เป็นแนวได้ ดังนั้น จึงต้องมีการสอนให้เครื่องจักรเรียนรู้ลักษณะสำคัญของแนว เพื่อที่จะสามารถจดจำแนวได้

ในการเรียนรู้ของเครื่องจักรจะต่างจากการเรียนรู้ของคน เนื่องจาก คนมีขีดความสามารถในการจดจำและมีความคิด ส่วนเครื่องจักรจะมีเพียง ขีดความสามารถในการจดจำเท่านั้น นอกจากนี้ข้อมูลที่เครื่องจักรได้รับ ก็เป็นชุดข้อมูลทางคณิตศาสตร์ ซึ่งต่างจากคนที่จดจำเป็นรูปภาพ ดังนั้น จึงต้องใช้วิธีการสอนเครื่องจักรที่ต่างออกไป โดยจะมีขั้นตอนหลัก อยู่ ๕ ขั้นตอนดังภาพที่ ๒



ภาพที่ ๒ ขั้นตอนการเรียนรู้ของเครื่อง

๑.๑ การรวบรวมข้อมูล เป็นขั้นตอนแรกของการเรียนรู้ของเครื่อง ข้อมูลที่จะนำมาใช้ในการเรียนรู้สามารถมาได้จากหลายแหล่ง เช่น ข้อมูลจาก เซ็นเซอร์ต่าง ๆ ข้อมูลจากการบันทึก ข้อมูลสถิติ เป็นต้น จากข้อมูลต่าง ๆ ที่มีมากมายเหล่านี้จำเป็นต้องมีกระบวนการคัดเลือกเฉพาะข้อมูลที่เกี่ยวข้อง เพื่อนำมาใช้ต่อไป

๑.๒ การดำเนินการวิธีข้อมูล จะกระทำเมื่อข้อมูลได้ผ่านการคัดเลือก มาแล้ว ข้อมูลเหล่านั้นจะถูกนำมาเตรียมสำหรับให้เครื่องเรียนรู้ ซึ่งต้องมีการดำเนินการหลายขั้นตอน เช่น จัดรูปแบบข้อมูลให้เหมาะสม ตรวจสอบ ความถูกต้องของข้อมูล นำข้อมูลที่ผิดพลาดหรือเพี้ยนออก ใส่ข้อมูลที่ขาดหาย เพิ่มเติม การติดป้ายกำกับ เป็นต้น

๑.๓ การเลือกข้อมูล จะดำเนินการหลังจากมีข้อมูลที่พร้อมแล้ว โดยจะคัดเลือกเฉพาะคุณสมบัติที่เกี่ยวข้อง ไม่ใช่ข้อมูลทั้งหมด มาใช้ในการป้อนข้อมูลในอัลกอริทึมการเรียนรู้ ยกตัวอย่างเช่น ในการเรียนรู้จดจำใบหน้า จะเริ่มต้นจากการค้นหาใบหน้าในรูปนั้นก่อน แล้วค่อยเรียนรู้ว่าใบหน้านั้นคือใคร จากคุณสมบัติเฉพาะทางกายภาพของบุคคลนั้น เช่น รูปทรงใบหน้า ระยะห่างระหว่างคิ้ว ลักษณะดวงตา เป็นต้น

๑.๔ การเรียนรู้ เป็นขั้นตอนสำคัญที่ให้ผลผลิตเป็นโมเดลปัญญาประดิษฐ์ การทำงานของขั้นตอนนี้จะเกิดขึ้นหลังจากป้อนข้อมูลเข้าสู่อัลกอริทึมแล้ว ข้อมูลเหล่านั้นจะถูกนำมาใช้ในการสอนเครื่องจักรตามรูปแบบอัลกอริทึมที่ได้เลือกไว้ทีละชุด ๆ จนหมด

๑.๕ การทดสอบ จะเกิดขึ้นหลังจากที่โมเดลปัญญาประดิษฐ์ได้ถูกพัฒนาแล้ว โดยมีวัตถุประสงค์เพื่อตรวจสอบประสิทธิภาพของโมเดลก่อนนำไปใช้จริง การทดสอบนี้อาจแบ่งได้เป็น ๒ ประเภทหลัก ๆ คือ

๑.๕.๑ การทดสอบในระหว่างการพัฒนาโมเดลปัญญาประดิษฐ์ การทดสอบนี้เป็นการทดสอบมาตรฐานที่ใช้กันทั่วไป ซึ่งจะแบ่งข้อมูลที่ได้เตรียมไว้ออกเป็น ๒ ส่วน คือ ส่วนที่ใช้สำหรับการเรียนรู้และส่วนที่ใช้ในการทดสอบ โดยผู้พัฒนาเป็นคนกำหนดอัตราส่วนข้อมูลในการเรียนรู้และทดสอบเอง ทั้งนี้ ได้มีรูปแบบการแบ่งอัตราส่วนที่นิยม ได้แก่ การแบ่งแบบ 10-fold ซึ่งแบ่งข้อมูลออกเป็น ๑๐ ส่วน โดยจะใช้ในการเรียนรู้ ๙ ส่วน ใช้ในการทดสอบ ๑ ส่วน และดำเนินการเรียนรู้จำนวน ๑๐ รอบ โดยแต่ละรอบจะใช้ชุดข้อมูลในการทดสอบต่างกันโดยเริ่มที่ชุดทดสอบที่ ๑ จนครบชุดที่ ๑๐

๑.๕.๒ การทดสอบในสภาพแวดล้อมการทำงานจริง เป็นการนำผลผลิตโมเดลปัญญาประดิษฐ์ที่ได้ไปใช้ในสภาพแวดล้อมจริงเพื่อตรวจสอบประสิทธิภาพการทำงานของโมเดลนั้น ๆ ในการพัฒนาโมเดลหนึ่ง อาจมีการทดสอบโดยวิธีนี้หรือไม่ก็ได้ เนื่องจากขึ้นอยู่กับความต้องการของผู้ผลิตผู้ใช้และขีดความสามารถในการวัดผลของระบบที่โมเดลนั้นถูกนำไปใช้จริง

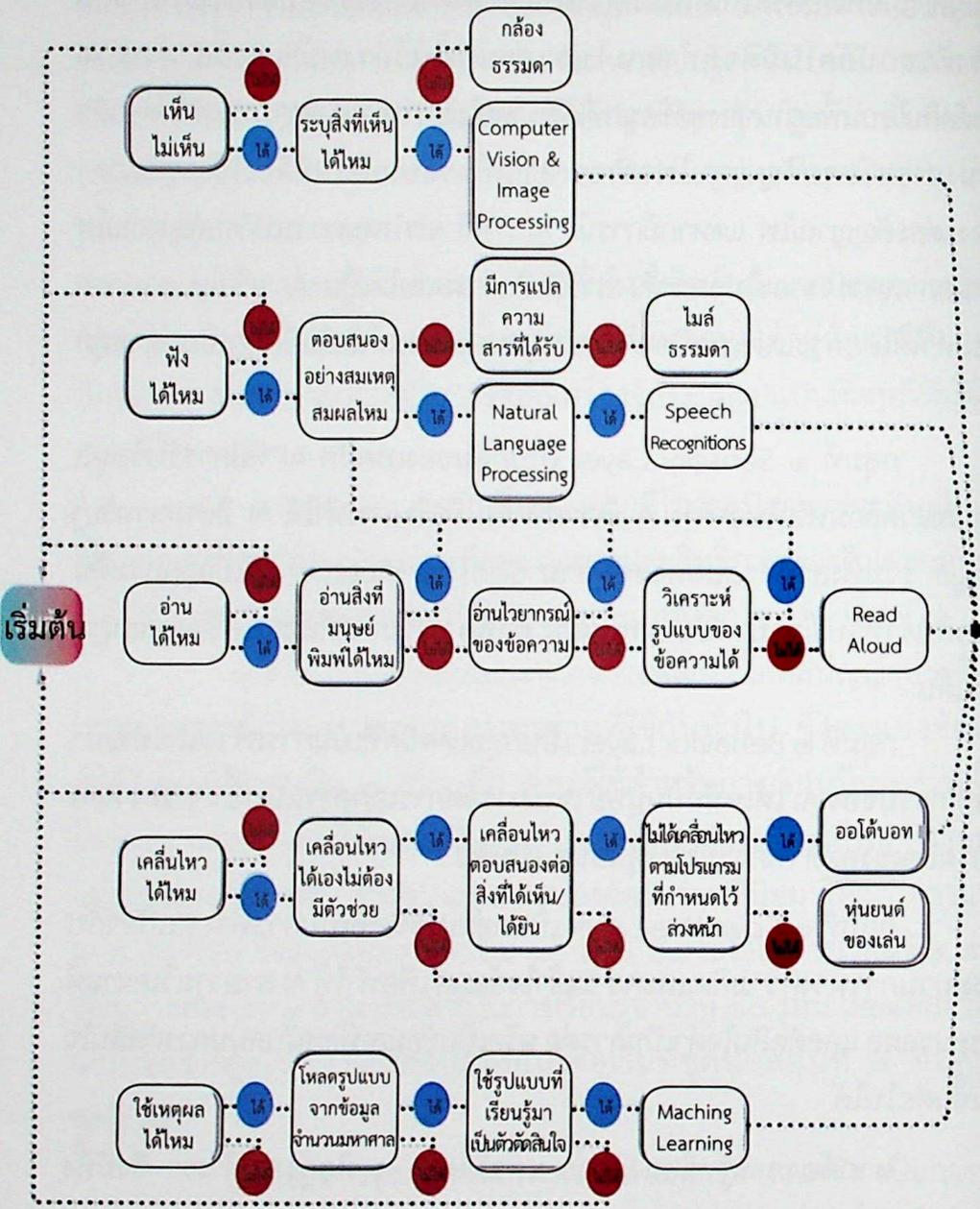
ในปัจจุบันคำว่า AI ได้ถูกนำมาใช้อย่างแพร่หลาย และมีหลายกรณีที่มีผู้เข้าใจผิดเรียกระบบอัตโนมัติว่าเป็น AI ซึ่งทั้งสองระบบมีความแตกต่างกันตรงที่ระบบอัตโนมัติจะทำตามโปรแกรมที่ตั้งไว้ล่วงหน้าเท่านั้น ส่วน AI จะตัดสินใจบนพื้นฐานของชุดข้อมูลที่ได้รับ โดยไม่มีการกำหนดการกระทำไว้ตายตัว เช่น การควบคุมสัญญาณไฟจราจร หากเป็นระบบอัตโนมัติจะใช้เวลาตั้งเวลาของแต่ละสัญญาณไฟ แต่หากมีการนำ AI มาใช้ จะกำหนดการเปลี่ยนสัญญาณไฟตามสภาพการจราจรในขณะนั้น การตัดสินใจว่าระบบใดเป็น AI หรือไม่ สามารถกระทำได้โดยการแบ่งเทคนิค AI ตามมุมมองของเทคโนโลยีออกเป็น ๓ กลุ่มดังนี้

กลุ่มที่ ๑ Sensory Layer เป็นกลุ่มของเทคนิค AI ที่มีการรับข้อมูลจากสิ่งแวดล้อมหรือในจุดต่าง ๆ ที่เรากำหนด ซึ่งเป็นการทำให้ AI มีประสาทรับรู้ข้อมูล รวมทั้งสามารถแสดงออกตาม Sensory Feeling ได้เมื่อถูกกระตุ้นจากสิ่งเร้าที่รับรู้เข้ามา เช่น ภาพ เสียง คำพูด การมองเห็นของเครื่องอูณหภูมิตั้งเป็นต้น

กลุ่มที่ ๒ Behavior Layer เป็นกลุ่มเทคนิคที่เน้นการสร้างและพัฒนาพฤติกรรมของ AI ให้เหมือนมนุษย์ เช่น การจัดการเอกสารแบบซ้ำ ๆ ของ RPA การผลิตเชิงอุตสาหกรรมของหุ่นยนต์ เป็นต้น

กลุ่มที่ ๓ Cognitive Layer เป็นกลุ่มเทคนิคที่เน้นการทำงานเกี่ยวกับกระบวนการทางความคิดและความเข้าใจข้อมูล เพื่อให้ AI สามารถวิเคราะห์ประมวลผล และตัดสินใจดำเนินการต่อ หรือเป็นข้อมูลเพื่อสนับสนุนการตัดสินใจในขั้นต่อไปได้

หากต้องการรู้หรือสงสัยว่า แล้วสิ่งต่าง ๆ ที่อยู่รอบตัวเรา ซึ่งมีทั้งเทคโนโลยี นวัตกรรม สิ่งประดิษฐ์ หรืออุปกรณ์ดิจิทัลเป็น AI หรือไม่ สามารถใช้ภาพที่ ๓ เป็นผังการวิเคราะห์ AI



ภาพที่ ๓ การวิเคราะห์ขีดความสามารถของเครื่องว่าเป็น AI หรือไม่
 ที่มา : ปรีชาพล ชูศรี และคณะ, พศศกิจจานุ ๒๕๖๒, หน้า ๕๕

จากภาพจะแบ่งการวิเคราะห์ออกเป็น ๕ หัวข้อ คือ ๑. เห็น ๒. ฟัง ๓. อ่าน ๔. เคลื่อนไหว ๕. ใช้เหตุผล ในแต่ละหัวข้อจะมีจำนวนขั้นในการประเมินแตกต่างกันไปโดยเริ่มจากการตรวจสอบความสามารถขั้นพื้นฐานไปจนถึงขั้นประยุกต์หรือใกล้เคียงความสามารถของมนุษย์ ทำให้สามารถแยกแยะเทคโนโลยีในปัจจุบันว่าเป็น AI หรือไม่

๒. การแบ่งประเภทของ AI

เพื่อให้เกิดความเข้าใจและสามารถศึกษา AI ในเชิงลึกนั้น มีความจำเป็นต้องเรียนรู้ประเภทของเทคโนโลยีนี้ เนื่องจาก AI นั้นสามารถแบ่งประเภทได้หลากหลายรูปแบบ และในแต่ละรูปแบบมีความแตกต่างกันทั้งขีดความสามารถของชุดอัลกอริทึม ทฤษฎีที่เกี่ยวข้อง การเตรียมชุดข้อมูล และการนำไปใช้ หากใช้เกณฑ์ความสามารถของ AI ในปัจจุบันนั้น สามารถแบ่งออกได้เป็น ๖ ประเภท ดังนี้

๒.๑ ความสามารถในการเรียนรู้ของเครื่อง (Machine Learning: ML) เป็นความสามารถในการเรียนรู้และวิเคราะห์ข้อมูลของเครื่องคอมพิวเตอร์ เพื่อพยากรณ์ผลลัพธ์ โดยผลลัพธ์ที่ได้จะแบ่งออกเป็น ๒ รูปแบบใหญ่ ๆ คือ การจัดหมวดหมู่ (Classification) และการพยากรณ์ตัวเลข (Regression) มีเทคนิคย่อยที่สำคัญ ๔ รูปแบบ คือ Supervised, Unsupervised, Semi-Supervised และ Reinforcement ที่มีความแตกต่างกันด้วยอัลกอริทึมการเรียนรู้ ข้อมูลที่กำหนดให้เรียนรู้ และวัตถุประสงค์ในการใช้งาน

๒.๒ ความสามารถในการประมวลผลภาษาธรรมชาติ (Natural Language Processing: NLP) เป็นเทคนิคที่ทำให้เครื่องเข้าใจภาษามนุษย์ โดยมีกระบวนการหลักคือ การตัดคำและตีความ ซึ่งแตกต่างจากการแปลตามพจนานุกรมเพราะจะต้องมีการนำบริบทแวดล้อมมาประกอบการพิจารณาด้วย NLP จะเพิ่มความสามารถในการวางแผน (Automated Planning, Scheduling & Optimization) เป็นการทำให้เครื่องสามารถตัดสินใจและเลือกการดำเนินงานที่บรรลุเป้าหมายอย่างมีประสิทธิภาพ

๒.๓ ความสามารถในการวิเคราะห์แบบผู้เชี่ยวชาญ (Expert System) เป็นเทคนิคการเลียนแบบความสามารถในการตัดสินใจแบบมนุษย์ การตัดสินใจ

ดังกล่าวจะนำข้อมูลที่ได้รับจากแหล่งต่าง ๆ มาทำการวิเคราะห์ ประเมินสถานการณ์ และตกลงใจ ความสามารถในด้านนี้มีความซับซ้อนและพัฒนาได้ยาก เนื่องจากการเรียนรู้จะเกิดจากการประเมินความถูกต้องและความผิดพลาดในการตัดสินใจที่ไม่มีเกณฑ์ชัดเจนและเป็นมาตรฐาน ซึ่งขึ้นอยู่กับปัจจัยหลายอย่าง ทั้งที่ควบคุมได้และควบคุมไม่ได้ เช่น ชุดข้อมูลที่ได้รับ แนวทางการตัดสินใจ และเกณฑ์การประเมินค่าประสิทธิภาพในการตัดสินใจ เป็นต้น

๒.๔ ความสามารถในการรู้จำคำพูด (Speech) เป็นเทคนิคการทำให้เครื่องรู้จำเสียงพูดและโครงสร้างภาษาของมนุษย์ และวิเคราะห์ข้อมูลจากเสียงนั้น ในการทำงานนั้นระบบจะรับเสียงจากไมโครโฟนหรือไฟล์เสียงแล้วแปลงออกมาเป็นคำพูด ในทางกลับกันระบบก็สามารถแปลงคำพูดที่เป็นตัวพิมพ์ออกมาเป็นเสียงได้เช่นกัน ทำให้เครื่องจักรหรือหุ่นยนต์สามารถรับคำสั่งหรือโต้ตอบด้วยภาษามนุษย์ได้

๒.๕ Computer Vision เป็นเทคนิคทำให้เครื่องจักรมองเห็นและเข้าใจโครงสร้างภาพเพื่อวิเคราะห์ข้อมูลจากภาพได้ โดยอาศัยกระบวนการต่าง ๆ เช่น การรู้จำแบบ การเรียนรู้เชิงสถิติ เรขาคณิตเชิงภาพฉาย การประมวลผลภาพ ทฤษฎีกราฟ และอื่น ๆ มาเชื่อมโยงกันเป็นโครงข่ายประสาทเทียม ปัจจุบันมีการใช้งานเทคนิคด้านนี้อย่างเป็นรูปธรรม เช่น การตรวจจับ ตัดแบ่งขอบเขตระบุตำแหน่ง การรู้จำ การติดตามวัตถุที่ต้องการในภาพ การประเมินการณ์ท่วงท่าของมนุษย์ เป็นต้น

๒.๖ วิทยาการหุ่นยนต์ (Robotics) เป็นสาขาวิชาที่พัฒนาเครื่องยนต์ให้มีรูปร่างและเคลื่อนไหวได้แตกต่างกันไปตามวัตถุประสงค์การใช้งานที่ศึกษาเกี่ยวกับการออกแบบ การผลิต การควบคุม และการประยุกต์ใช้งานหุ่นยนต์ หุ่นยนต์สามารถประยุกต์ใช้ได้หลากหลายสถานการณ์ และใช้งานได้หลากหลายวัตถุประสงค์ เช่น การช่วยเหลือมนุษย์ในการทำงานในชีวิตประจำวัน การทำงานที่เป็นอันตรายหรือทำงานในสภาวะแวดล้อมที่มนุษย์ไม่สามารถมีชีวิตอยู่ได้ เป็นต้น

๒.๗ นอกจากนี้ในแต่ละความสามารถข้างต้น ยังสามารถจัดระดับการเรียนรู้ของเครื่องจักร แบ่งออกได้เป็น ๓ ระดับ คือ

๒.๗.๑ Machine Learning (ML) เป็นชุดอัลกอริทึมที่เครื่องจักรสามารถเลียนแบบมนุษย์อย่างง่ายจากชุดข้อมูลที่ได้รับ ในปัจจุบัน Machine Learning ในระดับนี้มักจะเป็นทักษะที่เกี่ยวข้องกับการเลียนแบบประสาทสัมผัส หรือ การตัดสินใจอย่างง่าย เช่น ตรวจสอบใบหน้า การจัดหมวดหมู่สิ่งของ เป็นต้น

๒.๗.๒ Machine Intelligence (MI) ใช้เทคนิคขั้นสูงขั้นที่พบได้มากขึ้น ในปัจจุบัน การพัฒนาเหล่านี้ทำให้เครื่องจักรมีความสามารถที่สูงขึ้น เช่น การตรวจจับใบหน้าที่แม่นยำขึ้น ความสามารถในการค้นพบคุณสมบัติที่จะใช้ในการแบ่งแยกหมวดหมู่โดยอัตโนมัติ ซึ่งต่างจาก ML ที่จำเป็นต้องได้รับข้อมูลเหล่านี้จากผู้ให้ข้อมูลโดยตรง

๒.๗.๓ Machine Consciousness (MC) เป็นการพัฒนา AI ในระดับสูงสุด ซึ่งถ้า AI ในระดับนี้มีขึ้นอย่างเต็มรูปแบบ จะสามารถนำข้อมูลต่าง ๆ มาเชื่อมโยงกัน คล้ายกับสมองของมนุษย์ ทำให้มีขีดความสามารถในการคิด วิเคราะห์ และตัดสินใจอย่างมีเหตุผล แบบมนุษย์

๓. การนำ AI มาใช้ในกองทัพเรือ

ตามวิสัยทัศน์ของกองทัพเรือที่ว่า “เป็นหน่วยงานความมั่นคงทางทะเล ที่มีบทบาทนำในภูมิภาคและเป็นเลิศในการบริหารจัดการ” จึงได้มีการกำหนดพันธกิจเพื่อให้บรรลุวิสัยทัศน์ดังกล่าวจำนวน ๔ ด้าน ได้แก่

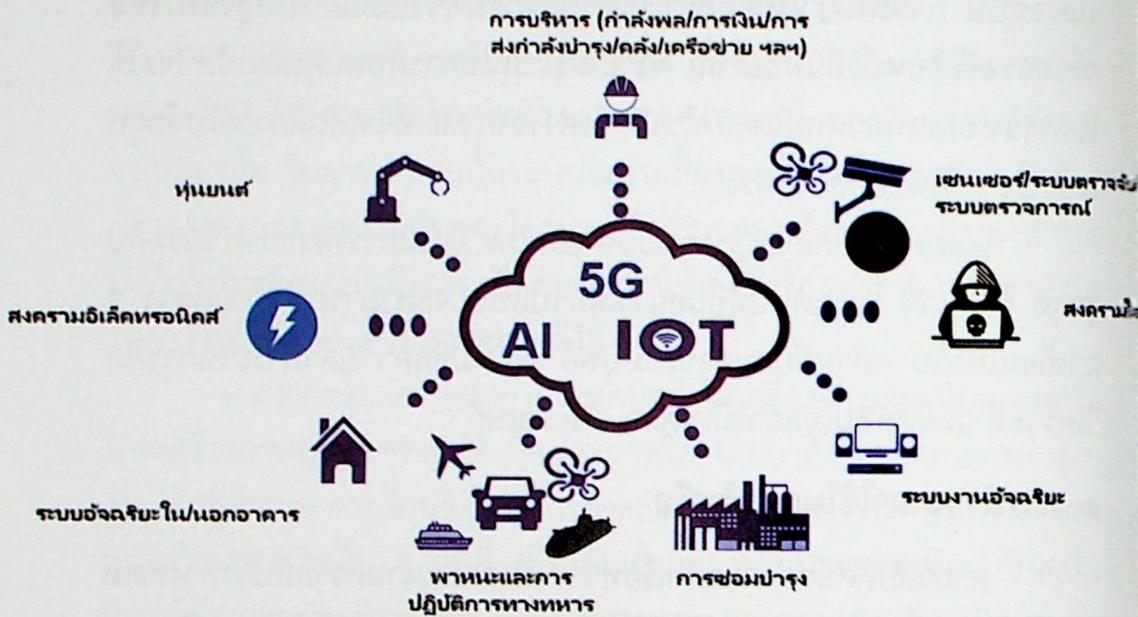
๓.๑ จัดเตรียมกำลังพล ยุทธโศปกรณ์และระบบการส่งกำลังบำรุงที่สมดุลงกะทัดรัดและทันสมัย เพื่อดำรงความพร้อมรบในการป้องกันประเทศและคุ้มครองรักษาผลประโยชน์ของชาติทางทะเล

๓.๒ ใช้กำลังทางทหารเพื่อการรักษาอธิปไตย และผลประโยชน์ของชาติทางทะเล การถวายความปลอดภัยและถวายพระเกียรติสถาบันพระมหากษัตริย์ รวมทั้งการปฏิบัติการกิจ ทางทหารอื่น ๆ ตามที่ได้รับมอบ

๓.๓ ใช้ศักยภาพและขีดความสามารถของกองทัพเพื่อสนับสนุนรัฐบาลในการพัฒนาประเทศ การแก้ไขปัญหาสังคม การช่วยเหลือประชาชน และการบรรเทาสาธารณภัย

๓.๔ บริหารจัดการกองทัพภายใต้กรอบการบริหารกิจการบ้านเมืองที่ดี

๓.๕ จะเห็นได้ว่าการปฏิบัติงานของกองทัพเรือ นั้น ไม่ได้จำกัดอยู่ที่มิติความมั่นคงทางทะเลเพียงอย่างเดียวเท่านั้น แต่ยังมีภารกิจในการปฏิบัติงานด้านอื่น ๆ เช่น การให้บริการสาธารณสุขของรัฐ การสนับสนุนรัฐบาลในการพัฒนาประเทศ การปฏิบัติตามภารกิจเฉพาะ การบริหารจัดการภาครัฐ เป็นต้น ซึ่งสามารถนำ AI มาใช้งานในแทบทุกส่วน ดังแสดงตัวอย่างในรูปที่ ๔



ภาพที่ ๔ ลักษณะงานที่สามารถนำ AI ไปใช้งานได้

จากภาพที่ ๔ นั้น สามารถอธิบายและยกตัวอย่างการใช้งาน AI ได้ดังนี้

๓.๕.๑ เซนเซอร์/ระบบตรวจจับ/ระบบตรวจการณ์ สามารถนำ AI มาช่วยในการวางแผนการลาดตระเวน พิสูจน์ทราบ เป็นต้น

๓.๕.๒ สงครามไซเบอร์สามารถนำ AI มาใช้ในการพัฒนาโปรแกรมในการป้องกันภัยคุกคามทางไซเบอร์ การใช้ AI ในการป้องกันการโจมตีโดย AI การพัฒนา AI ในการโจมตีทางไซเบอร์ เป็นต้น

๓.๕.๒ ระบบงานอัจฉริยะ สามารถนำ AI มาช่วยในการแปลงรูปภาพเป็นตัวอักษร การช่วยตีความประเด็นข้อขัดแย้ง เป็นต้น

๓.๕.๔ การซ่อมบำรุงสามารถใช้ AI ในการช่วยทำนายอายุการใช้งานของยุโรปกรณ์ ความต้องการอะไหล่ตามวงจรรอบ เป็นต้น

๓.๕.๕ พาหนะและการปฏิบัติการทางทหาร สามารถใช้ AI ได้หลายระบบ เช่น ระบบเดินเรืออัจฉริยะ ระบบตรวจการณ์อัจฉริยะ ระบบช่วยการตัดสินใจของระบบควบคุมบังคับบัญชา เป็นต้น

๓.๕.๖ ระบบอัจฉริยะใน/นอกอาคาร สามารถนำ AI มาช่วยในการควบคุมการเข้าออกอาคาร ที่จอดรถ ควบคุมการใช้พลังงานในอาคาร การตรวจจับสิ่งผิดปกติ เช่น เปลวไฟ คิว้น คนหมดสติ เป็นต้น

๓.๕.๗ สงครามอิเล็กทรอนิกส์ สามารถใช้ AI มาช่วยในการวิเคราะห์คลื่น ทำนายค่าพารามิเตอร์ เป็นต้น

๓.๕.๘ หุ่นยนต์สามารถนำ Chat Bot มาช่วยในงานประชาสัมพันธ์ หรือนำหุ่นยนต์/ยานไร้คนขับไปใช้ในงานที่เสี่ยงอันตราย เป็นต้น

๓.๕.๙ การบริหาร (กำลังพล/การเงิน/การส่งกำลังบำรุง/คลัง/เครือข่าย ฯลฯ) สามารถนำ AI มาช่วยในการบริหารได้ เช่น การสรรหา คัดเลือก ฝึกอบรมกำลังพล การประเมินความเสี่ยงทางการเงิน การบริหารคลังหลัก คลังสาขา เป็นต้น

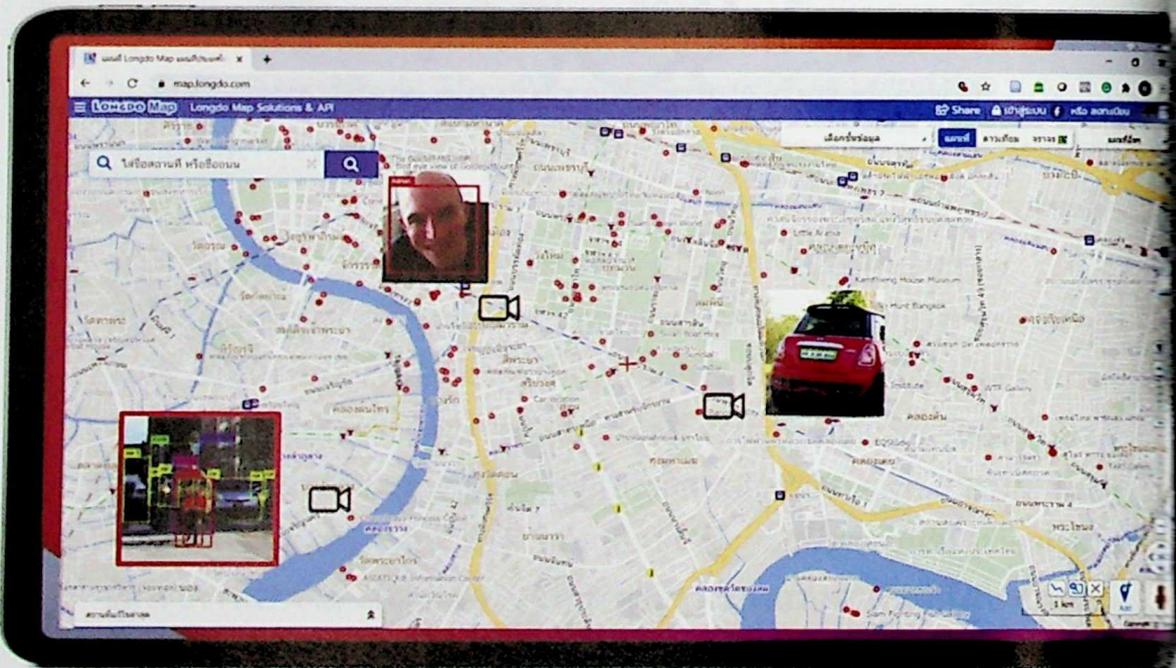
การประยุกต์ใช้ AI ในทางทหาร ควรมีการสำรวจปัญหาหรือความต้องการในการใช้งานที่ชัดเจน จากนั้นควรศึกษาเทคโนโลยีที่เกี่ยวข้องที่สามารถนำมาใช้แก้ปัญหาหรือตอบสนองความต้องการเหล่านั้นได้ ทั้งนี้พึงระลึกเสมอว่าการแก้ปัญหาหรือตอบสนองความต้องการเหล่านั้นสามารถกระทำได้หลากหลายวิธี บ่อยครั้งที่ปัญหาสามารถถูกแก้ไขได้ด้วยวิธีการแบบง่าย ๆ โดยไม่จำเป็นต้องใช้ AI เสมอไป ทั้งนี้ หากหน่วยต่าง ๆ ตกลงใจที่จะนำ AI มาใช้แล้ว จะสามารถดำเนินการได้ ๒ แนวทาง คือ ๑. การนำ AI มาใช้ ในภารกิจทางทหารทั่ว ๆ ไป ๒. การพัฒนา AI สำหรับภารกิจเฉพาะทางทหาร ในสงคราม โดยสามารถอธิบายและยกตัวอย่างการใช้งานเพิ่มเติมได้ดังนี้

๔. การนำ AI มาใช้ในภารกิจทางทหารทั่ว ๆ ไป

แนวทางนี้เป็นการนำเทคโนโลยีด้าน AI ที่มีความเสถียรแล้วและมีการใช้ในเชิงพาณิชย์ มาปรับใช้ตามความต้องการเพื่อตอบสนองต่อภารกิจที่ได้รับ

ซึ่งในปัจจุบันมีเทคโนโลยีที่มีใช้อย่างแพร่หลาย เช่น Computer Vision ได้แก่ การตรวจจับใบหน้า อ่านแผ่นป้ายทะเบียน ตรวจจับวัตถุ การประมวลผลภาษาธรรมชาติ หุ่นยนต์ แชนบอท เป็นต้น ที่สามารถนำมาประยุกต์ใช้ได้ดังตัวอย่างต่อไปนี้

๔.๑ การนำ Computer Vision มาใช้ในการรักษาความปลอดภัยหน่วยนับเป็นหนึ่งในตัวอย่างการใช้งาน AI ในชีวิตประจำวันที่เราเห็นได้มากที่สุด เช่น การนำกล้อง AI ไปติดตั้งบริเวณจุดที่มีความสำคัญ เช่น ทางเข้า-ออกอาคารเพื่อใช้ในการตรวจจับบุคคล วัตถุ ต้องสงสัย นอกจากการติดตั้งกล้อง AI แบบประจำที่แล้ว ยังสามารถนำ AI ไปติดตั้งในกล้องแบบเคลื่อนที่ แล้วนำกล้องต่าง ๆ มาเชื่อมต่อกันเป็นระบบการตรวจการณ์ด้วยกล้องอัจฉริยะเพื่อการติดตามสถานการณ์ในภาพกว้างได้ดังภาพที่ ๕



ภาพที่ ๕ ระบบการรักษาความปลอดภัยด้วยกล้อง AI

๔.๒ การใช้ NLP กับงานด้านกฎหมาย เพื่อลดข้อขัดแย้งระหว่างผู้รักษากฎหมายและผู้กระทำผิด/ผู้ต้องสงสัย โดยสร้างแพลตฟอร์มที่สามารถเข้าถึง

ได้ง่าย เช่น เว็บ แอป แชนแนล ที่ประชาชนหรือเจ้าหน้าที่สามารถปรึกษา
ข้อกฎหมายได้โดยอาศัยการป้อนข้อมูลการกระทำลงไป จะทำให้การบังคับใช้
กฎหมายเป็นไปตามกฎหมายและเป็นมาตรฐานเดียวกัน ทำให้ลดการใช้
วิจารณญาณของเจ้าหน้าที่ หรือช่วยเหลือเจ้าหน้าที่ที่ไม่สามารถวินิจฉัยได้
เนื่องจากกฎหมายมีความซับซ้อนหรือเป็นกฎหมายใหม่ ซึ่งสามารถแสดง
การใช้งานได้ดังภาพที่ ๖

ข้อความที่ใส่: นายแดงขับรถเร็ว 150 กม./ชม. ในเขตเมืองลักษณะย้อนศรแล้วชนแมว
นายแดง: ขับรถเร็วเกินกฎหมายกำหนด ผิด พรบ. จราจร พ.ศ. xx หมวด xx ปรับ 500-1000 บาท
นายแดง: ขับรถย้อนศร ผิด พรบ. จราจร พ.ศ. xx หมวด xx ปรับ 500-1000 บาท
นายแดง: ขับรถชนสัตว์ไม่ผิดกฎจราจร แต่ขอให้ปรับด้วยความระมัดระวังไม่ประมาท

ข้อความที่ใส่: นายแดงขับรถเร็ว 150 กม./ชม. ในเขตเมืองแล้วชนแมว
นายแดง: ขับรถเร็วเกินกฎหมายกำหนด ผิด พรบ. จราจร พ.ศ. xx หมวด xx ปรับ 500-1000 บาท
นายแดง: ขับรถชนสัตว์ไม่ผิดกฎจราจร แต่ขอให้ปรับด้วยความระมัดระวังไม่ประมาท

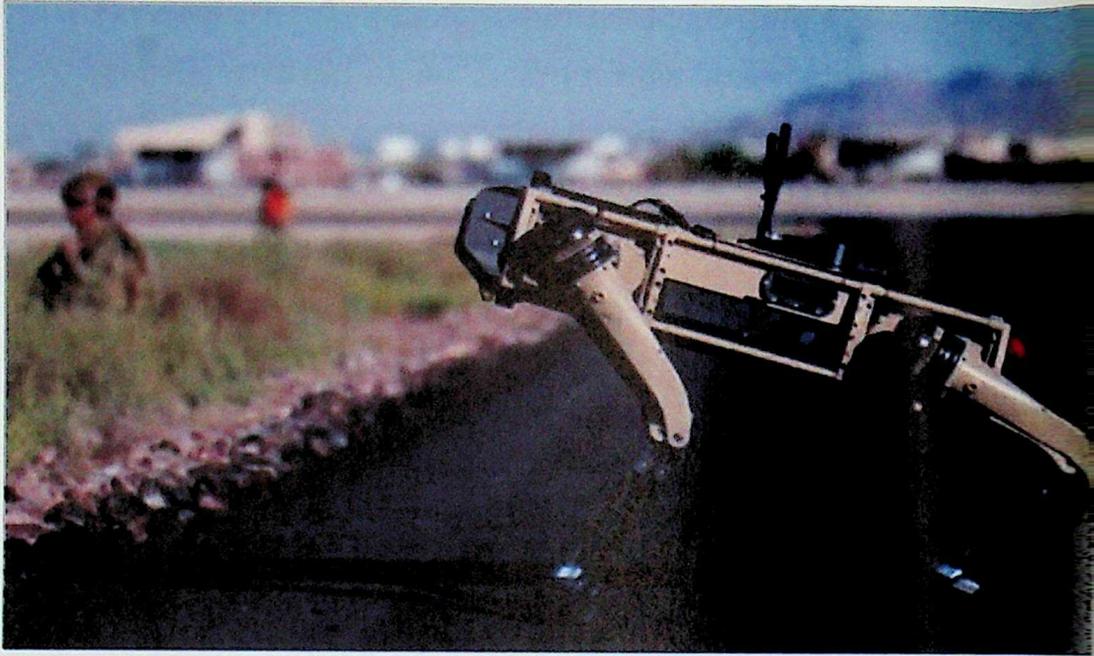
ข้อความที่ใส่: นายแดงขับรถเร็ว 70 กม./ชม. ในเขตเมืองลักษณะย้อนศรแล้วชนแมว
นายแดง: ขับรถย้อนศร ผิด พรบ. จราจร พ.ศ. xx หมวด xx ปรับ 500-1000 บาท
นายแดง: ขับรถชนสัตว์ไม่ผิดกฎจราจร แต่ขอให้ปรับด้วยความระมัดระวังไม่ประมาท

ข้อความที่ใส่: นายแดงขับรถเร็ว 70 กม./ชม. ในเขตเมืองแล้วชนคน
นายแดง: ขับรถชนคน ผิด พรบ. จราจร พ.ศ. xx หมวด xx จำคุก 1 เดือน - 1 ปี

ภาพที่ ๖ การใช้ NLP ในงานด้านกฎหมาย

การนำหุ่นยนต์มาใช้ในการกิจการทางทหาร ไม่ได้ถูกจำกัดอยู่เพียงการใช้
เป็นอาวุธเท่านั้น เนื่องจากหุ่นยนต์สามารถนำมาใช้ได้หลากหลายวัตถุประสงค์
เช่น การทำงานในพื้นที่เสี่ยง การยกหรือลำเลียงของหนัก การตรวจตรา
สิ่งผิดปกติ ดังตัวอย่างเช่น กองทัพอากาศสหรัฐฯ จะนำหุ่นยนต์สุนัขออกมา
ภายนอกยานพาหนะเพื่อตรวจหาสิ่งอันตรายก่อนที่จะมีเจ้าหน้าที่จะออกไป
ปฏิบัติการ ซึ่งเจ้าสุนัขหุ่นยนต์นี้สามารถออกปฏิบัติการได้ในทุกพื้นที่หรือ

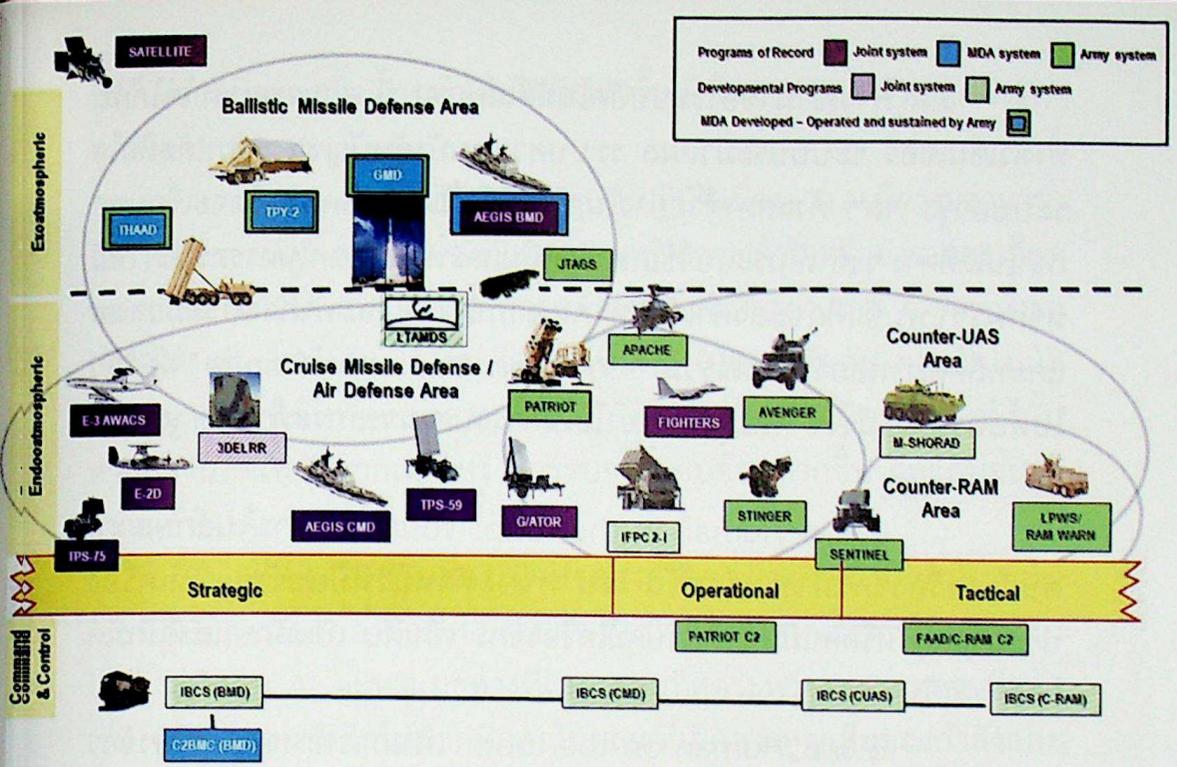
ทุกสภาพแวดล้อมและสามารถปรับให้ติดเซ็นเซอร์และวิทยุได้ ทำให้เพิ่มความมั่นใจ ลดความเสี่ยงและการสูญเสียของเจ้าหน้าที่ได้ดังภาพที่ ๗



ภาพที่ ๗ การนำหุ่นยนต์มาใช้ทางยุทธวิธี
ที่มา : Tom Fish, กันยายน ๒๕๖๓

๕. การพัฒนา AI สำหรับภารกิจเฉพาะทางทหารในสงคราม

แนวทางนี้จะเป็นการพัฒนาระบบ AI เป็นของตนเองให้เหมาะสมกับฉากการรบที่อาจเกิดขึ้น โดยฉากการรบในอนาคตมีแนวโน้มที่จะเป็นสงครามที่มีการปฏิบัติการหลากมิติ (Multidomain Operations: MDO) ซึ่งเป็นปฏิบัติการทางทหารในยุคใหม่ที่มีความซับซ้อนและเปลี่ยนแปลงรวดเร็ว ต้องการการตอบสนองที่ทันท่วงที ปฏิบัติการนี้จะอาศัยระบบอัตโนมัติและเครือข่าย รวมถึง AI เป็นปัจจัยสำคัญในการเชื่อมต่ออุปกรณ์และระบบอำนาจการรบในหลากหลายมิติ ตั้งแต่ พื้นดิน พื้นน้ำ ห้วงอากาศ ห้วงอวกาศ และห้วงไซเบอร์ ดังภาพที่ ๘



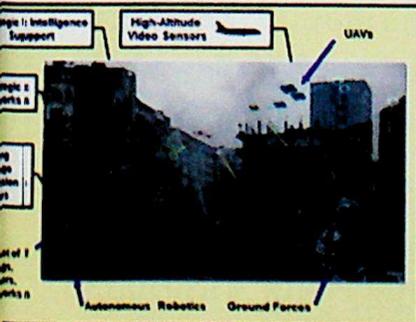
ภาพที่ ๘ การปฏิบัติการหลาภมิติ (Multidomain Operations: MDO)

ที่มา : Brig. Gen. Randall McIntire, ๒๕๖๑

AI/ML in Multi-Domain Operations

Environment & Implications for AI/ML

1. **Forward-deployed, may become isolated**
→ Multi-domain AI/ML for effects, organic AI/ML if isolated
2. **Complex urban terrain** → Deal with partial observability, complex mobility, more precision required
3. **Dynamic, distributed, resource-constrained**
→ Must adaptably learn on-the-fly with limited resources
4. **Contested** → Must be resilient to peer adversary attacks
5. **Unmodeled Phenomena** → Must learn/adapt to new jammers, threats (e.g. drone swarm), network or AI attacks, multi-domain deception techniques, ...



1 SEE
Sense the enemy to aid protection, deception, isolation

2 ISOLATE
Converge ground forces, fires, EW, deception to isolate enemy physically, virtually, cognitively

3 DEFEAT
Multi-Domain convergence to defeat enemy in dense urban terrain even when isolated

Example AI Capabilities

NARROW	LIMITED	BROAD
ISR: Single Sensor, Single Technology → Target detection, classification, tracking → Identify, locate, jammers, networks, IoT → Cue ISR to critical areas	Intel Collection Management → Mapping intel needs with available multi-domain assets → Manoeuvre or cue ISR assets for maximum impact	Rhythm of the Megacity → Identifying & understanding complex activities city-wide → Learn emergent group behaviors → Target anomalous behaviors for deeper analysis
ISR supporting single domain isolation → Strikes based on ISR of enemy forces, air defense, EW → Exploit IoT, spectrum, enemy networks	Cross Domain Deception → Linking exploitation of deccys, EW, IoT, networks → Converges cross domain deception → Shapes environment for freedom of manoeuvre	Autonomous Robotic Manuever → Augment autonomous mobility with external ISR, deception forces → Reacting to environment, enemy forces, & EMD, IoT networks
Employ single, cross domain capabilities → Manoeuvre forces, strikes, cyber to meet objectives → Seize territory, enter buildings, destroy high value targets.	Autonomous Robotic Mobility → Linking perception (multi-sensors), navigation, control → Reacting to dynamic environment	

ภาพที่ ๙ การใช้ AI ใน MDO

ที่มา : Kelsey Reichmann, ๒๕๖๒

๕.๑ การเข้ามาของระบบอัตโนมัติและ AI นี้ สามารถปรับใช้ได้กับ ทั้งตัวเซ็นเซอร์ ระบบประมวลผล ระบบควบคุมบังคับบัญชา ระบบตัดสินใจ ระบบอาวุธ ฯลฯ ดังแสดงตัวอย่างในภาพที่ ๙ โดยแนวความคิดจะเชื่อมต่อ เทคโนโลยีต่าง ๆ เข้าเป็นระบบ ใช้โดรนภาคพื้นและทางอากาศในการตรวจการณ์ หากตรวจพบข้าศึกจะส่งค่าเป้าให้ AI จากนั้น AI จะทำการประมวลผล และพล็อตภาพสถานการณ์ร่วม “Common Operating Picture” (COP) ในพื้นที่รบการนำ AI หรือหุ่นยนต์มาใช้ในการรบสามารถกระทำได้ ๓ รูปแบบ คือ

๕.๑.๑ Human-in-the-loop: เป็นการทำงานในลักษณะที่ คนกับเครื่องจักรทำงานร่วมกัน เช่น คนจะทำหน้าที่ป้อนข้อมูลให้เครื่อง ประมวลผล หรือคนมีหน้าที่ควบคุมเครื่องจักร เป็นต้น เป็นลักษณะที่เห็นได้ โดยทั่ว ๆ ไป

๕.๑.๒ Human-on-the-loop: เป็นการทำงานที่เครื่องจักร จะควบคุมระบบโดยอัตโนมัติเป็นส่วนใหญ่ แต่คนสามารถเข้าไปควบคุมสั่งการ หรือตัดสินใจได้ตลอดเวลา เช่น ระบบพล็อตอัตโนมัติ เป็นต้น

๕.๑.๓ Human-out-of-the-loop: เป็นลักษณะการทำงาน ที่เครื่องจักรทำงานด้วยตนเองอย่างสมบูรณ์ ซึ่งในปัจจุบัน AI ยังไม่สามารถ ควบคุมระบบที่ซับซ้อนได้

๕.๒ การนำ AI มาใช้ในสงครามจะเปลี่ยนศาสตร์การรบในรูแบบเดิม ไปอย่างมาก โดย ศาสตราจารย์ Andrew Hill ประธานยุทธศาสตร์ วิทยาลัย กองทัพบกสหรัฐฯ ได้กล่าวในงานสัมมนาทางวิชาการของวิทยาลัยกองทัพบก (Army War College) ว่า หาก AI ถูกใช้เป็นหลักในการรบ จะต้องมีการทบทวน หรือแม้กระทั่งยกเลิกศาสตร์การรบบางอย่างที่กำลังสอนในโรงเรียนทหาร เนื่องจากหลักปฏิบัติเหล่านั้น เช่น ใช้กำลังต่อจุดตัดสินใจ ทำให้ข้าศึกคาดไม่ถึง มุ่งไปที่เป้าประสงค์ ฯลฯ ได้ถูกปฏิบัติกันมาจากประสบการณ์นับร้อย ๆ ปี โดยไม่ได้ใช้หลักการในการตกลงใจแบบเดียวกับกระบวนการตัดสินใจของ AI สิ่งหนึ่งที่นับเป็นความท้าทายด้านการพัฒนา AI ในการรบเป็นอย่างมากคือ การทำให้ AI อธิบายหรือให้เหตุผลที่มนุษย์สามารถเข้าใจได้ ซึ่งเรื่องนี้เป็น เรื่องที่สำคัญมากหากจะนำ AI มาใช้ในการรบจริง โดยที่ไม่มีใครมีความเข้าใจหรือ

ไม่ทันความคิดของมัน อาจทำให้เกิดปัญหาขึ้นได้ โดยจะขอยกตัวอย่างปัญหาพอสังเขป เช่น

๕.๒.๑ ความไม่เข้าใจของหน่วยปฏิบัติ เนื่องจาก AI มีความสามารถในการวิเคราะห์สูง ต่างจากคนที่ไม่สามารถทำความเข้าใจหรือจำรายละเอียดของสถานการณ์ได้หมด ดังนั้น พลรบต้องได้รับคำสั่งอย่างง่าย ๆ ที่สามารถเข้าใจได้ เช่น ไปที่นั่น ป้องกัน โจมตี เป็นต้น ในทางกลับกัน ยานอัตโนมัติจะสามารถจำได้หมดและสามารถปฏิบัติได้โดยไม่มีข้อผิดพลาด ดังนั้น หากมียานอัตโนมัติมากเท่าไร การรบจะยิ่งซับซ้อนมากขึ้น และคนจะทำความเข้าใจได้ยากยิ่งขึ้น

๕.๒.๒ ในส่วนของเป้าประสงค์ในการรบก็จะเปลี่ยนไป เช่น การปฏิบัติการโดยกองกำลังของคนต้องมีเป้าประสงค์ที่แน่นอนและชัดเจน ในทางกลับกัน AI จะหาแนวทางที่เหมาะสมที่สุดระหว่างหลากหลายปัจจัย เช่น การรุกรอนข้าศึกให้มากที่สุด ในขณะที่เกิดการสูญเสียของกำลังและมิผู้ได้รับผลกระทบจากความเสียหายข้างเคียงน้อยที่สุด เป็นต้น ดังนั้น หน้าที่ของคนจะเป็นเพียงการป้อนเกณฑ์ให้กับ AI ไม่ได้ร่วมวางแผน ทำให้เกิดปัญหาในการบังคับบัญชาและอำนาจสั่งการ ตามที่กล่าวมาข้างต้นว่า การใช้ AI ในการทำงานจะมีความซับซ้อนจนคนไม่อาจเข้าใจ รวมทั้งผู้สั่งการก็ไม่ได้ร่วมวางแผนกับ AI และไม่ได้กำหนดหนทางปฏิบัติ จึงทำให้คนไม่สามารถติดตาม ประเมินสถานการณ์ และสั่งการได้อย่างถูกต้อง

บทสรุป

AI เป็นเทคโนโลยีสำคัญที่กำลังเข้ามามีบทบาท และจะเปลี่ยนแปลงรูปแบบของกองทัพในทุกส่วน ทั้งส่วนบัญชาการ ส่วนกำลังรบ ส่วนยุทธบริการ ส่วนการศึกษาและวิจัย หน่วยเฉพาะกิจ และหน่วยงานอื่น ๆ ไปสู่ยุคใหม่ที่เป็นแบบดิจิทัลที่มีเครื่องจักรอัจฉริยะ

เป็นตัวขับเคลื่อน ช่วยให้งานมีประสิทธิภาพมากขึ้น ลดความซ้ำซ้อนในการทำงานและการใช้ทรัพยากร นอกจากนี้ยังทำให้ศาสตร์การรบเกิดการเปลี่ยนแปลงไปในรูปแบบของสงครามที่มีการปฏิบัติการหลากหลายมิติ ที่มนุษย์และ AI ดำเนินการร่วมกัน ทั้งนี้ การนำ AI มาใช้งานก็มีข้อควรระวังที่สำคัญคือ การใช้ตรรกะของมนุษย์อาจไม่ได้ผลสัมฤทธิ์แบบที่ต้องการเสมอไป เนื่องจากความแตกต่างของกำเนิดและวิธีการเรียนรู้ ทำให้ AI มีกระบวนการตัดสินใจที่มนุษย์ยังไม่สามารถทำความเข้าใจได้ ดังนั้น เพื่อให้การใช้งาน AI ในกองทัพเกิดประโยชน์สูงสุด ควรมีการสำรวจปัญหาหรือความต้องการในการนำ AI มาใช้งานที่ชัดเจนเป็นรูปธรรม พร้อมกันนั้นก็ควรเรียนรู้เทคโนโลยี AI ที่เกี่ยวข้อง และทำการทดลองก่อนนำไปใช้จริง เพื่อให้สามารถนำมาใช้เพื่อแก้ไขปัญหาหรือตอบสนองความต้องการเหล่านั้นได้ตรงตามวัตถุประสงค์

เอกสารอ้างอิง

- ปรีชาพล ชูศรี จิรณา น้อยมณี และ เกษม พันธุ์สิน. (๒๕๖๒). เทคโนโลยีปัญญาประดิษฐ์ สำหรับการบริหารงานและการบริการภาครัฐ. กรุงเทพฯ: ส.พีจิตรการพิมพ์. กองทัพเรือ. (๒๕๕๖). วิสัยทัศน์และพันธกิจกองทัพเรือ. สืบค้นเมื่อ ๒๐ เมษายน ๒๕๖๔, จาก https://www.navy.mi.th/index.php/today/detail/content_id/1435.
- SYDNEY J. FREEDBERG JR. (๒๕๖๒). How AI Could Change The Art Of War. สืบค้นเมื่อ ๒๐ เมษายน ๒๕๖๔, จาก <https://breakingdefense.com/2019/04/how-ai-could-change-the-art-of-war/>.



**เทคโนโลยีเรือดำน้ำ
กับสงครามในอนาคต**

นาวาโท สุระ บรรจงจิตร

บทคัดย่อ

เรือดำน้ำมีการใช้งานทางทหารอย่างจริงจังตั้งแต่ประมาณ ๑๕๐ ปีที่ผ่านมา โดยขีดความสามารถหลักของเรือดำน้ำคือ การซ่อนพราง ส่งผลให้เรือดำน้ำมีความได้เปรียบเมื่อเทียบกับกำลังทางเรือประเภทอื่น ซึ่งการพัฒนาเทคโนโลยีในปัจจุบันทำให้ยังคงมีโอกาสในการพัฒนาขีดความสามารถของเรือดำน้ำที่ส่งผลต่อสงครามทางเรือในอนาคต ไม่ว่าจะเป็นการพัฒนาเทคโนโลยีด้านระบบขับเคลื่อนเรือดำน้ำ ด้านการสื่อสารดิจิทัลใต้น้ำ ด้าน Artificial Intelligence กับการปฏิบัติการเรือดำน้ำ และด้านยานใต้น้ำไร้คนขับและเรือดำน้ำขนาดเล็ก อันจะเห็นได้ว่าการพัฒนาเทคโนโลยีด้านต่าง ๆ ยังคงเป็นการเน้นความสำคัญของขีดความสามารถหลักของเรือดำน้ำในการซ่อนพราง ส่งผลให้เรือดำน้ำจะยังคงเป็นอาวุธซ่อนพรางที่ค้นหาและตรวจจับได้ยาก และกำลังรบใต้น้ำจะยังคงมีบทบาทสำคัญในสงครามอนาคต

บทนำ

การซ่อนพรางเป็นหนึ่งในความได้เปรียบในการรบ ซึ่งเมื่อเปรียบเทียบกับมิติต่าง ๆ ของการรบทางเรือ ไม่ว่าจะเป็นผิวน้ำ บนอากาศ และใต้น้ำ จะพบว่ามีมิติที่เหมาะสมที่สุดสำหรับการซ่อนพรางในการรบทางเรือคือ มิติใต้น้ำ ส่งผลให้การใช้เรือดำน้ำทางทหารเป็นที่สนใจมาเป็นเวลานาน อย่างไรก็ตาม ความสำเร็จของเทคโนโลยีที่ช่วยให้เรือดำน้ำสามารถปฏิบัติการทางทหารได้อย่างมีประสิทธิภาพและปลอดภัยทำให้เริ่มมีการพัฒนาเรือดำน้ำทางทหารอย่างจริงจัง เมื่อประมาณ ๑๕๐ ปีที่ผ่านมา และเรือดำน้ำทางทหารเริ่มมีการใช้งานอย่างแพร่หลายในช่วงสงครามโลกครั้งที่ ๑ และสงครามโลกครั้งที่ ๒ แต่ “เรือดำน้ำ” ในสมัยสงครามโลกก็ยังคงถูกออกแบบให้ปฏิบัติการบนผิวน้ำเป็นหลักและดำลงเมื่อจำเป็นเท่านั้น โดยเรือดำน้ำในคำจำกัดความที่เราคุ้นเคยในปัจจุบันที่ถูกออกแบบเพื่อให้ปฏิบัติการใต้น้ำเป็นหลักและมีขีดความสามารถกับความคล่องตัวใต้น้ำมากกว่าบนผิวน้ำเพิ่งถูกพัฒนาขึ้นในช่วงปลายสงครามโลกครั้งที่ ๒ คือ เรือดำน้ำ Type XXI ของเยอรมนี และได้กลายเป็นต้นแบบเรือดำน้ำสมัยใหม่ของหลายประเทศ

หลังจากที่เยอรมนีแพ้สงคราม^๑ ดังนั้น จึงกล่าวได้ว่าเรือดำน้ำทางทหารยังเป็นเทคโนโลยีใหม่ที่เริ่มใช้งานจริงมาไม่นาน และยังมีโอกาสในการพัฒนาต่อไปได้อีกในอนาคต



ภาพที่ ๑ พิพิธภัณฑสถานเรือดำน้ำ Wilhelm Bauer (Type XXI)
ที่เมือง Bremerhaven เยอรมนี

ที่มา : <https://m.facebook.com/KringsakTao160760/posts/893543757678652>

บทความนี้จะกล่าวถึงการพัฒนาเทคโนโลยีเรือดำน้ำสมัยใหม่ และผลกระทบต่อการรบทางเรือกับสงครามในอนาคต โดยแบ่งออกเป็นการพัฒนาเทคโนโลยีด้านต่าง ๆ ได้แก่ เทคโนโลยีระบบขับเคลื่อนเรือดำน้ำ เทคโนโลยีการสื่อสารดิจิทัลใต้น้ำ เทคโนโลยี Artificial Intelligence กับการปฏิบัติการเรือดำน้ำ และเทคโนโลยียานใต้น้ำไร้คนขับและเรือดำน้ำขนาดเล็ก

เทคโนโลยีระบบขับเคลื่อนเรือดำน้ำ

การพัฒนาาระบบขับเคลื่อนเรือดำน้ำ เป็นส่วนสำคัญให้การใช้งานเรือดำน้ำทางทหารมีความเป็นไปได้มากขึ้นในช่วงปลายคริสต์ศตวรรษที่ ๑๙

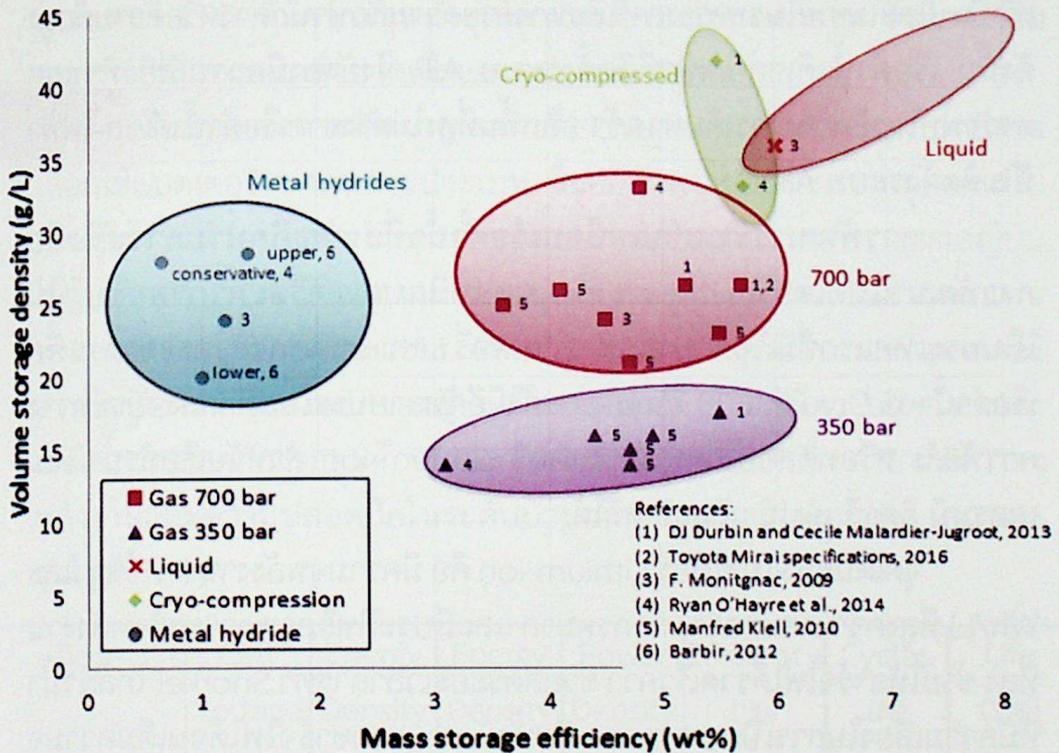
เป็นต้นมา โดยเฉพาะอย่างยิ่งการเก็บพลังงานในแบตเตอรี่สำหรับมอเตอร์ขับเคลื่อนใต้น้ำ ซึ่งเรือดำน้ำดีเซล-ไฟฟ้าในปัจจุบันใช้มอเตอร์ไฟฟ้าเพียงอย่างเดียวในการขับเคลื่อนทั้งบนผิวน้ำและใต้น้ำ โดยใช้เครื่องยนต์ดีเซลเป็นเครื่องกำเนิดไฟฟ้าเท่านั้น และต่อมาในช่วงสงครามเย็นได้มีการพัฒนาระบบขับเคลื่อนนิวเคลียร์ที่ช่วยให้เรือดำน้ำมีขีดความสามารถในการซ่อนพรงใต้น้ำได้อย่างแท้จริงโดยไม่ต้องพึ่งพาอากาศจากบนผิวน้ำ และมีระยะเวลาปฏิบัติการใต้น้ำที่ถูกจำกัดด้วยเสบียงอาหารและความอดทนของมนุษย์เท่านั้น

ในส่วนของเรือดำน้ำดีเซล-ไฟฟ้าในปัจจุบันได้มีการพัฒนาระบบ AIP (Air Independent Propulsion) ช่วยให้เรือดำน้ำดีเซล-ไฟฟ้าสามารถปฏิบัติการใต้น้ำต่อเนื่องได้นานขึ้น โดยหลักการทำงานของระบบ AIP คือ การนำออกซิเจนเหลวและเชื้อเพลิงไปกับเรือดำน้ำเพื่อผลิตกระแสไฟฟ้าโดยไม่ต้องใช้อากาศจากภายนอก ระบบ AIP ได้มีการพัฒนาขึ้นมาหลายแบบ เช่น ระบบ AIP แบบ Stirling Engine ที่ใช้หลักการทำงานของเครื่องยนต์สันดาปภายนอกในการผลิตกระแสไฟฟ้า และมีใช้ในเรือดำน้ำของสวีเดน ญี่ปุ่น และจีน รวมทั้งเรือดำน้ำ S26T ที่กองทัพเรือกำลังจัดหาจากจีนด้วย

ข้อจำกัดของระบบ AIP ที่ผลิตกระแสไฟฟ้าด้วยการสันดาป เช่น ระบบ Stirling Engine คือ ประสิทธิภาพการใช้เชื้อเพลิง (Fuel Efficiency) ที่ค่อนข้างต่ำ เนื่องจากต้องแปลงพลังงานความร้อนจากการสันดาปเป็นพลังงานกลก่อนที่จะแปลงเป็นพลังงานไฟฟ้า และการมีไอเสียจากการสันดาปทำให้แนวโน้มการพัฒนาเทคโนโลยีระบบ AIP ในอนาคตเปลี่ยนไปเป็นแบบ Fuel Cell ที่ใช้หลักการปฏิกิริยาเคมีระหว่างออกซิเจนกับไฮโดรเจนแทนการสันดาปในการผลิตกระแสไฟฟ้า ช่วยให้ประสิทธิภาพดีกว่า และผลผลิตที่ได้มีเพียงกระแสไฟฟ้ากับน้ำเท่านั้น

ระบบ AIP แบบ Fuel Cell เริ่มมีใช้ในเรือดำน้ำชั้น 212A ของเยอรมนีในปี ค.ศ. ๒๐๐๓^๒ และปัจจุบันมีประเทศที่กำลังพัฒนาระบบ AIP แบบ Fuel Cell ในเรือดำน้ำทางทหาร ได้แก่ ฝรั่งเศส สเปน อินเดีย เกาหลีใต้ และรัสเซีย อย่างไรก็ตาม ถึงแม้ว่าระบบ AIP แบบ Fuel Cell จะมีประสิทธิภาพดีกว่าระบบ AIP แบบอื่น แต่ก็มีคามยุ่งยากในการเก็บไฮโดรเจนไปกับเรืออย่างปลอดภัย และเป็นส่วนหนึ่งที่ทำให้การพัฒนาระบบ AIP แบบ Fuel Cell

ในเรือดำน้ำเป็นไปอย่างล่าช้า ยกเว้นเยอรมนีที่เลือกใช้วิธีจัดเก็บไฮโดรเจนในรูปแบบของ Metal Hydride ที่ให้ก๊าซแทรกตัวอยู่ในโลหะที่เป็นของแข็ง และเป็นวิธีจัดเก็บที่มีความปลอดภัยสูง แต่ก็ต้องแลกด้วยประสิทธิภาพการจัดเก็บที่ต่ำในเชิงน้ำหนัก ซึ่งน้ำหนักและปริมาตรนับเป็นข้อจำกัดสำคัญในการออกแบบโครงสร้างเรือดำน้ำ



ภาพที่ ๒ ประสิทธิภาพการจัดเก็บไฮโดรเจนในรูปแบบต่าง ๆ แสดงถึงประสิทธิภาพการจัดเก็บเชิงน้ำหนัก (แกนนอน) ค่ายิ่งมกยิ่งดี คือ เก็บไฮโดรเจนได้มากต่อน้ำหนัก กับความหนาแน่นการจัดเก็บเชิงปริมาตร (แกนตั้ง) ค่ายิ่งมกยิ่งดี คือ เก็บไฮโดรเจนได้มากต่อปริมาตร

ที่มา : Nevesbu, Undersea Defense Technology 2019

แนวความคิดการพัฒนาระบบ AIP แบบ Fuel Cell ของหลายประเทศในปัจจุบันเป็นการผลิตไฮโดรเจนด้วย Hydrogen Reformer จากสารไฮโดรคาร์บอน เช่น Methanol หรือน้ำมันดีเซล ซึ่งอยู่ในสถานะของเหลวที่สามารถจัดเก็บได้ง่าย แต่ข้อด้อยของระบบ Hydrogen Reformer คือ ผลผลิตข้างเคียงที่ไม่ต้องการ เช่น คาร์บอนไดออกไซด์ และสารเคมีอื่นซึ่งขึ้นอยู่กับ

กับสารตั้งต้นที่นำมาใช้กับ Hydrogen Reformer เช่น กำมะถันในกรณีของ น้ำมันดีเซล ซึ่งต้องกำจัดออกนอกตัวเรือ

อย่างไรก็ดี ระบบ AIP ทุกแบบมีข้อจำกัดที่สำคัญคือ การให้กำลังไฟฟ้าที่ต่ำมาก เมื่อเทียบกับแบตเตอรี่หรือเครื่องกำเนิดไฟฟ้า ดังนั้น ระบบ AIP จึงเป็นเพียงแหล่งพลังงานเสริมสำหรับใช้งานในช่วงการลาดตระเวนที่ความเร็วต่ำเท่านั้น และไม่ช่วยในระหว่างการเดินทางด้วยความเร็วปานกลางหรือความเร็วสูง ดังนั้น เรือดำน้ำดีเซล-ไฟฟ้าที่ติดตั้งระบบ AIP จึงยังคงมีความเสี่ยงที่จะถูกตรวจพบในระหว่างการเดินทางเข้า-ออกพื้นที่สูงไม่ต่างจากเรือดำน้ำดีเซล-ไฟฟ้าที่ไม่ติดตั้งระบบ AIP

การพัฒนาระบบขับเคลื่อนเรือดำน้ำที่สำคัญอีกประการหนึ่งคือ การพัฒนาแบตเตอรี่ Lithium-ion ทดแทนแบตเตอรี่ตะกั่วกรด ซึ่งญี่ปุ่นเป็นประเทศแรกที่มีเรือดำน้ำติดตั้งแบตเตอรี่ Lithium-ion เข้าประจำการ คือ เรือดำน้ำ JS Oryu และ JS Toryu และยังมีอีกหลายประเทศที่กำลังอยู่ระหว่างการพัฒนาหรือทดสอบทดลองแบตเตอรี่ Lithium-ion สำหรับเรือดำน้ำ เช่น เยอรมนี อิตาลี สเปน และเกาหลีใต้

จุดเด่นของแบตเตอรี่ Lithium-ion คือ มีความจุพลังงาน (Wh/kg และ Wh/L) ที่สูงกว่าแบตเตอรี่ตะกั่วกรดมาก และมีประสิทธิภาพการชาร์จพลังงานที่สูง ช่วยให้ชาร์จไฟได้รวดเร็วกว่า ช่วยลดระยะเวลาการทำ Snorkel ใกล้เคียงน้ำที่มีความเสี่ยงในการเปิดเผยตนเอง อีกทั้งยังสามารถชาร์จไฟได้จนเต็มความจุ โดยไม่มีข้อจำกัด ในขณะที่แบตเตอรี่ตะกั่ว-กรดจะทำการชาร์จไฟในทะเลได้ถึง Gas Voltage ที่แบตเตอรี่จะเริ่มปล่อยก๊าซไฮโดรเจนเท่านั้น ทำให้ไม่สามารถชาร์จไฟได้เต็มที่ขณะอยู่ในทะเล (การชาร์จไฟถึง Gas Voltage จะต้องทำในท่าเรือตามวงรอบการบำรุงรักษาแบตเตอรี่และต้องมีการระบายอากาศเพื่อไม่ให้เกิดการสะสมของก๊าซไฮโดรเจนในเรือดำน้ำ) นอกจากนี้แบตเตอรี่ Lithium-ion ยังต้องการการบำรุงรักษาน้อยกว่าและมีอายุการใช้งานที่นานกว่าแบตเตอรี่ตะกั่วกรด ดังนั้น ถึงแม้ว่าแบตเตอรี่ Lithium-ion จะมีราคาในการจัดหาสูงกว่าแบตเตอรี่ตะกั่วกรด แต่ก็มีค่าใช้จ่ายในระหว่างอายุการใช้งานที่ต่ำ

แบตเตอรี่ Lithium-ion ในปัจจุบันมีหลายประเภท ขึ้นอยู่กับส่วนประกอบทางเคมี เช่น แบตเตอรี่ Lithium Nickel Cobalt Aluminum

Oxide (LiNiCoAlO_2) หรือ NCA แบตเตอรี่ Lithium Nickel Manganese Cobalt Oxide (LiNiMnCoO_2) หรือ NMC และแบตเตอรี่ Lithium Titanate ($\text{Li}_4\text{Ti}_5\text{O}_{12}$) หรือ LTO ซึ่งแบตเตอรี่ Lithium-ion แต่ละประเภทมีความจุพลังงานและคุณลักษณะอื่นที่แตกต่างกันไป และมีการนำไปใช้ที่ต่างกัน เช่น แบตเตอรี่ NCA กับ NMC มีความจุพลังงานสูงจึงนิยมใช้ในรถยนต์ไฟฟ้า และ แบตเตอรี่ LTO ที่มีความจุพลังงานต่ำและมีความปลอดภัยสูง จึงนิยมใช้ใน อุปกรณ์อิเล็กทรอนิกส์ขนาดเล็กและอุปกรณ์การแพทย์

ในส่วนของ การพัฒนาแบตเตอรี่ Lithium-ion สำหรับเรือดำน้ำ มีการเลือกใช้แบตเตอรี่หลากหลายประเภท ขึ้นอยู่กับความต้องการของผู้ออกแบบ และผู้ใช้งาน ตัวอย่างเช่น เรือดำน้ำของกองกำลังป้องกันตนเองทางทะเลญี่ปุ่น ใช้แบตเตอรี่ NCA เนื่องจากมีความจุพลังงานสูงมาก โดยเป็นการทดแทนทั้งแบตเตอรี่ตะกั่วกรดและระบบ AIP แบบ Stirling Engine ในขณะที่แบตเตอรี่ สำหรับเรือดำน้ำรุ่นส่งออกของญี่ปุ่นเป็นแบตเตอรี่ LTO ที่มีความจุพลังงานต่ำ แต่มีความปลอดภัยมากกว่า^๓ หรืออิตาลีที่กำลังพัฒนาแบตเตอรี่ NMC ที่มีความจุพลังงานและความปลอดภัยในระดับปานกลางสำหรับเรือดำน้ำชั้น 212NFS รุ่นใหม่^๔

Type	Cell Voltage (V)	Energy Density (Wh/kg)	Energy Density (Wh/L)	Power Density (W/kg)	Efficiency (%)	Cycles (N)	Life (Yrs)	
Type	2.0	30-40	60-75	180	70-85	600-1500	5-12	
Li-ion	LCO	3.6	160	270	1800	99	1200	5
	NCA	3.6	240	600	1000	98	3000	15
	LMO	4.0	140	250	2000	98	2000	10
	NMC	3.7	140-160	300	3000	98	5000	10
	LFP	3.25	100-140	220	6000	98	3000	10
	LTO	2.3	90	160	10000	95	10000	20

ตารางที่ ๑ ตารางเปรียบเทียบคุณลักษณะแบตเตอรี่ Li-ion และแบตเตอรี่ตะกั่วกรด

ที่มา : Vincenzo Pennino, Lithium-ion Battery for U212NFS, 2019

ด้านความเสี่ยงและอันตรายจากแบตเตอรี่ ถึงแม้ว่าแบตเตอรี่ตะกั่วกรด จะมีความเสี่ยงในการเกิดก๊าซไฮโดรเจนจากการใช้งาน และการเกิดก๊าซคลอรีน จากการสัมผัสน้ำทะเล แต่แบตเตอรี่ตะกั่วกรดเป็นเทคโนโลยีเก่าที่มีใช้มา ตั้งแต่เรือดำน้ำในยุคก่อนสงครามโลก ทำให้ความเสี่ยงดังกล่าว มีข้อมูลเป็นที่รู้จัก เป็นอย่างดีและมีมาตรการป้องกันที่ยอมรับได้ อย่างไรก็ตาม แบตเตอรี่ Lithium-ion ยังเป็นเทคโนโลยีใหม่และถึงแม้ว่าในปัจจุบันจะมีข้อมูลความเสี่ยงการเกิด ปรากฏการณ์ Thermal Runaway (การเกิดความร้อนและบวม เมื่อแบตเตอรี่ ต่อกับชาร์จเจอร์) อยู่บ้าง แต่ยังไม่เคยมีการใช้งานจริงในแบตเตอรี่ขนาดใหญ่อย่าง แบตเตอรี่เรือดำน้ำมาก่อน และยังคงต้องรอการศึกษาข้อมูลการใช้งานจริง เปรียบเทียบกับผลการศึกษาจากแบบจำลองต่อไป

เทคโนโลยีการสื่อสารดิจิตอลใต้น้ำ

หนึ่งในข้อจำกัดสำคัญของเรือดำน้ำคือ การสื่อสาร เนื่องมาจาก ทั้งเหตุผลด้านการปฏิบัติการและด้านหลักฟิสิกส์ของการแพร่คลื่น โดยเรือดำน้ำ จะพยายามจำกัดการสื่อสารให้น้อยที่สุดเพื่อลดการเปิดเผยตัว และการสื่อสาร จากสถานีฝั่งไปยังเรือดำน้ำจะเป็นการสื่อสารทางเดียวในลักษณะของการ Broadcast ตามวงรอบโดยที่เรือดำน้ำไม่จำเป็นต้องตอบรับในทันที

ในด้านหลักฟิสิกส์ของการแพร่คลื่น การดูดกลืนคลื่นแม่เหล็กไฟฟ้า ในน้ำทะเลมีมากกว่าในอากาศประมาณ ๓,๐๐๐ เท่า และความถี่ยิ่งสูงขึ้น การดูดกลืนจะยิ่งสูงมากขึ้น ส่งผลให้คลื่นวิทยุส่วนมากไม่สามารถเดินทางผ่าน น้ำทะเลได้ ในขณะที่คลื่นเสียงเดินทางในน้ำทะเลได้ดีกว่าในอากาศ โดยคลื่นเสียง เดินทางในน้ำทะเลได้เร็วกว่าในอากาศประมาณ ๕ เท่า

การสื่อสารของเรือดำน้ำแบ่งได้เป็น ๒ ลักษณะ คือการสื่อสาร เหนือผิวน้ำ และการสื่อสารใต้น้ำ ในส่วนของการสื่อสารเหนือผิวน้ำ เรือดำน้ำ สามารถใช้การสื่อสารทางวิทยุในย่านความถี่ต่าง ๆ ได้เช่นเดียวกับเรือผิวน้ำ แต่เรือดำน้ำจำเป็นต้องซักสายอากาศสื่อสารขึ้นเหนือผิวน้ำซึ่งจะเพิ่ม ความเสี่ยงในการถูกตรวจจับของฝ่ายตรงข้ามได้

การสื่อสารใต้น้ำของเรือดำน้ำสามารถทำได้โดยใช้คลื่นวิทยุ ย่านความถี่ต่ำมาก หรือ VLF (Very Low Frequency) ที่สามารถเดินทาง ผ่านความลึกน้ำลงไปได้ประมาณ ๒๐ ม. อย่างไรก็ตาม คลื่นวิทยุย่าน VLF มีความยาวคลื่นในช่วง ๑๐-๑๐๐ กม. ทำให้ต้องใช้สายอากาศส่งขนาดใหญ่ กับสถานีส่งที่มีการลงทุนสูงมาก และความยาวคลื่นกับกำลังส่งที่สูงมาก

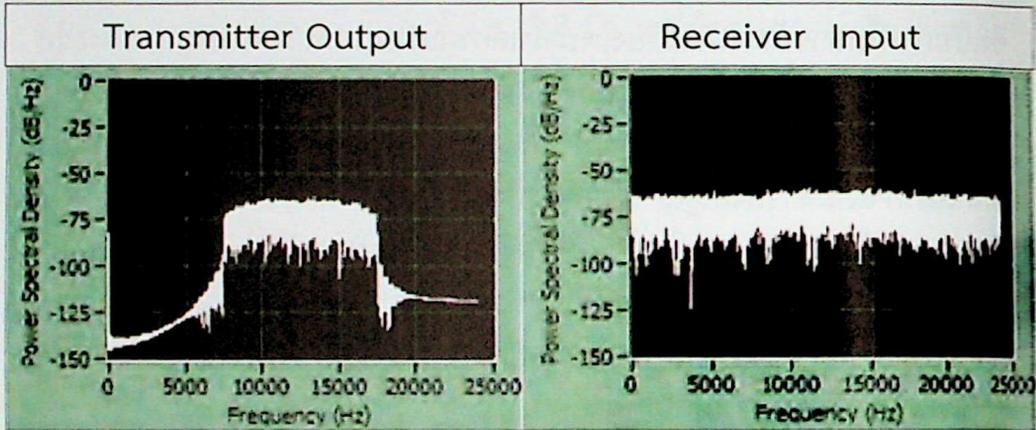
ทำให้การสื่อสารย่านความถี่ VLF เป็นการสื่อสารทางเดียวจากสถานีฝั่ง ไปยังเรือดำน้ำเท่านั้น ส่วนเรือดำน้ำยังคงต้องติดต่อกลับไปยังสถานีฝั่ง ทางย่านความถี่ HF หรือการสื่อสารดาวเทียม ด้วยเหตุนี้จึงมีเพียงไม่กี่ประเทศ ที่ลงทุนสร้างสถานีสื่อสารย่าน VLF

การสื่อสารใต้น้ำของเรือดำน้ำอีกรูปแบบหนึ่งคือ การใช้โทรศัพท์ใต้น้ำ ซึ่งเป็นการสื่อสารด้วยคลื่นเสียงใต้น้ำในลักษณะของการรับ-ส่งสัญญาณมอร์ส ทางคลื่น CW และสื่อสารทางเสียงด้วยการผสมคลื่นแบบ AM (Amplitude Modulation) อย่างไรก็ตาม การสื่อสารทางเสียงด้วยโทรศัพท์ใต้น้ำมีระยะ ไม่ไกลมาก และการส่งสัญญาณมอร์สทางคลื่น CW กับการผสมคลื่นแบบ AM สามารถถูกดักจับและถอดข้อความจากสัญญาณได้ง่าย ดังนั้น โทรศัพท์ใต้น้ำ จึงใช้ในการสื่อสารระยะใกล้ในการฝึกหัดระหว่างเรือดำน้ำกับเรือผิวน้ำ หรือ ระหว่างเรือดำน้ำกับเรือดำน้ำ และเป็นอุปกรณ์การสื่อสารฉุกเฉินในการช่วยเหลือ ภัยเรือดำน้ำที่ประสบเหตุฉุกเฉินใต้น้ำ

ความยุ่งยากของการสื่อสารใต้น้ำคือ ความไม่แน่นอนของลักษณะ สภาพแวดล้อมใต้น้ำและสัญญาณรบกวนจากแหล่งกำเนิดอื่น ซึ่งถึงแม้ว่า คลื่นเสียงจะเดินทางในน้ำได้ดี แต่การเดินทางของคลื่นเสียงใต้น้ำก็ได้รับ ผลกระทบจากความเปลี่ยนแปลงของสภาพแวดล้อมใต้น้ำเป็นอย่างมาก เช่น อุณหภูมิ ความเค็ม และความกดอากาศ นอกจากนี้สภาพแวดล้อมใต้น้ำ ยังมีเสียงรบกวนที่ไม่พึงประสงค์ค่อนข้างมาก ทำให้การสื่อสารใต้น้ำนอกเหนือ ไปจากโทรศัพท์ใต้น้ำที่ใช้รูปแบบการสื่อสารอย่างง่าย เช่น CW และการผสมคลื่น แบบ AM เป็นสิ่งที่ทำได้ยาก อย่างไรก็ตาม ในช่วง ๑๐ ปีที่ผ่านมา การพัฒนา ด้านแบบจำลองสภาพแวดล้อมใต้น้ำและการประมวลผลสัญญาณดิจิทัล ช่วยให้การสื่อสารดิจิทัลใต้น้ำมีความเป็นไปได้มากขึ้น

การสื่อสารดิจิทัลใต้น้ำคือ การแปลงข้อมูลเป็นสัญญาณดิจิทัล และทำการส่งสัญญาณด้วยการผสมสัญญาณไปกับคลื่นเสียงใต้น้ำในลักษณะ เดียวกับของโมเด็มโทรศัพท์ ซึ่งมีข้อดีคือเป็นการเพิ่มความอ่อนตัวและ เพิ่มรูปแบบการสื่อสารที่มีมากขึ้นกว่าสัญญาณมอร์สและสัญญาณเสียง เช่น การส่งข้อความสั้น การรายงานข้อมูลเป้า และการวัดระยะ (Digital Distance Measurement Function) ที่ช่วยลดภาระงานของเจ้าหน้าที่ กับเพิ่มความรวดเร็วและความแม่นยำในการปฏิบัติ นอกจากนี้ความก้าวหน้า ในการประมวลผลสัญญาณดิจิทัลยังช่วยให้สามารถใช้เทคนิคต่าง ๆ ร่วมกับ

การสื่อสารดิจิทัลใต้น้ำ เช่น การใช้เทคนิค Direct Sequence Spread Spectrum (DSSS) ในโหมด MASQ (Multichannel Acoustic Signaling Quality of Service) ของโทรศัพท์ใต้น้ำ UT3000 ที่ช่วยลดการถูกรบกวนสัญญาณและลดการเปิดเผยตัว



ภาพที่ ๓ เทคนิคการผสมคลื่นแบบ MASQ Spread Spectrum ในโทรศัพท์ใต้น้ำ UT3000
ที่มา : UT3000 MASQ, L3 ELAC Nautik, 2011

ที่ผ่านมารูปแบบการสื่อสารดิจิทัลใต้น้ำจะเป็นรูปแบบเฉพาะขึ้นอยู่กับอุปกรณ์และผู้ผลิต ซึ่งผู้ส่งและผู้รับจะต้องใช้อุปกรณ์เดียวกัน หรือ อุปกรณ์จากผู้ผลิตเดียวกัน ส่งผลให้ยังไม่มีการใช้งานเป็นที่แพร่หลาย และหนึ่งในปัจจัยสำคัญในการทำให้การสื่อสารดิจิทัลใต้น้ำมีความเป็นไปได้ ในทางปฏิบัติคือ การกำหนดมาตรฐานกลางที่เป็นที่ยอมรับของผู้ผลิตต่าง ๆ ซึ่งศูนย์วิจัยและทดลองทางทะเล หรือ Centre for Maritime Research and Experimentation (CMRE) ของนาโตได้กำหนดมาตรฐาน Protocol การสื่อสารดิจิทัลใต้น้ำ เรียกว่า JANUS^๖ โดยมีวัตถุประสงค์เพื่อเป็นมาตรฐานเปิดสำหรับนานาชาติ ประกอบด้วย รูปแบบการผสมคลื่น และรูปแบบ Data Packet ที่รองรับอุปกรณ์และโทรศัพท์ใต้น้ำที่มีอยู่ในปัจจุบัน และมีความอ่อนตัวต่อความไม่แน่นอนและการเปลี่ยนแปลงสภาพแวดล้อมใต้น้ำ

การสื่อสารดิจิทัลใต้น้ำ ช่วยเพิ่มความเร็วและความถูกต้องแม่นยำของการรับ-ส่งข้อมูล และสามารถนำไปประยุกต์ใช้กับภารกิจได้หลากหลาย

ตัวอย่างเช่น การช่วยเหลือกู้ภัยเรือดำน้ำ การส่งข้อมูลเป้าและภาพสถานการณ์ผิวน้ำให้กับเรือดำน้ำ และการปฏิบัติการร่วมกันระหว่างเรือดำน้ำกับยานใต้น้ำไร้คนขับ โดยศูนย์วิจัย CMRE ของนาโต้ ได้ทดลองการส่งข้อมูลเรือดำน้ำที่ประสบเหตุฉุกเฉินใต้น้ำตามบรรณสาร ATP-57 The Submarine Search and Rescue Manual ในการฝึก Dynamic Monarch 2017 พบว่าการสื่อสารทางข้อความด้วยมาตรฐานการสื่อสารดิจิทัลใต้น้ำ JANUS ใช้เวลาเพียง ๓ วินาที ในขณะที่การส่งข้อมูลเดียวกันทางเสียงผ่านโทรศัพท์ใต้น้ำต้องใช้เวลาราว ๗๘ วินาที



JANUS-based service for AIS and Distress

Info visualized on GUI at the control station and on the Arpão



JANUS-Based AIS

- Contacts from GPS, AIS, AUVs, operator transmitted via JANUS to the Arpão
- Arpão willing to inject contacts in her combat system

```
>>> DISTRESS <<< At 25
PT
Pos: 38N21.8394 5W5.133
Speed/Heading: 3.3 knt | 78°
Depth: 80 m
O2: 20.3% | CO2: 2.9%
CO: 1.0 ppm | H2: 0.3%
Pressure: 1.0 atm
Temperature: 21.0°C
Survivors: 35 pax
```

JANUS-Based Distress

Status and position transmitted from the Arpão and received at the control station

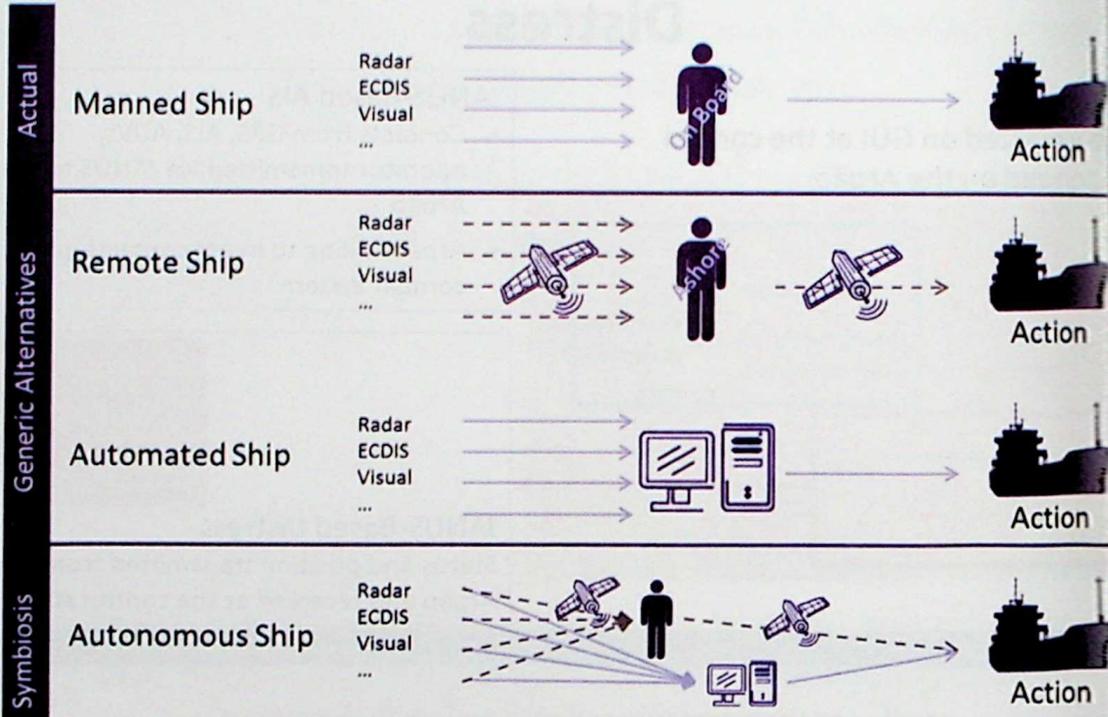
ภาพที่ ๔ การส่งภาพสถานการณ์ผิวน้ำและข้อมูลอื่นด้วย JANUS

ในการฝึกสาธิตร่วมกับกองทัพเรือโปรตุเกส

ที่มา : JANUS: A New Digital Underwater Communications Capability
for SMER, NATO SMERWG 2019

เทคโนโลยี Artificial Intelligence กับการปฏิบัติการเรือดำน้ำ

เทคโนโลยีปัญญาประดิษฐ์ หรือ Artificial Intelligence (AI) เป็นเทคโนโลยีระบบประมวลผลที่มีการวิเคราะห์เชิงลึกและสามารถเรียนรู้ได้จากข้อมูลที่มีอยู่จำนวนมาก คล้ายกับความสามารถในการวิเคราะห์และเรียนรู้ของมนุษย์ เพื่อนำไปใช้ในการตัดสินใจและการแก้ปัญหาต่าง ๆ ซึ่งในปัจจุบันเริ่มมีการศึกษาวิจัยและการนำมาใช้ในทางทหาร โดยเครือข่ายความร่วมมือการวิจัย MUNIN (Maritime Unmanned Navigation Through Intelligence in Networks) ของสหภาพยุโรป ได้แบ่งระดับการใช้งานเทคโนโลยี AI ในส่วนของการปฏิบัติการทางเรือออกเป็น การใช้มนุษย์ควบคุมทั้งหมด (Manned และ Remote) กับการใช้ AI มาช่วยสนับสนุนการตัดสินใจ (Automated และ Autonomous)



ภาพที่ ๕ ระดับการใช้เทคโนโลยี AI ร่วมกับมนุษย์
ที่มา : เครือข่ายความร่วมมือการวิจัย MUNIN

ในส่วนของการปฏิบัติการเรือดำน้ำ การใช้งานเทคโนโลยี AI ที่ทำงานโดยอิสระยังเป็นไปได้ยาก เนื่องจากความซับซ้อนของสภาพแวดล้อมใต้น้ำ ข้อจำกัดในการสื่อสารใต้น้ำ รวมถึงความเสี่ยงอันตรายและความรุนแรงของผลกระทบที่อาจเกิดขึ้นได้หากเกิดข้อผิดพลาด โดยแนวความคิดการใช้เทคโนโลยี AI ในปัจจุบันจะเป็นการสนับสนุนการวิเคราะห์และการตัดสินใจของมนุษย์ที่เป็นผู้ปฏิบัติงานในลักษณะของ Augmented Intelligence มากกว่าที่จะเป็นระบบอิสระในลักษณะของ Automated System หรือ Autonomous System

แนวความคิดการใช้งานเทคโนโลยี AI สนับสนุนการตัดสินใจของมนุษย์ในเรือดำน้ำที่กำลังเป็นที่สนใจในปัจจุบัน จะเน้นไปที่การใช้งานในระบบตรวจจับเพื่อแยกแยะ ติดตาม และพิสูจน์ทราบเป้า ทั้งในส่วนของโซนาร์ที่เป็นระบบตรวจจับหลักของเรือดำน้ำ และระบบตรวจจับอื่น เช่น กล้อง Periscope โดยเป้าเรือแต่ละประเภทจะมีลักษณะและองค์ประกอบของความถี่เสียงที่ต่างกันไป ซึ่งการใช้เทคโนโลยี AI ในระบบโซนาร์จะช่วยในการพิสูจน์ทราบเป้า โดยแยกแยะรูปแบบ (Pattern Recognition) และวิเคราะห์ลักษณะของเส้นความถี่เสียงที่ตรวจจับได้จากโซนาร์ Passive ภายใต้สภาพแวดล้อมที่มีเสียงรบกวน ด้วยการเรียนรู้จากฐานข้อมูลความถี่เสียงของเป้าประเภทต่าง ๆ

อีกแนวความคิดหนึ่งในการใช้เทคโนโลยี AI ในการปฏิบัติการเรือดำน้ำ คือ การช่วยแยกแยะและพิสูจน์ทราบเป้าจากกล้อง Periscope และกล้อง Optronic ซึ่งเรือดำน้ำจะพยายามใช้กล้อง Periscope และกล้อง Optronic ให้น้อยที่สุดเพื่อเป็นการซ่อนพรางและลดความเสี่ยงในการถูกตรวจจับ และในอดีตนายทหารยามเรือดำน้ำจะถูกฝึกให้แยกแยะ พิสูจน์ทราบ และรวบรวมข้อมูลเป้าด้วยสายตาอย่างรวดเร็วภายในเวลาไม่กี่วินาที เพื่อลดเวลาการชกกล้องขึ้นเหนือผิวน้ำ ซึ่งในปัจจุบันได้มีการพัฒนากล้อง Optronic ที่สามารถหมุนตรวจการณ์ได้อย่างรวดเร็วและถ่ายภาพเก็บไว้เพื่อทำการวิเคราะห์ในภายหลัง แต่การวิเคราะห์ภาพที่ได้จากกล้อง Optronic ยังคงต้องทำโดยผู้ปฏิบัติงานที่อาจต้องใช้เวลาอันยาวนานและมีโอกาสมองไม่เห็นเป้าหมายขนาดเล็กกระยะไกลได้ ซึ่งเทคโนโลยี AI สามารถทำงานร่วมกับกล้อง Periscope และ Optronic

เพื่อช่วยในการตรวจจับและแยกแยะเป้าที่มองเห็นได้ยากได้ถูกต้องและรวดเร็วขึ้น ช่วยลดความเสี่ยงในการเปิดเผยตัวและเพิ่มประสิทธิภาพในการปฏิบัติการของเรือดำน้ำ

Digital Crew – Automated Intelligence



- **Digital Crew: Artificial intelligence and machine learning**
 - Automatically detect, classify and track targets
 - Quick Look Round (QLR) – programmable options
 - Minimum exposure and maximum performance with lowest signature

ภาพที่ ๖ การใช้ AI ช่วยแยกแยะและติดตามเป้าจากฉากหลังในกล้อง Periscope เรือดำน้ำ
ที่มา : Thales UK

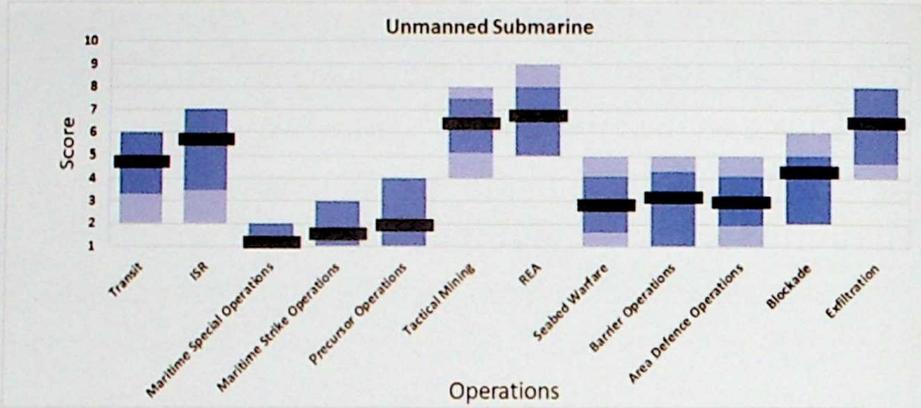
เทคโนโลยียานใต้น้ำไร้คนขับและเรือดำน้ำขนาดเล็ก

จากความสำเร็จในการพัฒนาและการใช้งานเทคโนโลยีอากาศยานไร้คนขับ (Unmanned Aerial Vehicle: UAV) กับยานผิวน้ำไร้คนขับ (Unmanned Surface Vehicle: USV) ในปัจจุบัน ทำให้เทคโนโลยียานใต้น้ำไร้คนขับ หรือ UUV (Unmanned Underwater Vehicle) กำลังเป็นที่สนใจในหลายประเทศ อย่างไรก็ตาม สาเหตุที่ทำให้การพัฒนาเทคโนโลยียานใต้น้ำไร้คนขับเกิดขึ้นช้ากว่าการพัฒนาเทคโนโลยีอากาศยานไร้คนขับและยานผิวน้ำไร้คนขับคือ สภาพแวดล้อมใต้น้ำที่มีความซับซ้อนและมีข้อจำกัดในการตรวจการณ์และการสื่อสาร ส่งผลให้การพัฒนาเทคโนโลยียานใต้น้ำไร้คนขับมีความท้าทายที่จะต้อง

สามารถปฏิบัติการได้โดยอาศัยการควบคุมน้อยกว่าอากาศยานไร้คนขับ และยานใต้น้ำไร้คนขับ และต้องสามารถตรวจจับและพิสูจน์ทราบเป้า จากโซนาร์ภายใต้สภาพแวดล้อมที่มีเสียงรบกวนได้ด้วยตัวเอง

หนึ่งในคำถามที่น่าสนใจคือ ยานใต้น้ำไร้คนขับในอนาคตจะเข้ามาทดแทนเรือดำน้ำ และส่งผลให้เรือดำน้ำกลายเป็นอาวุธที่ล้าสมัยได้หรือไม่ ซึ่งสถาบันวิจัยวิทยาศาสตร์ประยุกต์ของเนเธอร์แลนด์ หรือ TNO (Toegepast Natuurwetenschappelijk Onderzoek) ได้ทำการศึกษาความเป็นไปได้ในการใช้ยานใต้น้ำไร้คนขับทดแทนเรือดำน้ำดีเซล-ไฟฟ้า ในหัวข้อ The Unmanned Underwater Vehicle: An Alternative for the SSK or a Valuable Addition? เป็นส่วนหนึ่งของการเตรียมโครงการเรือดำน้ำทดแทนเรือดำน้ำชั้น Walrus โดยได้กำหนดเป้าหมายหลักทางยุทธศาสตร์ ๔ ประการ ในการทดแทนเรือดำน้ำ ได้แก่ การสร้างอิทธิพลทางยุทธศาสตร์ การโจมตีที่รุนแรงและแม่นยำ การรวบรวม-วิเคราะห์-แลกเปลี่ยนข้อมูลข่าวสาร และการปฏิบัติการพิเศษ และพิจารณาขีดความสามารถของยานใต้น้ำไร้คนขับที่ควรจะมีในปี ค.ศ. ๒๐๒๗ (ซึ่งเป็นช่วงเวลาที่เรือดำน้ำชั้น Walrus จะถูกทดแทน) จากพื้นฐานเทคโนโลยีในปี ค.ศ. ๒๐๑๘ กับการประเมินการปฏิบัติการกิจ ๑๒ แบบ ด้วยวิธี Delphi ประยุกต์จากผู้เชี่ยวชาญ ๘ คน ในการให้คะแนนความเหมาะสม ๑-๑๐ คะแนน ผลการประเมินพบว่า การพัฒนาเทคโนโลยียานใต้น้ำไร้คนขับยังไม่สามารถทดแทนความต้องการเรือดำน้ำของกองทัพเรือเนเธอร์แลนด์ ในปี ค.ศ. ๒๐๒๗ ได้ เนื่องจากข้อจำกัดเรื่องระยะปฏิบัติการและอำนาจการยิง การพัฒนาระบบ AI ที่ยังไม่สามารถทำให้ยานใต้น้ำปฏิบัติการได้โดยอิสระในสภาพแวดล้อมที่มีความซับซ้อน และมีค่าใช้จ่ายที่สูงเกินไป ในการพัฒนาระบบที่มีขีดความสามารถตรงตามความต้องการ อย่างไรก็ตาม ผลการศึกษาดังกล่าวพบว่า ยานใต้น้ำไร้คนขับสามารถเป็นตัวทวีกำลัง (Force Multiplier) ที่ช่วยเสริมขีดความสามารถของเรือดำน้ำ และข้อมูลจากการปฏิบัติการร่วมกันระหว่างเรือดำน้ำกับยานใต้น้ำไร้คนขับในอนาคต จะสามารถนำมาใช้เป็นประโยชน์ในการพัฒนายานใต้น้ำไร้คนขับที่ปฏิบัติการได้โดยอิสระอย่างสมบูรณ์หรือ Autonomous Underwater Vehicle (AUV)

SCORES OF THE UNMANNED SUBMARINE AGAINST THE 12 NOTIONAL OPERATIONS



ภาพที่ ๗ ผลการประเมินการใช้นานใต้น้ำไร้คนขับในภารกิจ ๑๒ แบบ ของเนเธอร์แลนด์ แสดงให้เห็นว่าภารกิจที่เหมาะสมกับยานใต้น้ำไร้คนขับคือการรวบรวมข่าวสาร (ISR) การวางทุ่นระเบิด การรวบรวมข้อมูลสภาพแวดล้อม (REA) และการเล็ดลอดออกจากพื้นที่
ที่มา : Toegepast Natuurwetenschappelijk Onderzoek (TNO)

จากข้อจำกัดของเทคโนโลยียานใต้น้ำไร้คนขับในปัจจุบันที่ยังไม่สามารถทดแทนเรือดำน้ำที่มีคนปฏิบัติงานภายในได้ ทำให้เรือดำน้ำขนาดเล็กหรือ Midget Submarine ยังคงเป็นที่น่าสนใจ เนื่องจากเป็นทางเลือกตรงกลางระหว่างยานใต้น้ำไร้คนขับ กับเรือดำน้ำดีเซล-ไฟฟ้าขนาดกลาง ที่มีความเหมาะสมกับภารกิจการป้องกันฝั่งและการปฏิบัติการพิเศษ โดยเรือดำน้ำขนาดเล็กมีข้อได้เปรียบในการปฏิบัติการในพื้นที่จำกัดใกล้ชายฝั่งคล้ายกับยานใต้น้ำไร้คนขับ แต่การมีคนบังคับอยู่ภายใน ส่งผลให้สามารถประมวลข้อมูลและทำการตัดสินใจในพื้นที่ปฏิบัติการได้ดีกว่าเทคโนโลยียานใต้น้ำไร้คนขับ ส่งผลให้ในปัจจุบันยังคงมีการวิจัยและพัฒนาเทคโนโลยีใหม่ ๆ เกี่ยวกับเรือดำน้ำขนาดเล็ก

ข้อได้เปรียบหลักของเรือดำน้ำขนาดเล็กคือ ความสามารถในการปฏิบัติการในพื้นที่จำกัดใกล้ฝั่ง ตัวอย่างเช่น เรือดำน้ำขนาดเล็ก แบบ DG160 จากบริษัท Drass ของอิตาลี ที่ถูกออกแบบให้มีความคล่องตัวในพื้นที่ปฏิบัติการ

ที่มีความลึกน้ำน้อยกว่า ๒๐๐ ม. มีความยาวประมาณ ๓๒ ม. ระวังงขั้บน้ำ ๑๖๙ ตัน ใช้กำลังพลประจำเรือ ๗ นาย ระวังรับชุดปฏิบัติการพิเศษ ๘ นาย ใช้ระบบขับเคลื่อนดีเซล-ไฟฟ้า มีระยะปฏิบัติการไกลสุด ๒,๐๐๐ ไมล์ทะเล ติดตั้งตอร์ปิโดหนักขนาด ๕๓๓ มม. จำนวน ๒ ลูก ระวังรับยาน SDV (Swimmer Delivery Vehicle) สำหรับรับ-ส่งชุดปฏิบัติการพิเศษได้ ๒ ลำ และสามารถติดตั้งอุปกรณ์เสริมด้านข้างตัวเรือ (Lateral Equipment) ได้แก่ ท่อยิงตอร์ปิโดหนักขนาด ๕๓๓ มม. เพิ่มเติมจำนวน ๒ ลูก หรือเรือยางสำหรับชุดปฏิบัติการพิเศษ หรือทุ่นระเบิด จำนวน ๖ ลูก นอกจากนี้ยังมีจุดเด่นที่สำคัญคือ สามารถถอดแยกชิ้นส่วนตัวเรือทนความดันได้เป็น ๔ ส่วน เพื่อความสะดวกในการซ่อมบำรุงและการขนส่งทางบก

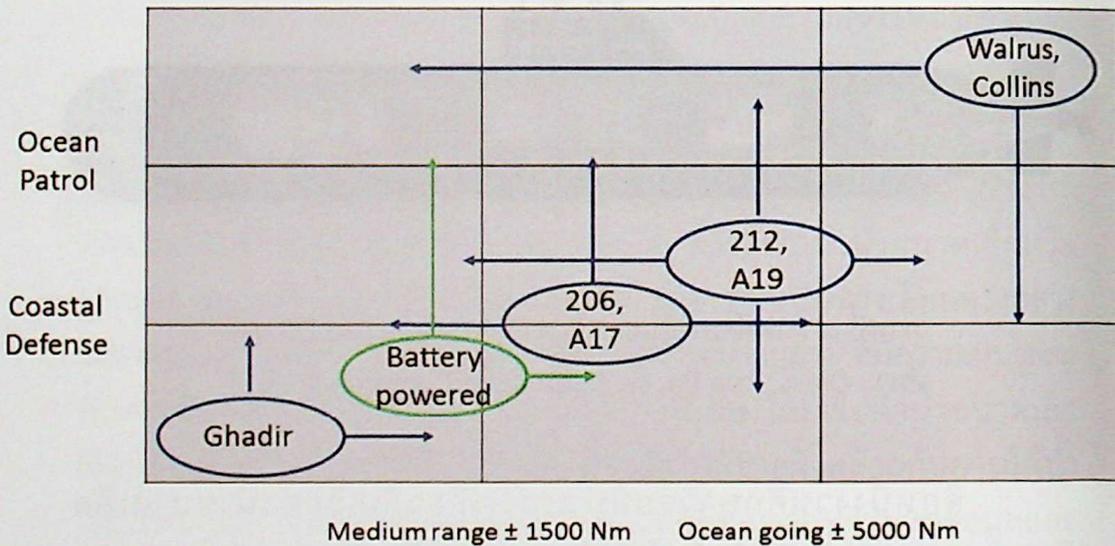


ภาพที่ ๘ ภาพตัดภายในของเรือดำน้ำขนาดเล็กแบบ DG160

ที่มา : Drass, Asia Pacific Submarine Conference 2017

อีกหนึ่งงานศึกษาวิจัยที่น่าสนใจเกี่ยวกับเรือดำน้ำขนาดเล็ก คือ การออกแบบเรือดำน้ำที่ใช้พลังงานจากแบตเตอรี่ Lithium-ion เพียงอย่างเดียวโดยบริษัท Nevesbu ของเนเธอร์แลนด์^{๑๐} ซึ่งมีข้อดีในการช่วยลดการเปิดเผยตัว เนื่องจากไม่จำเป็นต้อง Snorkel เพื่อชาร์จแบตเตอรี่ ลดความซับซ้อนของระบบเครื่องกำเนิดไฟฟ้าดีเซลและระบบน้ำมันเชื้อเพลิง รวมถึงลดค่าใช้จ่ายในการซ่อมบำรุง โดยบริษัท Nevesbu ได้ทดลองปรับปรุงจากต้นแบบเรือดำน้ำชั้น Moray ที่มีระวางขั้บน้ำบนผิวน้ำ ๑,๗๐๐ ตัน

แต่ติดตั้งแบตเตอรี่ Lithium-ion แบบ NMC (Lithium Nickel Manganese Cobalt Oxide) ทั้งหมดโดยไม่มีเครื่องกำเนิดไฟฟ้าดีเซล ผลการคำนวณพบว่าเรือดำน้ำชั้น Moray ติดตั้งแบตเตอรี่ Lithium-ion โดยไม่มีเครื่องกำเนิดไฟฟ้าดีเซลจะมีระยะปฏิบัติการไกลสุดประมาณ ๒,๐๐๐ ไมล์ทะเล และมีระยะเวลาปฏิบัติการประมาณ ๒ สัปดาห์ ซึ่งน้อยเกินไปสำหรับเรือดำน้ำขนาดกลางระหว่างขั้วน้ำประมาณ ๑,๕๐๐ - ๑,๗๐๐ ตัน ในปัจจุบันที่มีระยะปฏิบัติการไกลสุดประมาณ ๑๐,๐๐๐ ไมล์ทะเล และมีระยะเวลาปฏิบัติการประมาณ ๔ สัปดาห์ อย่างไรก็ตาม ผลการศึกษาของเนเธอร์แลนด์พบว่า แนวความคิดการออกแบบเรือดำน้ำที่ใช้พลังงานจากแบตเตอรี่ Lithium-ion เพียงอย่างเดียวมีความเป็นไปได้สำหรับเรือดำน้ำขนาดเล็ก ระหว่างขั้วน้ำน้อยกว่า ๑,๐๐๐ ตัน ที่มีระยะปฏิบัติการประมาณ ๒,๐๐๐ ไมล์ทะเล และมีระยะเวลาปฏิบัติการประมาณ ๒ สัปดาห์



ภาพที่ ๙ แนวความคิดการใช้แหล่งพลังงานแบตเตอรี่ล้วน มีความเป็นไปได้สำหรับเรือดำน้ำขนาดเล็ก ระหว่างขั้วน้ำน้อยกว่า ๑,๐๐๐ ตัน
ที่มา : Nevesbu, Undersea Defense Technology 2018

บทสรุป

จากข้อจำกัดของสภาพแวดล้อมที่มีความซับซ้อนแล้วเป็นอันตรายต่อการปฏิบัติการ ทำให้เทคโนโลยีเรือดำน้ำทางทหารยังเป็นเทคโนโลยีค่อนข้างใหม่เมื่อเทียบกับยานรบประเภทอื่น และเริ่มมีการใช้งานอย่างได้ผลและแพร่หลายในช่วงประมาณ ๑๕๐ ปีที่ผ่านมา และยังมีโอกาสในการพัฒนาเทคโนโลยีต่อไปได้อีกในอนาคต ทั้งในด้านระบบขับเคลื่อน การสื่อสารใต้น้ำ การใช้เทคโนโลยี AI มาช่วยในการติดตาม แยกแยะ และพิสูจน์ทราบเป้า และการพัฒนายานใต้น้ำไร้คนขับกับเรือดำน้ำขนาดเล็ก ทั้งนี้ จะเห็นได้ว่าแนวโน้มการพัฒนาเทคโนโลยีเรือดำน้ำในด้านต่าง ๆ มักเป็นการให้ความสำคัญกับจุดแข็งของเรือดำน้ำในการซ่อนพรางซึ่งจะมีผลกระทบต่อสงครามทางเรือในอนาคต คือ มิติใต้น้ำจะยังคงเป็นมิติที่เหมาะสมที่สุดในการซ่อนพราง และเรือดำน้ำจะยังคงเป็นอาวุธซ่อนพรางที่ค้นหาและตรวจจับได้ยาก ส่งผลให้กำลังรบใต้น้ำจะยังคงมีบทบาทสำคัญในสงครามอนาคต และเป็นปัจจัยสำคัญในการเพิ่มศักยภาพสงครามให้กับฝ่ายเดียวกัน รวมถึงเป็นปัจจัยที่จะเพิ่มความยุ่งยากในการตัดสินใจและการระวังป้องกันของฝ่ายตรงข้ามเป็นอย่างมาก

น.ท.สุระ บรรจงจิตร รับราชการในกองทัพเรือมากกว่า 20 ปี ได้เคยผ่านประสบการณ์การปฏิบัติงานสำคัญที่เกี่ยวข้องกับเรือดำน้ำ ได้แก่ หลักสูตรวิทยาการและเทคโนโลยีเรือดำน้ำเยอรมนี กำลังพลรับเครื่องฝึกศูนย์ยุทธการเรือดำน้ำ ผู้สังเกตการณ์การฝึกในเรือดำน้ำ ชั้น Los Angeles ของกองทัพเรือ

สหรัฐอเมริกา ผู้สังเกตการณ์การฝึกในเรือดำน้ำ ชั้น 212A ของกองทัพเรือเยอรมนี
หัวหน้าชุดฝึกศูนย์ยุทธการเรือดำน้ำ และครูฝึกเรือดำน้ำของกองเรือดำน้ำ
กองเรือยุทธการ น.ท.สุระ ฯ ได้ลาออกจากราชการเมื่อปี ๒๕๖๒ ปัจจุบันเป็น
ที่ปรึกษาอิสระและผู้เชี่ยวชาญด้านเรือดำน้ำ

เอกสารอ้างอิง

- ^a Silent Fleet, 5th edition. (Hamburg: Howaldtswerke-Deutsche Werft GmbH, 2011), pp. 39-40
- ^b Angela Psoma, Gunter Sattler “Fuel cell systems for submarines: from the first idea to serial production.” Journal of Power Sources Vol. 106 Issues 1-2 (London: Elsevier, 2002), pp.381-383
- ^c Masao Kobayashi, “Lithium Ion Batteries in Submarines – Giving Greater Discretion and Endurance for Conventionally Powered Submarines.” UDT Asia 2017
- ^d Vincenzo Pennino, “Lithium-ion Battery for U212NFS” Undersea Defense Technology 2019
- ^e Sabrina Schreiber, Ivor Nissen, “Digital distance and channel measurements with the UT3000.” Undersea Defense Technology 2015
- ^f John Potter, Joao Alves, Dale Green, Giovanni Zappa, Ivor Nissen, Kim McCoy, “The JANUS Underwater Communications Standard.” IEEE Underwater Communications Networking Conference, September 2014
- ^g Roberto Petrocchia, “JANUS: A New Digital Underwater Communications Capability for SMER.” NATO Submarine Escape and Rescue Working Group 2019
- ^h Eva Artusi, Fabien Chaillan, “Automatic Recognition of Underwater Acoustic Signature for Naval Applications.” 1st Maritime Situational Awareness Workshop 2019

- “ Jeroen de Jonge, Jan Bruggeman, Koen Blom, Nicole van Elst, Hilvert Fitski, Leon Kester, Wouter Noordkamp, “The Unmanned Under water Vehicle: An Alternative for the SSK or a Valuable Addition?” UDT Asia 2019
- “ Sven Los, Wahyu Schiks, “Total Battery Powered Submarine Design, A New Way of Thinking.” Undersea Defense Technology 2018



พลังความร่วมมือ เพื่อพลังงานที่ยั่งยืน



ปตท.สผ. ก่อตั้งขึ้นเมื่อปี 2528 ในฐานะบริษัทสำรวจและผลิตปิโตรเลียมของคนไทยที่มีพันธกิจในการสร้างความมั่นคงทางพลังงาน จากจุดเริ่มต้นการกิจการค้นหา ทำให้เราค้นพบแหล่งพลังงานเพื่อคนไทย พร้อมขับเคลื่อนเศรษฐกิจและทุกชีวิตให้เติบโต พบว่าเมื่อร่วมใจก็สามารถสร้างสังคมที่ดียั่งยืนและพบว่าถ้าเคียงข้างกันไปยากแค่ไหนก็ไปได้ไกลกว่า

www.pttep.com



UNMANNED SURFACE VEHICLE FOR RTN's
FUTURE WARFARE : CONCEPTUAL DESIGN
OF SUITABLE PLATFORM

เรือผิวน้ำไร้คนขับ

สำหรับสงครามอนาคตของกองทัพเรือไทย
: การออกแบบตัวเรือและระบบขับเคลื่อน
ในระดับเบื้องต้น

อ่าทึ่ นากาโท ปริญญ์ กึนอยู่
หัวหน้าออกแบบและทดลองเรือ กองแผนและประมาณการช่าง
อู่ทหารเรือธนบุรี กรมอู่ทหารเรือ

บทคัดย่อ

ในช่วงทศวรรษที่ผ่านมา เรือผิวน้ำไร้คนขับ (Unmanned Surface Vessels: USVs) ได้รับการพัฒนาและนำมาประยุกต์ใช้ในหลากหลายภารกิจโดยเฉพาะภารกิจทางทหาร เพื่อเป็นการตอบสนองความต้องการการใช้เรือตามแผนยุทธศาสตร์กองทัพเรือ ๒๐ ปี แผนการจัดการเรือดำน้ำ และแผนการปฏิบัติงานของ ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) แพลตฟอร์มพื้นฐานสำหรับติดตั้งระบบ Mission Modules และระบบควบคุมสั่งการ AI ได้ถูกออกแบบขึ้นตามหลักการทางนาเวศสถาปัตยกรรม ผสมผสานกับเทคนิคการออกแบบเรือสมัยใหม่ ทำให้เป็นจุดเริ่มต้นของการพัฒนาออกแบบและผลิต USVs ขึ้นมาใช้ราชการในกองทัพเรืออย่างเหมาะสมและสมบูรณ์แบบ

คำสำคัญ

USVs, Trimaran, Mission Modules

บทนำ

๑. สงครามอนาคตและทิศทางการเลือกใช้ประเภทของยูโรเปียนท์ในยุทธรนาวิ

ในช่วงทศวรรษที่ผ่านมา การพัฒนาทางด้านวิทยาศาสตร์ เทคโนโลยี และวิศวกรรม ดำเนินไปอย่างก้าวกระโดด ส่งผลกระทบโดยตรงการดำเนินกิจกรรมทางด้านต่าง ๆ ของมนุษย์อย่างหลีกเลี่ยงไม่ได้ โดยทางด้านมิติของความมั่นคงทั้งในระดับจุลภาคและมหภาค เพื่อป้องกันภัยคุกคามในรูปแบบต่าง ๆ ที่อาจเกิดขึ้นได้จากความก้าวหน้าทางเทคโนโลยีเหล่านี้ กองทัพเรือในฐานะหน่วยงานผู้ดูแลรับผิดชอบทางด้านความมั่นคง และการรักษาผลประโยชน์ของชาติทางทะเล ตระหนักถึงผลกระทบต่าง ๆ จากความก้าวหน้าทางเทคโนโลยี ได้วางแผนยุทธศาสตร์กองทัพเรือ ๒๐ ปี เพื่อรองรับการเปลี่ยนแปลงที่จะเกิดขึ้น จึงจำเป็นต้องมีความพร้อมทั้งในส่วนของกำลังทางเรือ ระบบสนับสนุน รวมทั้งอุตสาหกรรมเพื่อการป้องกันประเทศที่เกี่ยวข้องต้องได้รับการพัฒนาอย่างเป็นระบบ โดยตามแผนยุทธศาสตร์ดังกล่าว กองทัพเรือจะมีแนวทางการใช้กำลังทางเรือที่สามารถควบคุมสถานการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ

ซึ่งแนวทางที่เหมาะสมกับสถานการณ์และธรรมชาติของกำลังรบทางเรือคือ การป้องกันเชิงรุก (Active Defense) ด้วยขนาดของกำลังที่เหมาะสม

เมื่อพิจารณาถึงประเภทเรือต่าง ๆ ตามแผนกำลังรบหลักตามยุทธศาสตร์ กองทัพเรือ ๒๐ ปี และแนวทางของเทคโนโลยีทางด้านนาวิกาสถาปัตยกรรมผนวกกับเทคโนโลยีของสงครามในอนาคต USV (Unmanned Surface Vehicle) เรือผิวน้ำไร้คนขับ มีความเหมาะสมในการพิจารณานำมาประยุกต์ใช้งาน ในภารกิจต่าง ๆ ของกองทัพเรือ อีกทั้งยังสามารถบูรณาการร่วมกับเทคโนโลยี Mission Module เพื่อให้ได้ยานผิวน้ำที่ทรงคุณประโยชน์ และตอบสนอง ความต้องการทางยุทธวิธีรอบด้าน โดยมีข้อดีสำหรับนำมาใช้ในการพิจารณา ดังนี้

๑.๑ USV สามารถปฏิบัติงานได้ในพื้นที่ที่รกรากและอันตราย อันเป็นข้อจำกัดที่มนุษย์ไม่สามารถเข้าถึงได้

๑.๒ USV มีความอ่อนตัวในแง่ของขนาดมิติ เมื่อเทียบกับเรือทั่วไป ที่สามารถปฏิบัติการกิจได้เหมือนกัน

๑.๓ Mission Module เป็นแนวทางที่สามารถนำมาประยุกต์บูรณาการ ร่วมกับ USV เพื่อให้ Platform พื้นฐานของยานหนึ่งลำ สามารถปฏิบัติการกิจ ที่หลากหลายได้

จากข้อดีของ USV ที่กล่าวมาข้างต้นสามารถลบจุดอ่อนสำคัญของ เรือผิวน้ำธรรมดาได้ในหลายประการ ทำให้มีความอ่อนตัวในการนำมาใช้ อีกทั้ง หากบูรณาการเข้ากับ Modularity Concept จะสามารถประยุกต์ใช้ USV ได้ในหลากหลายภารกิจบน Platform หลักหนึ่งหน่วย ซึ่งลดต้นทุนการผลิต และการดำเนินการกิจ จึงเป็นทางเลือกของยุทธโศปกรณ์ที่มีความเหมาะสม ในการพิจารณาจัดหาและนำมาประจำการใช้ในกองทัพเรือเพื่อตอบสนอง ภารกิจตามแผนยุทธศาสตร์กองทัพเรือ ๒๐ ปี

๒. ประวัติและบทบาทของ USV

Unmanned Surface Vessels (USVs) หรือบางครั้งถูกเรียกว่า Autonomous Surface Crafts (ASC) มีจุดเด่นจากนิยาม “ไร้คนขับ”^๑ ที่ทำให้มีศักยภาพในการปฏิบัติงานได้หลากหลายมากขึ้นเมื่อเทียบกับเรือทั่วไป

ผนวกกับความก้าวหน้าทางเทคโนโลยีของระบบนำร่อง ระบบควบคุม และระบบปัญญาประดิษฐ์ ทำให้ USV ในช่วงทศวรรษที่ผ่านมาถูกใช้ในหลายกิจกรรม ทั้งสำรวจ กู้ภัย และวัตถุประสงค์ทางทหาร แต่จำนวนของหน่วยที่ถูกนำมาใช้ก็ยังมีน้อยกว่าเมื่อเทียบกับ Unmanned Undersea Vehicles (UUVs) ด้วยข้อจำกัดบางประการ จึงทำให้เป็นความท้าทายสำหรับสถาบันวิจัยต่าง ๆ ได้สามารถพัฒนา USVs ให้มีคุณสมบัติเทียบเท่ากับ UUVs ในทุก ๆ การใช้งานในภารกิจ

ในปี ค.ศ.๑๙๙๓ ซึ่งเป็นช่วงเริ่มต้นของการพัฒนา USVs^๖ Massachusetts Institute of Technology (MIT) ได้สร้าง USV ชื่อ ARTEMIS โดยพัฒนาสายเส้นตัวเรือมาจากเรือประมงอวนลากแล้วย่อขนาดลงให้เป็นแพลตฟอร์มที่สามารถติดตั้งระบบทำร่องและระบบควบคุมต่าง ๆ ที่จำเป็นสำหรับ USV และถูกนำไปใช้เป็นเครื่องมือในการเก็บข้อมูล Bathymetry ในแม่น้ำ Charles ในบอสตัน ข้อบกพร่องสำคัญของ ARTEMIS คือ มีขนาดเล็กซึ่งส่งผลไปยังคุณสมบัติทางระยะปฏิบัติการ และคุณสมบัติความคงทนทะเล นอกจากนี้ พื้นที่ปฏิบัติการยังถูกจำกัดได้เพียงแคในแม่น้ำ Charles และสามารถประยุกต์ใช้ได้แค่เพียงการเก็บข้อมูลทางวิทยาศาสตร์ จุดบกพร่องเหล่านี้ได้รับการแก้ไขโดยการพัฒนา USV รุ่นใหม่ที่มีขนาดใหญ่ขึ้น สามารถรองรับอุปกรณ์นำร่อง อุปกรณ์ควบคุม ปัญญาประดิษฐ์ และอุปกรณ์สำรวจตามภารกิจต่าง ๆ ได้หลากหลายและอ่อนตัวมากขึ้น โดยยังคงความสะดวกและง่ายในการปล่อยออกปฏิบัติการ จึงทำให้ USVs เริ่มพัฒนาเข้าสู่แพลตฟอร์มที่มีศักยภาพในการปฏิบัติงานในพื้นที่ชายฝั่งมากขึ้น (จากจุดเริ่มต้นเพียงในแต่แม่น้ำ) ส่งผลให้ USVs เริ่มมีการนำมาประยุกต์ใช้ในหลากหลายภารกิจมากยิ่งขึ้น นอกเหนือไปจากเพียงแค่การเก็บข้อมูลทางวิทยาศาสตร์

ในช่วง ๕ ปีที่ผ่านมา การพัฒนาเทคโนโลยีของ USVs เป็นไปอย่างก้าวกระโดด US Navy เริ่มต้นพัฒนา UUVs อย่างกว้างขวางมาก่อน ก่อนที่จะเริ่มให้ความสำคัญและความจริงจังในการพัฒนา USVs โดยเริ่มต้นด้วยการนำ USVs มาเป็นฐานเคลื่อนที่ในการขยายสัญญาณการสื่อสารระหว่าง UUVs กับห้องควบคุมภาคพื้น เพื่อเป็นการขยายระยะปฏิบัติการของ UUVs ให้เป็นแบบไร้คนขับอย่างสมบูรณ์แบบ จากนั้นได้มีการพัฒนาประยุกต์ในกิจการ

ทางทหารมากขึ้น เช่น การตรวจการณ์ชายฝั่ง การล่าทำลายทุ่นระเบิด เป็นต้น แพลตฟอรม์ที่ใช้สำหรับสร้าง USVs คือ เรือผิวน้ำขนาดเล็กปกติทั่วไปที่ได้รับการติดตั้งระบบนำร่อง ควบคุมสั่งการ ปัญญาประดิษฐ์ และอุปกรณ์สำหรับภารกิจต่าง ๆ อาจกล่าวได้ว่า เรือขนาดเล็กทุกชนิดสามารถนำมาใช้เป็นแพลตฟอร์มพื้นฐานของ USVs ได้ทั้งหมด ทำให้บรรลุวัตถุประสงค์หลักตามนิยามของ USVs คือการที่สามารถใช้งานได้ในภารกิจที่มนุษย์ยากจะเข้าถึง และมีอันตรายอย่างไรก็ดี ในภารกิจทางทหารบางประเภท เช่น ภารกิจการช่วยเหลือตัวประกัน และการเข้าจู่โจม USVs ไม่สามารถเป็นพาหนะไร้คนขับได้อย่างสมบูรณ์แบบ โดยเมื่อเข้าพื้นที่ปฏิบัติการ ระบบควบคุมจะถูกส่งกลับไปทีสถานี่ควบคุมที่มีมนุษย์คอยสั่งการผ่านทางระบบควบคุมระยะไกล เพื่อหลีกเลี่ยงผลที่ไม่พึงประสงค์จากการประมวลผลของปัญญาประดิษฐ์ ในภารกิจที่มีความอ่อนไหวเป็นอย่างสูง

ในภารกิจทางด้านการสำรวจ นอกเหนือจากเรือท้องเดี่ยว (Monohull) แล้ว เรือสองท้อง (Catamaran) ยังได้รับความนิยมในการนำมาประยุกต์ใช้เป็นแพลตฟอร์มหลัก ด้วยคุณสมบัติที่ได้เปรียบเมื่อเทียบกับเรือท้องเดี่ยว เช่น น้ำหนักและพื้นที่บรรทุกที่เพิ่มมากขึ้น การทรงตัว ความสะดวกทนทะเล เป็นต้น ในขณะเดียวกัน ภารกิจการสำรวจบางประเภท เช่น การสำรวจทางอุทกศาสตร์ เลือกใช้แพลตฟอร์มประเภท Semi-Submersible ซึ่งได้รับการพัฒนามากจาก SWATH โดยใช้ท้องเรือเพียงท้องเดียว พื้นที่ส่วนใหญ่ของแพลตฟอร์มประเภทนี้จะอยู่ใต้น้ำ ยกเว้นส่วนเสาอากาศที่ใช้สื่อสารกับห้องควบคุม ข้อได้เปรียบของแพลตฟอร์มประเภทนี้คือ คุณสมบัติความคงทนทะเล ที่จะสามารถนำภารกิจประเภทนี้ไปได้ไกลมากขึ้น

๓. การใช้ USVs ในยุทธนาวี

Heo^๓ ได้ทบทวนวรรณกรรม สรุป และเปรียบเทียบข้อมูลของ Military USVs ไว้อย่างครอบคลุม US Navy ได้พัฒนา USVs มาใช้ในหลากหลายภารกิจ เช่น Anaconda 2.0 สำหรับภารกิจลาดตระเวน และการหาข่าวทางยุทธวิธีระดับสูง ACTUV (Anti-Submarine Warfare Continuous Trail Unmanned Vehicle) สำหรับภารกิจลาดตระเวน และการตรวจหา

เรือดำน้ำ USVs ระดับสูง ทั้งสองชุดนี้เป็นชุดที่ได้รับการพัฒนาอย่างจริงจัง และมีเทคโนโลยี AI สูงที่สุดในปัจจุบันนี้ จนอาจกล่าวได้ว่าเป็น USVs ที่ปฏิบัติการโดยไร้คนขับได้อย่างสมบูรณ์แบบ นอกจากนี้ USVs ที่ใช้ใน US Navy ยังมี CUSV (Common Unmanned Surface Vehicle) สำหรับภารกิจลาดตระเวน และหาข่าวชายฝั่งทั่วไป และ ASW USV (Anti-Submarine Warfare Unmanned Surface Vehicle) สำหรับภารกิจการต่อต้านเรือดำน้ำทั่วไป ในขณะเดียวกัน กองทัพเรือชาติอื่น ๆ ได้ทำการพัฒนา USVs ให้มีความทันสมัยตอบสนองกับภัยคุกคามที่กำลังเผชิญอยู่ เช่น Israel Navy ได้พัฒนา KATANA สำหรับภารกิจรักษาความปลอดภัยชายฝั่ง และทำเรือ Silver Marine สำหรับภารกิจลาดตระเวนหาข่าวทั้งกลางวันและกลางคืน เป็นต้น

๓.๑ การใช้ USV ในกองทัพเรือไทย

๓.๑.๑. แนวความคิดในการใช้ USV ของกองทัพเรือไทย

จากการพัฒนาอย่างต่อเนื่องของแนวทางการใช้ USV ทำให้เกิดผลกระทบที่ต้องพิจารณาทั้งในแง่มุมมองของเครื่องมือที่ทันสมัยสำหรับภารกิจทางทหาร และในแง่มุมมองของสิ่งที่จะมาเป็นภัยคุกคามในรูปแบบใหม่ภายในกองทัพเรือได้มีงานวิจัยที่มีผลผลิตออกมาเป็น USVs (ไม่นับรวมเรือไร้คนขับบังคับด้วยวิทยุ: Remoted Control Vessel) อยู่ ๒ โครงการ โดยผลการทำงานของทั้งสองโครงการสามารถสรุปได้ว่า ภารกิจที่เป็นโจทย์หลักสามารถดำเนินการลุ่ลวงได้ด้วย USVs โครงการที่ ๑ ดำเนินการสร้าง USV ขึ้นมาบนพื้นฐานการปฏิบัติการในลำน้ำ มีคุณสมบัติความคงทนทะเลที่ระดับ Sea State 2 ตัวเรือเป็นแบบมาตรฐาน Hard Chined V-Shape ที่มี Deadrise Angel (มุมท้องเรือ) ไม่สูง สามารถยกตัว (Planing) ได้ง่ายในน้ำเรียบ ระบบควบคุมสั่งการ (Command and Control) สามารถตอบสนองภารกิจ และยุทธวิธีของเรือปฏิบัติการลำน้ำได้ดี แต่ก็ถูกจำกัดพื้นที่ปฏิบัติการไว้เพียงแต่ในลำน้ำเท่านั้น โครงการที่ ๒ ได้นำเอาเรือยางท้องแข็ง (RHIB) มาใช้เป็นแพลตฟอร์มพื้นฐาน ซึ่งเรือประเภทนี้โดยทั่วไปถูกนำมาใช้เป็นเรือเร็วปฏิบัติการเอนกประสงค์ โดยมีจุดเด่นในเรื่องของน้ำหนักที่เบา และสามารถขนย้ายได้ง่าย อีกทั้งยังสามารถปฏิบัติการในทะเลเปิดที่ต้องมีคุณสมบัติความคงทนทะเลที่สูง อย่างไรก็ตาม ด้วยข้อจำกัดเรื่องขนาดของ

แพลตฟอร์มของทั้งสองโครงการ อุปกรณ์ที่จำเป็นต้องใช้ในการกิจประเภทต่าง ๆ จะถูกจำกัดให้สามารถนำลงไปติดตั้งในแพลตฟอร์มได้เพียงพอต่อการปฏิบัติภารกิจนั้น ๆ เท่านั้น การจะติดตั้งอุปกรณ์ชุดใหม่สำหรับปฏิบัติการที่แตกต่างไม่สามารถทำได้โดยสะดวก และยืดหยุ่นคล่องตัว ส่งผลต่อความยืดหยุ่นในการปฏิบัติงาน ทำให้เกิดแนวความคิดใหม่ในการเตรียมการออกแบบให้แพลตฟอร์มของ USVs สามารถรองรับการปฏิบัติการได้หลากหลายมากขึ้น จึงเป็นที่มาของระบบ Modularity^{๔,๕}

แนวความคิดในการใช้ระบบ Modularity เริ่มต้นมาตั้งแต่ทศวรรษ ๑๙๗๐ และมีการพัฒนานำมาใช้ทั้งในเรื่องปฏิบัติการภารกิจทางพลเรือนและเรือรบ มีจุดเด่นในด้านของความยืดหยุ่น และความคุ้มค่าในการติดตั้ง และปรับปรุงให้ทันสมัย โดยเรือที่ออกแบบมาภายใต้แนวความคิดนี้จะถูกวางแผนการปฏิบัติการในอนาคตระยะยาว เพื่อวางแผนในการปรับปรุงให้ยืดหยุ่นและทันสมัยกับภารกิจที่แตกต่างกัน และมีความสะดวกในการติดตั้งอุปกรณ์ที่ตอบสนองต่อภารกิจใหม่ที่แตกต่างกันไปนั้น ๆ แนวความคิดนี้ได้รับความสนใจเป็นอย่างสูงในเทคโนโลยีวิศวกรรมเรือรบด้วยประสิทธิภาพที่สามารถเปลี่ยนแปลงภารกิจการปฏิบัติการได้ตามความเหมาะสมบนพื้นฐานของแพลตฟอร์มเดียวกัน ส่งผลให้สามารถลดต้นทุนในการจัดหายุทธโปกรณ์หลักคือ ตัวแพลตฟอร์มสำหรับปฏิบัติการกิจนั้น ๆ ซึ่งประเภทของ Modularity สามารถพิจารณาแบ่งเป็น ๓ ประเภท ที่แตกต่างกันคือ

ประเภทที่ ๑ Common Modules คือลักษณะของ Module ที่เป็นมาตรฐาน ที่สามารถประยุกต์ติดตั้งเข้าไปในแพลตฟอร์มหลากหลายประเภท โดยที่แพลตฟอร์มนั้น ๆ จะได้รับการออกแบบด้วยแนวคิดมาตรฐานตามที่ Module ตั้งไว้เพื่อให้สามารถรองรับการติดตั้งได้ เช่น ห้องพัก และห้องน้ำในเรือโดยสารขนาดใหญ่ที่ผู้ออกแบบเรือสามารถออกแบบเพื่อรองรับ Module นั้น ๆ ที่สามารถหาได้ในท้องตลาด

ประเภทที่ ๒ Self-Contained Modules คือ Module ที่มีขอบเขตชัดเจนที่จะติดตั้งลงในแพลตฟอร์ม โดยมี Connectors และ Interphase ที่เป็นมาตรฐาน โดยที่อุปกรณ์ภายในและฟังก์ชันการทำงานของอุปกรณ์สามารถเปลี่ยนได้หลากหลายรูปแบบตามการใช้งานภายใต้ขอบเขต

ของ Module นั้น เช่น ตู้คอนเทนเนอร์ในเรือขนคอนเทนเนอร์ และระบบ VLS ในเรือฟริเกต

ประเภทที่ ๓ Modular Installations คือ ลักษณะ Module ที่มีคุณสมบัติแตกต่างกันตามภารกิจ ที่สามารถติดตั้งลงในแพลตฟอร์มชนิดเดียวกันหนึ่งระบบได้ โดยแต่ละ Module นี้ จะถูกออกแบบให้ติดตั้งในเรือลำใดลำหนึ่งเท่านั้น หรือติดตั้งในเรือประเภทที่แตกต่างกันก็ได้ แพลตฟอร์มที่ใช้ Module ประเภทนี้ส่วนใหญ่จะเป็นเรือรบประเภทเรือลาดตระเวนชายฝั่ง ที่ติดตั้ง Mission Modules สำหรับ Anti-Submarine Warfare (ASW) Mine Countermeasure (MCM) หรือ Surface Warfare (SUW) เป็นต้น

ด้วยคุณสมบัติตามประเภทของ Modularity ทั้ง ๓ ประเภท มีความเหมาะสมที่จะนำมาประยุกต์ใช้ในแพลตฟอร์มของ USVs เพื่อให้ USVs มีความเป็นเรือเอนกประสงค์และมีความยืดหยุ่นคล่องตัวในการปฏิบัติการกิจตามคุณลักษณะที่เป็นจุดเด่นของแพลตฟอร์มประเภทนี้ที่ได้กล่าวไว้ในเบื้องต้น Mission Modules ตามภารกิจต่าง ๆ ที่จะนำมาใช้ ต้องได้รับการออกแบบอย่างละเอียดอีกครั้ง เพื่อให้สามารถติดตั้งเข้ากับตัวแพลตฟอร์มหลักที่กำลังดำเนินการออกแบบได้อย่างเหมาะสม และมีประสิทธิภาพสูงสุด

๓.๑.๒ คุณลักษณะเบื้องต้นของแพลตฟอร์ม USV

เพื่อให้ตอบสนองความต้องการในการปฏิบัติการกิจ USVs ควรมีคุณสมบัติพื้นฐานเรื่องความคล่องตัว สามารถปฏิบัติการได้ทั้งในย่านความเร็วสูง และความเร็วต่ำ เพื่อตอบสนองภารกิจที่หลากหลาย ซึ่งโดยทั่วไปลักษณะของตัวเรือที่ใช้สร้างเป็นแพลตฟอร์มของ USVs ในภารกิจทางทหารจะเป็นประเภท Monohull (ห้องเดียว) บนพื้นฐานของความสะดวกในการสร้างหรือการนำแพลตฟอร์มของเรือเล็กที่มีอยู่แล้วมาดัดแปลง เรือประเภท Multihull (หลายห้อง) มีปรากฏให้เห็นบ้างใน USVs ในภารกิจทางพลเรือน แต่เนื่องจากในปัจจุบัน เรือรบประเภทเรือตรวจการณ์ชายฝั่ง ได้ใช้เรือประเภท Multihull มากขึ้น จากเหตุผลของข้อได้เปรียบหลายประการทางนาวาสถาปัตยกรรม การพิจารณาเลือกเรือประเภท Multihull มาใช้ใน USVs จึงเป็นประเด็นที่ได้รับความสนใจ

เรือ Multihull ที่ใช้หลากหลายในปัจจุบันมี ๒ ประเภท คือ Catamaran (สองห้อง) และ Trimaran (สามห้อง) เรือ Multihull เหล่านี้ ถูกออกแบบและนำมาใช้บนพื้นฐานหลักการของการลดพื้นที่ดัดน้ำของเรือ (Waterplane Area) เมื่อเทียบกับเรือ Monohull ที่มีมิติหลักเท่ากัน (Length x Beam x Draft: ยาว x กว้าง x กินน้ำลึก) การลด Waterplane Area ทำให้ลดแรงต้านทานการขับเคลื่อน โดยเฉพาะอย่างยิ่งแรงต้านทานการขับเคลื่อนที่เกิดจากคลื่น (Wave Resistance) เมื่อสามารถลดแรงต้านทานได้แล้วจะสามารถประหยัดพลังงานและกำลังที่ใช้ในการขับเคลื่อน ทำให้สามารถลดขนาดของเครื่องต้นกำลังขับเคลื่อน หรือรักษาขนาดของเครื่องไว้แล้วเพิ่มความเร็วที่ต้องการขึ้นมาได้ การได้ความเร็วเพิ่มขึ้น และการประหยัดพลังงานขับเคลื่อน จึงเป็นจุดเด่นหลักของเรือ Multihull อย่างไรก็ดี นอกเหนือจากประเด็นแรงต้านทานการเคลื่อนที่แล้ว คุณสมบัติอื่นอีก ๒ ประการที่นาวาสถาปนิกต้องคำนึงถึงคือ คุณสมบัติการทรงตัว (Stability) และคุณสมบัติความคงทนทะเล (Seakeeping)^๖

การเปรียบเทียบคุณสมบัติทางนาวาสถาปัตยกรรมทั้ง ๓ ข้อ จำเป็นต้องเปรียบเทียบบนพื้นฐานความคล้ายคลึงของมิติที่เทียบเคียงกัน และต้องเปรียบเทียบคู่ต่อคู่แยกเป็นแต่ละกรณี ดังนี้^๖

กรณีที่ ๑ การเปรียบเทียบเรือ Monohull กับเรือ Catamaran ที่มีมิติความยาว และความกว้างเท่ากัน Hull (ห้องเรือ) ของเรือ Monohull จะกินน้ำลึกน้อยกว่า Demihull (ห้องเรือแต่ละห้อง) ของเรือ Catamaran แต่เรือ Monohull จะมี Waterplane Area มากกว่า ส่งผลให้เรือ Catamaran มีแรงต้านทานการเคลื่อนที่น้อยกว่า ใช้พลังงานมากกว่า และสามารถทำความเร็วได้สูงกว่า หากติดตั้งเครื่องจักรขับเคลื่อนที่มีกำลังเท่ากัน เมื่อพิจารณาถึงคุณสมบัติทางด้าน Stability เรือ Catamaran จะมีค่า Metacenter (GMT) สูงกว่า ส่งผลให้ GZ Curve ของ Catamaran อยู่สูงกว่า Monohull มีโมเมนต์ตั้งตรงสูงกว่า และดึงเรือกลับมาอยู่ในสภาพ Static Equilibrium ได้ดีกว่า และเมื่อพิจารณาคงทนทะเล Seakeeping สืบเนื่องจากลักษณะของ GZ Curves เส้นกราฟของ RAO (Response Amplitude Operator) ของเรือ Catamaran จะอยู่สูงกว่า RAO ของ Monohull ส่งผลให้เรือ Catamaran ตอบสนองคลื่นไว

และรุนแรงกว่าเรือ Monohull แต่อย่างไรก็ดีประเด็นคุณสมบัติ Seakeeping ต้องได้รับการพิจารณาอย่างละเอียด เพื่อที่จะสามารถทำการสรุปเป็นกรณี ๆ ไป เพราะมีปัจจัยอื่น ๆ ที่ส่งผลต่อคุณสมบัตินี้ และสามารถหักล้างปัจจัยที่เกี่ยวข้องออกไป เช่น Waterplane Area ที่สามารถปรับได้ตามความเหมาะสมของลายเส้นตัวเรือ

กรณีที่ ๒ การเปรียบเทียบเรือ Monohull กับเรือ Trimaran คุณลักษณะเทียบเคียงของเรือทั้งสองประเภทจะถูกพิจารณาแตกต่างออกไปโดยทั่วไปแล้ว รูปทรงของเรือ Trimaran จะมีพื้นฐานมาจากเรือ Monohull ต้นแบบที่ถูกขยายปีกออกไปทั้งสองข้าง ส่วนปีกที่ขยายออกทั้งสองข้างถูกเรียกว่า Amas จะมีส่วนที่จมน้ำอยู่เพียงเล็กน้อยเท่านั้น แรงลอยตัว (Buoyancy) ๘๐% - ๙๐% จะอยู่ที่ตัวเรือหลัก (Main Hull) ส่งผลให้แรงต้านทานการเคลื่อนที่ไม่แตกต่างจาก Monohull มากนัก แต่มีโมเมนต์ตั้งตรงสูงกว่าเรือ Monohull จากการที่มีการกระจายตัวของจุดศูนย์กลางแรงลอยตัว (Center of Buoyancy) ไปที่ Amas ทั้งสองด้าน และมีคุณสมบัติ Seakeeping ใกล้เคียงกับเรือ Monohull บนพื้นฐานข้อได้เปรียบของพื้นที่ระวางบรรทุกที่สูงขึ้น

จากคุณสมบัติทางนาวาสถาปัตยกรรมที่กล่าวมาข้างต้น แพลตฟอร์มพื้นฐานสำหรับ USVs ต้นแบบลำนี้ จะยกลายเส้นตัวเรือของ Monohull รายการหนึ่ง มาทำการพัฒนาขยายแบบเป็น Trimaran เปรียบเทียบคุณสมบัติพื้นฐานทางด้าน Resistance Stability และ Seakeeping และบูรณาการร่วมกับแนวความคิด Modularity เพื่อพิจารณาเตรียมการพื้นที่ในการจัดวาง Mission Modules ที่เหมาะสม สามารถตอบสนองภารกิจต่าง ๆ ตามที่กำหนดไว้ และเกิดประโยชน์สูงสุด

๓.๒ ขั้นตอนการออกแบบในระดับ Conceptual Design

๓.๒.๑ การออกแบบรูปทรงและลายเส้นตัวเรือ

คุณสมบัติที่ใช้เป็นปัจจัยหลักในการออกแบบ USVs เอนกประสงค์ลำนี้ คือ การตอบสนองภารกิจที่หลากหลาย ภายใต้แพลตฟอร์มหลักหนึ่งเดียว อุปกรณ์ที่ใช้ในการปฏิบัติการกิจแต่ละภารกิจจะถูกติดตั้งอยู่ใน Mission Modules ที่แตกต่างกันในฟังก์ชัน แต่มีมิติเดียวกันสำหรับติดตั้งลงใน

แพลตฟอร์มหลัก ดังนั้น ปัจจัยถัดมาที่ต้องคำนึงถึงในการออกแบบแพลตฟอร์มที่เหมาะสมคือ มิติหลักของแพลตฟอร์ม และความเร็วที่ใช้ในการปฏิบัติการ

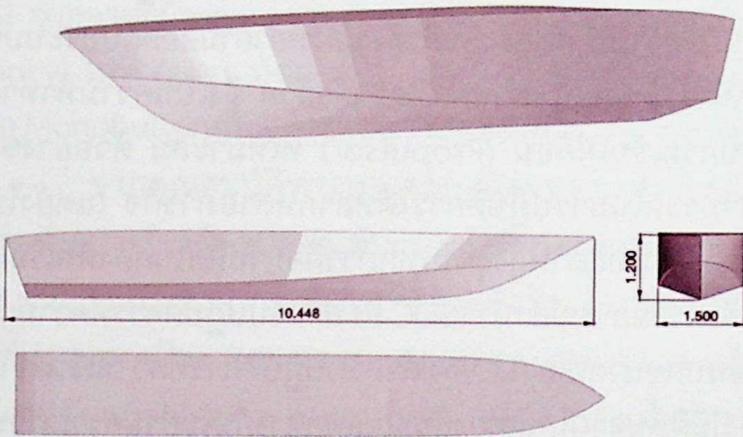
ในด้านปัจจัยมิติหลักของแพลตฟอร์ม เรือที่ใช้การในหลากหลายภารกิจจะมีต้นแบบมิติแนวคิดมาจากเรือประเภเรือใช้งานทั่วไป (Work Boat) โดยจะมีมิติหลัก ๆ ใกล้เคียงกันที่ความยาวตลอดลำระหว่าง ๑๐ - ๑๕ เมตร อัตราส่วนความยาวต่อความกว้าง L/B ระหว่าง ๓ - ๕ ระบายชั้นน้ำเต็มที่ ระหว่าง ๒ - ๗ ตัน

ในด้านปัจจัยความเร็วปฏิบัติการ โดยทั่วไป ในระหว่างการออกแบบ เรือหนึ่งลำจะถูกออกแบบให้ปฏิบัติการกิจที่ย่านความเร็วหลักเพียงหนึ่งย่านความเร็วเท่านั้น ด้วยข้อจำกัดทางนาวิสถาปัตยกรรมในการเลือกใช้ระบบขับเคลื่อนที่ตอบสนองภารกิจในหลากหลายย่านความเร็ว เป็นสิ่งที่ทำได้ยาก หากต้องการออกแบบแพลตฟอร์มที่สามารถปฏิบัติการกิจหลายย่านความเร็ว ให้ยึดความเร็วสูงสุดเป็นตัวตั้ง แล้วพยายามออกแบบระบบขับเคลื่อนให้มีประสิทธิภาพสูงสุดในย่านความเร็วต่ำด้วย จึงเป็นความท้าทายของการคัดเลือกอุปกรณ์ขับเคลื่อน (Propulsor) ที่เหมาะสม ตัวอย่างของเรือที่มีขีดความสามารถในการปฏิบัติการได้หลากหลายภารกิจ (แต่ยังไม่สามารถยืนยันได้ว่ามีประสิทธิภาพสูงสุดในทุกภารกิจ) ที่มีใช้ในกองทัพเรือในปัจจุบัน ได้แก่ เรือเร็วตรวจการณ์ลำน้ำ (SOC-R) สำหรับปฏิบัติการที่ความเร็วสูง และเรือยกพลขึ้นบกขนาดเล็ก (LCVP) สำหรับปฏิบัติการที่ความเร็วต่ำ เรือทั้งสองประเภทนี้ มีมิติพื้นฐานใกล้เคียงกัน แต่แตกต่างกันในย่านความเร็วปฏิบัติการ เมื่อผสมผสานคุณลักษณะหลักของเรือทั้งสองประเภท เพื่อออกแบบแพลตฟอร์มพื้นฐาน ทำให้สามารถกำหนดมิติเบื้องต้นได้ดังนี้

- ความยาวตลอดลำ
- ความกว้าง
- ความลึก
- กินน้ำลึก
- ระบายชั้นน้ำ
- ความเร็วสูงสุด

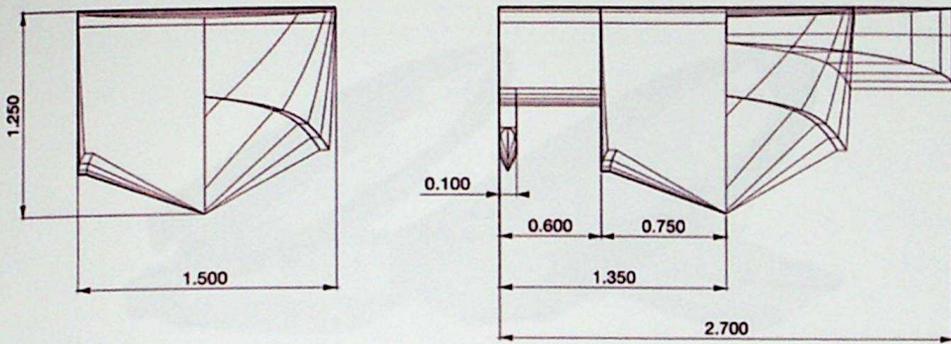
มิติต่าง ๆ ด้านบน จะถูกนำมาใช้สร้างเรขาคณิตและ
 ลายเส้นตัวเรือ (Hull Geometries and Lines Plan) สำหรับกันหอยออกแบบ
 วงแรกเมื่อพิจารณาสมมติฐานที่ตั้งไว้ว่าจะใช้เรือ SOC-R เป็นเรือเทียบเคียง
 เรือ Trimaran จะมีความยาวเท่ากับเรือเทียบเคียง มีความกว้างสูงสุดเท่ากัน
 แต่จะมีตัวเรือหลัก (Main Hull) ที่มีความกว้างน้อยกว่า เพื่อใช้ประโยชน์จาก
 คุณสมบัติความเพรียว (Slenderness) ในการลดแรงต้านทานการขับเคลื่อน
 ทำให้ได้ Main Hull ที่มีมิติหลักดังนี้ (ภาพที่ ๑)

- $L_{OA} = 10.448\text{m}$
- $B = 1.5\text{m}$
- $D = 1.25\text{m}$



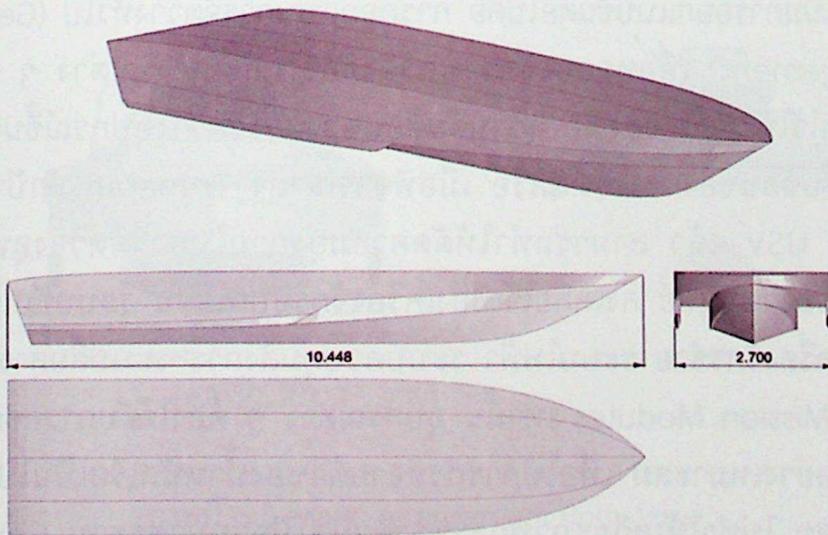
ภาพที่ ๑ ตัวเรือหลัก (Main Hull)

Main Hull ที่มีความกว้างน้อยกว่าเรือเทียบเคียงนี้
 จะมีคุณสมบัติช่วยลดกำลังที่จำเป็นต้องใช้ในการขับเคลื่อน จากคุณลักษณะ
 Slender Body และเพื่อให้มีคุณสมบัติในการจัดวาง Pay Load เทียบเท่ากับ
 เรือเทียบเคียง ส่วนต่อขยายเพื่อปรับสภาพตัวเรือให้เป็น Trimaran จะพิจารณา
 ต่อเติมให้ได้สัดส่วนที่เหมาะสม ตามภาพที่ ๒

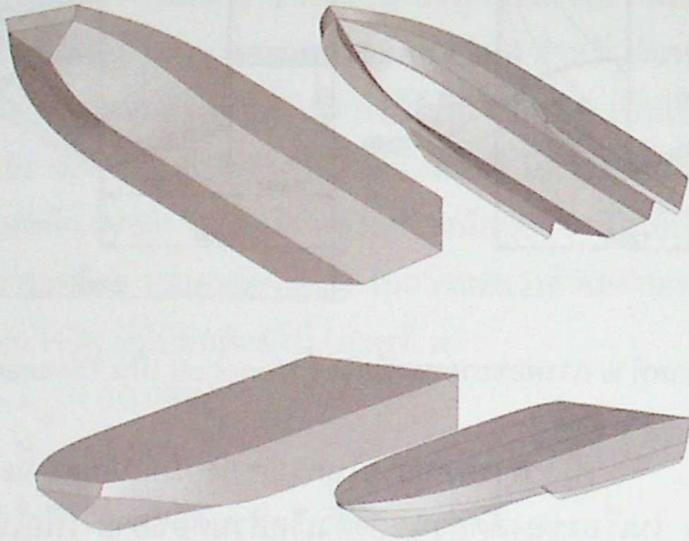


ภาพที่ ๒ การต่อขยายทรงเรือจาก Monohull เป็น Trimaran

การต่อขยายในกรณีของ Trimaran จะแตกต่างกับ Catamaran ในเรื่องของสัดส่วนของตัวเรือส่วนต่อขยาย เพื่อให้เป็นไปตามแนวคิดของเรือ Trimaran ที่ให้แรงลอยตัวส่วนใหญ่เกิดขึ้นที่ Main Hull ตัวเรือส่วนต่อขยายของ Trimaran จะมีความยาวประมาณครึ่งหนึ่งของความยาวตลอดลำ โดยอาจเริ่มต่อขยายจาก Transom หรือจุดอื่นที่เหมาะสมที่ไม่เกิน ๑๐% ของระยะจาก Transom เมื่อปรับสัดส่วนจนมีความเหมาะสมแล้ว จะได้รูปทรงเรือที่ต้องการ ตามภาพที่ ๓ และมีมิติหลักเป็นไปในแนวทางเดียวกับเรือเทียบเคียง (เรือเร็วตรวจการณ์ลำน้ำ: SOC - R) ตามภาพที่ ๔



ภาพที่ ๓ ตัวเรือ Trimaran ตามคุณลักษณะที่ต้องการ



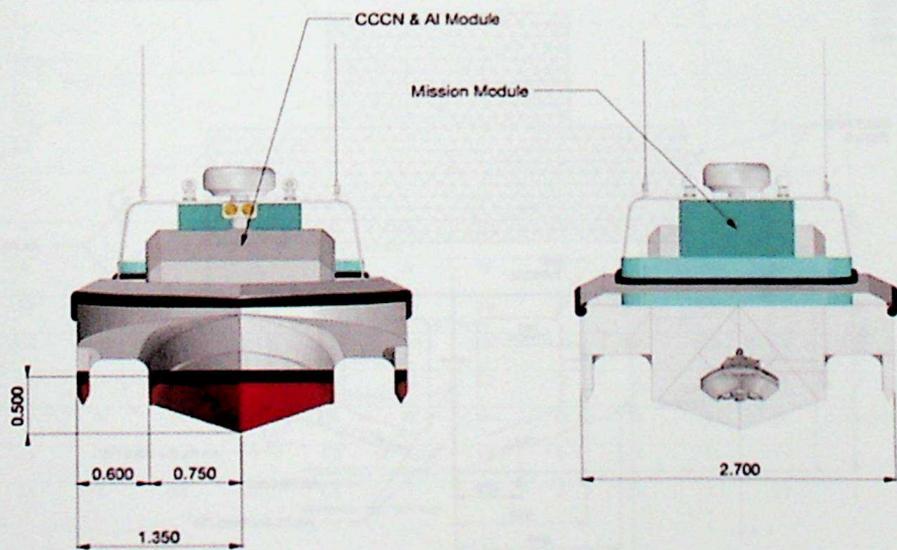
ภาพที่ ๔ Monohull (SOC-R) VS Trimaran

๓.๒.๒ การออกแบบการจัดวางทั่วไปของเรือ (General Arrangement: GA)

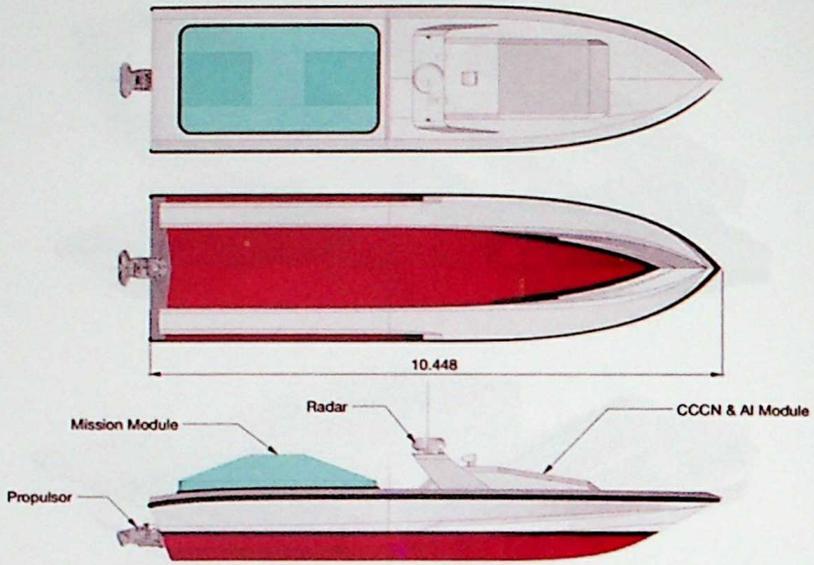
เมื่อสามารถกำหนดรูปทรงและลายเส้นของตัวเรือได้แล้ว การดำเนินการออกแบบขั้นต่อไปคือ การออกแบบการจัดวางทั่วไป (General Arrangement) เพื่อทดลองจัดวางเครื่องจักร และอุปกรณ์ต่าง ๆ ตามที่กำหนดไว้ในภารกิจของเรือ ความซับซ้อนของการจัดวางอุปกรณ์ขึ้นอยู่กับความซับซ้อนของการใช้งานเรือ เมื่อพิจารณาถึง Trimaran ลำปัจจุบัน ซึ่งเป็น USV แล้ว สามารถทำให้ตัดความยุ่งยากในการจัดวางอุปกรณ์ที่เกี่ยวข้องกับมนุษย์ คงเหลือไว้เพียงเครื่องจักรขับเคลื่อน ระบบขับเคลื่อน ระบบเครื่องจักรช่วย ระบบไฟฟ้า ระบบควบคุมสั่งการ ระบบสื่อสาร และระบบ Mission Modules เท่านั้น อุปกรณ์ต่าง ๆ ต้องได้รับการออกแบบจัดวางอย่างเหมาะสม เพื่อให้การกระจายตัวของน้ำหนักเรือเป็นไปอย่างเหมาะสม ไม่ทำให้เสถียรภาพการทรงตัวผิดไปจากมาตรฐาน General Arrangement ของ Trimaran ลำปัจจุบัน แสดงให้เห็นตามภาพที่ ๕ - ภาพที่ ๘



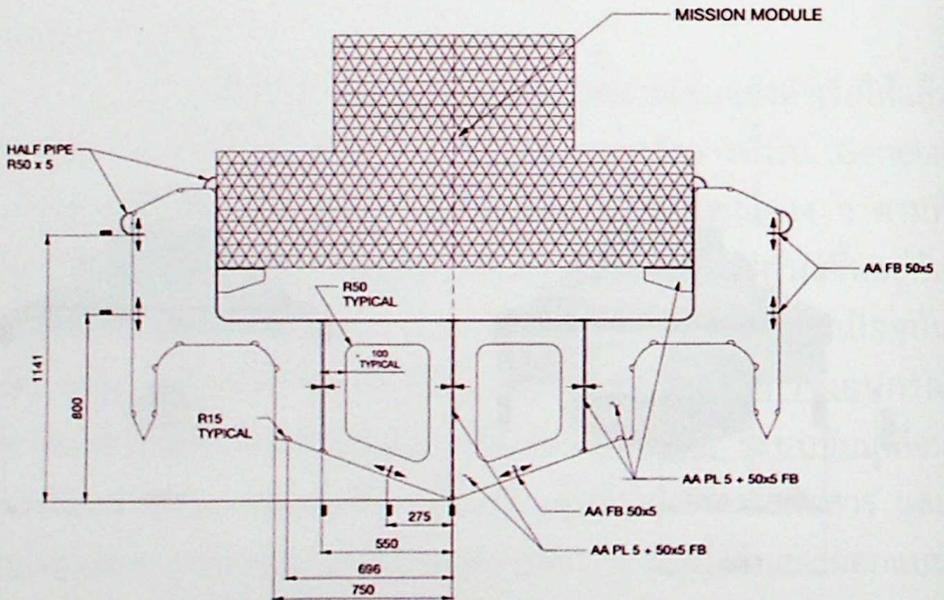
ภาพที่ ๕ General Arrangement 3D Perspective



ภาพที่ ๖ General Arrangement Body View



ภาพที่ ๗ General Arrangement Plan View and Profile View

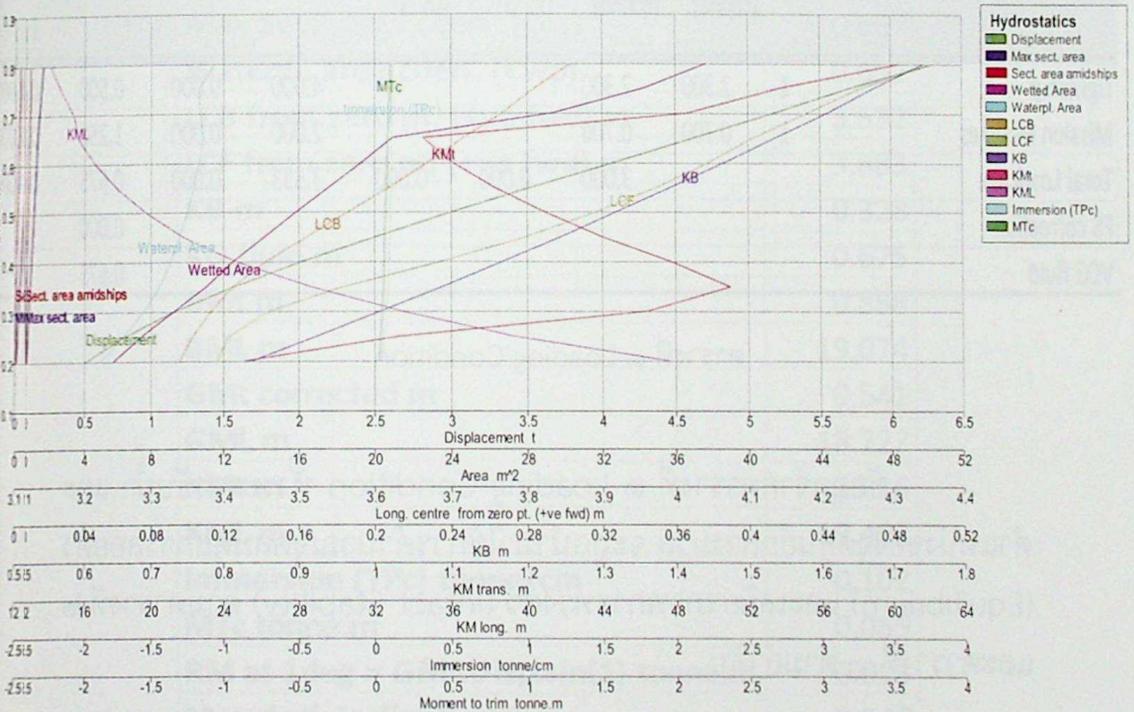


ภาพที่ ๘ Midship Section

๓.๒.๓ การศึกษาคุณสมบัติทาง Hydrostatics and Stability

เบื้องต้น

Hydrostatic Data เป็นข้อมูลเบื้องต้นที่สำคัญที่นาา สถาปนิกต้องดำเนินการประมาณการในช่วงเริ่มต้นของการออกแบบ เพื่อนำ ข้อมูลมาใช้ในการประเมินน้ำหนักรวมของเรือตามระยะแนวน้ำที่กำหนดไว้ เบื้องต้น และใช้เป็นข้อมูลในการประมาณการและจำกัดน้ำหนักบรรทุกของ ระวาง อีกทั้งยังสามารถใช้ประมาณการความสูงของ Metacenter: GMt เพื่อ ปรับรูปทรงของตัวเรือให้มีเสถียรภาพการทรงตัว (Initial Stability) ที่เหมาะสม ข้อมูล Hydrostatic เบื้องต้นที่ $Trim = 0.00 m$ ของ Trimaran ลำปัจจุบัน แสดงตามรูปที่ ๙



ภาพที่ ๙ Upright Hydrostatic Data in Graphic Form

ในการออกแบบ Trimaran ลำปัจจุบัน ระยะกินน้ำลึกเบื้องต้น (Design Draught) ถูกกำหนดให้อยู่ที่ระดับ $T = 0.500\text{ m}$ ทำให้มีระวางขับน้ำรวม $\Delta = 3.000\text{ tonne}$ ต้องมีการประมาณการกระจายตัวของน้ำหนักอย่างเหมาะสม ข้อมูลที่ตกผลึกสำหรับการประมาณการกระจายตัวนี้ในระดับ Conceptual Design หรือวงรอบแรกของกันหอยการออกแบบจะใช้ข้อมูลของเรือที่มีลักษณะและคุณสมบัติใกล้เคียงเป็นแนวทางการกระจายตัวของน้ำหนักเรือและจุดศูนย์กลางมวลของเรือ แสดงให้เห็นตามตารางที่ ๑

Item Name	Quantity	Unit	Total	Unit	Total	LCG (m)	TCG (m)	VCG (m)	Total FSM (tonne.m)
		Mass (tonne)	Mass (tonne)	Volume (m ³)	Volume (m ³)				
Lightship	1	2.300	2.300			4.000	0.000	0.500	0.00
Mission Modules	1	0.700	0.700			2.000	0.000	1.250	0.00
Total Loadcase			3.000	0.000	0.000	3.533	0.000	0.675	0.00
FS correction								0.000	
VCG fluid								0.675	

ตารางที่ ๑ Loading Condition

ข้อมูลจากตารางที่ ๑ Loading Condition ทั้งระวางขับน้ำ และตำแหน่งของจุดศูนย์กลางมวล จะถูกนำมาใช้ในการคำนวณจุดสมดุลการลอยตัว (Equilibrium) และเสถียรภาพการทรงตัว (Intact Stability) ตามตารางที่ ๒ และตารางที่ ๓ ตามลำดับ

Parameters/Conditions	Full Load
Draft Amidships m	0.500
Displacement t	3.000
Heel deg	-0.200
Draft at FP m	0.493
Draft at AP m	0.507
Draft at LCF m	0.501
Trim (+ve by stern) m	0.014
WL Length m	9.010
Beam max extents on WL m	2.700
Wetted Area m ²	15.867
Waterpl. Area m ²	9.980
Prismatic coeff. (Cp)	0.540
Block coeff. (Cb)	0.377
Max Sect. area coeff. (Cm)	0.697
Waterpl. area coeff. (Cwp)	0.652
LCB from zero pt. (+ve fwd) m	3.532
LCF from zero pt. (+ve fwd) m	3.883
KB m	0.328
KG fluid m	0.675
BMt m	0.888
BML m	19.074
GMt corrected m	0.541
GML m	18.727
KMt m	1.216
KML m	19.402
Immersion (TPc) tonne/cm	0.102
MTc tonne.m	0.065
RM at 1deg = GMt.Disp.sin(1) tonne.m	0.028
Max deck inclination deg	0.247
Trim angle (+ve by stern) deg	0.092

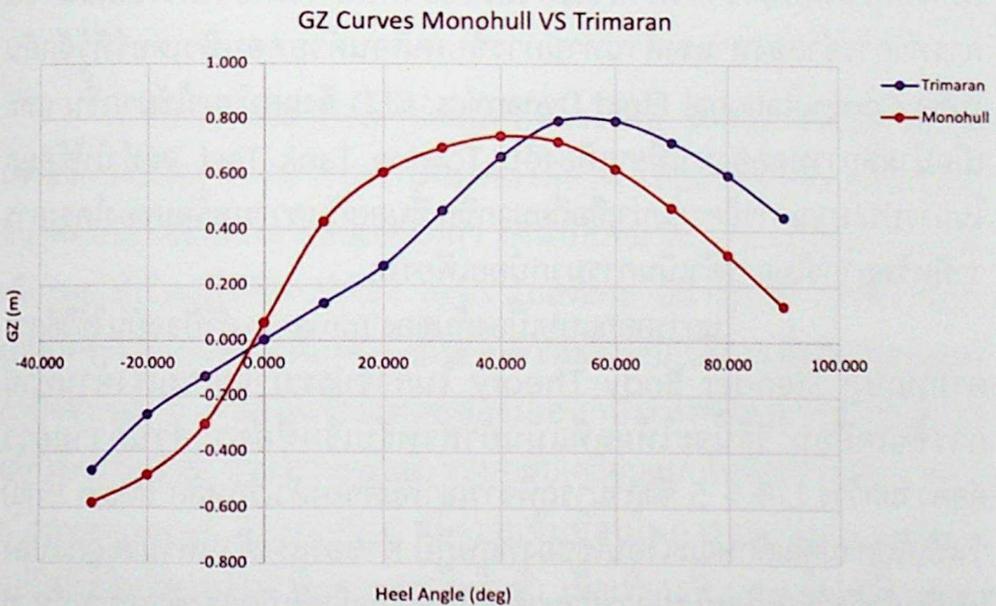
ตารางที่ ๒ Equilibrium

Heel to Starboard (deg)	-30.000	-20.000	-10.000	0.000	10.000	20.000	30.000	40.000	50.000	60.000	70.000	80.000	90.000
GZ (m)	-0.391	-0.240	-0.100	0.005	0.106	0.244	0.394	0.525	0.581	0.553	0.457	0.329	0.187
Area under GZ curve from zero heel (m.rad)	0.092	0.037	0.008	0.000	0.009	0.040	0.095	0.176	0.274	0.374	0.463	0.532	0.577
Displacement (tonne)	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000	3.000
Draft at FP (m)	0.377	0.461	0.487	0.493	0.487	0.461	0.377	0.241	0.045	-0.301	-1.026	-3.116	n/a
Draft at AP (m)	0.335	0.434	0.501	0.507	0.499	0.432	0.332	0.194	0.032	-0.176	-0.511	-1.463	n/a
WL Length (m)	8.991	9.100	9.081	9.009	9.080	9.099	8.992	9.139	9.305	9.374	9.383	9.391	9.456
Beam max extents on WL (m)	1.978	2.078	2.701	2.700	2.700	2.075	1.976	1.836	1.619	1.369	1.187	1.108	1.070
Wetted Area (m ²)	20.940	19.784	17.018	15.886	17.390	20.506	21.682	22.518	23.358	23.425	24.060	24.360	24.381
Waterpl. Area (m ²)	11.908	11.742	10.449	9.995	10.412	11.734	11.905	11.204	9.487	6.781	5.013	4.167	3.735
Prismatic coeff. (Cp)	0.556	0.541	0.530	0.541	0.534	0.545	0.560	0.553	0.533	0.503	0.465	0.434	0.408
Block coeff. (Cb)	0.227	0.250	0.318	0.377	0.321	0.251	0.228	0.222	0.227	0.258	0.269	0.276	0.279
LCB from zero pt. (+ve fwd) (m)	3.535	3.534	3.533	3.533	3.533	3.535	3.535	3.536	3.534	3.528	3.517	3.504	3.492
LCF from zero pt. (+ve fwd) (m)	4.123	3.901	3.734	3.878	3.740	3.899	4.123	4.291	4.329	4.253	4.182	3.949	3.773
Max deck inclination (deg)	30.001	20.001	10.000	0.090	10.000	20.001	30.001	40.001	50.000	60.001	70.004	80.006	90.000
Trim angle (+ve by stern) (deg)	-0.277	-0.173	0.092	0.090	0.081	-0.188	-0.295	-0.314	-0.090	0.830	3.409	10.831	n/a

ตารางที่ ๓ Intact Stability

ในสภาพ Equilibrium เรือ Trimaran ลำปัจจุบันมีค่า $trim = 0.014$ แสดงให้เห็นว่า เรือในจุดสมดุลการลอยตัวอยู่ในสภาพเกือบตั้งตรง (Even Keel) หัวเรืออยู่ในสภาพยกขึ้นเล็กน้อย เหมาะสมต่อการเคลื่อนที่และเปลี่ยนสภาพการลอยตัวจาก Displacement Mode สู่ Planing Mode เมื่อเคลื่อนที่ที่ความเร็วสูง

ในขณะเดียวกัน Intact Stability เป็นข้อมูลสำคัญในการออกแบบเบื้องต้นที่ใช้บ่งบอกคุณสมบัติการทรงตัวของเรือ คุณภาพของ Stability จะถูกชี้วัดโดยคุณลักษณะของแกนโมเมนต์ตั้งตรง (GZ) ซึ่งแปรผันตามมุมเอียงของเรือในระดับต่าง ๆ เมื่อถูกแรงภายนอก เช่น แรงลม แรงคลื่น แรงกระแสน้ำ และแรงสู่ศูนย์กลางเมื่อหันเลี้ยว เป็นต้น ค่า GZ นี้ จะถูกนำเสนอในรูปแบบของกราฟ $GZ - \Phi$ คุณภาพของ GZ จะถูกกำหนดมาตรฐานโดยองค์กรที่เกี่ยวข้องกับการเดินเรือและความปลอดภัยในการปฏิบัติงานทางเรือต่าง ๆ ซึ่งสำหรับเรือประเภท Trimaran นี้ จะมีจุดเด่นที่ชัดเจนในเรื่องของคุณภาพของ GZ ที่ดีกว่าเมื่อเทียบกับเรือเทียบเคียง ดังที่แสดงในภาพที่ ๑๐ กราฟ GZ ของเรือ Trimaran จะอยู่สูงกว่า และมีจุดสูงสุดที่มุมเอียงที่มากกว่า ทำให้มีเสถียรภาพการทรงตัวที่ดีกว่า



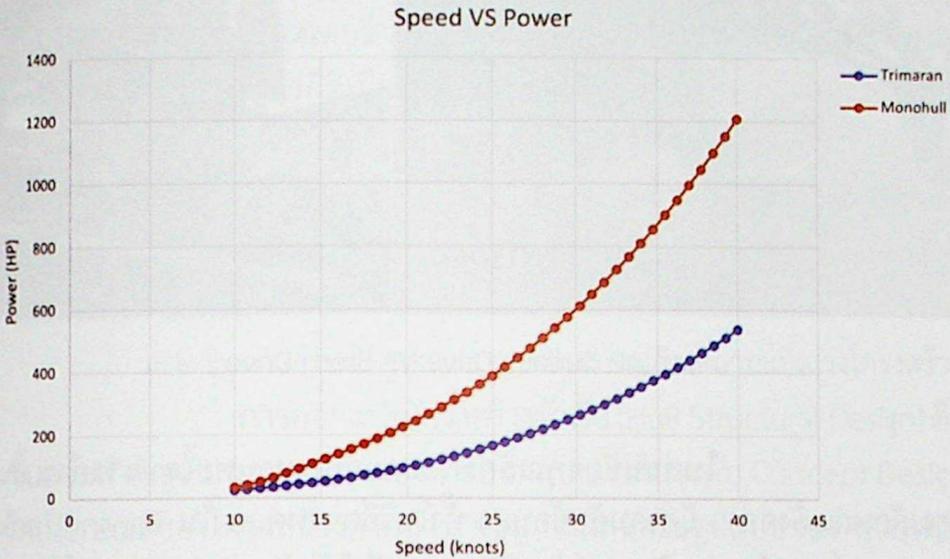
ภาพที่ ๑๐ GZ Curves

๓.๒.๔ การประมาณการแรงต้านทาน แรงขับเคลื่อน ประเภทของระบบขับเคลื่อน และคุณสมบัติความคงทนทะเล

เมื่อได้ตัวเรือที่มีคุณสมบัติเบื้องต้นทาง Hydrostatic และ Stability ที่เหมาะสมแล้ว นาวาสถาปนิกจะดำเนินการประมาณการกำลังที่ใช้ในการขับเคลื่อน ตามคุณลักษณะเบื้องต้นทางด้านความเร็วหลักที่จะใช้ในการปฏิบัติการกิจ กำลังที่ใช้ในการขับเคลื่อนจะถูกประมาณการบนหลักการของกำลังที่ใช้ในการผลักเรือให้มีความเร็วตามที่ต้องการ เพื่อเอาชนะแรงต้านทานที่เกิดขึ้นเมื่อเรือวิ่งที่ความเร็วนั้น ๆ อย่างไรก็ดี เรือเป็นยานพาหนะที่เคลื่อนที่ในของไหลสองโดเมน (น้ำและอากาศ) การประมาณการแรงต้านทานที่เกิดขึ้นตามทฤษฎีจึงมีความซับซ้อนเป็นอย่างมาก ในยุคเริ่มต้นของทฤษฎีทางนาวาสถาปัตยกรรม วิธีการประมาณการแรงต้านทานการขับเคลื่อนที่มีความแม่นยำและนิยมใช้มากที่สุดคือ การทำการทดลองเรือจำลองที่มีรูปทรงเดียวกันในคลองทดสอบ (Resistance Experiment in Towing Tank) นาวาสถาปนิกจะทำการวัดค่าแรงต้านทานที่เกิดขึ้นในเรือจำลอง และนำข้อมูลที่ได้นี้มาขยายผลให้เป็นแรงต้านทานการขับเคลื่อนในเรือจริง อย่างไรก็ดี การทำการทดลองประเภทนี้มีความยุ่งยากและสิ้นเปลืองทรัพยากรเป็นอย่างมาก เมื่อเทคโนโลยีทางการคำนวณด้วยเครื่องคอมพิวเตอร์มีการพัฒนาขึ้น การทำการจำลองหาแรงต้านทานการขับเคลื่อนด้วยคอมพิวเตอร์ที่รู้จักกันในชื่อ Computational Fluid Dynamics: CFD จึงถูกนำมาใช้มากขึ้น และเมื่อนำผลการทดลองมาเทียบเคียงกับ Towing Tank Test จะทำให้ข้อมูลในการประมาณการมีความน่าเชื่อถือมากขึ้น ขึ้นอยู่กับความพร้อมของโครงการว่ามีทรัพยากรในการดำเนินการมากน้อยเพียงใด

ในการออกแบบเบื้องต้นของ Trimaran ลำปัจจุบัน ใช้วิธีการตามทฤษฎี Slender Body Theory ในการประมาณการแรงต้านทานการขับเคลื่อน วิธีนี้จะให้ผลที่แม่นยำสำหรับเรือที่อัตราส่วนความยาวต่อความกว้าง $L/B > 5$ ซึ่งสามารถพิจารณาที่มิติของตัวเรือหลัก (Main Hull) ว่าเป็นไปตามคุณลักษณะเงื่อนไขของทฤษฎีนี้ ค่าของแรงต้านทานจะถูกแปลงให้เป็นกำลังขับเคลื่อนโดยการนำมาคูณกับความเร็วที่เกิดแรงต้านทานนั้น ๆ ร่วมกับประสิทธิภาพ (Efficiency) ที่สูญเสียกำลังไปในแนวของระบบขับเคลื่อน

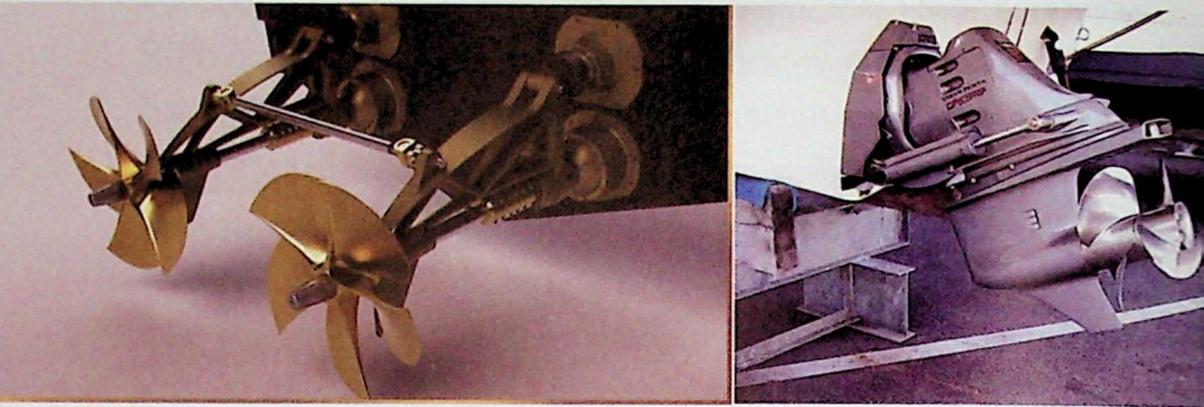
(เกียร์ และเพลลา) และนำมานำเสนอคู่กับช่วงความเร็วนั้น ๆ ตามรูปที่ ๑๑ ซึ่งจะเห็นได้ว่า Trimaran ที่มีมิติหลักเดียวกันกับเรือเร็วตรวจการณ์ลำน้ำ (SOC-R) จะใช้กำลังในการขับเคลื่อนน้อยกว่าที่ความเร็วเท่ากัน ซึ่งเป็นผลมาจากคุณสมบัติของความเพรียวที่มีมากกว่า



ภาพที่ ๑๑ Speed VS Power

ขนาดของกำลังเครื่องยนต์ที่ต้องใช้คือ 300HP เป็นขนาดของเครื่องยนต์ดีเซลที่สามารถหาได้ในท้องตลาด โดยในปัจจุบันเครื่องยนต์ขนาดดังกล่าวมีอัตราการสิ้นเปลืองต่ำ ถังน้ำมันขนาด ๑,๐๐๐ ลิตร สามารถเพียงพอให้เรือปฏิบัติการได้ถึง ๓๐๐ ไมล์ทะเล อย่างไรก็ตาม การพิจารณากำหนดระบบขับเคลื่อนต้องคำนึงถึงย่านความเร็วที่ปฏิบัติการ ซึ่งเรือ Trimaran ลำปัจจุบันถูกกำหนดให้เป็นแพลตฟอร์มเอนกประสงค์ที่สามารถปฏิบัติการได้ทั้งที่ความเร็วสูง และความเร็วต่ำ ระบบขับเคลื่อนแบบใบจักรทางเสื่อธรรมดา (Conventional Propeller) มีความซับซ้อนในการออกแบบและติดตั้ง แต่มีประสิทธิภาพดีกว่าในย่านความเร็วต่ำ เมื่อเทียบกับระบบขับเคลื่อนแบบเครื่องพ่นน้ำ (Waterjet) ที่สามารถออกแบบและติดตั้งได้ง่ายกว่า ทางเลือกอื่น ๆ

ที่สามารถตอบสนองความต้องการในการปฏิบัติการนี้ได้คือ ระบบขับเคลื่อนแบบ Stern Drive และระบบขับเคลื่อนแบบ Surface Drive ซึ่งเป็นการผสมผสานใบจักรแบบธรรมดาเข้ากับ Module ของระบบที่สะดวกในการติดตั้ง



ภาพที่ ๑๒ Surface Drive VS Stern Drive

ในส่วนของคุณลักษณะความคงทนทะเล การคำนวณคุณลักษณะดังกล่าว มีความซับซ้อนสูง ทั้งในวิธีการทดลองใน Towing Tank และการจำลองในคอมพิวเตอร์ด้วยวิธี CFD ซึ่งใช้ทรัพยากรมหาศาลในการดำเนินการ จึงเป็นขั้นตอนที่จะถูกวางแผนดำเนินการในระดับวงรอบลึก ๆ ของการออกแบบ อย่างไรก็ตาม คุณสมบัติสามารถอนุมานเบื้องต้นได้จากคุณสมบัติเสถียรภาพการทรงตัว เรือที่มีเส้นโค้ง GZ Curve สูง ซึ่งเป็นผลมาจาก Water Plan ที่สูง จะส่งผลกระทบต่อ Response Amplitude Operator: ROA ที่มีค่าสูงกว่าในทุกย่านความถี่ นับเป็นข้อจำกัดที่ต้องแลกมากับเสถียรภาพการทรงตัว อย่างไรก็ตาม คุณสมบัตินี้ความคงทนทะเล จะถูกชี้วัดโดยสิ่งที่เกี่ยวข้องหลัก ๒ ประการคือ ๑) ความแข็งแรงของตัวเรือที่ทนทะเลในระดับนั้น ๆ ได้ และ ๒) ผู้ปฏิบัติงานสามารถทำงานบนเรือที่ทะเลระดับนั้น ๆ ได้ ตัวชี้วัดตัวหลังสามารถถูกตัดออกไปได้ในกรณีของเรือ USVs และในส่วนของความแข็งแรงโครงสร้าง สามารถออกแบบให้มีความเหมาะสมได้ตามมาตรฐานที่สมาคมจัดชั้นเรือได้ระบุไว้

๓.๒.๕ ระบบเครื่องจักรช่วย และระบบไฟฟ้ากำลัง

ในกรณีของเรือทั่วไปที่มีผู้ปฏิบัติงานบนเรือ ระบบเครื่องจักรช่วย และระบบไฟฟ้า จะมีความสำคัญทั้งต่อการทำงานของ

ตัวเรือเอง และการทำงานของผู้ปฏิบัติงาน อย่างไรก็ตาม ในเรือเทียบเคียงที่มีมิติ และภารกิจใกล้เคียงกับ Trimaran USV ลำปัจจุบัน ระบบเครื่องจักรช่วย จะประกอบไปด้วยเพียงระบบเครื่องจักรช่วยเครื่องจักรใหญ่ เช่น ปั๊มน้ำมัน เชื้อเพลิง ปั๊มสูบน้ำดับความร้อนเครื่องจักรใหญ่ ซึ่งถูกติดตั้งอยู่ในหน่วย เดียวกันกับเครื่องจักรใหญ่แล้ว และระบบไฟฟ้า จะใช้พลังงานจากแหล่งหลัก เพียงอย่างเดียวคือ แบตเตอรี่ ส่งผลให้เรือขนาดนี้ไม่มีความซับซ้อนในทั้งสอง ระบบนี้มากนัก อย่างไรก็ตามเมื่อเรือ Trimaran ลำปัจจุบัน ถูกกำหนดให้เป็น เรือเอนกประสงค์ รองรับ Mission Modules กำลังไฟฟ้าที่ใช้ในภารกิจต่าง ๆ จะต้องได้รับการประมาณการอย่างละเอียดอีกครั้งด้วยวิธีการ Electrical Load Analysis เพื่อสามารถพิจารณาแหล่งพลังงานที่เหมาะสมได้ ทั้งแบตเตอรี่ และเครื่องกำเนิดไฟฟ้า

๓.๒.๖ การกำหนดรูปแบบ และประมาณการความแข็งแรงโครงสร้าง การออกแบบโครงสร้างตัวเรือ (Hull Structural Design) คือ ขั้นตอนสำคัญขั้นตอนสุดท้ายของการออกแบบเรือในระดับ Concept Design โดยลักษณะของโครงสร้างดังกล่าว จะถูกนำเสนอในรูปแบบของ Midship Section ตามรูปที่ ๘ ซึ่งเป็นแบบที่นำเสนอโครงสร้างหลักที่บริเวณกลางลำ ที่สามารถนำมาขยายผลในการออกแบบโครงสร้างส่วนอื่น ๆ ได้ตามความเหมาะสมต่อการใช้งานในแต่ละบริเวณ

ในการออกแบบโครงสร้างตัวเรือ นาวาสถาปนิกจะทำการ กำหนดรูปแบบการจัดวางโครงสร้าง ประเภทของโครงสร้างที่จะนำมาใช้ ขนาดของโครงสร้าง และคำนวณความแข็งแรงให้เพียงพอที่จะรับแรงกระทำ จากภายนอกเมื่อนำไปปฏิบัติงาน การออกแบบโครงสร้างนี้ นาวาสถาปนิก จะกำหนดตามรูปแบบของเรือเทียบเคียง และปรับให้เหมาะสมกับรูปแบบปัจจุบัน ตามธรรมเนียมปฏิบัติ โครงสร้างเรือจะประกอบด้วย ๔ องค์ประกอบหลัก ได้แก่ ๑) เปลือกเรือ ๒) โครงสร้างตามยาว ๓) โครงสร้างตามขวาง และ ๔) พื้นเรือ โดยในการประกอบ จะทำการตั้งโครงสร้างทั้งสองแนวให้แล้วเสร็จ แล้วประกอบเปลือกเรือตามเข้าไป ในลักษณะของการตามเสริมความแข็งแรง โครงสร้างแยกเป็นชิ้น ๆ เข้ากับเปลือกในส่วนต่าง ๆ อย่างไรก็ตาม ด้วยเทคโนโลยี ในการตัดและการเตรียมชิ้นงานในปัจจุบัน แนวทางการออกแบบโครงสร้าง

จึงมีการพัฒนาตามมาอย่างเหมาะสม โดยลักษณะการเดินโครงสร้างในเรือ Trimaran ลำปัจจุบันใช้วิธีการตัดแผ่น Plate ให้เข้ากับเปลือกเรือ เดินเต็มแผ่นตลอดแนว แล้วตัดให้สอดรับกับเปลือกเรือในจุดต่าง ๆ จากนั้น หากต้องการลดน้ำหนักของโครงสร้าง จะใช้วิธีการเจาะ Lightning Holes ที่แผ่นโครงสร้างตามความเหมาะสม

การคำนวณและตรวจสอบความแข็งแรงของโครงสร้างสามารถทำได้โดย ๒ วิธีหลัก คือ ๑) การคำนวณโดยตรง (Direct Calculation) ด้วยวิธี Finite Element Analysis ซึ่งเทคโนโลยีของคอมพิวเตอร์ในปัจจุบันสามารถทำให้ดำเนินการได้สะดวกมากขึ้น และ ๒) การกำหนดโครงสร้างแล้วตรวจสอบด้วยกฎข้อบังคับของสมาคมจัดชั้นเรือ (Classification Societies)

๓.๒.๗ การนำไปประยุกต์ใช้ร่วมกับระบบ Modularity และ AI

เพื่อให้การออกแบบ Trimaran USV เป็นไปอย่างครบถ้วนตามวัตถุประสงค์ที่ตอบสนองภารกิจต่าง ๆ ของกองทัพเรือ เมื่อสามารถกำหนดคุณสมบัติของแพลตฟอร์มที่เหมาะสมได้แล้ว การกำหนดคุณลักษณะของ Mission Modules และระบบควบคุมสั่งการให้ได้อย่างเหมาะสม ภารกิจสำคัญที่อาจถูกกำหนดให้เป็นภารกิจพื้นฐานของ Trimaran USV ลำนี้ เช่น การลาดตระเวนถ่ายภาพนิ่งและภาพเคลื่อนไหวของสถานการณ์ปัจจุบันที่บริเวณเส้นเขตแดนทางทะเล ที่อาจมีการลักลอบจากเรือต่างสัญชาติ หรือการลักลอบเข้าไปในประเทศเพื่อนบ้านของเรือสัญชาติไทย เพื่อตอบสนองภารกิจการรักษาผลประโยชน์ของชาติทางทะเลของ ศรชล. การปฏิบัติภารกิจประเภทนี้ เรือจะปฏิบัติการที่ย่านความเร็วต่ำ ซึ่งแพลตฟอร์มสามารถปฏิบัติการได้อย่างมีประสิทธิภาพตามคุณลักษณะของระบบขับเคลื่อนที่ได้กำหนดไว้ Mission Module ต้องได้รับการออกแบบให้สามารถดำเนินการกิจได้อย่างต่อเนื่อง บริเวณพื้นที่ติดตั้ง Mission Modules ต้องได้รับการออกแบบให้เหมาะสมสอดคล้องกับตัว Unit ของ Mission Modules สามารถยก Module ตัวหนึ่งออก และติดตั้ง Modules อื่นหนึ่งภารกิจที่อาจถูกกำหนดให้เป็นภารกิจหลักคือ การใช้ USV เป็นฐานขยายสัญญาณการสื่อสารของเรือดำน้ำ เพื่อตอบสนองการขยายขีดความสามารถของเรือดำน้ำที่กองทัพเรือจะได้รับมอบเร็ว ๆ นี้ สำหรับภารกิจอื่น ๆ เช่น การล่าทำลายทุ่นระเบิด การจู่โจม ได้ด้วยคุณลักษณะแบบ Plug

and Play รวมถึงระบบควบคุมสั่งการ ที่ต้องสามารถกำหนดให้เรือปฏิบัติการกิจด้วยตัวเองได้อย่างลุล่วง และสามารถคืนการบังคับบัญชาให้กับผู้ควบคุมที่สถานีควบคุม เมื่อเกิดสถานการณ์จำเป็น โดยการออกแบบ Mission Modules และระบบควบคุมสั่งการ จะมีรายละเอียดมากขึ้นในขั้นตอนต่อไปของการออกแบบ

บทสรุป

เมื่อพิจารณาขั้นตอนการออกแบบแพลตฟอร์มของ Multihull Vessel ประเภท Trimaran ตามหัวข้อ Conceptual Design แล้ว สรุปได้ว่า แพลตฟอร์มในรูปแบบ Trimaran ปัจจุบัน มีความเหมาะสมที่จะติดตั้งระบบควบคุมสั่งการ ระบบสื่อสาร และระบบปัญญาประดิษฐ์บูรณาการเข้ากับระบบ Modularity เพื่อกำหนดให้เป็น Trimaran Unmanned Surface Vessel with Capability of Mission Modules ซึ่งเป็นการรวมเอาข้อดีของคุณสมบัติทางนาวาสถาปัตยกรรมของเรือประเภท Trimaran มาใช้เป็นแพลตฟอร์มสำหรับการติดตั้ง Mission Modules ที่บรรจุระบบ และอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติการกิจที่หลากหลาย ตั้งแต่การลาดตระเวนหาข่าวด้วย Real Time Videos การล่าทำลายทุ่นระเบิด การเป็นแพลตฟอร์มส่วนขยายของการสื่อสารของเรือดำน้ำ ที่ย่านความเร็วต่ำ ไปจนถึงภารกิจโจมตี ช่วยเหลือตัวประกัน ที่ย่านความเร็วสูง จึงสามารถกล่าวได้ว่า แพลตฟอร์มนี้มีความเหมาะสมที่จะนำมาเป็นจุดเริ่มต้นในการพัฒนาการออกแบบ Modularity USVs ที่สมบูรณ์ โดยการบูรณาการร่วมกับเทคโนโลยี Modularity และ AI ที่จะเข้ามาเป็นหัวข้อลำดับต่อไปในการพัฒนา USVs ลำปัจจุบันนี้ ให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้

เอกสารอ้างอิง

- ๑ Y. Liu, H. Pu, J. Luo, S. Xie, Y. Peng, Y. Yang, X. Li, Z. Su, S. Gao, W. Shao, C. Zhu, J. Ke, J. Cui และ D. Qu, “Development of and Unmanned Surface Vehicle for the Emergency Response Mission of the ‘Sanchi’ Oil Tanker Collision and Explosion Accident,” *Applied Sciences*, 2020.
- ๒ J. E. Manly, “Unmanned Surface Vehicles, 15 Years of Development,” *IEEE*, 2008.
- ๓ J. Heo, J. Kim และ Y. Kwon, “Analysis of Design Directions for Unmanned Surface Vehicles,” *Journal of Computer and Communications*, pp. 92-100, 2017.
- ๔ J. F. Schank, S. Savitz, K. Munson, B. Perkinson, J. McGee and J. M. Sollinger, *Designing Adaptable Ships*, Santa Monica, California: RAND Corporation, 2016.
- ๕ D. Manley, “The NATO Drive to Mission Modularity,” ใน *Warship 2018: Procurement of Future Surface Vessel*, London, UK, 2018.
- ๖ R. B. Luhulima, D. Setyawan และ I. K. A. P. Utama, “Selecting Monohull, Catamaran and Trimaran as Suitable Passenger Vessels Based on tability and Seakeeping Criteria,” ใน *The 14th International Ship Stabiltiy Workshop (ISSW)*, Kuala Lumpur, 2014.
- ๗ H. Sun, J. Zou, Z. Sun และ S. Lu, “Numerical Investigations on the Resistance and Longitudinal Motion Stability of aHigh-Speed Planing Trimaran,” *Marine Science and Engineering*, 2020.



การพัฒนาาระบบควบคุมภัยพิบัติ

นางสาวเอก วิทยา ปัญญา
ผู้อำนวยการกองอำนวยการสื่อสารและเทคโนโลยีสารสนเทศ
สำนักนโยบายและแผน กรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

บทคัดย่อ

“ตามทฤษฎีของสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง ให้ความสำคัญกับการปฏิบัติที่สอดประสานกัน (Self Synchronization) ซึ่งจะเป็นการเพิ่มโอกาสในการใช้อาวุธ แล้วก่อให้เกิดการทวีกำลังรบ และนำไปสู่การเพิ่มพูนประสิทธิภาพในการปฏิบัติการทางอากาศในที่สุด โดยองค์ประกอบที่สำคัญคือการสร้างความตระหนักรู้ในสถานการณ์ (Situation Awareness) ซึ่งได้มาจากระบบควบคุมบังคับบัญชา โดยที่การพัฒนาระบบฯ ขึ้นอยู่กับบริบทและความต้องการของผู้ใช้ ควรมีการพัฒนาการปฏิบัติคู่ขนานกันไป และมีการประเมินผล เพื่อทำให้รับทราบระดับความสำเร็จของการพัฒนา แล้วนำบทเรียนที่ได้กลับไปทบทวนและปรับปรุงการพัฒนาในก้าวต่อไป”

บทนำ

ด้วยการพัฒนาเทคโนโลยีอย่างรวดเร็ว ที่เราเรียกกันว่า เทคโนโลยีเปลี่ยนโลก หรือ Disruptive Technologies ประกอบกับมีความต้องการปฏิบัติการทางทหารที่เพิ่มขึ้น เพื่อให้รองรับกับภัยคุกคามรูปแบบใหม่ (Non-Traditional Threat) รวมทั้งการปฏิบัติการทางทหารที่ไม่ใช่สงคราม เช่น การต่อต้านการก่อการร้าย การปฏิบัติการทางไซเบอร์ และการรักษาผลประโยชน์ของชาติ ทำให้ปัจจุบันมีเทคโนโลยีทางทหารใหม่ ๆ ถูกนำเสนอให้เห็นอยู่ทั่วไป ดังเช่นบทความอื่น ๆ ของวารสารฉบับนี้ เพื่อให้ฝ่ายเราสามารถเห็นภาพสถานการณ์ได้กว้างไกลกว่าเดิม เข้าใจความเปลี่ยนแปลงได้อย่างรวดเร็ว ตัดสินใจได้อย่างชาญฉลาด สามารถชิงลงมือปฏิบัติอย่างมีชั้นเชิงและปลอดภัย เพื่อให้ได้รับชัยชนะต่อฝ่ายข้าศึกในที่สุด ซึ่งเป็นไปตามทฤษฎีวงรอบการตัดสินใจของ OODA Loop นั่นเอง

ตามแนวความคิดที่กล่าวว่า ภัยคุกคาม (Threat) เกิดจากขีดความสามารถการทำลายของอาวุธ (Capability) ความตั้งใจ (Intention) และโอกาสในการใช้อาวุธ (Opportunity) นั้น เราสามารถย้อนกลับนำไปกำหนดปัจจัยพลังอำนาจทางทหารของฝ่ายเราที่จะเป็นภัยคุกคามให้กับฝ่ายตรงข้ามได้เช่นกัน ขณะเดียวกันทฤษฎีของสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare) ได้ให้ความสำคัญกับการปฏิบัติที่สอดประสานกัน (Self Synchronization) ซึ่งจะเป็นการเพิ่มโอกาสในการใช้อาวุธ และสร้างจังหวะความสอดคล้องในการทำลายเป้าหมายสำคัญ ที่จะก่อให้เกิดการทวีกำลังรบ (Force Multiplier)

อันจะนำไปสู่การเพิ่มพูนประสิทธิภาพในการปฏิบัติการกิจ (Mission Effectiveness) ในที่สุด โดยองค์ประกอบสำคัญที่สร้างการปฏิบัติที่สอดคล้องประสานกัน นั่นคือ ความตระหนักรู้ในสถานการณ์ (Situation Awareness) ซึ่งได้มาจากระบบควบคุมบังคับบัญชาที่จะนำไปสู่การตัดสินใจได้อย่างชาญฉลาดนั่นเอง

สำหรับบทความนี้จะนำเสนอแนวทางการพัฒนาระบบควบคุมบังคับบัญชา โดยไม่มีรายละเอียดที่เป็นขั้นความลับ มีการวิเคราะห์ข้อมูลตามทฤษฎีสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง และเป็นบทวิเคราะห์ของผู้เขียน มิใช่ความเห็นของหน่วยงานใด ๆ ที่เกี่ยวข้อง

ความสำคัญของระบบควบคุมบังคับบัญชา

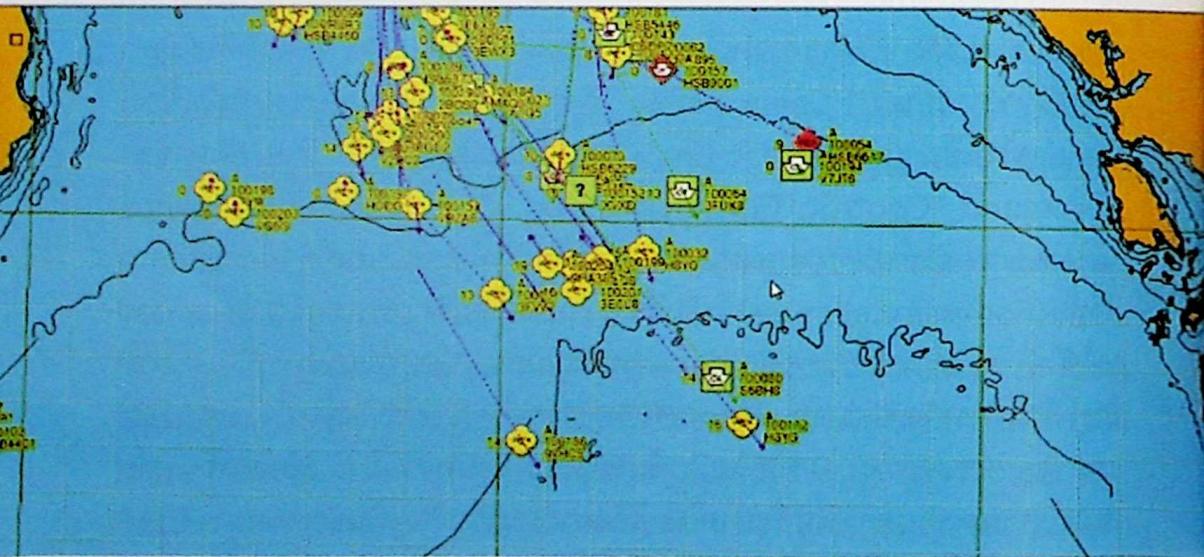
ระบบควบคุมบังคับบัญชา^๑ (Command and Control System: C²) ทำหน้าที่ประมวลผลข้อมูลและสั่งการต่าง ๆ รวมทั้งการดำเนินกรรมวิธี เพื่อช่วยเหลือการผลิตข่าวกรอง ให้มีความถูกต้องรวดเร็วทันต่อสถานการณ์ที่เกิดขึ้นอย่างต่อเนื่อง ซึ่งจะทำให้ผู้บังคับบัญชาสามารถวางแผน สั่งการ และควบคุมการปฏิบัติของหน่วยรบได้อย่างมีประสิทธิภาพ อีกทั้งยังเป็นองค์ประกอบสำคัญในการประสานการปฏิบัติทางข้างอีกด้วย ขณะเดียวกันยังเป็นเครื่องมือในการรายงานผลการปฏิบัติของหน่วยรบให้กับหน่วยเหนือได้รับทราบสถานภาพและความเคลื่อนไหวของสถานการณ์

จากเดิมที่มีเพียงการสื่อสารแบบอนาล็อก สำหรับการสื่อสารทางโทรศัพท์ โทรสาร และวิทยุ แต่ด้วยก้าวหน้าของเทคโนโลยี ทำให้ระบบควบคุมบังคับบัญชาที่เคยเรียกว่าระบบ C² (Command & Control) ได้รับการพัฒนาอย่างต่อเนื่อง จนกลายเป็น C³ หรือ C⁴I และ C⁴ISR ในที่สุด โดยที่ C⁴ISR ย่อมาจาก Command, Control, Communication, Computer, Intelligence Surveillance and Reconnaissance ซึ่งเป็นการนำเทคโนโลยีด้านการสื่อสาร ดิจิทัล (Communication) เทคโนโลยีสารสนเทศและคอมพิวเตอร์ (Computer) มาใช้ในการแลกเปลี่ยนข้อมูล และการประมวลผล ตลอดจนมีการเชื่อมต่อกับ ข้อมูลด้านการข่าวกรอง (Intelligence) และข้อมูลจากระบบตรวจจับ (Surveillance และ Reconnaissance) ที่ใช้ในการค้นหาและพิสูจน์ทราบฝ่าย เพื่อใช้สร้างภาพสถานการณ์ครอบคลุมพื้นที่ขนาดใหญ่ได้อย่างรวดเร็ว ปัจจุบันมักพบคำว่า C³ISR และ C⁴ISR ซึ่ง C ที่เพิ่มขึ้นมา หมายถึง “Cyber” และ “Combat System” อย่างไม่ก็ตาม ในแต่ละประเทศ อาจจะมีทฤษฎีและแนวความคิดที่ต่างกัน

ทำให้ยังคงใช้คำว่า “C²” เหมือนเดิม โดยไม่ขึ้นกับเทคโนโลยีที่เพิ่มเข้ามา หรือ อาจเปลี่ยนไปใช้คำอื่นแทนเลย

ในการควบคุมบังคับบัญชา เช่น ที่ศูนย์บัญชาการทางทหาร มีความต้องการขีดความสามารถที่เรียกว่า การทำความเข้าใจที่ลึกซึ้ง หรือ Sensemaking อันจะก่อให้เกิดการตัดสินใจและการกำหนดหนทางปฏิบัติที่ถูกต้อง จนนำไปสู่การปฏิบัติที่สอดประสานกัน (Self Synchronization) ทั้งนี้ ความสามารถทำความเข้าใจที่ลึกซึ้ง (Sensemaking)^๓ เกิดจากความตระหนักรู้ในสถานการณ์ (Situation Awareness: SA) และความเข้าใจ (Understanding) ที่เกี่ยวข้องกับกิจ เจตนาารมณ์ของผู้บังคับบัญชา รวมทั้งสภาพแวดล้อมและเงื่อนไขหรือข้อจำกัดต่าง ๆ

สำหรับความตระหนักรู้ในสถานการณ์^๔ นั้น เป็นแนวคิดทางทฤษฎีที่เกี่ยวข้องกับความเข้าใจของแต่ละบุคคล ที่เกี่ยวกับสถานการณ์ โดยแบ่งออกเป็น ๓ ระดับ ประกอบด้วย SA ระดับที่ ๑ การรับรู้ (Perception) เป็นการรับรู้สถานการณ์ปัจจุบัน ภายในระยะเวลาและภายในพื้นที่หนึ่ง ๆ SA ระดับที่ ๒ การเข้าใจ (Comprehension) คือ ความเข้าใจเหตุผลของสิ่งที่ได้เกิดขึ้น และ SA ระดับที่ ๓ การทำนายอนาคต (Projection) สามารถคาดเดาสถานการณ์ในอนาคตอันใกล้ได้



ภาพที่ ๑ ตัวอย่างการแสดงผลภาพสถานการณ์หรือ SA ระดับที่ ๑ การรับรู้ (Perception)

ทั้งนี้ ความตระหนักรู้ในสถานการณ์ (SA) เปรียบเทียบได้กับการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) ของภาคพลเรือน ใน ๓ ชั้นแรก ซึ่งประกอบด้วย การรับรู้ว่าจะเกิดอะไรขึ้น (Descriptive) การเข้าใจว่าสิ่งนั้นเกิดขึ้นเพราะอะไร (Diagnostic) และจะเกิดอะไรขึ้นต่อไป (Predictive) ในขณะที่ชั้นสูงกว่าถัดไปคือ ถ้าทำแบบนี้แล้วจะเกิดอะไรขึ้น (Prescriptive) อยู่ในระดับเดียวกับความเข้าใจที่ลึกซึ้ง (Sensemaking) ในการช่วยกำหนดหนทางปฏิบัติ และตัดสินใจ นั่นเอง

สรุปง่าย ๆ ความตระหนักรู้ในสถานการณ์เป็นองค์ประกอบหนึ่งในการสร้าง “การรู้เขา รู้เรา” โดยที่ความตระหนักรู้ในสถานการณ์ จะได้มาจากระบบควบคุมบังคับบัญชา ที่ทำการรวบรวมข้อมูลจากแหล่งต่าง ๆ หรือที่เรียกว่าข้อมูล ISR (Intelligence Surveillance Reconnaissance) แล้วนำมาวิเคราะห์ ประมวลผล และนำเสนอในลักษณะภาพ ดังตัวอย่างในภาพที่ ๑ โดยในปัจจุบันยังจำเป็นต้องใช้เจ้าหน้าที่ผู้เชี่ยวชาญมาทำการวิเคราะห์ อย่างไรก็ตาม ได้มีความพยายามนำเอาเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เข้ามาช่วย เพื่อให้เกิดความรวดเร็ว และง่ายขึ้น โดยที่ข้อมูลด้านการข่าวกรองมีความสำคัญอย่างมาก ในการวิเคราะห์เพื่อการจัดการกับข้อมูลที่มีความไม่แน่นอน ไม่สมบูรณ์ หรือเชื่อถือไม่ได้ ขณะเดียวกันระบบควบคุมบังคับบัญชาจะต้องกระจายข้อมูล เพื่อทำให้เกิดความตระหนักรู้ในสถานการณ์ร่วมกัน (Shared Situation Awareness) นอกเหนือจากนี้ การประสานงานร่วมกัน (Collaboration) ด้วยการใช้เครื่องมือสื่อสารและระบบสารสนเทศอื่น ๆ เพิ่มเติม จะทำให้เกิดการแลกเปลี่ยนความเข้าใจ (Shared Understanding) ที่เกี่ยวข้องกับสภาพแวดล้อมและข้อจำกัด เพื่อก่อให้เกิดความเข้าใจที่ลึกซึ้ง (Sensemaking) ต่อไป

ตัวอย่างที่สำคัญของกองทัพเรือคือ การจัดหมู่เรือปราบปรามโจรสลัดไปปฏิบัติหน้าที่รักษาผลประโยชน์ของชาติทางทะเล บริเวณอ่าวเอเดนและชายฝั่งประเทศโซมาเลีย จำนวน ๒ ครั้ง ในช่วงปี พ.ศ.๒๕๕๓ ถึง พ.ศ.๒๕๕๔ โดยมีการติดตั้งระบบควบคุมบังคับบัญชาของกองทัพเรือบนเรือหลวงสิมิลัน และเชื่อมโยงข้อมูลด้วยระบบสื่อสารผ่านดาวเทียมมายังศูนย์บัญชาการทหารหลักของกองทัพเรือ นอกจากนี้มีการติดตั้งระบบเชื่อมโยงข้อมูลย่านความถี่ VHF

เพื่อแลกเปลี่ยนข้อมูลทางยุทธวิธีระหว่างเรือหลวงสิมิลัน กับเรือตรวจการณ์ไกลฝั่ง ชุดเรือหลวงปัตตานี แม้ว่าระบบฯ ยังมีข้อจำกัด แต่สามารถทำให้ทุกหน่วยมีความตระหนักรู้ในสถานการณ์ร่วมกัน สามารถทำความเข้าใจและประสานการปฏิบัติตามหน้าที่ที่รับผิดชอบทั้งในทะเลและบนฝั่งได้อย่างมีประสิทธิภาพ

ในขณะที่การปฏิบัติร่วมกับกองกำลังผสมทางทะเลนานาชาติ มีการติดตั้งระบบ CENTRIXS (Central Enterprise Regional Information Exchange System) ของกองทัพเรือสหรัฐฯ ใช้งานผ่านระบบสื่อสารผ่านดาวเทียมภาคเอกชนที่มีการเข้ารหัส เพื่อเป็นระบบควบคุมบังคับบัญชาและแลกเปลี่ยนข้อมูลที่มีชั้นความลับ ระหว่างเรือในกองเรือผสมเฉพาะกิจ และกองบัญชาการกองกำลังผสมทางทะเล ณ ราชอาณาจักรบาห์เรน ทั้งนี้ ระบบ CENTRIXS นอกจากใช้แสดงภาพสถานการณ์ทางทะเลแล้ว ยังสามารถสนับสนุนการสื่อสารอื่น ๆ เช่น Chat VOIP และ E-Mail สำหรับการแลกเปลี่ยนข้อมูลข่าวสาร และข่าวกรอง เพื่อให้หน่วยที่เกี่ยวข้องทั้งในทะเลและบนฝั่ง สามารถสร้างความเข้าใจที่ลึกซึ้ง (Sensemaking) และปฏิบัติงานร่วมกันได้อย่างสอดประสาน

ตัวอย่างการพัฒนาระบบควบคุมบังคับบัญชา

ในการพัฒนาระบบควบคุมบังคับบัญชา มีบริบทที่สำคัญที่ต้องพิจารณา ได้แก่ ภัยคุกคามที่ต้องจัดการ และรูปแบบการควบคุมบังคับบัญชา ขณะเดียวกัน ควรพิจารณานำเทคโนโลยีที่มีมาใช้ แต่พึงระวังไม่ทำให้เป็นระบบฯ ที่โดดเดี่ยว เชื่อมต่อกับระบบอื่นไม่ได้ โดยมีตัวอย่างแนวทางการพัฒนาระบบควบคุมบังคับบัญชา ซึ่งกำหนดให้มีการพิจารณาส่วนที่สำคัญ ๓ ส่วน^๕ ดังนี้

๑. เริ่มต้นจากการกำหนดเทคโนโลยีการสร้างแบบจำลอง (Architecture Modeling Technology) ในอดีตมีการนำสมการของ Lanchester มาใช้งานเพื่อประเมินกำลังอำนาจทางทหาร โดยใช้จำนวนและขีดความสามารถของระบบอาวุธมาเปรียบเทียบกัน แล้วนำมาตัดสินใจว่าฝ่ายไหนจะได้รับชัยชนะ ในปัจจุบันมีการนำระบบปัญญาประดิษฐ์มาประยุกต์ใช้งาน^๖ ในการวิเคราะห์ข้อมูลและประเมินผล เพื่อให้เกิดความรวดเร็ว แต่อย่างไรก็ตาม สำหรับการกำหนดหนทางปฏิบัติยังต้องใช้เจ้าหน้าที่

๒. ลำดับต่อไปคือ กระบวนการออกแบบและพัฒนา (Design Method and Development Process) ตัวอย่างในเอกสาร DoD Architecture Framework ของกระทรวงกลาโหมสหรัฐฯ ได้ให้คำแนะนำการพัฒนา โดยเป็น แนวความคิดที่ใช้ข้อมูลเป็นศูนย์กลาง^๗ และมีมุมมองหลัก ๆ ที่ต้องพิจารณา ประกอบด้วย มุมมองของเจ้าหน้าที่ปฏิบัติงาน (Operational View) มุมมองของเจ้าหน้าที่ดูแลระบบ (Systems and Service View) ที่ให้การสนับสนุน การทำงานของระบบฯ มุมมองของเจ้าหน้าที่เทคนิค (Technical View) ในการ ติดตั้งและซ่อมบำรุงให้ระบบฯ ทำงานเป็นปกติ และมุมมองของภาพรวมทั้งหมด (All View)

๓. สุดท้ายเป็นการประเมินและตรวจสอบ (Evaluation Measurement and Verification Method) เพื่อวิเคราะห์ประสิทธิภาพในการตอบสนองภารกิจ ที่กำหนด โดยแยกเป็น ๒ ส่วน คือ ประสิทธิภาพในยามสงบ เป็นการประเมิน ความสมบูรณ์ โดยตรวจสอบความสามารถในการฝึก การเตรียมความพร้อม และการเฝ้าตรวจ ที่สะท้อนคุณลักษณะแบบคงที่ (Static Characteristic) และ ประสิทธิภาพในการปฏิบัติงาน หมายถึง ระดับความสามารถในการทำงาน และ ผลของการปฏิบัติ ในสภาพแวดล้อมเฉพาะของการรบ ซึ่งสะท้อนคุณลักษณะ แบบพลวัต (Dynamic Characteristic) ที่เปลี่ยนแปลงได้ตามสภาพแวดล้อม ในขณะนั้น

ระบบทางทหารมักไม่สามารถรองรับความต้องการในการปฏิบัติงาน ได้ทั้งหมด ยังมีช่องว่างระหว่างระบบฯ ในอุดมคติ กับระบบฯ ที่พัฒนาได้จริง ซึ่งช่องว่างดังกล่าวสามารถควบคุมให้อยู่ในขอบเขตที่ยอมรับได้ ด้วยการกำหนด การปฏิบัติที่เหมาะสม ขณะเดียวกันจะมีความพยายามในการพัฒนาเทคโนโลยี ใหม่ ๆ เพื่อนำมาแก้ปัญหาเหล่านี้ต่อไป

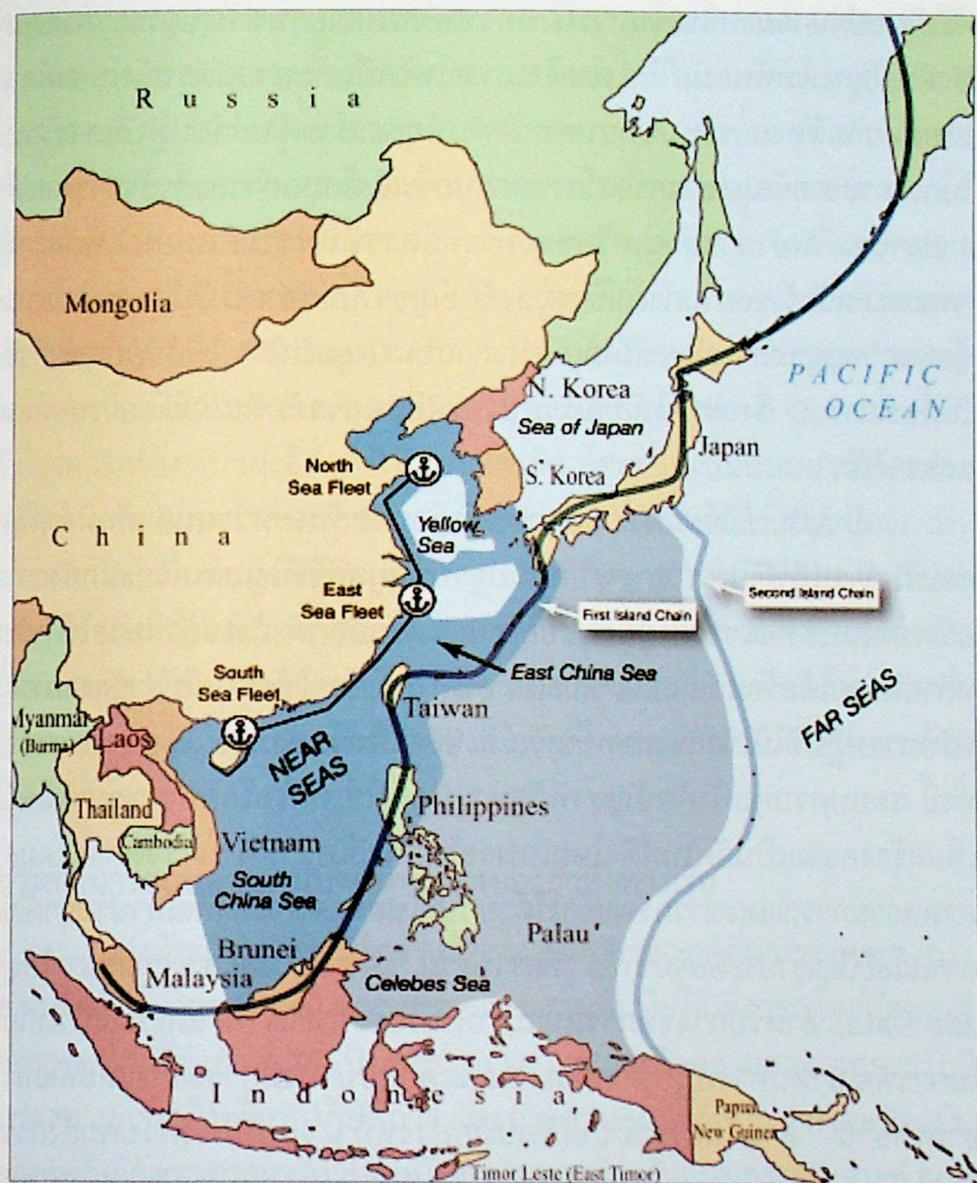
ตัวอย่างระบบควบคุมบังคับบัญชาที่มีความก้าวหน้าในการพัฒนา อย่างเป็นรูปธรรมคือ ระบบของกองทัพอากาศ โดยที่กองทัพอากาศใช้การ บังคับบัญชาแบบรวมการควบคุม แยกการปฏิบัติ (Centralized Control and Decentralized Execution) และมีการพัฒนาระบบควบคุมบังคับบัญชา เพื่อนำไปสู่กองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force) ประกอบด้วย ระบบบัญชาการและควบคุมทางอากาศ (กองทัพอากาศ

ใช้คำนี้แทนคำว่าระบบควบคุมบังคับบัญชา) เป็นเครื่องมือในการวางแผนการรบ ควบคุมและติดตามการปฏิบัติการทางอากาศโดยตรง สามารถเชื่อมต่อกับ เครื่องบินรบด้วยระบบเชื่อมโยงข้อมูลทางยุทธวิธี รวมทั้งรับข้อมูลจากส่วน ตรวจการณ์โดยตรง เพื่อการสร้างความตระหนักรู้ในสถานการณ์ได้อย่าง รวดเร็ว นอกจากนี้ยังมีระบบสารสนเทศสำหรับงานฝ่ายอำนวยการ ในการ บูรณาการข้อมูลจากกรมฝ่ายอำนวยการ เพื่อสร้างความเข้าใจ ส่งผลทำให้เกิด ความเข้าใจที่ลึกซึ้ง (Sensemaking) ที่จะนำไปสู่การวางแผนและตัดสินใจ ได้อย่างถูกต้องและรวดเร็ว ทั้งนี้ จากรูปแบบการควบคุมบัญชาการใช้กำลัง ทางอากาศ ทำให้ระบบบัญชาการและควบคุมทางอากาศต้องประสานและ ควบคุมการปฏิบัติหน่วยใช้กำลัง (Shooter/Effector) ได้ จึงให้ความสำคัญ กับระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link) ในการแลกเปลี่ยน ข้อมูลแบบใกล้เคียงเวลาจริง (Near Real Time : Near RT) อีกทั้งสามารถ รับส่งคำสั่งและรายงานที่เป็นรูปแบบเฉพาะได้อย่างรวดเร็วและปลอดภัย ขณะเดียวกันยังมีระบบสื่อสารอื่น ๆ ที่ติดต่อกับเครื่องบินได้โดยตรง เพื่อช่วย ในการประสานความเข้าใจอีกด้วย

สำหรับกองทัพในต่างประเทศ ที่มีภัยคุกคามที่รุนแรง เช่น ซีปนาวุธ ข้ามทวีป (Ballistic Missile) การแลกเปลี่ยนข้อมูลจะมีความเข้มข้นมากขึ้น เพื่อให้ตอบโต้และทำลายได้ทันที เช่น ระบบ Aegis Ballistic Missile Defense (Aegis BMD) ต้องการทั้งระบบตรวจการณ์และระบบอาวุธต่อต้าน ที่มีประสิทธิภาพสูงหลายระบบทำงานร่วมกัน ขณะเดียวกันต้องการเครือข่าย การสื่อสารเฉพาะที่รองรับการแลกเปลี่ยนข้อมูลแบบเวลาจริง (RT) เช่น เทคโนโลยีแบบ Cooperative Engagement Capability (CEC) เพื่อรวบรวม ข้อมูลคุณภาพสูงทั้งหมดจากระบบตรวจการณ์และระบบอาวุธของเรือ อากาศยาน หน่วยต่าง ๆ เข้าไว้ด้วยกัน และรวมเป็นข้อมูลอันหนึ่งอันเดียวกัน ส่งผลให้ได้ภาพสถานการณ์ที่กว้างไกล มีความรวดเร็ว และความถูกต้องแม่นยำสูง ขณะเดียวกันหน่วยใช้กำลังที่อยู่ในเครือข่าย ไม่ว่าจะอยู่ในพื้นที่ใดก็ตาม สามารถนำข้อมูลดังกล่าว มาทำการใช้อาวุธทำลายได้ทันที

ตัวอย่างอื่น ๆ ที่คล้ายกัน เช่น กองทัพเรือเกาหลีใต้ ได้พัฒนาให้มี การเชื่อมต่อข้อมูลระบบควบคุมบังคับบัญชา ทั้งในระดับยุทธวิธีและระดับยุทธการ

รวมกับระบบประมวลผลข้อมูลดิจิทัลที่เป็นระบบเฉพาะ และเครือข่าย Real Time Text ให้เป็นเครือข่ายเดียวกันและรับส่งข้อมูลได้รวดเร็วแบบเวลาจริง (RT) ในขณะที่กองทัพสิงคโปร์^{๑๑} ซึ่งมีพื้นที่ขนาดเล็กมาก ๆ จึงให้ความสำคัญกับการเชื่อมต่อข้อมูลระบบควบคุมบังคับบัญชาทั้งระบบตรวจจับและระบบอาวุธ เพื่อให้การปฏิบัติการทางทหาร จนถึงขั้นการใช้อาวุธสามารถดำเนินการได้อย่างทันเวลาและสอดคล้องประสานกัน



ภาพที่ ๒ : ตัวอย่างพื้นที่ปฏิบัติการของกองทัพเรือจีน^{๑๑}

ยังมีตัวอย่างการพัฒนาในต่างประเทศ ที่น่าสนใจนำเสนอคือ กองทัพอากาศ^{๓๓} ซึ่งได้สันนิษฐานกันว่า มีการพัฒนาตามบริบทที่เปลี่ยนแปลงอย่างมาก โดยที่กำลังทางเรือในพื้นที่ทะเลใกล้ชายฝั่งทะเล (Near Seas) ตามภาพที่ ๒ ซึ่งต้องทำงานประสานกับหน่วยราชการอื่น ๆ และมีประเด็นความละเอียดอ่อนในพื้นที่ที่อ้างสิทธิ์ทับซ้อน ยังคงใช้การควบคุมบังคับบัญชาแบบรวมอำนาจ ในขณะที่กองเรือในพื้นที่ไกลออกไปมีแนวโน้มปรับเป็นแบบกระจายอำนาจมากขึ้น ในการนี้ กองทัพอากาศพยายามปรับปรุงการควบคุมบังคับบัญชาให้ทันสมัย^{๓๔} ทั้งในด้านเทคโนโลยีและการจัดรูปแบบองค์กร โดยมีความต้องการระบบควบคุมบังคับบัญชาสำหรับการปฏิบัติการร่วมในการกระจายข้อมูลข่าวกรอง ภาพสถานการณ์ ข้อมูลการส่งกำลังบำรุง และรายงานสภาพอากาศผ่านเครือข่ายการสื่อสารที่มีความยืดหยุ่น เพื่อสร้างความตระหนักรู้ในสถานการณ์ของผู้บังคับบัญชา นอกจากนี้ ยังมีความต้องการข้อมูลภาพสถานการณ์แบบใกล้เคียงเวลาจริง (Near RT) ให้กับผู้บัญชาการในพื้นที่การรบ ซึ่งจะทำให้สามารถปรับเปลี่ยนการตัดสินใจได้อย่างถูกต้องและรวดเร็ว

ปัจจุบันได้มีการส่งมอบระบบฯ ที่เชื่อมต่อกันระหว่างเหล่าทัพที่จำเป็นสำหรับการปฏิบัติการร่วม ตลอดจนมีฐานข้อมูลดิจิทัลและเครื่องมือสั่งการอย่างอัตโนมัติ ที่จะช่วยให้ผู้บังคับบัญชาสามารถออกคำสั่งไปยังหน่วยใช้กำลังหลายหน่วยได้พร้อมกัน แม้ในขณะเคลื่อนที่ และช่วยให้หน่วยใช้กำลังสามารถปรับการปฏิบัติให้เข้ากับสภาพการณ์ที่เปลี่ยนไปในพื้นที่รบได้อย่างรวดเร็ว ทั้งนี้ ระบบควบคุมบังคับบัญชาที่จัดหา มีการใช้เทคโนโลยีปัญญาประดิษฐ์ เพื่อสร้างความเป็นอัตโนมัติ โดยเฉพาะในการวิเคราะห์ การจัดการข้อมูล ภาพสถานการณ์และข่าวกรองเข้าไว้ด้วยกัน ในอนาคตจะยิ่งพัฒนาประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์มากขึ้น เพื่อรวบรวม วิเคราะห์ และส่งข้อมูลขนาดใหญ่ (Big Data) สำหรับการจัดการสนามรบให้มีประสิทธิภาพ และอาจนำไปใช้ในการพัฒนาหนทางปฏิบัติอีกด้วย ขณะเดียวกัน ยังมีการสร้างและพัฒนาอากาศยาน^{๓๕} สำหรับเป็นระบบเตือนภัยล่วงหน้า ระบบการควบคุมสั่งการทางอากาศ การลาดตระเวนทางอิเล็กทรอนิกส์ และอากาศยานไร้คนขับ (UAV) ที่มีแนวโน้มเพิ่มขึ้นเรื่อย ๆ ทั้งด้านจำนวน รัศมีปฏิบัติการ และปริมาณเครื่องมือ

ตรวจจับที่ติดตั้ง นอกจากนี้ยังนำเทคโนโลยีอวกาศมาใช้ในการลาดตระเวน
หาข่าว การสื่อสาร การหาตำแหน่งและเทียบเวลา เพื่อให้สามารถปฏิบัติการ
ได้ทั่วโลก และพร้อมที่จะก้าวขึ้นเป็นขั้วมหาอำนาจของโลกต่อไป

เนื่องจากการพัฒนาขีดความสามารถของสงครามที่ใช้เครือข่าย
เป็นศูนย์กลาง มีความต้องการในการนำเทคโนโลยีต่าง ๆ มาเชื่อมต่อกัน
ในระดับสูง โดยเรามักพบเห็นได้จากรูปจำลองที่แสดงเครือข่ายและความสัมพันธ์
ขององค์ประกอบต่าง ๆ อย่างซับซ้อน และในสภาพแวดล้อมของการปฏิบัติ
ทางทหารจริง ฝ่ายตรงข้ามจะพยายามสร้างความไม่แน่นอนและขัดขวาง
การสื่อสาร ทำให้ข้อมูลข่าวสารขาดความครบถ้วน ดังนั้น ผู้บังคับบัญชา
ต้องจัดการกับความผันผวนของข้อมูล ความไม่แน่นอนในสนามรบ รวมทั้ง
มีการวิเคราะห์และใช้ประโยชน์จากข้อมูลความรู้เหล่านี้ จึงเป็นที่มาของ
แนวความคิดแบบ Decision-Centric Warfare^{๕๕} ที่เน้นการทำความเข้าใจและ
ตัดสินใจจากข้อมูลที่มืออยู่ ร่วมกับการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์
นอกจากนี้ ยังมีแนวความคิดแบบ Distributed Maritime Operations^{๕๖}
ที่ต้องการสร้างหน่วยใช้กำลังให้มีขนาดเล็ก โดยเน้นเป็นแบบยานไร้คนขับ
ที่มีความคล่องแคล่ว สามารถบรรจุอุปกรณ์ตรวจจับหรืออาวุธได้ และถูกส่ง
กระจายไปทั่วพื้นที่ปฏิบัติการ สามารถปรับเปลี่ยนการปฏิบัติได้ง่าย ทำให้เกิด
การขยายรัศมีการตรวจการณ์ และการใช้อาวุธได้จากหลายทิศทางพร้อมกัน
เพื่อตอบสนองต่อภัยคุกคามในหลายรูปแบบอย่างมีประสิทธิภาพ อีกทั้ง
เป็นการลดความเสี่ยงในการถูกทำลาย และยังสร้างความสับสนให้กับฝ่ายตรงข้าม
ได้ง่ายยิ่งขึ้น

การพัฒนาระบบควบคุมบังคับบัญชาของกำลังทางเรือ

กองทัพเรือได้กำหนดการสร้างความมั่นคงของชาติทางทะเล ตามแนว
ความคิดที่กล่าวว่า “สองฝั่งมหาสมุทรและสามพื้นที่ปฏิบัติการ” โดยใช้ทฤษฎี
ของสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง มาสร้างขีดความสามารถการรับรู้
ภาพสถานการณ์ในพื้นที่ปฏิบัติการ และการควบคุมบังคับบัญชา โดยปัจจุบัน
กองทัพเรือใช้แนวทางการควบคุมบังคับบัญชาคล้ายกับแบบการกระจายอำนาจ
(Decentralization) มีการแบ่งมอบอำนาจให้ทัพเรือภาคเป็นผู้กำกับดูแล

การปฏิบัติ เรือแต่ละลำมีระบบตรวจการณ์ ระบบควบคุมสั่งการหรือระบบ
อำนวยความสะดวก และระบบอาวุธในตนเอง ในกรณีมีเหตุการณ์ไม่ปกติ มักมอบหมาย
ให้หน่วยที่เข้าถึงพื้นที่ก่อนรับผิดชอบเป็นผู้บัญชาการเหตุการณ์ ระบบควบคุม
บังคับบัญชาที่ต้องการในระดับยุทธการจึงเน้นการสร้างภาพสถานการณ์
เพื่อทำให้เกิดความตระหนักรู้ในสถานการณ์ร่วมกันเป็นหลัก โดยมีระบบสื่อสาร
ต่าง ๆ ช่วยในการประสานทำความเข้าใจ ซึ่งแตกต่างจากระบบอำนวยความสะดวก
(Combat Management System: CMS) ที่เป็นระบบในระดับยุทธวิธี และ
เชื่อมต่อกับระบบอาวุธบนเรือโดยตรง นอกจากนี้ ตามรูปแบบการควบคุม
บังคับบัญชาของการใช้กำลังทางเรือดังกล่าว ยังต้องให้ความสำคัญกับภาวะผู้นำ
ของผู้บังคับบัญชาในแต่ละระดับ และความไว้วางใจระหว่างกันอีกด้วย

ตามโครงการพัฒนาขีดความสามารถสำหรับสงครามที่ใช้เครือข่าย
เป็นศูนย์กลาง กองทัพเรือได้ให้ความสำคัญกับการพัฒนาระบบควบคุมบังคับ
บัญชา เบื้องต้นได้ทำการศึกษาความต้องการทางยุทธการจากโครงการพัฒนา
ระบบงานหลัก (Core Application) ของระบบควบคุมบังคับบัญชา ต่อมา
ได้ดำเนินการจัดซื้อซอฟต์แวร์ระบบควบคุมบังคับบัญชา โดยส่วนหนึ่งบริษัท
คู่สัญญาเป็นผู้ที่ติดตั้งระบบฯ เพื่อการทดสอบ แต่สำหรับการขยายผลการติดตั้ง
เพิ่มเติมให้กับศูนย์บัญชาการบนฝั่ง และหน่วยใช้กำลัง เป็นการดำเนินการ
โดยเจ้าหน้าที่กองทัพเรือเอง ระบบฯ ดังกล่าวเป็นระบบฯ ที่ได้รับการพัฒนา
มาก่อนแล้ว และปรับปรุงเพิ่มเติมให้สอดคล้องกับความต้องการของกองทัพเรือ
ดังนั้น จึงไม่ต้องการกระบวนการออกแบบและพัฒนาที่ซับซ้อน แต่ยังคงต้องม
ีการกำหนดการปฏิบัติให้เหมาะสมและครบทุกมุมมอง ทั้งนี้ การสร้างแบบจำลอง
เป็นลักษณะการกำหนดหลักนิยมหรือรูปแบบปฏิบัติ ร่วมกับการกำหนดจำนวน
และขีดความสามารถของระบบอาวุธ แล้วนำมาเปรียบเทียบกัน ซึ่งระบบ
ควบคุมบังคับบัญชานี้ยังนำมาประยุกต์ใช้เป็นระบบจำลองยุทธสำหรับการฝึกได้
โดยมีขั้นตอนสุดท้ายตามแนวทางการพัฒนา คือ การประเมินและตรวจสอบ
ที่จะต้องดำเนินการต่อไป

ระบบควบคุมบังคับบัญชาสามารถควบคุมการทำงานของอุปกรณ์
ตรวจการณ์หลักทั้งเรดาร์และกล้องตรวจการณ์ที่จัดหาใหม่ตามโครงการ ทำให้
ได้ข้อมูล SR โดยตรง พร้อมการเชื่อมต่อข้อมูลกับระบบฯ ของศูนย์บัญชาการ

ทางทหารบนฝั่งที่รับผิดชอบ นอกจากนี้ ในปัจจุบันเรือรบที่มีคุณค่าทางยุทธการสูง ได้รับการติดตั้งระบบอำนวยการรบ พร้อมกับระบบเชื่อมโยงข้อมูลทางยุทธวิธี สำหรับแลกเปลี่ยนข้อมูลแบบใกล้เคียงเวลาจริง (Near RT) เพื่อการสร้าง ความตระหนักรู้ในสถานการณ์ร่วมกันและการประสานการปฏิบัติในระดับ ยุทธวิธีระหว่างกัน เรือรบบางลำยังได้รับการติดตั้งระบบบัญชาการและควบคุม ทางอากาศเพิ่มเติม เพื่อการปฏิบัติการร่วมกับกำลังทางอากาศของกองทัพอากาศ ในขณะที่เรือรบเก่าที่เข้าประจำการอยู่ก่อนหน้าแล้ว ไม่สามารถใช้ประโยชน์ จากเครือข่ายของระบบเชื่อมโยงข้อมูลทางยุทธวิธีได้ ยังต้องสื่อสารทางเสียงเป็นหลัก เพื่อจัดการกับข้อจำกัดดังกล่าว จึงได้มีแผนขยายเครือข่าย ระบบควบคุมบังคับบัญชาออกไปยังหน่วยเรือหรือหน่วยใช้กำลัง ซึ่งจะเป็น ก้าวที่ท้าทายต่อไป ทั้งในด้านเทคนิคและด้านการปฏิบัติ โดยประโยชน์ที่คาดว่าจะ ได้รับคือ เรือในพื้นที่ปฏิบัติการจะทำหน้าที่เป็นส่วนตรวจการณ์โดยอัตโนมัติ ทำให้เรือภายในกองเรือด้วยตัวเอง และศูนย์บัญชาการบนฝั่งกับเรือในทะเล มีความตระหนักรู้ในสถานการณ์ร่วมกัน เนื่องจากการควบคุมบังคับบัญชา ในระดับยุทธการ ไม่นำมาใช้ในการควบคุมอาวุธ และเป้าพื้นน้ำมีความเร็วต่ำ จึงสามารถนำข้อมูลทั้งแบบใกล้เคียงเวลาจริง (Near RT) และแบบไม่ใช้ เวลาจริง (Non RT) มาผสมผสาน รวมกับข้อมูลด้านการข่าวกรอง เพื่อประกอบกัน สร้างความตระหนักรู้ในสถานการณ์ระดับยุทธการขนาดใหญ่ร่วมกันได้ และนำมา ประติดประต่อกันจนครอบคลุมพื้นที่ปฏิบัติการหลักในที่สุด โดยที่การปฏิบัติ ต้องได้รับการสร้างและพัฒนาคู่ขนานกันไปด้วย

สำหรับการเชื่อมโยงข้อมูลบนฝั่ง เราสามารถสร้างระบบโทรคมนาคม ขึ้นมารองรับได้ง่าย ในขณะที่การสื่อสารระยะไกลระหว่างฝั่งกับเรือ นั้น เป็นลักษณะผสมผสานให้เกิดความยืดหยุ่น เพื่อสร้างความเชื่อถือได้รวดเร็ว และปลอดภัย โดยเรือที่มีคุณค่าทางยุทธการสูงได้รับการติดตั้งระบบสื่อสาร ผ่านดาวเทียมเรียบร้อยแล้ว เนื่องจากขนาดช่องสัญญาณดาวเทียมมีจำกัด ในการปฏิบัติจึงต้องมีการคัดกรองและกำหนดลำดับความสำคัญของข้อมูลที่จะ แลกเปลี่ยน อย่างไรก็ตาม เครือข่ายการสื่อสารผ่านดาวเทียมยังมีความเปราะบาง ตามแนวความคิดของการต่อต้านการเข้าถึง/การปฏิเสธไม่ให้เข้าพื้นที่ (A2/AD) ดังนั้น กองทัพเรือจึงมีระบบสื่อสารย่านความถี่ HF สำหรับการสื่อสารทางเสียง

และข้อความสั้น เนื่องจากระบบสื่อสารย่านความถี่ HF มีข้อจำกัดทางธรรมชาติ ในการส่งข้อมูลดิจิทัล ทำให้การประยุกต์ใช้งานกับระบบควบคุมบังคับบัญชา ที่ทำงานบนเครือข่ายอินเทอร์เน็ต ต้องคำนึงถึงข้อจำกัดทางเทคนิคในการ เชื่อมต่อกันอย่างสมบูรณ์และการรองรับความเป็นพลวัตของข้อมูล รวมทั้ง การปฏิบัติต้องคัดกรองแบบเฉพาะเจาะจง และมีความถี่การรับส่งตามขนาด ความจุช่องสัญญาณ เพื่อให้แลกเปลี่ยนเหลือเฉพาะข้อมูลข่าวสารที่จำเป็น เท่านั้น

นอกจากนี้ ด้วยความก้าวหน้าของเทคโนโลยีด้านการสื่อสาร สามารถ นำมาประยุกต์ใช้สร้างเครือข่ายอินเทอร์เน็ตภายในระยะขอบฟ้า (Line of Sight) หรือโดยเฉพาะสำหรับภายในหมู่เรือได้ง่ายขึ้น ขณะเดียวกันเครือข่าย ดาวเทียมภาคเอวกชนมีการพัฒนาทางเทคโนโลยีและการแข่งขันกันสูงขึ้น เช่น Inmarsat Iridium Starlink Thuraya แต่เนื่องจากเครือข่ายดาวเทียมฯ ดังกล่าว ของกองทัพเรือไม่สามารถควบคุมได้ ดังนั้น เบื้องต้นจึงไม่ควรนำมา ใช้งานทางยุทธการ แต่หากไม่มีทางเลือกต้องพิจารณาถึงความจำเป็น ความเร่งด่วน และมาตรการรักษาความปลอดภัยของข่าวสารนั้น ๆ อย่างมาก ดังตัวอย่าง ระบบ CENTRIX ของกองทัพเรือสหรัฐฯ เป็นต้น

ในส่วนข้อมูลเป่าบนบก ปัจจุบันในระดับยุทธวิธีจะมีระบบ Blue Force Tracking ที่รับข้อมูลตำบลที่จากเครื่องรับส่งวิทยุสื่อสารประจำหน่วยรบ และ ระบบควบคุมเฝ้าระวังและควบคุมสถานการณ์ที่เชื่อมต่อกับกล้องติดบุคคล แต่สำหรับการเชื่อมต่อข้อมูลกับเหล่าทัพอื่นสำหรับการปฏิบัติการร่วม ยังต้องมี ระเบียบและข้อตกลงร่วมกัน ทั้งนี้ หากมีระบบควบคุมบังคับบัญชาที่แตกต่างกัน และมีข้อจำกัดทางเทคนิคต่าง ๆ ก็ยังไม่จำเป็นต้องพัฒนาให้รวมเป็นระบบ เดียวกัน แต่แยกระบบกันทำงาน และให้มีการแลกเปลี่ยนข้อมูลระหว่างกัน เพื่อให้เกิดความเสถียร ง่ายต่อการซ่อมบำรุง และสามารถขยายต่อได้ในอนาคต อย่างไม่จำกัด ต้องกำหนดกระบวนการปฏิบัติที่เหมาะสมขึ้นมาเพิ่มเติมด้วย

สำหรับการรวบรวมข้อมูล ISR ให้ครอบคลุมพื้นที่ที่สนใจ จำเป็นต้อง เชื่อมต่อข้อมูลกับระบบอื่น ๆ เช่น ข้อมูลการรักษาผลประโยชน์ของชาติทางทะเล แต่เนื่องจากข้อมูลมีระดับชั้นความลับที่แตกต่างกัน จึงไม่ควรนำระบบควบคุม บังคับบัญชาที่ใช้สำหรับการปฏิบัติการทางทหารไปเชื่อมต่อกันโดยตรง ดังนั้น

จำเป็นต้องมีระบบที่ทำหน้าที่เป็นตัวกลาง ซึ่งใช้ในการสร้างความตระหนักรู้ ในสถานการณ์ทางทะเล (Maritime Domain Awareness: MDA) ร่วมกับ หน่วยงานภาคพลเรือนและภาคเอกชน ส่งข้อมูลมายังระบบควบคุมบังคับบัญชาฯ ในลักษณะส่งทางเดียว

อนึ่ง การขยายการเชื่อมต่อระบบควบคุมบังคับบัญชาฯกับระบบอื่น หรืออุปกรณ์ตรวจจับเพิ่มเติมในภายหลัง เราต้องพิจารณาว่ามีวัตถุประสงค์อะไร และต้องการข้อมูลอย่างไร ตัวอย่างเช่น หากมีวัตถุประสงค์เพื่อสร้างภาพ สถานการณ์ และต้องการรับข้อมูลเป้า (Track) จากเรดาร์ ดังนั้น ในการจัดหาระบบเรดาร์ใหม่ จึงต้องกำหนดช่องทางกายภาพในการเชื่อมต่อที่เป็นมาตรฐาน พร้อมมีรายละเอียดข้อมูลที่เกี่ยวข้องในการเชื่อมต่อ รวมทั้งซอฟต์แวร์ที่จำเป็น ซึ่งข้อมูลดังกล่าวเป็นข้อมูลแบบคงที่ (Static) แต่สำหรับระบบมีความซับซ้อน และเป็นระบบเฉพาะ จะต้องการรายละเอียดข้อมูลที่มีลักษณะเป็นแบบพลวัต (Dynamic) ทำให้มีความจำเป็นต้องใช้ในระบบจำลอง (Simulator) ร่วมด้วย เพื่อให้สามารถทดสอบและปรับแต่งการเชื่อมต่อให้มีความถูกต้องและเกิดความเสถียร

การพัฒนาการปฏิบัติให้รองรับระบบควบคุมบังคับบัญชา

การมุ่งเน้นการสร้างองค์ความรู้เพียงอย่างเดียว จะทำให้ขาดความสนใจ ในการพัฒนาการปฏิบัติเพื่อให้ใช้งานระบบควบคุมบังคับบัญชาได้อย่างมีประสิทธิภาพ และขาดข้อมูลสะท้อนกลับอย่างมีหลักการและเหตุผล เพื่อใช้ในการพัฒนาระบบฯ ก้าวต่อ ๆ ไปในอนาคต ในการนี้ การพัฒนาองค์ประกอบต่าง ๆ ไม่ควรรอให้ระบบหรือเครื่องมือมีความพร้อม แต่ควรดำเนินการด้านต่าง ๆ คู่ขนานกันไป โดยเงื่อนไขสำคัญของก้าวแรกของการพัฒนา คือ การให้บุคลากรที่เกี่ยวข้องมีส่วนร่วม^{๓๓} ขณะเดียวกัน เพื่อให้การทำงานร่วมกันมีประสิทธิภาพ จำเป็นต้องมีการฝึกองค์บุคคลให้เกิดความชำนาญ มีภาวะผู้นำ และเกิด “ความไว้วางใจ (Trust)” ระหว่างกัน ซึ่งความไว้วางใจ^{๓๔} อธิบายง่าย ๆ คือ การมีความตั้งใจ (Moral Courage) ที่จะทำในสิ่งที่ถูกต้อง และมีความสามารถ (Competence) ที่จะทำสิ่งที่ถูกต้องตามที่ตั้งใจนั้นไว้ได้ สำหรับการพัฒนาการปฏิบัติให้รองรับระบบควบคุมบังคับบัญชา โดยสรุป ประกอบด้วย

๑. **กระบวนการปฏิบัติ** เนื่องจากวัตถุประสงค์หลักของการพัฒนาระบบควบคุมบังคับบัญชาคือ การทำให้เกิดความตระหนักรู้ในสถานการณ์ร่วมกัน และการสร้างความเข้าใจร่วมกัน ดังนั้น กระบวนการปฏิบัติขั้นเริ่มต้นจึงต้องมีความง่ายใช้งานได้ร่วมกัน ไม่เป็นลักษณะระบบเฉพาะส่วนบุคคล และให้กำลังพลที่เกี่ยวข้องได้มีส่วนร่วม ตลอดจนถึงต้องมีการสร้างกระบวนการปฏิบัติในการประสานงานร่วมกันระหว่างหน่วยอีกด้วย และเนื่องจากระบบทางทหารมักไม่สามารถรองรับความต้องการในการปฏิบัติงานได้ทั้งหมด ดังนั้น จึงต้องมีการกำหนดการปฏิบัติงานรองรับในประเด็นนี้ด้วย และการพัฒนากระบวนการปฏิบัติก้าวถัดไปคือ การพิจารณาให้ครอบคลุมถึงการจัดการกับความผันผวนของข้อมูล และความไม่แน่นอนในสนามรบ เพื่อให้การปฏิบัติมีความยืดหยุ่น และทำให้วงจรการตัดสินใจตาม OODA Loop สั้นและเร็วกว่าฝ่ายตรงข้าม

๒. **ด้านกำลังพล** การนำระบบควบคุมบังคับบัญชามาใช้ จำเป็นต้องมีเจ้าหน้าที่ทำงานประจำ เช่น ที่ห้องติดตามภาพสถานการณ์ของศูนย์บัญชาการทางทหาร สำหรับเจ้าหน้าที่ประจำสถานีตรวจการณ์จะเปลี่ยนบทบาทจากพนักงานเรดาร์ กลายเป็นเจ้าหน้าที่ระบบควบคุมบังคับบัญชาแทน โดยยังทำงานในขั้นตอนการค้นหา ติดตาม พิสูจน์ทราบ และการคัดกรองเพื่อส่งข้อมูลออกหรือประสานกับหน่วยเกี่ยวข้องเพื่อการปฏิบัติต่อไป ทั้งนี้ ในยามสงบ เนื่องจากเป้าที่สนใจมักมีปริมาณน้อย สามารถลดจำนวนเจ้าหน้าที่ลงได้ แต่เมื่อมีความต้องการที่มากขึ้นของการตรวจการณ์ เช่น ในสถานการณ์วิกฤต ขึ้นตอบโต้ และป้องกันประเทศ จะต้องเพิ่มจำนวนเจ้าหน้าที่ตามภาระงานที่เกิดขึ้น ในขณะที่เดียวกันเจ้าหน้าที่สนับสนุน ต้องทยอยสร้างให้เพียงพอกับความต้องการประกอบด้วย เจ้าหน้าที่ดูแลระบบ และเจ้าหน้าที่ช่างเทคนิค ในส่วนนี้อาจจะต้องนำไปสู่การปรับรูปแบบขององค์กรในกองทัพ เพื่อจะได้มีเจ้าหน้าที่เพียงพอในการรองรับความเปลี่ยนแปลงที่เกิดขึ้น

๓. **การฝึก** สำหรับการฝึกขั้นพื้นฐาน โดยส่วนใหญ่ มักจะแบ่งระดับของการฝึก ออกเป็น ๓ ระดับ ประกอบด้วย ระดับ “ผู้ใช้” คือ เจ้าหน้าที่ผู้ใช้งานระบบ ระดับ “ซ่อมบำรุง” คือ เจ้าหน้าที่ที่มีขีดความสามารถในการซ่อมบำรุงระดับหน่วยสนับสนุน โดยอาจจะรวมหรือแยกออกเป็น เจ้าหน้าที่ดูแลระบบ และเจ้าหน้าที่ช่างเทคนิค ขึ้นอยู่กับความเหมาะสม และสุดท้ายคือ

ระดับ “ครู” เพื่อทำหน้าที่สร้างบุคลากรในอนาคต ขณะเดียวกันจะต้องมีการฝึกในขั้นสูงขึ้นไป ซึ่งเป็นการฝึกเจ้าหน้าที่ผู้ใช้ ให้สามารถประสานงานและมีความไว้วางใจร่วมกัน

๔. การประเมินผลและตรวจสอบ เพื่อวิเคราะห์ประสิทธิภาพในการตอบสนองภารกิจที่กำหนด ในการนี้ สามารถประยุกต์ใช้ลำดับชั้นของการประเมิน (Hierarchy for Metrics) ซึ่งได้รับการพัฒนาโดย Military Operations Research Society (MORS)^{๑๙} ประกอบด้วย การวัดประสิทธิภาพการใช้อำกำลัง (Measures of Force Effectiveness) ของหน่วยกำลังรบ ภายหลังปฏิบัติการกิจ หรือระดับของความสำเร็จที่ได้ การวัดประสิทธิภาพ (Measures of Effectiveness) เมื่อนำระบบควบคุมบังคับบัญชามาใช้ การวัดการดำเนินการ (Measures of Performance) ขององค์ประกอบภายในระบบ และการวัดคุณลักษณะเฉพาะ (Dimensional Parameters) ของระบบควบคุมบังคับบัญชา โดยที่สองหัวข้อแรกสำหรับประเมินคุณลักษณะแบบพลวัต (Dynamic Characteristic) ในขณะที่สองหัวข้อหลังสำหรับการประเมินคุณลักษณะแบบคงที่ (Static Characteristic) ได้ตามลำดับ การประเมินผลและตรวจสอบควรดำเนินการเป็นประจำทุก ๆ ปี เพื่อจะได้ทราบถึงความก้าวหน้า รวมทั้งนำผลลัพธ์มาปรับกระบวนการปฏิบัติ และการฝึก ทบทวนแผนและการดำเนินการต่าง ๆ ตลอดจนเป็นข้อมูลเพื่อการพัฒนาระบบฯ ต่อไปในอนาคต

๕. การป้องกันความเสี่ยง ที่จะไม่ทำให้เกิดผลสำเร็จในการพัฒนาระบบควบคุมบังคับบัญชา หรือนำระบบฯ ไปใช้งานแล้วไม่เกิดประโยชน์ตามทฤษฎีในภาคธุรกิจ มีข้อให้พึงระวัง เมื่อนำแผนหรือโครงการไปปฏิบัติ โดยมักจะมีสิ่งท้าทาย^{๒๐} เนื่องจากการมีมุมมองที่แตกต่างของบุคลากรในองค์กร มีปัจจัยหลายอย่างเข้ามาเกี่ยวข้อง โดยที่ปัจจัยเหล่านี้มีความสัมพันธ์กันอย่างซับซ้อน ซึ่งยากที่จะระบุความสัมพันธ์ระหว่างกัน ดังนั้น นอกจากการพัฒนาการปฏิบัติคู่ขนานกันแล้ว การประเมินผลและตรวจสอบในหัวข้อก่อนหน้านี้ จึงมีความสำคัญ เพื่อที่จะได้ตรวจสอบความก้าวหน้า แล้วนำผลลัพธ์ดังกล่าวมาทบทวนปรับปรุงแผนหรือโครงการ หรือแม้กระทั่งทบทวนเป้าหมายหรือผลลัพธ์สุดท้ายที่ต้องการด้วย ในลักษณะของการเรียนรู้แบบสองวงรอบ (Double Loop Learning)^{๒๑} แต่ทั้งนี้ ความถี่หรือวงรอบของการปรับปรุงเปลี่ยนแปลง ต้องไม่ก่อให้เกิดความสับสนกับเจ้าหน้าที่และกำลังพลที่เกี่ยวข้อง

สำหรับการใช้เครื่องมือให้เกิดประโยชน์และมีประสิทธิภาพ เราจำเป็นต้องรู้จักข้อจำกัดในการนำมาใช้งาน และกำหนดมาตรการขึ้นมาเสริมเพื่อป้องกันความเสี่ยงเหล่านั้น เช่น การมีปริมาณข้อมูลข่าวสารมากจนทำให้เกิดภาวะในการวิเคราะห์ข้อมูล รวมถึงการลวงจากฝ่ายตรงข้าม ขณะเดียวกันเจ้าหน้าที่อาจเกิดความเคยชินในการพึ่งพาข้อมูลมากเกินไป หากเครือข่ายการสื่อสารโดนทำลาย จะทำให้ขาดความมั่นใจ จนไม่สามารถวิเคราะห์หรือคิดอะไรได้นอกจากนี้ระบบที่เชื่อมต่อกันด้วยเครือข่ายคอมพิวเตอร์ยังมีอันตรายจากไซเบอร์ (Cyber) ได้ตลอดเวลา

บทสรุป

จากคำกล่าว “In preparing for battle I have always found that plans are useless but planning is indispensable.” โดย Dwight D. Eisenhower นั้นได้เน้นย้ำความสำคัญของความตระหนักรู้ในสถานการณ์ซึ่งได้มาจากระบบควบคุมบังคับบัญชา ที่จะทำให้การปรับเปลี่ยนแผนและการตัดสินใจเป็นไปได้อย่างรวดเร็วและถูกต้อง ตามแนวความคิดของ OODA Loop

การพัฒนาระบบควบคุมบังคับบัญชา ขึ้นกับบริบทและความต้องการของหน่วยผู้ใช้ รวมทั้งมีปัจจัยภายนอกที่สำคัญคือ เทคโนโลยีในขณะนั้น นอกจากนี้การพัฒนากฎปฏิบัติเป็นสิ่งจำเป็นที่ขาดไม่ได้ เพื่อให้ใช้งานระบบควบคุมบังคับบัญชาได้อย่างมีประสิทธิภาพ โดยที่องค์บุคคลและกระบวนการปฏิบัติ เป็นองค์ประกอบที่มีความสำคัญที่สุด และยังสามารถปรับให้เข้ากับสถานการณ์ที่ผันผวนได้ดีที่สุด ขณะเดียวกันสำหรับกองทัพที่ใช้การควบคุมบังคับบัญชาแบบกระจายอำนาจ

ควรให้ความสำคัญกับการฝึก เพื่อสร้างความเป็นผู้นำให้กับผู้บังคับบัญชา และความไว้วางใจระหว่างกัน สุดท้ายคือ การประเมินผลและตรวจสอบ เพื่อรับทราบความก้าวหน้าในการพัฒนา และทำบทเรียนข้อมูลสะท้อนกลับ ซึ่งจะได้ นำมาปรับปรุงการพัฒนาฯ อย่างเป็นทางการและมีเหตุผลต่อไป

เอกสารอ้างอิง

- ๑ กองบัญชาการกองทัพไทย. (๒๕๕๐). หลักนियมการปฏิบัติการร่วมกองทัพไทย พ.ศ.๒๕๕๐ ด้านสื่อสารร่วม.
- ๒ Zoran Karavidić, Goran Radovanović, Vladimir Ristić. (2019). Project management in the development of a command-information system for the needs of defence systems of small states, in Proceedings of the 5th IPMASENET Project Management Conference (SENET 2019). Retrieved April 13, 2021 from https://www.researchgate.net/publication/338443895_Project_management_in_the_development_of_a_command-information_system_for_the_needs_of_defence_systems_of_small_states
- ๓ Eva Jensen. (2006). Good Sensemaking is More Important than Information for the Quality of Plans, in 11th ICCRTS Coalition Command and Control in the Networked Era. Retrieved April 13, 2021 from https://www.researchgate.net/publication/255429342_Good_Sensemaking_is_More_Important_than_Information_for_the_Quality_of_Plans

- α Magdalena Granåsen. (2019). Exploring C2 Capability and Effectiveness in Challenging Situations: Interorganizational Crisis Management, Military Operations and Cyber Defence, Thesis, Linköping University, Sweden.
- α Wang Mingqian. (2020). A survey on C 4 ISR system architecture technique, in Global Journal of Engineering and Technology Advances. Retrieved April 13, 2021 from <http://gjeta.com/content/survey-c4isr-system-architecture-technique>
- b Bryan Clack. (2020). Mosaic Warfare Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations, Center for Strategic and Budgetary Assessments. Retrieved April 13, 2021 from <https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations>
- α Zhang Xuemin. (2012). The Process of Information Systems Architecture Development, in 2012 International Workshop on Information and Electronics Engineering (IWIEE), Procedia Engineering 29. Retrieved April 13, 2021 from <https://www.sciencedirect.com/science/article/pii/S1877705812000501>
- α Panagiotis Lytrivis. (2009). Sensor Data Fusion in Automotive Applications. in Sensor and Data Fusion. Retrieved April 13, 2021 from https://www.researchgate.net/publication/221787812_Sensor_Data_Fusion_in_Automotive_Applications
- α US Congressional Research Service. (2021). Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress. Retrieved April 13, 2021 from <https://fas.org/sgp/crs/weapons/RL33745.pdf>
- α Dae Young Kim. (2020). South Korean navy completes C4I system upgrade, in Janes, 07 September 2020. Retrieved April 13, 2021 from <https://www.janes.com/defence-news/news-detail/south-korean-navy-completes-c4i-system-upgrade>

- ๑๑ Michael Raska. (2019). The SAF After Next Incarnation. (RSIS Commentaries, No. 041). RSIS Commentaries, Nanyang Technological University, Singapore. Retrieved April 13, 2021 from <https://dr.ntu.edu.sg/bitstream/10220/47931/1/CO19041.pdf>
- ๑๒ Kimberly Jackson. (2020). Command and Control in U.S. Naval Competition with China. Santa Monica, CA: RAND Corporation. Retrieved April 13, 2021 from https://www.rand.org/pubs/research_reports/RRA127-1.html.
- ๑๓ US Office of the Secretary of Defense. (2020). Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2020. Retrieved April 13, 2021 from <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>
- ๑๔ Peter Wood. (2020). Chinese Airborne C4ISR, China Aerospace Studies Institute, Air University, US. Retrieved April 13, 2021 from <https://www.airuniversity.af.edu/CASI/Display/Article/2450727/chinese-airborne-c4ISR/>
- ๑๕ Bryan Clack. (2020). Mosaic Warfare Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations, Center for Strategic and Budgetary Assessments. Retrieved April 13, 2021 from https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf
- ๑๖ Ronald O'Rourke. (2019). Navy Force Structure and Shipbuilding Plans: Background and Issues for Congress. US Congressional Research Service. Retrieved April 13, 2021 from https://www.everycrsreport.com/files/20190724_RL32665_7bea2e4f25267bb1883fa3ecdf1583d268bf457a.pdf
- ๑๗ Martin Neujahr. (2004). Vernetzte Operationsführung und das neue operative Umfeld: Gesteigerte Einsatzwirksamkeit durch verbesserte

Führungsfähigkeit, in Vernetzte Sicherheit: Leitidee der Sicherheitspolitik im 21. Jahrhundert, Edition: Vernetzte Sicherheit Band 1, Verlag E.S. Mittler & Sohn.

- ๑๘ Will Meddings. (2020). The Future of Command and Control: Four Models to Provoke Thought. Retrieved April 13, 2021 from <https://thearmyleader.co.uk/future-of-command-and-control/>
- ๑๙ Soon-Chia Lim. (2004). Network centric warfare: a command and control perspective. Thesis, Naval Postgraduate School, Monterey, California, US. Retrieved April 13, 2021 from <https://core.ac.uk/download/pdf/36695391.pdf>
- ๒๐ จักรี ศรีจารุเมธีญาณ. (๒๕๖๓). “กลยุทธ์การปรับตัวองค์กรเข้าสู่ยุค ๔.๐” ใน วารสารพุทธมัตต์. ศูนย์วิจัยธรรมศึกษา สำนักเรียนวัดอาวุธวิกสิตาราม. ปีที่ ๕. ฉบับที่ ๑ (มกราคม-มิถุนายน ๒๕๖๓). สืบค้นเมื่อ ๑๓ เม.ย.๖๔ เข้าถึงได้จาก <https://so01.tci-thaijo.org/index.php/bdm/article/view/240610>
- ๒๑ Sabinne Lee. (2020). Policy learning and crisis policy-making: quadruple-loop learning and COVID-19 responses in South Korea, Policy and Society, 39:3. Retrieved April 13, 2021 from <https://www.tandfonline.com/doi/full/10.1080/14494035.2020.1785195>



แนวคิด “*Informatized Distributed
Maritime Operation: IDMO*”
ในการปฏิบัติการทางเรือในอนาคต
(FNOG)

นางวาทก ศิลปี พันธุรังษี
นักศึกษาวิชาสายการทัพเรือ
รุ่นที่ ๕๓ ปีการศึกษา ๒๕๖๔

บทคัดย่อ

สหรัฐอเมริกาจะใช้แนวคิดการล่าทำลายแบบกระจายศูนย์ (Distributed Lethality: DL) ควบคุมทะเลในอินโด-แปซิฟิก หากเกิดวิกฤติขัดแย้ง เพื่อทะเลวงแนวป้องกัน Anti Access/ Area/ Denial (A2/AD) และจุดโจมตีทำลายระบบบูรณาการป้องกันภัยทางอากาศ (Integrated Air Defense System: IADS) ของจีน แนวคิดนี้จึงแพร่หลายเข้าสู่ประเทศเพื่อนบ้านที่มีความขัดแย้งพิพาทในเส้นเขตแดนกับไทย กระทั่งต่อการรักษาความมั่นคงทางทะเลของกองทัพเรือต่อมาสหรัฐฯ ปรับปรุงแนวคิดปฏิบัติการทางทะเลแบบกระจายศูนย์ (Distributed Maritime Operation: DMO) ให้ครอบคลุมปฏิบัติการทุกโดเมนและการรวบรวม ผสมผสานเทคโนโลยีสมัยใหม่แบบ Artificial Intelligence (AI) และเทคโนโลยีอัตโนมัติ ลดบทบาทการพึ่งพาระบบ Network Centric Warfare (NCW) แต่พึ่งพิงการตัดสินใจรวมศูนย์ (Decision Centric Warfare: DCW) โดยในระดับกองเรือใช้เครือข่ายแบบ Fleet Centric ดำรงความเป็นเลิศด้านข้อมูลข่าวสาร (Information Superiority) ในขณะที่จีนใช้ยุทธศาสตร์คล้ายกัน แต่ประสิทธิภาพสูงกว่าคือ Informatization โดยบทความนี้ได้บูรณาการแนวคิดของจีนและสหรัฐฯ เข้าด้วยกันเป็นหลักการใหม่คือ “ปฏิบัติการทางทะเลแบบกระจายศูนย์ด้วยความเป็นเลิศด้านข้อมูลข่าวสาร (Informatized Distributed Maritime Operation: IDMO) สำหรับใช้รักษาความมั่นคงทางทะเลที่ครอบคลุมภารกิจและบทบาทกองทัพเรือในอนาคตอย่างครบถ้วน

คำสำคัญ

Distributed Lethality, Distributed Maritime Operation, Informatization, Informatized Warfare, Intelligentized Warfare, Mosaic Warfare, Information Superiority, Information Dominance, Network Centric, Fleet Centric, Decision Centric, C Dome และ Battle Network.

บริบทด้านความมั่นคงสำหรับกำลังรบทางเรือในอนาคต

Global Trend 2040^๑ กำหนดบริบททางยุทธศาสตร์ระดับโลก ภายใต้การระบาดของโควิด ๑๙ ว่าเทคโนโลยีปัญญาประดิษฐ์ (AI) จะมีบทบาทสูง ต่อสงครามในอนาคต ประเทศที่ประยุกต์ AI ทางทหารย่อมได้เปรียบ สามารถ เพิ่มสมรรถนะการอาวุธ การป้องกัน การรักษาความปลอดภัยทั้งกายภาพ และ ไซเบอร์ สอดคล้องกับ RAND Corporation^๒ ที่วิเคราะห์สงครามในปี ๒๐๓๐ ว่าแนวโน้ม AI ที่เกี่ยวข้องกับสหรัฐฯ จะต่อสู้ภายใต้เงื่อนไขวิเคลียร์ การใช้ Iron Dome ในต้นเดือน พ.ค.๖๔ ของอิสราเอลร่วมกับที่ใช้ยานไร้คนขับโดรน และ AI สร้างมิติป้องกันภัยทางอากาศต่อต้านจรวดและอาวุธปล่อยของปาเลสไตน์ ได้อย่างมีประสิทธิภาพ จะเร่งให้ทุกชาติแข่งขันพัฒนาแนวคิดแบบ Iron Dome และ C Dome ตามภาพที่ ๑ การสื่อสารที่รวดเร็วทำให้ปัจจัยสงคราม ได้แก่ Time, Space และ Forces ถูกนำเสนอผ่านระบบ NCW แบบ Real Time นำไปสู่แนวคิดการกระจายกำลังรบ (Distributed Forces) มิลาน วิโก้ กล่าวว่า NCW จะเกิดผลสูงสุดก็ต่อเมื่อมีการบริหารแนวคิดการตัดสินใจ แบบกระจายศูนย์ และรวมศูนย์อย่างกลมกลืน^๓ นำไปสู่แนวคิดการล่าทำลาย แบบกระจายศูนย์ (Distributed Lethality: DL) ตามภาพที่ ๒



C Dome แบบ Iron Dome ของอิสราเอล ภาพที่ ๒ แนวคิดแบบ Distributed Lethality (DL)
ที่มา: Rafael Brochure & Rafael Clips

แนวคิดการล่าทำลายแบบกระจายศูนย์ (Distributed Lethality: DL)

การล่าทำลายแบบกระจายศูนย์ คือสภาพการเพิ่มศักยภาพสงครามเชิงรุก ในทุกปัจจัยสงครามของกำลังรบผิวน้ำ ออกปฏิบัติการในลักษณะกระจาย ด้วยกลุ่มการรบผิวน้ำ (SAG) ในพื้นที่ A2/AD สร้างความสับสนมิให้ฝ่ายตรงข้าม ค้นหาและพิสูจน์เป้า คุกคามการควบคุมทะเล โดยในระดับยุทธศาสตร์ ควบคุมทะเลด้วยกลุ่มเรืออเนกประสงค์ (AFP) หลายกลุ่ม ระดับยุทธการ ควบคุมพื้นที่ด้วยกลุ่มเรือ AFP สามารถปรับกองกำลังให้เหมาะสมกับ ภัยคุกคาม^๖ ระดับยุทธวิธีมุ่งควบคุมยุทธบริเวณ ล่าทำลายศัตรูด้วยกลุ่ม การรบผิวน้ำ (SAG) ออกปฏิบัติการในลักษณะ “นักล่า นักฆ่า (Hunter-Killer SAG)” โดยการลวง พิสูจน์ทราบเป้า และทำลายด้วยหลักนิยม ผบ.เรือต้องคิด ริเริ่ม Outthink, Out Scout และ Out Shoot เน้นหลักการ ๔ T คือ Tactics, Talent Tools และ Training สามารถปฏิบัติการรบข้ามโดเมน หากระบบ C2 ขัดข้อง เรือต้องสามารถรบต่อไปได้

องค์ประกอบที่จะก่อให้เกิดสภาพเงื่อนไข DL หลักการพื้นฐานนี้ มีองค์ประกอบ ๓ ประการ คือ เพิ่มอำนาจการทำลายล้างให้เรือรบ ด้วยการ ติดตั้งยุทธโศปกรณ์เชิงรุกพร้อมเซ็นเซอร์ทันสมัย เสริมด้วยยานไร้คนขับที่เป็น ทั้งเครื่องสื่อสาร เซ็นเซอร์และอาวุธ ปฏิบัติการแบบฝูง (Swarm) สหรัฐฯ ใช้แนวคิดนี้ โดยลดจำนวนเรือขนาดใหญ่ เพิ่มเรือขนาดเล็ก^๗ เช่น LCS, CG, DDG, LSD, LHA^๘ เรือลำเลียง เรือช่วยรบ และเรือระบายพลแบบ LCAC^๙ มาติดตั้งอาวุธแบบ DL ปฏิบัติการในเขตชายฝั่ง กระจายสมรรถนะการรุก ไปทุกสภาพพื้นที่ ออกปฏิบัติการเพียงลำพัง ๑ ลำ หรือเป็นกลุ่มเล็ก ครอบคลุม พื้นที่ในทะเลเปิด ทะเลแคบ และหมู่เกาะ แนวคิด DL จะใช้การลวง พราง และหลบหลีก เรือต้องบริหารจัดการทรัพยากร ให้สู้รบได้นานและต่อเนื่อง ใช้ยาน UxV ร่วมกับเรือที่ซ่อนพรางหาเป้าเชิงรับ ทั้ง ผบ.เรือ และลูกเรือ ต้องมีความคิดริเริ่ม^{๑๐}

ปัญหาจากแนวคิดแบบ DL ที่จะส่งผลกระทบต่อกองทัพเรือ

แนวคิดแบบ DL แพร่หลายเข้าสู่ประเทศเพื่อนบ้าน กระทบต่อแนวคิด การใช้กำลังทางเรือคือ ปัญหาจากการลวง ค้นหา และทำลาย ปัญหาต่อยุทธศาสตร์

กองทัพเรือและกำลังรบใน ๒๐ ปี ข้อจำกัดด้านภูมิยุทธศาสตร์ ปัญหาด้านสภาพ
ยุทธโปกรณ์ สงครามไซเบอร์ ภัยคุกคามจากประเทศมหาอำนาจที่ขัดแย้ง
ในทะเลจีนใต้ และที่สำคัญสูงสุดคือ ปัญหาภัยคุกคามจากความขัดแย้งกรณี
พิพาทเส้นเขตแดนกับประเทศเพื่อนบ้านที่มีมหาอำนาจหนุนหลัง จำเป็นต้องหา
หนทางแก้ไข และต่อต้านแนวคิดแบบ DL

แนวคิดปฏิบัติการทางทะเลแบบกระจายศูนย์ (Distributed Maritime Operation: DMO)

แนวคิดแบบ DMO เป็นแนวคิดต่อยอดจาก DL ในการทำสงครามทางเรือ
แต่ยกระดับการตัดสินใจให้สูงขึ้นในระดับยุทธการและรบร่วม เพื่อให้ครอบคลุม
ทั้ง ๕ โดเมน และสเปกตรัมแม่เหล็กไฟฟ้า (EMS) สหรัฐฯ ใช้แนวคิดนี้ร่วมกับ
ปฏิบัติการในเขตชายฝั่งที่มีการต่อต้าน (LOCE)^{๑๑} สามารถตัดสินใจรวมศูนย์
ควบคุมทะเล ด้วยแนวคิดทางยุทธการแบบปัจจุบัน แต่เปลี่ยนแนวคิดทาง
ยุทธวิธีใหม่ โดยใช้อยานไร้คนขับ ระบบอัตโนมัติ และ AI แทนแนวทางเดิม
เพื่อปฏิบัติการสงครามทางเรือและการรักษาความมั่นคงทางทะเล

๑. หลักการ (Tenets) คือ เพิ่มความซับซ้อนกำลังรบผิวน้ำเพื่อให้
ข้าศึกสับสน บีบให้ฝ่ายตรงข้ามเพิ่มจำนวนการระดมยิงอาวุธปล่อย ด้วยการลง
ตรวจการณ์เชิงรับ และกระจายศูนย์เพิ่มสมรรถนะเชิงรุก ผสมผสานการออกแบบ
กับแนวคิดทางยุทธการคือ (๑) ใช้อยานอัตโนมัติสนับสนุนยุทธการและการส่ง
กำลังบำรุง (๒) สร้างทีมงานร่วมมือระหว่างยานแบบ Unmanned และ Manned
(๓) ปรับเปลี่ยนโครงสร้างองค์กรและการควบคุมบังคับบัญชาด้วย ๓ แนวคิด
คือ บูรณาการเชื่อมต่อ กระจายกำลัง และดำเนินกลยุทธ์

๒. ฟังก์ชันทางยุทธการ แนวคิดทางยุทธวิธีและมาตรการ สร้างความ
ซับซ้อนจากห่วงโซ่การตอบโต้หลายรูปแบบเมื่อทำงานร่วมกับสมรรถนะเชิงรุก
จะทำให้ ผบ.หน่วยกำลังรบผิวน้ำสามารถตัดสินใจเลือกปฏิบัติได้อย่าง
รวดเร็ว ตรวจการณ์โดยเพิ่มสมรรถนะกองเรือผิวน้ำด้วยยุทธวิธี ๕ หนทาง คือ
(๑) ใช้อยุทธวิธีป้องกันระยะใกล้ร่วมกับ EW สร้างความสับสนและเพิ่มจำนวนเป้า
(๒) ใช้อยานไร้คนขับและยานอื่นค้นหาเรือดำน้ำและอาวุธทำลายใต้น้ำ (๓) เลือก
ใช้อาวุธหลายภารกิจและยานไร้คนขับเพิ่มสมรรถนะเชิงรุก (๔) ต้องพึ่งเซ็นเซอร์

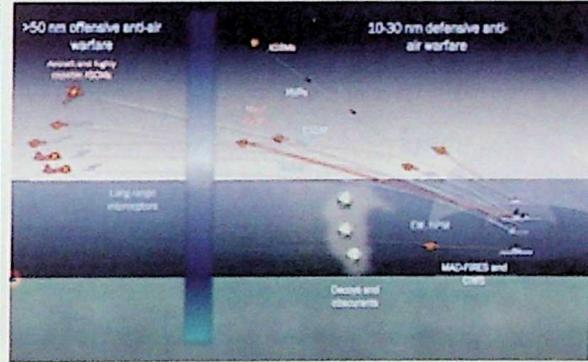
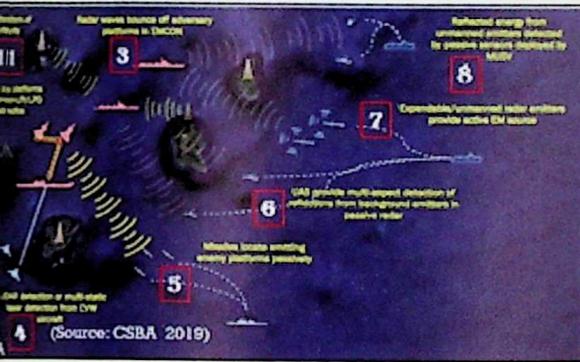
เชิงรับ หรือ ทฤษฎีภูมิในการค้นหา และพิสูจน์เป้า และ (๕) แยกการปฏิบัติ ในลักษณะกระจายกลุ่มย่อย สร้างความสับสนให้ข้าศึก โดยมียุทธวิธี ๔ กลุ่ม คือ (๑) ปฏิบัติการแบบฝูง (Swarm) ทั้งเชิงรับและเชิงรุกในการลวง (๒) ปฏิบัติการ ทางกล/กายภาพ เช่น การลวงทางสายตา (๓) มาตรการต่อต้านเรดาร์ EO/IR การแพร่คลื่น และควบคุมการแพร่คลื่น และ (๔) การรบกวนทางคลื่นแม่เหล็กไฟฟ้า รบกวนแบบต่าง ๆ รวมทั้งการรบกวนวิทยุดิจิทัล (DRFM) การรบกวน GPS เปลี่ยนห่วงโซ่การทำลาย (Kill Chain) เป็น Find-Target-Engage^{๑๒}

๓. การออกแบบสถาปัตยกรรม DMO ตอบสนองแนวคิดที่ต้องการ ความแม่นยำ และรวดเร็วของข้อมูลสนับสนุนหน่วยรบ กลุ่มกำลังรบ และกองเรือ ประกอบด้วยสถาปัตยกรรมคือ (๑) กริด (Grid) ทางยุทธวิธีที่เชื่อมต่อกับโหนดต่าง ๆ แบบกระจาย (๒) ฐานข้อมูล สมรรถนะการประมวลผล และเทคโนโลยีเกี่ยวเนื่อง รวมทั้งโหนด (๓) ยุทธศาสตร์ที่ครอบคลุมการใช้ข้อมูล และ (๔) เครื่องมือวิเคราะห์ ที่สนับสนุนการตัดสินใจอย่างรวดเร็ว เช่น ปัญญาประดิษฐ์ (AI) การเรียนรู้ เชิงเครื่องมือกล (Mechine Learning: ML) หรือบริการอื่น^{๑๓} การใช้ UAV (๑) เซ็นเซอร์เพื่อขยายพื้นที่ปฏิบัติการ (๒) อาวุธ ขยายแนวการรุก (๓) อุปกรณ์ การสื่อสารเป็นสถานีเชื่อมโยง

๔. การนำแนวคิด DMO ในการรักษาความมั่นคงทางทะเล/การใช้กำลัง อำนาจทางทะเล แนวคิดแบบ DL และ DMO มุ่งควบคุมทะเล ใช้อำนาจการรบ ที่เหนือกว่า สนับสนุนได้ดีกว่าโดยรูปแบบการปฏิบัติการในอดีตและปัจจุบัน สรุปได้ดังนี้

๔.๑ การข่าว ลาดตระเวน ตรวจการณ์และพิสูจน์เป้า (Intelligence, Surveillance, Reconnaissance, and Targeting: IRST) โดยแนวคิดเดิม ใช้เรดาร์แบบปฐมภูมิ หรือฟิงพาเซ็นเซอร์ภายนอก เช่น ดาวเทียมหรืออากาศยาน ได้ผลดีเมื่อกองเรืออยู่ในระยะไกล แต่มีข้อจำกัดจากยุทธบริเวณที่มีการต่อต้าน โดยเฉพาะบริเวณเขตชายฝั่ง กองเรือผิวน้ำขนาดใหญ่ในอดีตจึงตกเป็นเป้านี้ แต่แนวคิดทางยุทธวิธีใหม่ กองเรือผิวน้ำจำเป็นต้องไม่เปิดเผยตำแหน่ง และอาศัยเทคนิคการค้นหา คือ (๑) ใช้ประโยชน์สถานีวิทยุ/เรดาร์ของฝ่าย ตรงข้าม (๒) ใช้ Low Probability of Intercept/Detect Radar (LPI/LPD) (๓) เรดาร์ปฐมภูมิที่จำลองเรดาร์เรือสินค้า (๔) เรดาร์ปฐมภูมิของพื้นธมิต

(๕) เครื่องส่ง/ออกอากาศที่หาได้ในพื้นที่ที่ใช้การผสมผสานทั้งตำแหน่งและระยะห่างเหมาะสม ใช้ยานไร้คนขับแพร่คลื่นให้เรือตนรับตามภาพที่ ๓ สำหรับการ Counter IRST นั้น เมื่อพบเป้าจะพิสูจน์ทราบ ซึ่งบางครั้งต้องต่อต้าน ISRT ป้องกันฝ่ายตรงข้ามที่ต้องการทราบมิติในการระดมยิงของฝ่ายเรา ส่วนฝ่ายเราก็ต้องคำนวณขนาดการระดมยิงของฝ่ายตรงข้ามเช่นกัน ถ้าการต่อต้าน IRST ได้ผล ฝ่ายตรงข้ามจะไม่สามารถแยกเป้าได้มาจากเป้าลวง บีบให้ฝ่ายตรงข้ามเพิ่มขนาดการระดมยิงทำลายทุกเป้าเป็นการสิ้นเปลืองอาวุธ ซึ่งจะทำให้เรือ SAG ฝ่ายเรา มีโอกาสชนะสูงขึ้น



ภาพที่ ๓ การค้นหาแบบเชิงรับ IRST

ภาพที่ ๔ การป้องกันภัยทางอากาศ (AMD) ใหม่

ที่มา: CBSA Taking Back the Sea, 2019

๔.๒ การป้องกันภัยทางอากาศ (AMD) สำหรับเรือ เป็นการป้องกันการโจมตีจากอากาศยาน และอาวุธปล่อยนำวิถี จากแนวคิดการกระจายศูนย์ จะทำให้ฝ่ายตรงข้ามเพิ่มจำนวนการระดมยิง ในการต่อต้านของสหรัฐฯ จำเป็นต้องกระจายศูนย์ และ Counter-IRST ด้วยสมรรถนะการป้องกันสูงสุด ในการป้องกันสามารถใช้เรดาร์ SPY-1, SPY-6 และหาคู่คลื่นวิทยุ/เรดาร์ ส่วนแนวคิดการใช้อาวุธ ปัจจุบันใช้ระยะไกลเกิน ๕๐ ไมล์ทะเล ด้วย SM-2 และ SM-6 ส่วนแนวคิดใหม่ป้องกันระยะกลาง ๑๐ - ๓๐ ไมล์ทะเล ด้วย ESSM, HVP, HPM, และระยะใกล้ ใช้ MAD-FIRES, CIWS, RAM ตามภาพที่ ๖ สามารถประหยัดทรัพยากรลงได้มาก

๔.๓ สงครามต่อต้านภัยใต้น้ำ (ASW) แนวคิดปัจจุบันใช้อาวุธปล่อยใต้น้ำต่อต้านเรือที่ปล่อยจากเรือดำน้ำ หรือยานไร้คนขับขนาดกลางขึ้นไป ที่ปัจจุบันมีพิสัยไกล ความเร็ว และฉลาดขึ้นมากปฏิบัติการต่อต้านภัยใต้น้ำใช้ ฮ. กับ Dipping Active Sonar ปล่อยตอร์ปิโดจาก ฮ. ที่มีระยะปฏิบัติการจำกัด ส่วนแนวคิดใหม่จะใช้เครือข่ายและการกระจายศูนย์ของยานไร้คนขับร่วมกับอากาศยานปราบเรือดำน้ำที่มีอาวุธปล่อยขนาดเล็กกอดันเรือดำน้ำสามารถใช้สถานีตรวจการณ์ประจำที่แบบย้ายได้ (TRAPS) ด้วยการติดตั้งเชิงรุกเพื่อตรวจหาเรือดำน้ำตามเส้นทาง จุดใช้ศพอยด์ หรือหน้าท่าเรือฝ่ายตรงข้าม

๔.๔ ปฏิบัติการปราบเรือดำน้ำ แนวคิดในการปฏิบัติการ (Engage) ก็เปลี่ยนไปคือ แนวคิดปัจจุบัน หลังตรวจพบเรือดำน้ำแล้ว จะพิสูจน์ทราบตำแหน่ง (Localization) เพื่อที่จะใช้อาวุธ ASROC /ตอร์ปิโด ทุกรูปแบบจากเรือ อากาศยาน หรือยิงจากฝั่งรุมทำลายเรือดำน้ำ ส่วนแนวคิดใหม่ไม่จำเป็นต้องพิสูจน์ทราบตำแหน่ง เนื่องจากแนวคิดปราบเรือดำน้ำแบบใหม่จะใช้วิธีหยุดยั้ง (Suppression) ความตั้งใจปฏิบัติของฝ่ายตรงข้ามด้วยการสื่อสารให้กำลังพลเรือั้นทราบว่าคุณกำลังถูก Counter Detected อยู่ และกำลังจะถูกตอบโต้ได้ตลอดเวลา ด้วยจุดอ่อนของเรือดำน้ำคือ ความเร็วที่ไม่สูง ขาดยุทธโศปกรณ์ป้องกันตนเอง ขาดเซ็นเซอร์ที่ละเอียดแม่นยำ เป็นการยากจะรวมการโจมตีของคุณสำเร็จผล ส่วนใหญ่เรือดำน้ำจะไม่ผิวน้ำในพื้นที่อันตรายนาน ต้องการอยู่แบบล่องหนมากกว่าการเปิดเผยตัวตน จึงไม่จำเป็นต้องบรรทุกอาวุธทำลายเรือดำน้ำมากมาย อากาศยานอาจใช้ตอร์ปิโดขนาดเบาหรือ Depth Bombs และประหัตตอร์ปิโดราคาแพง เช่น MK54 ไว้ใช้ยามจำเป็น อาจใช้ VLA กับเป้าหมายเรือผิวน้ำแทน

๔.๕ ปฏิบัติการสงครามผิวน้ำและการโจมตีทางทะเล สหรัฐฯ มีแนวคิดปัจจุบันคือ ใช้เรือบรรทุกเครื่องบินเป็นกำลังหลักในการโจมตีทางทะเล และภาคพื้นบนฝั่งตามระยะเวลา เนื่องจากอากาศยานต้องกลับไปโหลดแม็กกะซีนที่เรือบรรทุกเครื่องบิน ส่วนเรือบรรทุกเครื่องบินก็ต้องกลับไปโหลดอาวุธกลางทะเล ซึ่งแนวคิดนี้เกิดช่องโหว่จากเครือข่ายบูรณาการป้องกันภัยทางอากาศ (IADS) ของจีนที่บีบให้สหรัฐฯ ต้องเปิดฉากโจมตีจากเรือบรรทุกเครื่องบินในระยะ ๑๐๐๐ ไมล์ทะเล จำเป็นต้องเปลี่ยนแนวคิดใหม่ ใช้หลัก DL

อย่างมีประสิทธิภาพในโอกาสแรก เลือกจู่โจมโดยไม่เปิดเผยที่ตั้ง ดำรงความ
 ต่อเนื่องในการใช้อาวุธโดยหมุนเวียนผลัดเปลี่ยนเรือส่วนหนึ่งไปโหลดอาวุธ
 ในสถานที่ปลอดภัย ส่วนเรือที่เหลือยังสร้างเป้าลวง (Decoy) ที่ยิงจากปืนหัว
 ลูก Decoy จะแยกตัวกลางอากาศเป็น ๓ เป้าลวง แพร่คลื่นลวงกลางอากาศ
 ถ่วงเวลาด้วยร่ม เมื่อเป้าลวงน้ำก็สร้างเป้าลวงเสมือนเรือรบ ๓ ลำ ลวงเรดาร์
 ตรวจการณ์ได้ ตามภาพที่ ๕



ภาพที่ ๕ ยิง Decoy จากปืนหัวสร้างภาพเรือลวง
 ที่มา: SRC Technology, Advertised Video

๔.๖ ปฏิบัติการสงครามทุ่นระเบิดและการต่อต้านยานไร้คนขับใต้น้ำ
 แนวคิดปัจจุบัน สหรัฐฯ ใช้เรือต่อต้านทุ่นระเบิด พร้อม ฮ. โดยมีแนวคิดใหม่
 ใช้ยานไร้คนขับร่วมกับเซ็นเซอร์แบบใหม่ติด ฮ. ด้วยความทันสมัยของระบบ
 Unmanned MCM ช่วยเพิ่มมิติการวางทุ่นระเบิดและทำลายทุ่นระเบิด
 ส่วนการกวาดทุ่นระเบิด สหรัฐฯ ก็มีแนวคิดใช้เรือ LCS พร้อมใช้ ฮ. MH-60S
 ติดตั้งระบบตรวจจับแบบเลเซอร์และระบบทำลายทุ่นระเบิด และใช้ยานไร้คนขับ
 ผิวน้ำปราบทุ่นระเบิดแทน ฮ. MH-53 การวางทุ่นระเบิด ใช้ความได้เปรียบ
 ในการผสมผสานสมรรถนะต่อเรือทุ่นระเบิด และยาน UUV สามารถ
 วางทุ่นระเบิดเชิงรุกด้วยยาน UUV ขนาดเล็ก ลดการถูกตรวจจับ และยังมีข้อดี
 ที่ช่วยในการลวงใต้น้ำ การวางทุ่นระเบิดเชิงรุกสามารถวางในเส้นทางหรือพื้นที่
 ฝ่ายตรงข้ามด้วย UUV

๔.๗ ปฏิบัติการจากทะเลโจมตีเป้าหมายบนฝั่ง ใช้แนวคิดเดียวกัน คือ การใช้ยานไร้คนขับในการลวง ใช้แผนพระนเรศวรตีเมืองคัง โดยใช้ยานไร้คนขับ ลวงซ้ายขวา ลวงจุดอื่น แล้วเข้าตีตรงหน้าสร้างความสับสน ตามภาพที่ ๖ นอกจากนี้ ยังมีการใช้ EMW นำการปฏิบัติ โดยใช้แนวคิดเดียวกันคือ ยานไร้คนขับลวง สร้างความสับสน



ภาพที่ ๖ ใช้ UAV ลวงตามแผนพระนเรศวรตีเมืองคัง

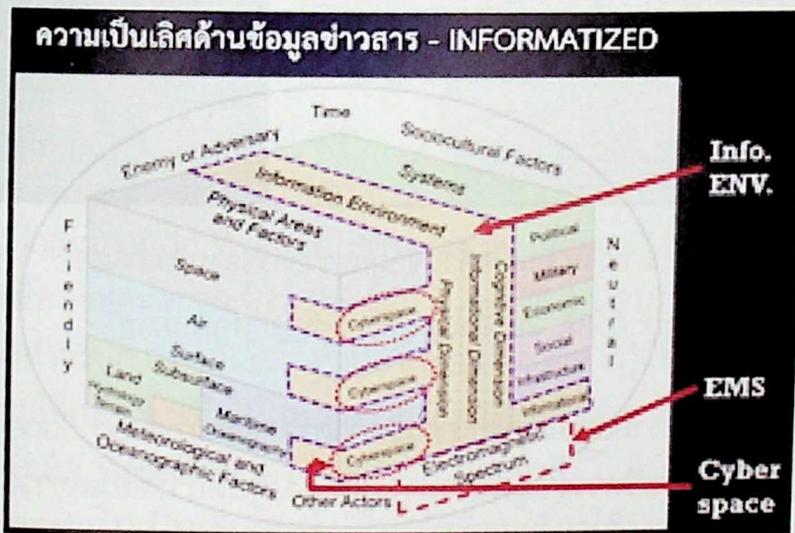
ที่มา: CBSA Air & Missile Defense, 2020

๔.๘ การป้องกันฝั่ง คือ ต้านปฏิบัติการจากทะเลของฝ่ายตรงข้าม โดยแนวคิดปัจจุบันจะใช้การป้องกันทางลึก (Defend In Depth) เป็นแนวระดับหรือเป็นวงแหวนหลัก ประกอบด้วย Blunt Layer, Contact Layer) ส่วนแนวคิดใหม่^{๑๔} จะประยุกต์การป้องกันทางลึก โดยยังคงป้องกันเป็นวงแหวนเช่นเดิมโดยเฉพาะเซ็นเซอร์ แต่เพิ่มวงแหวนอิสระหลายวงที่ทั้งอยู่ในวงเดิม และนอกวงที่ประกอบด้วยยานอัติโนมติ (UAS) และยานไร้คนขับ ทำหน้าที่ออกไปพิสูจน์ทราบ และสกัดกั้นข้าศึก ทั้งในและนอกวงป้องกันหลักด้วยอาวุธทันสมัย โดยมีการกระทำในลักษณะกระจายศูนย์เครือข่ายการสกัดกั้น

ความเป็นเลิศด้านข้อมูลข่าวสาร (Informatization)

“เป้าหมายในสงครามมิใช่ทหาร แต่เป็นสภาพการการรับรู้ (จิตใจ) หากเราปฏิบัติต่อกำลังรบ ย่อมมีผลต่อจิตใจและความตั้งใจของ ผบ.หน่วยรบ”
Captain Sir B.H. Liddel-Hart, British Army^{๑๕} สรุปได้ดังนี้

๑. หลักการ ความเป็นเลิศด้านข้อมูลข่าวสารของสหรัฐอเมริกา และจีน ล้วนมีแนวคิดเดียวกันคือ ปฏิบัติการต่อพื้นที่การรับรู้ เพื่อให้ผู้บังคับบัญชา หน่วยรบฝ่ายตรงข้ามไม่สามารถตัดสินใจได้ หรือตัดสินใจได้ไม่ทันเวลาที่ต้องการ เล็กน้อยความคิดที่จะต่อสู้ ทั้งนี้จะใช้ความได้เปรียบฝ่ายตนในการแลกเปลี่ยน ข้อมูลสภาพสนามรบแบบเสมือนจริง ซึ่งมีความแตกต่างจากสงครามในอดีต ที่มุ่งทำลายกำลังการรบ แต่สงครามยุคใหม่ จะเน้นควบคุมการตัดสินใจของ ผบ.หน่วยรบ และสนับสนุนการรับรู้ของผู้นำฝ่ายเราให้ตัดสินใจอย่างเหมาะสม ตามภาพที่ ๗



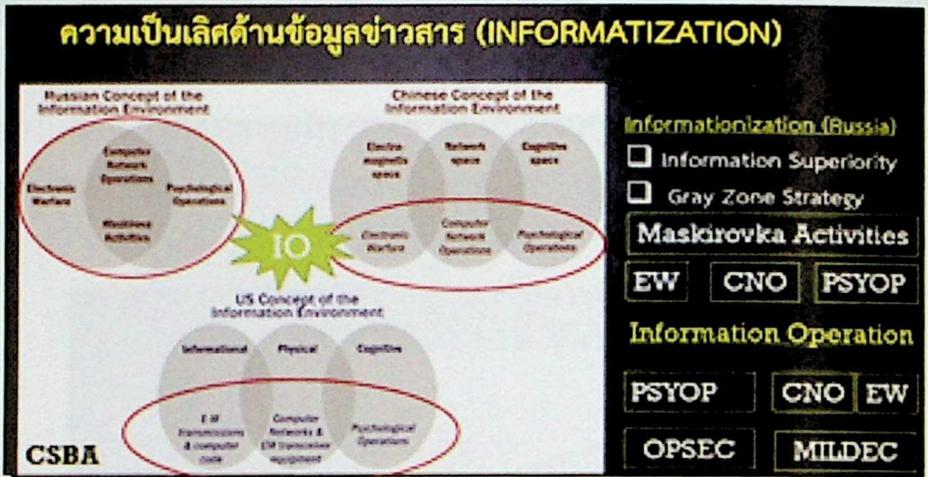
ภาพที่ ๗ สงครามไซเบอร์ในทุกโดเมน

ที่มา: JP-05 Oct 2020

๑.๑ สงครามข้อมูลข่าวสาร (Information Warfare: IW) หมายถึง ปฏิบัติการให้บรรลุความเป็นเลิศด้านข้อมูลข่าวสาร (Information Superiority) ด้วยการปฏิเสธ ใช้ประโยชน์ บั่นทอน ทำลายข้อมูลข่าวสาร หรือฟังก์ชัน ที่เกี่ยวข้องกับข้อมูลข่าวสารของฝ่ายตรงข้าม เป็นการปฏิบัติการข่าวสาร (IO) ในระหว่างความขัดแย้งหรือสงคราม เพื่อส่งเสริมหรือให้บรรลุวัตถุประสงค์ เฉพาะต่อฝ่ายตรงข้าม

๑.๒ สถานะแวดล้อมด้านข่าวสาร (Information Environment) เป็นศูนย์รวมของบุคคล หน่วยงานและระบบ ในการรวบรวม จัดทำ แจกจ่าย และปฏิบัติเกี่ยวกับข่าวสาร ประกอบด้วย ๓ มิติ คือ มิติทางกายภาพ มิติเกี่ยวกับ

ข่าวสาร และมีมติเกี่ยวกับการรับรู้ ทั้งรัสเซีย สหรัฐฯ และจีน นิยามสภาวะแวดล้อม ด้านข่าวสารต่างกัน ตามภาพที่ ๘ แต่มุ่งสู่การรับรู้เหมือนกัน (PSYOP, CNO และ EW)



ภาพที่ ๘ ความเป็นเลิศด้านข้อมูลข่าวสารของมหาอำนาจ
ที่มา: CSBA, 2020 และผู้เขียนอธิบายเพิ่มในภาพ

๑.๓ ความเหนือกว่าด้านข้อมูลข่าวสาร (Information Superiority)^{๑๖} ประกอบด้วย การบริหารข้อมูลข่าวสาร (IM) ปฏิบัติการข้อมูลข่าวสาร (IO) และการข่าวกรอง การเฝ้าตรวจและการลาดตระเวน (ISR) จำแนกตามโดเมนได้ ๕ มิติ คือ (๑) การข่าวกรองทางอวกาศ ใช้เซ็นเซอร์บนดาวเทียมตรวจการณ์ ปัจจุบันโซนาร์ย่านความถี่ต่ำและออปติคสามารถตรวจจับเรือดำน้ำได้ลึก ๕๐๐ เมตร^{๑๗} มีกล้อง IR ตรวจกลางคืน ซึ่งในการต่อต้าน ISR นั้น ใช้การยับยั้งทำให้ชั่วคราว (Reversible) และทำลายถาวร (Irreversible)^{๑๘} (๒) การตรวจการณ์ทางอากาศ คือการค้นหา เก็บภาพจาก UAV, อากาศยาน และ บ.ตรวจการณ์ FLIR สามารถระบุความร้อนได้ในระยะ ๖๐ กม. โครงการป้องปรามด้วยการตรวจจับ (Deterrence by Detection) ที่ใช้อากาศยานไร้คนขับตรวจการณ์พื้นที่ทางทะเลในทะเลจีนใต้^{๑๙} (๓) การตรวจการณ์ผิวน้ำ ประกอบด้วย สถานีตรวจการณ์ประจำที่และเคลื่อนที่ ได้แก่ เรือผิวน้ำ ยาน USV รวมทั้ง สถานีตรวจการณ์ชายฝั่ง การดักจับคลื่นความถี่วิทยุในลักษณะเชิงรับแบบ Bi/ Multi-static ย่านความถี่ VHF/UHF^{๒๐} จนถึงยุคการใช้ควันทัมเรดาร์

ที่จะมาแรงในอนาคต^{๒๑} (๔) การตรวจการณ์ใต้น้ำ ในอดีตสงครามใต้น้ำเน้นโซนาร์เชิงรับ การดำรงความเงียบมีเทคนิคการค้นหาหลายแบบตั้งแต่ใช้อากาศยานติดเซ็นเซอร์ใต้น้ำ การตรวจใต้น้ำแบบต่าง ๆ ใช้เทคนิคใหม่แทนการค้นหาแบบ MAD ที่มีระยะตรวจจับใกล้ หากติดตั้งใต้น้ำมีภาระการบำรุงรักษาและการสื่อสาร แนวคิดใหม่จึงใช้การตรวจการณ์บนอากาศ ที่จิ้นสามารถตรวจการณ์ได้ดีกว่า ๖๐๐ เมตร ไม่รวมเทคโนโลยีควินต์มโซนาร์ (SQUID) ที่หลายประเทศกำลังมุ่งพัฒนา แม้แต่เทคนิคเดิมแบบ Ekelund ที่สามารถตรวจจับเรือดำน้ำได้ ๕๐ ไมล์ทะเล ปัจจุบันสหรัฐฯ เลือกใช้โซนาร์เชิงรุกย่านความถี่ต่ำ (๒) มาตรการต่อต้านโซนาร์เชิงรุก (๓) ใ้ยาน UUV ขนาดเล็กที่เลือดลดการตรวจจับและอุปกรณ์ใต้น้ำ^{๒๒} และ (๕) การตรวจการณ์ทางไซเบอร์

๒. ประเทศที่ใช้แนวคิด

๒.๑ สหรัฐฯ กำหนดยุทธศาสตร์ Information Superiority พัฒนา Information Warfare ที่ครอบคลุม Cyber, EMW, Space C4ISR-T ที่สอดคล้องกับยุทธศาสตร์การป้องกันประเทศ NDS 2018 ในบทบาทของข้อมูลข่าวสารสำหรับการตัดสินใจ^{๒๓} ด้วยวิสัยทัศน์ “คิดค้น ปฏิบัติจริง และมีสมรรถนะตามเกมส์ที่เปลี่ยน เพื่อให้เหนือกว่าฝ่ายตรงข้ามในด้านข้อมูลข่าวสาร รวมทั้งการตัดสินใจ ทั้ง ผบ.หน่วยรบ กำลังรบ และชาติ”^{๒๔} ด้วยหลักการใหม่ ๆ คือทุกแพลตฟอร์มเป็นเซ็นเซอร์ เจ้าหน้าที่คนเดียวใช้งานหลายแพลตฟอร์มทุกเซ็นเซอร์เป็นเครือข่าย เน้นแพลตฟอร์มแบบไร้คนขับและอัตโนมัติ สร้างน้อยทดลองมาก ใ้ยานไร้คนขับในทะเล ทบหนวนการจัดหา เพย์โหลดใช้เซ็นเซอร์แบบ Plug and Play ลดจำนวนพนักงานใ้ยาน มุ่งสู่การควบคุมระยะไกล และอัตโนมัติ สืบค้นข้อมูลและเข้าใช้ข้อมูลได้เหมือนกัน ทุกหน่วยรบต้องสามารถเลือกใช้อุปกรณ์เป้าหมายจากเซ็นเซอร์ใดก็ได้ แนวคิด IW ครอบคลุมการเข้าถึงทุกโดเมนและ Distributed Lethality ด้วย^{๒๕}

๒.๒ รัสเซีย จีนและรัสเซียล้วนประยุกต์ใช้สงครามข้อมูลข่าวสารเรียกว่า “Informationized Warfare” เพื่อเป็นยุทธศาสตร์ทางทหาร โดยมีความหมายว่า “เป็นสงครามที่ใช้ข้อมูลข่าวสารสำหรับอาวุธ ยุทธโปกรณ์และเครือข่าย ใช้ยุทธวิธีที่เหมาะสมในการปฏิบัติการร่วมในโดเมนทางบก ทะเล อากาศ และอวกาศ แม่เหล็กไฟฟ้าและสนามรบแห่งการรับรู้ (Cognitive Arena)”^{๒๖}

ตามภาพที่ ๙ โดยหวังบั่นทอนทำลายการตัดสินใจ (Decision Making) ของผู้นำฝ่ายตรงข้าม ด้วยการตบแต่งข้อมูลข่าวสารในยามสงบ และสร้างความได้เปรียบด้านข้อมูลข่าวสารในยามสงครามซึ่งเป็นแก่นหลักของ Informationized Warfare ยุทธศาสตร์ใหม่ของรัสเซียนี้นิยมเรียกว่า “New Generation Warfare” ด้วยการโฆษณาชวนเชื่อ ใช้ตัวแทน และนักรบนอกเครื่องแบบ และการสร้างมวลชน โดย US DOD เรียกแนวคิดแบบนี้ว่า “โซนสีเทา (Gray Zone)”



ภาพที่ ๙ แนวคิด Mosaic Warfare ในการยกขึ้นบก
ที่มา: CSBA 2020, Mosaic Warfare

๒.๓ จีน ในปี ค.ศ.๒๐๑๕ จีนกำหนดยุทธศาสตร์สงคราม “ชนะสงครามในภูมิภาคที่ใช้ข้อมูลข่าวสาร (Informatized Local War)”^{๒๓} และสหรัฐฯ มองว่ารูปแบบของสงครามกำลังพัฒนาด้วยอัตราเร่งไปสู่ Informatization^{๒๔} โดยนิยามคำนี้ว่า “สงครามที่มีการใช้ข้อมูลข่าวสารกับอาวุธ อุปกรณ์ และเครือข่าย ร่วมกับยุทธวิธี ปฏิบัติการร่วมในโดเมนทางบก ทะเล อากาศ อวกาศ และแม่เหล็กไฟฟ้า รวมทั้งสนามรบแห่งความรู้เข้าใจสถานการณ์ (Cognitive Arena)”^{๒๕} เพื่อใช้แก้ปัญหาคความขัดแย้งในภูมิภาคด้วยความเป็นเลิศด้านข้อมูลข่าวสาร บูรณาการเครือข่ายข้อมูลระบบ C2 แบบเสมือนจริง ใช้ยุทธศาสตร์ป้องกันเชิงรุก โดยมีแนวคิดใช้ความสามารถของกำลังรบด้านเทคโนโลยีข้อมูลข่าวสาร และระบบการสื่อสารที่ทันสมัยให้ได้เปรียบทางยุทธการต่อฝ่ายตรงข้าม Informatization ของจีนยังรวมถึง

ยุทธศาสตร์โซนสีเทา (Gray Zone) ที่ใช้ทหารนอกเครื่องแบบปฏิบัติการ
แก้ปัญหาผู้รุกร้ำเขตพื้นที่รอบหมู่เกาะสแปรตลีย์ของจีน^{๓๐} จีนใช้ยุทธศาสตร์
การหลอมรวมข้อมูลข่าวสารจากเทคโนโลยีทางทหารและเอกชน (Military
Civil Fusion: MCF)^{๓๑} เพื่อพัฒนาประเทศตั้งแต่ปี ค.ศ.๒๐๑๔ จีนประสบ
ความสำเร็จในการพัฒนาประเทศในปี ค.ศ.๒๐๒๑ แม้ว่าสมุดปกขาวจีน
ในปี ค.ศ.๒๐๑๙ จะเปิดเผยยุทธศาสตร์ที่ทำทนายสหรัฐฯ แต่ก็ยังไม่จำเป็นต้อง
ต้องแก้ปัญหาด้วยการสร้างความขัดแย้ง^{๓๒} ทั้งนี้ ยุทธศาสตร์ MCF ประกอบด้วย
(๑) การหลอมรวมอุตสาหกรรมทหารและเอกชน (๒) การบูรณาการถ่วงน้ำหนัก
ความคิดริเริ่มด้านวิทยาศาสตร์และเทคโนโลยี (๓) การบ่มเพาะ Talent ร่วมกัน
ระหว่างทหาร และเอกชน (๔) การกำหนดความต้องการทหารสอดคล้อง
โครงสร้างพื้นฐานเอกชน (๕) การถ่วงน้ำหนักความสำคัญของเอกชนกับการ
ส่งกำลังบำรุง และ (๖) ขยายและลงรายละเอียดด้านการป้องกันประเทศ
เพื่อขับเคลื่อนระบบให้พร้อมลงสนามแข่งขันและทำสงคราม

ความเป็นเลิศด้านข้อมูลข่าวกรอง (Intelligentized)

ทั้งแนวคิด Intelligentization ของจีนและ Mosaic Warfare ของ
สหรัฐฯ ล้วนบูรณาการ Automation ยาน UxV, AI และเทคโนโลยีใหม่
ในลักษณะ “คนสั่งการยานควบคุม” เพื่อสงครามในอนาคต สรุปได้ดังนี้

๑. Intelligentized Warfare US DOD^{๓๓} วิเคราะห์ว่า จีนจะอาศัย
ความเป็นผู้นำด้าน AI ใช้แนวคิด Intelligentized Warfare ซึ่งเป็นแนวคิดใหม่
ที่ต่อเนื่องจากความเป็นเลิศด้านข้อมูลข่าวสาร (Informatized) โดยมีแนวโน้ม
จะสมบูรณ์ในปี ค.ศ.๒๐๓๕ เน้นปฏิบัติการร่วมของ AI และเทคโนโลยีใหม่
สำหรับพัฒนาการทัพ โดยใช้ AI ช่วยตัดสินใจ ทำงานร่วมกับระบบอัตโนมัติ
ปรับปรุงเซ็นเซอร์เชิงรับ อาวุธเล็กกลง เสริมขีดความสามารถด้านสงคราม
อิเล็กทรอนิกส์และไซเบอร์จะสร้างความสับสนต่อข้าศึก โดยฝ่ายเราสามารถ
เลือกโจมตีเป้าหมายสำคัญ แนวคิดใหม่นี้พยายามบูรณาการภารกิจและ
สมรรถนะใหม่ผ่านการบังคับบัญชาในโดเมนใหม่ เช่น ไซเบอร์และอวกาศ
ด้วยกองกำลังสนับสนุนทางยุทธศาสตร์ การเติบโตของสมรรถนะด้านไซเบอร์
และสงครามอิเล็กทรอนิกส์ ทำให้จีนขยายขีดความสามารถที่เผชิญหน้า

ด้านอวกาศโดยบูรณาการอวกาศ และภาคพื้นเพื่อปฏิบัติการร่วมหลายโดเมน ซึ่งต้องบูรณาการทะเล อากาศระยะไกลร่วมกับปฏิบัติการทางเรือ สร้างความมั่นคงทางอากาศ ทะเล และความเป็นเลิศด้านข้อมูลข่าวสารในระยะไกลที่ครอบคลุมปฏิบัติการในพื้นที่ส่วนหน้า

๒. สงครามโมเสค (Mosaic Warfare) เนื่องจากปัญหาในอนาคต ฝ่ายตรงข้ามพัฒนาระบบ EW, C2W และ Counter-C2ISR การต่อต้านสงครามเครือข่ายรวมศูนย์ (NCW) จะทำให้เกิดช่องโหว่ ส่งผลให้ ผบ.หน่วยรบขาดข้อมูลข่าวสารในยุทธบริเวณและไม่เห็นภาพสถานการณ์ จึงไม่สามารถควบคุมกองเรือเฉพาะกิจได้^{๓๔} ต้องพึ่งสงครามการตัดสินใจแบบรวมศูนย์ (DCW) ที่อยู่ได้ท่ามกลางแรงเสียดทานและเมฆหมอกแห่งสงคราม (Fog of War) การใช้ AI และระบบอัตโนมัติช่วยในการตัดสินใจ พร้อมยานไร้คนขับและเครือข่ายการสื่อสารแบบ Context Centrix C3 ตามภาพที่ ๑๐ ที่ยาน UAV เป็นทั้งข่ายการสื่อสาร ตรวจการณ์ และการควบคุมบังคับบัญชา (C2) หาก ผบ.เรือมอบอำนาจโดยการกดปุ่มหน้าจอควบคุม แนวคิด Mosaic Warfare นี้ คิดโดย DARPA อาศัยความได้เปรียบเชิงอสมมาตร ด้วยการสร้างความซับซ้อนสับสนต่อฝ่ายตรงข้าม ด้วยการล่องละเมิดจากความเป็นพลวัต การประสานงานและระบบอัตโนมัติ เปลี่ยนความซับซ้อนเป็นอาวุธที่ทรงพลังจากเครือข่ายการรวมเซ็นเซอร์ราคาถูกลงผ่านโหนด C2 หลายโดเมน และการประสานงานร่วมของระบบ Manned/Unmanned”^{๓๕} ซึ่งศูนย์ประเมินยุทธศาสตร์และงบประมาณ (CSBA) สหรัฐฯ ทดสอบ War Game ๓ ครั้ง ได้ข้อสรุปคือ



ภาพที่ ๑๐ Context Centrix C3
ที่มา: CSBA 2020, Mosaic Warfare

(๑) ผบ.หน่วยรบสามารถเชื่อใจการควบคุมโดยระบบกล (๒) ช่วยเพิ่มความซับซ้อนให้กำลังรบฝ่ายเราและลดทอนการตัดสินใจฝ่ายตรงข้าม (๓) ช่วยให้ผบ.หน่วยรบสามารถปฏิบัติซ้ำ ๆ สร้างความสับสนและเอาชนะการตัดสินใจของศัตรู (๔) การออกแบบกำลังรบแบบโมเสค และกระบวนการ C2 จะช่วยเพิ่มความเร็วในการตัดสินใจของ ผบ.หน่วยรบให้ควบคุมจังหวะ (๕) ช่วยให้ผบ.หน่วยรบสร้างสรรค์กลยุทธ์มากกว่าการรบ ภาพที่ ๙ แสดงการยกพลขึ้นบกลดกระบวนการจากเดิม ๓ ขั้นตอน คือ การยิงฝั่งระยะไกล การทำลายเป้าหมายเรือ/ฝั่งระยะกลาง และการใช้พลร่มลงซีเป่าให้อากาศยานโจมตีเป็นแนวคิดใหม่เหลือ ๒ ขั้นตอน คือการโจมตีระยะไกลพร้อมใช้ยานไร้คนขับประเภทต่าง ๆ (UxV) ทำลายเป้าหมายข้างเคียง และการซีเป่าให้อากาศยานโจมตี

เครือข่ายการรบ (Battle Network)

เครือข่ายการรบพัฒนาจาก Platform Centrix เป็น C3I, C4ISR, NCW และ DCW ตามภาพที่ ๑๑

๑. แนวคิดปัจจุบันแบบ NCW อยู่บนพื้นฐานจากระบบ C3I ที่เป็นเสมือนศูนย์รวมประสาทของเซ็นเซอร์และอาวุธ การกระจายศูนย์ระบบ C3I ช่วยเพิ่มความอยู่รอดในอนาคต^{๓๖} การใช้บริการจากดาวเทียมในการสื่อสาร ตรวจสอบการณ์ มอนิเตอร์และหาตำแหน่ง ช่วยนำร่องอาวุธปล่อย ซึ่งต่อมาพัฒนาเป็นระบบ C4ISR และปฏิบัติการแบบรวมศูนย์ (NCO) สนับสนุนภาพสถานการณ์ระหว่างเหล่าทัพในการรบร่วมได้ ผู้บังคับบัญชาสามารถใช้ข้อมูล ISR ประกอบการตัดสินใจเลือกหนทางปฏิบัติที่เหมาะสม แต่ในภาวะสงครามข้าศึกจะมุ่งปฏิบัติต่อแหล่งกำเนิดทางกายภาพ ขั้นตอนการสื่อสาร หรือกระทำต่อข้อมูลเพื่อลดทอนหรือทำให้ข้อมูลล่าช้า ส่งผลต่อการรับรู้ข้อมูลข่าวสารของผู้บังคับบัญชา ทำให้ตัดสินใจบนพื้นฐานข้อมูลที่ไม่ชัดเจน “รู้ภาพในอดีต แต่สถานการณ์ปัจจุบันคลุมเครือ” อันเป็นข้อด้อยของแนวคิดแบบ NCW

๒. แนวคิดใหม่แบบการตัดสินใจรวมศูนย์ DCW ด้วยแนวคิดการปฏิบัติการแบบกระจายศูนย์ทั้งรูปแบบ DL DMO Informatization และ Mosaic Warfare อยู่บนพื้นฐานการตัดสินใจรวมศูนย์ที่แตกต่างจากแนวคิด

แบบ NCW กล่าวคือ แนวคิดนี้ผู้บังคับบัญชาสามารถตัดสินใจบนพื้นฐานข้อมูลที่ชัดเจน “รู้ภาพในอดีต ทราบสถานการณ์ปัจจุบัน และทำนายเหตุการณ์ในอนาคตได้อย่างแม่นยำ” ประกอบด้วย (๑) การตัดสินใจรวมศูนย์แบบกลุ่มเรือ (SAG Centrix) ซึ่งเป็นการปฏิบัติตามแนวคิดแบบ DL (๒) การตัดสินใจรวมศูนย์แบบกองเรือ (Fleet Centrix) เพื่อปฏิบัติการระดับกองเรือ หรือกองเรือเฉพาะกิจ (FCO) สำหรับการปฏิบัติแบบ DMO และ (๓) การรวมศูนย์กองเรือสำหรับการควบคุมบังคับบัญชา และการสื่อสาร (Fleet Centrix C3) เป็นการตัดสินใจในระดับยุทธการและยุทธวิธีในการควบคุม เลือกใช้ทั้งเซ็นเซอร์และอาวุธจากทุกแหล่งได้อย่างกลมกลืน สามารถประยุกต์ใช้แนวคิด DL, DMO, และ Mosaic Warfare แบบคนสั่งการยานควบคุม ทั้งโหมดปกติ และโหมดตอบโต้



ภาพที่ ๑๑ พัฒนาการเครือข่ายการรบ (Battle network)

ที่มา: Bing, Wikipedia, CSBA, C4ISR for Future Naval Strike Groups

แนวคิด “Informatized Distributed Maritime Operation: IDMO” ในการปฏิบัติการทางเรือ

แนวคิดในการปฏิบัติการทางเรือในอนาคต เพื่อให้กองทัพเรือปฏิบัติการกิจในการรักษาความมั่นคงทางทะเลได้อย่างครบถ้วนนั้น เริ่มจากมุมมองในการหาทางต่อต้านแนวคิดการล่าทำลายแบบกระจายศูนย์ (DL) ที่จะมีบทบาทสูงในภูมิภาคอาเซียน และในทะเลจีนใต้ ร่วมกับแนวคิด DMO และความเป็นเลิศด้านข้อมูลข่าวสารที่ครอบคลุมทุกโดเมนสงคราม โดยมีแนวทางในการพัฒนาแนวคิดสำหรับกองทัพเรือ ดังนี้

๑. การพัฒนาแนวคิดในการใช้กำลังของกองทัพเรือเพื่อใช้แก้ปัญหาจากแนวคิดแบบ DL

ข้อดีจากแนวคิดแบบ DL เหมาะสำหรับการปฏิบัติการสงครามทางเรือในการควบคุมทะเล แนวคิดแบบ DMO สามารถใช้ร่วมกับ นย. สอ.รฟ. และต่างเหล่าทัพ จำเป็นต้องพึ่งพาการสื่อสารที่รวดเร็วในลักษณะปฏิบัติการแบบรวมศูนย์ (NCO) จึงเหมาะสำหรับการทำสงครามเชิงรุกและป้องกันเชิงรุก ส่วนแนวคิด Informatization มีความเหมาะสมสำหรับใช้ข้อมูลข่าวสารให้เกิดประโยชน์ต่อการตัดสินใจของผู้นำ ทิ้งทหาร และพลเรือน อีกทั้งยังรองรับแนวคิดความเป็นเลิศด้านข้อมูลข่าวสาร (Intelligentized) หรือ Mosaic Warfare หลังปี ค.ศ.๒๐๓๕ แล้วแนวคิดนี้ของจีนยังใช้ข้อมูลข่าวสารตามยุทธศาสตร์ Military - Civil Fusion (MCF) เพื่อบูรณาการเทคโนโลยีร่วมระหว่างรัฐ สถาบันและเอกชนนำไปสู่การวิจัยเรียนรู้ร่วมกันได้เป็นอย่างดี ตามภาพที่ ๑๒ จึงสมควรหลอมรวมแนวคิดแบบ DMO ของสหรัฐฯ กับแนวคิด Informatization ของจีน เกิดเป็นหลักการใหม่คือ “ปฏิบัติการทางทะเลแบบกระจายศูนย์ด้วยความเป็นเลิศด้านข้อมูลข่าวสาร (Informatized DMO: IDMO) ที่เหมาะสมกับการรักษาความมั่นคงทางทะเลของไทย



ภาพที่ ๑๒ วิเคราะห์ Informatization ของจีน

ที่มา: Bing, Wikipedia, CSBA, C4ISR for Future Naval Strike Groups

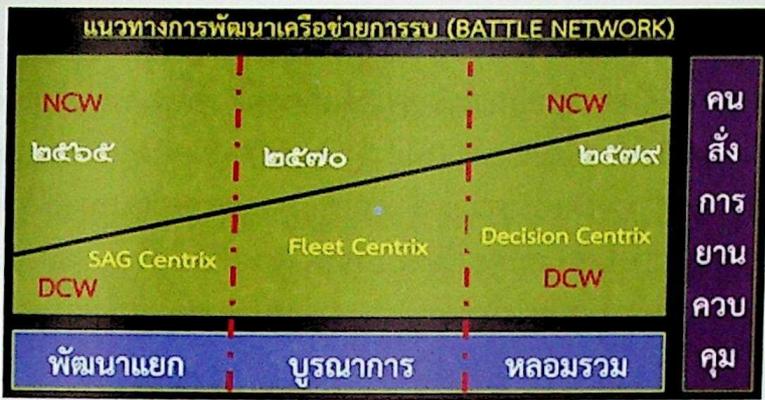
๒. แนวคิดในการใช้กำลังทั้งเชิงรับและเชิงรุกตามยุทธศาสตร์ IDMO

๒.๑ ใช้ความเป็นเลิศด้านข้อมูลข่าวสารรวบรวมข้อมูล ISR ในการป้องปรามประเทศมหาอำนาจที่จะสนับสนุนประเทศเพื่อนบ้านให้มีความก้าวร้าวต่อไทย หากพิสูจน์ได้ว่ามหาอำนาจนำเรือดำน้ำหรือยานใต้น้ำเข้ามาปฏิบัติการมิชอบในพื้นที่ทางทะเล รวมทั้งข้อมูลอื่น เช่น โซเบอร์ ดาวเทียม UAV อากาศยานค้างฟ้า ใช้ข้อมูลข่าวสารสำหรับการตัดสินใจของฝ่ายเราและทำลายข้อมูลฝ่ายตรงข้าม รวมทั้งสร้างการรับรู้สำหรับประชาชนให้เกิดความสามัคคี รักชาติและสถาบัน รวมทั้งใช้ในการบำรุงขวัญและกำลังใจของทหารในยามขัดแย้ง หรือวิกฤติ

๒.๒ ใช้แนวคิด DMO ในการรักษาความมั่นคงทางทะเล พร้อมแก้ปัญหาทั้งยามสงบ และยามวิกฤติ สนับสนุนการรวบรวมระหว่างเหล่าทัพ ใช้แนวทางการลวงและรบกวน โดยใช้ประโยชน์จากการลวงด้วย UxV เพื่อค้นหา พิสูจน์เป้า และทำลาย ซึ่งจะทำให้ ผบ.หน่วยรบสามารถรับรู้และตัดสินใจได้อย่างถูกต้องรวดเร็ว ส่วนการต่อต้านการพิสูจน์เป้าของข้าศึกควรใช้อาวุธพลังงานตรงและพลังงานจลน์ ลดทอนทำลายต้นกำเนิดข้อมูลข่าวสารฝ่ายตรงข้าม รวมทั้งใช้ Decoys ลวง ทั้งใต้น้ำและผิวน้ำเพื่อหลบเลี่ยง หากอาวุธปล่อยยังหลุดรอดเข้ามาได้ให้ใช้ระบบป้องกันตนระยะประชิด เช่น CIWS หรือปืนรองจัดการสามารถยิงสนับสนุนฝั่ง สนับสนุนกองทัพบก รักษาเส้นทางคมนาคม คุ่มกัน ขบวนสินค้า และภารกิจหลักอื่นในการรักษาความมั่นคงทางทะเล

การพัฒนาเครือข่ายการรบ (Battle Network) รองรับแนวคิด IDMO

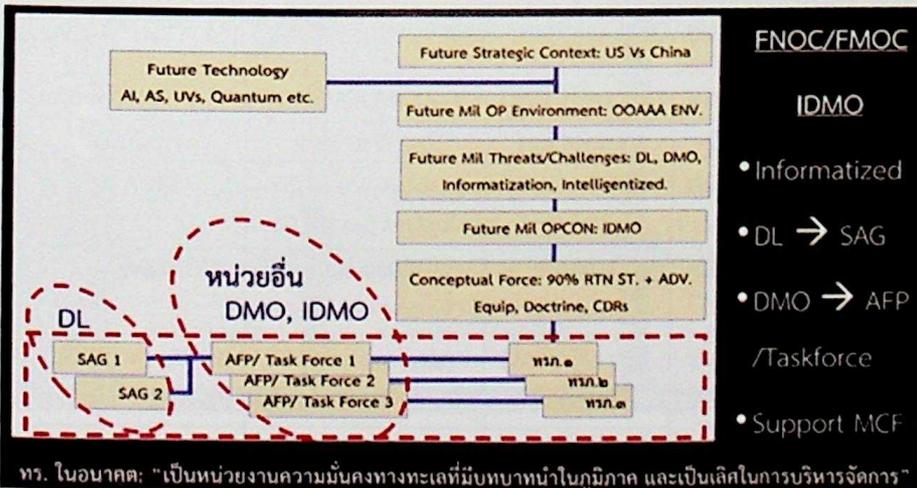
แนวโน้มการพัฒนาเครือข่ายการรบจำเป็นต้องเปลี่ยนทิศทางให้รองรับสงครามอนาคต ที่แม้ว่าแนวคิดแบบ NCW ยังคงมีความสำคัญอยู่ แต่ด้วยข้อจำกัดของแรงเสียดทานและเมฆหมอกสงคราม จึงมีความจำเป็นในการพัฒนาแนวคิดแบบ DCW ขึ้นมาใช้งานคู่ขนานกันไป และเพิ่มบทบาทมากขึ้นในอนาคต ตามภาพที่ ๑๓ ที่มีกรอบการพัฒนา ๕ ปี ๓ ระยะ สอดคล้องกับยุทธศาสตร์ชาติ ๒๐ ปี ที่เหลือเวลาอีก ๑๕ ปี และสิ้นสุดในปี ๒๕๗๙



ภาพที่ ๑๓ แนวทางการพัฒนาระบบเครือข่ายการรบ ๓ ระยะ สอดคล้องตามยุทธศาสตร์กองทัพเรือ ระยะ ๒๐ ปี

แนวคิดในการปฏิบัติการทางเรือในอนาคต (FNOC)

การปฏิบัติการทางเรือในอนาคตตามแนวคิด FNOC ตามภาพที่ ๑๔ โดยทัพเรือภาค สามารถจัดเรือแบบ SAG ตามแนวคิด DL ออกปฏิบัติการกิจโดยอิสระ แต่หากมีความขัดแย้งระดับสูงก็ใช้แนวคิด แบบ DMO ตั้งกองเรือเฉพาะกิจแบบอ่อนตัว (AFP) ร่วมกับแนวคิดความเป็นเลิศด้านข้อมูลข่าวสาร (Informatization) ปฏิบัติการรบรวมแบบ IDMO ที่กองทัพเรือ เป็นกองกำลังหลัก แต่หากเป็นสงครามขนาดใหญ่ที่ใช้การรบรวมโดยมี กองทัพไทยเป็นหน่วยควบคุมบังคับบัญชา จะใช้ยุทธศาสตร์ปฏิบัติการรบรวม บนความเป็นเลิศด้านข้อมูลข่าวสาร (Informatized Distributed Joint Operation: IDJO) โดยประยุกต์แนวคิดปฏิบัติการในทะเลแคบของมิลาโน วิโก้



ทร. ในอนาคต: "เป็นหน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค และเป็นเลิศในการบริหารจัดการ"

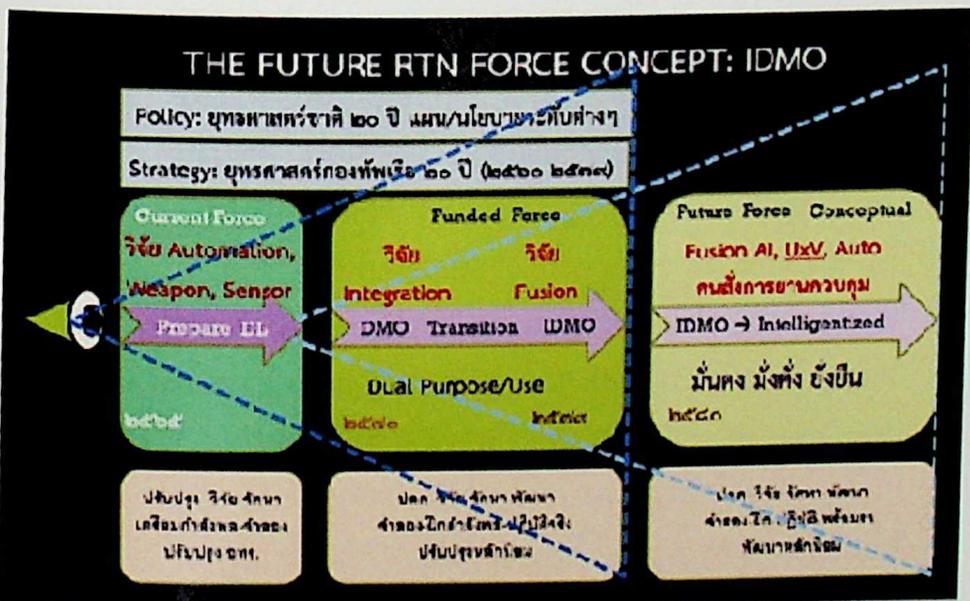
ภาพที่ ๑๔ การออกแบบ FNOC สำหรับกองทัพเรือในอนาคต

การบริหารความเสี่ยงนั้น ในระดับยุทธศาสตร์จะดำเนินการตามกระบวนการประเมินยุทธศาสตร์โดยทบทวนระดับความเสี่ยงที่ครอบคลุมทั้งโอกาสที่จะเกิดเหตุการณ์ในแต่ละวัตถุประสงค์ และผลกระทบ เพื่อจัดลำดับความเร่งด่วนในการจัดทำกำลักรบ โดยให้ความสำคัญกับการบรรลุวัตถุประสงค์ด้านการป้องกันประเทศซึ่งเป็นยุทธโศปกรณ์หลักก่อน และปรับใช้ให้บรรลุวัตถุประสงค์อื่น ๆ ตามมา ส่วนความเสี่ยงในระดับยุทธการ ได้พิจารณาบริหารความต้องการยุทธโศปกรณ์ที่จะบรรลุในแต่ละวัตถุประสงค์เฉพาะคือ (๑) ความสามารถในการรบ (๒) การดำรงสภาพของการรบ (๓) ความสามารถในการจัดหา โดยพิจารณาตามสภาพเศรษฐกิจ รวมทั้งกำหนดทางเลือกในการปรับปรุงกำลักรบที่มีอยู่ เพื่อลดความเสี่ยงหากไม่สามารถจัดหายุทธโศปกรณ์ตามต้องการได้ใน ๒ ทิศทาง คือ เลือกเพิ่มบางระบบเพื่อดำรงสภาพเรือให้คงเดิมหรือดีกว่า เช่น เพิ่มเซ็นเซอร์พร้อมยานไร้คนขับ เทคโนโลยีปัญญาประดิษฐ์ หรือระบบอัตโนมัติ ส่วนทิศทางที่ ๒ หากมีข้อจำกัดด้านงบประมาณจำเป็นต้องปรับลดเกรดเรือลง ๑ ชั้น เช่น เรือฟรีเกต เรือซูด ร.ล.เจ้าพระยา ทดแทนเรือตรวจการณ์ไกลฝั่ง (เรือ ตกก.) เรือตรวจการณ์ปราบเรือดำน้ำ (เรือ ตกต.) ทดแทน เรือตรวจการณ์ปืน (เรือ ตกป.) และ ร.ล.จักรีนฤเบศร ทดแทนเรือเอนกประสงค์ยกพล ทั้งนี้ ควรจัดหายุทธโศปกรณ์แบบโมดูลที่สามารถย้ายการติดตั้งให้หน่วยเรือและหน่วยบกได้ ตลอดจนใช้ยานไร้คนขับทำหน้าที่ทดแทนการสื่อสาร การลงการทำลาย ตามแนวคิดแบบ DL (๔) กำหนดกลุ่มเรือในการปรับปรุงตามอายุเรือ และสภาพยุทธโศปกรณ์ตาม ตารางที่ ๑

ตารางที่ ๑ การกำหนดกลุ่มเรือในการพัฒนาเรือตามแนวคิด IDMO และการบริหารความเสี่ยง

อายุเรือ (ปี) /ปรับปรุง	แนวทางการพัฒนาปรับปรุงเรือตามแนวคิด IDMO			การบริหารความเสี่ยง	
	เซ็นเซอร์	ออฟเพ็คเตอร์	สื่อสาร และ C2	คงระดับเรือ	ลดระดับเรือ
เรือใหม่ < ๑๙ ปี	เพิ่มระยะ และ UxV,	เพิ่มระยะ, แบบตู้, UCAV, UxV	UxV, AI และ AUS Context Centrix C3	N/A	N/A
๑๙ - ๓๖ ปี ปรับปรุงเรือแล้ว	เพิ่มระยะ และ UxV,	เพิ่มระยะ,แบบตู้ UCAV, UxV	UxV, AI และ AUS Context Centrix C3	N/A	N/A
๑๙ - ๓๖ ปี ไม่เคยปรับปรุง	เพิ่มระยะ และ UxV,	ใช้แบบตู้ UCAV, UxV	UxV, AI และ AUS Context Centrix C3	หากสภาพเรือยังดี	สภาพเรือเก่า ลด ๑ ระดับ
มากกว่า ๓๖ ปี	เพิ่มระยะ และ UxV,	ใช้แบบตู้ UCAV, UxV	UxV, AI และ AUS Context Centrix C3	N/A	ลด ๑ ระดับ

สำหรับการตัดสินใจของผู้นำปฏิบัติการรบในอนาคตใช้ยุทธศาสตร์ IDMO ด้วยบันได ๓ ขั้น คือ “มีกำลังรบทางกลแบบ Manned/Unmanned มุ่งสู่ยุทธศาสตร์ IDMO ในปี ๒๕๗๐ เป็นเลิศด้านข้อมูลข่าวสาร ในปี ๒๐๗๙ และเป็นเลิศในด้านข้อมูลข่าวกรองในปี ๒๐๘๙” ตามแนวคิดในภาพที่ ๑๕ แนวคิดทางยุทธการแบบ FNOC นั้น ส่วนใหญ่ยังคงสอดคล้องกับยุทธศาสตร์ กองทัพเรือในระยะ ๒๐ ปี แต่เน้นใช้แนวความคิดทางยุทธการแบบ IDMO เป็นหลัก ส่วนการพัฒนากำลังรบนั้น พบว่ายุทธโศปกรณ์ที่เตรียมจัดหาตาม ยุทธศาสตร์กองทัพเรือในระยะ ๒๐ ปี ยังไม่เพียงพอรองรับสงครามรูปแบบใหม่ ในอนาคตจำเป็นต้องพัฒนาและจัดหายุทธโศปกรณ์แบบ Unmanned ซึ่งด้วย ข้อจำกัดด้านงบประมาณจากสถานการณ์โควิด เป็นการยากที่จะเสนอโครงการ จัดหา จึงควรจัดหาเท่าที่จำเป็น แต่มุ่งเน้นสร้างความร่วมมือวิจัยพัฒนา แบบสองวัตถุประสงค์ ระหว่างกองทัพเรือ สถาบันการศึกษา และเอกชน ตามแนวคิด MCF ของจีน โดยกรอบ ๕ ปีแรก มุ่งเน้นที่การพัฒนาส่วนแยก ห้าปีถัดไปให้พิจารณาจัดหาบางส่วนมาบูรณาการ (Integration) และห้าปี สุดท้าย (๒๕๗๕ - ๒๕๗๙) เป็นการหลอมรวม (Fusion) ทุกส่วนเข้าด้วยกัน จะทำให้บรรลุจุดมุ่งตามแนวคิด IDMO



ภาพที่ ๑๕ แนวคิดการพัฒนาทางเรือในอนาคต

บทสรุป

แนวคิดการล่าทำลายแบบกระจายศูนย์ (DL) ของสหรัฐฯ เข้ามาสู่ภูมิภาคจะสร้างปัญหาและส่งผลกระทบต่อการรักษาความมั่นคงทางทะเล ผลการวิจัยพบว่า กองทัพเรือต้องพัฒนาแนวคิดที่เหมาะสมคือ “ปฏิบัติการทางทะเลแบบกระจายศูนย์ด้วยความเป็นเลิศด้านข้อมูลข่าวสาร (IDMO)” ที่บูรณาการข้อดีจากยุทธศาสตร์ “Informatization” ของจีน และยุทธศาสตร์ DMO ของสหรัฐฯ เข้าด้วยกัน ซึ่งจะสามารถนำมาใช้รักษาความมั่นคงทางทะเลได้เป็นอย่างดี ในการพิจารณากำหนดความต้องการกำลังรบนั้น เห็นว่ายุทธศาสตร์กองทัพเรือในระยะ ๒๐ ปี กำหนดไว้ค่อนข้างมีความเหมาะสม เพียงแต่เพิ่มยานไร้คนขับ AI และยานอัตโนมัติ และอาวุธแบบ Soft Kill อาวุธสมัยใหม่ให้สอดรับจัดเตรียมกำลังพล ปรับปรุงหลักนิยม และสิ่งอำนวยความสะดวกให้รองรับแนวคิด IDMO รวมทั้งพัฒนาระบบเครือข่ายการรบ ด้าน DCW พร้อมแนวคิด Context Centrix C3 ในลักษณะ “คนสั่งการยานควบคุม” คู่ขนานและเชื่อมต่อ NCW ระหว่างเหล่าทัพ พัฒนาระบบ C2 ให้สามารถเชื่อมต่อระหว่างเรือ-บก-อากาศยาน ผ่านระบบสื่อสารทางยุทธวิธี อีกทั้งบริหารความเสี่ยงที่เหมาะสมจะทำให้กองทัพเรือสามารถรักษาความมั่นคงทางทะเลในอนาคต ทั้งนี้ มีข้อเสนอแนะให้กองทัพเรือใช้ยุทธศาสตร์ IDMO ในการรักษาผลประโยชน์แห่งชาติทางทะเล โดยหน่วยขึ้นตรงกองทัพเรื่อนำแนวคิด IDMO ไปปฏิบัติและเตรียมการในส่วนที่เกี่ยวข้อง พร้อมเสนอให้มีการศึกษาวิจัยร่วมกับสถาบันและหน่วยงานภายนอก

Mengxiong Chang, The Revolution in Military Affair: Weapon of 21st Century, Leonado DRS, Multidomain battle Management, <<https://fas.org/nuke/guide/china/doctrine>>

Vego N. Milan, Operational Warfare at Sea, Routledge, Milton Park, Abingdon, Oxon, 2009

Australia's Victorian Government Committee, Cyber Security Strategy's

US CSBA, Mark Gunzinger, et al, Force Planning for the era of Great Power Competition, 2017.

US CSBA, Clark Bryan, et al, Mosaic Warfare: Exploiting AI and Autonomous Systems to Implement Decision-Centric Operations, 2020.

US CSBA, Clark Bryan et al, Winning the Gray Zone: Using EM Warfare to Regain Escalation Dominance, 2017.

US CSBA, Renberg Carl and Gunzinger Mark, Air and Missile Defense at Crossroad: New Concepts and Technologies to defense America Oversea Bases, 2018

US CSIS, Cordesman Antony H., China New 2019 Defense White Paper, 2019.

US DOD, Military and Strategy Development of the PRC, Annual Report to Congress, Aug 21, 2020

US DOD, Military and Security Developments Involving the PRC, Annual Report to Congress, 2019.

US Defense Intelligence Agency, China Military Power: Modernizing a Force to Fight and Win, 2019.

US DOD JP-05, Oct 2020

US Marine Corp, Force Design 2030, 2020.

US National Security Strategy, December 2017

US Navy ISR Roadmap, Industry Day, 2010.

US Navy, A Design for Maintaining Maritime Superiority, Version 2.0 Dec 2018.

US Navy and US Marine Corps, Littoral Operation in a Contested Environment, 2017.

US NIC, Global Trend 2040, 2021.

Congressional Research Service, Navy Force Structure and Shipbuilding Plans: Background and Issues for Congress, Oct 7, 2020.

Morgan E. Forrest and Cohen S. Raphael, Military Trend and Future of Warfare, RAND, 2020.

Jeffrey J.E et al, A Tactical Doctrine for Distributed Lethality, Feb 22, 2016, Dudley Library, Naval Postgraduate School, Monterey, USA

Papa et al, DMO and Unmanned System Tactical Deployment, US Naval Post Graduate School, 2018.

Alan Coming, "Distributed Lethality: China is doing it Right," A CIMSEC Compendium, Feb 22, 2016, <http://www.cimsec.org/>

John Devlin, LCDR, "Refiguring a Cushioned Vehicle to Enhance Distributed Lethality," A CIMSEC Compendium, Feb 22, 2016.

Kline Jeffrey E., CAPT USN (ret), "A Tactical Doctrine for Distributed Lethality," Center of Maritime Security, Feb 22, 2016.

O'Connor Chris r, LCDR, "Distributed Leathernecks," A CIMSEC Compendium, Feb 22, 2016.

Sapaty Simon Peter, "Mosaic Warfare: From Philosophy to Model to Solutions," Med Crave, International & Automation Journal, Volume 5 Issue 5, 2109.

Uppal Rajesh, "US Navy Operating DMO, Strategy Integrating Diverse Autonomous Unmanned Vehicles UUV, USVs, UAVs", 2021.

Beeryl Pual T., et al, "Command and Control for Distributed Lethality," Conference Paper, ResearchGate, April, 2019.

CRUSER and Naval Post Graduate School, DMO Warfare Innovation Continuum, 2017.

Diane S. Cua, CDR, USN. Distributed Lethality and a Surface Experimental Test Squadron, Naval War College, New Port, RI, 29 May 2017.

Fox Collin, LCDR, "Implementing Distributed Lethality within the Joint Operation Access Concept," A CIMSEC Compendium, Feb 22, 2016.

Gerson Michael and Whiteneck Daniel, "Deterrence and Influence: The Navy's Role in Preventing War (Citing Lawrence Freedman)," 2020.

Gunzinger Mark et al, Force Planning for the Era of Great Power Competition, CSBA, 2017.

Popa Christopher H. et al, DMO and Unmanned Systems Tactical Employment Naval Post Graduate School, 2018.

Richards Scott K., Jr, The Advanced Surface Fleet, A Proposal for an Alternative Surface Force US CSBA, Mahnken G. Thomas, et al, Deterrence by Detection, 2020.

US Navy, Advantage at Sea: Prevailing with Integrated All-Domain Naval Power, 2020.

US CSBA, Mahnken G. Thomas, et al, Forging the Tools of 21st Century Great Power Competition, 2020.

US CSBA, Clark Bryan, The Future of Warfare, 2015. Control, 2016.

US CSBA, Clark Bryan and Timothy A. Walton, Taking Back the Sea, 2019.

- ๑ US NIC (2021), Global Trend 2040
- ๒ Morgan E. Forrest and Cohen S. Raphael, 2020, Military Trend and Future of Warfare, RAND pp.Vii.
- ๓ Vego Milan, 2009, Operational Warfare at Sea, pp.228-229
- ๔ National Security Strategy of USA, December 2017 p.13
- ๕ Jeffrey E. Kline, CAPT USN (ret), A Tactical Doctrine for Distributed Lethality, Center of Maritime Security, Feb 22, 2016, p.4.
- ๖ Jeffry J.E et al, "A Tactical Doctrine for Distributed Lethality", Feb 22, 2016, Dudley Library, Naval Postgraduate School, Monterey, USA
- ๗ Congressional Research Service, Navy Force: Background and Issues for Congress, Oct 7, 2020, p.5
- ๘ Chris O'Connor, LCDR, Distributed Leathernecks, A CIMSEC Compendium, Feb 22, 2016, p.16
- ๙ John Devlin, LCDR, Refiguring a Cushioned Vehicle to Enhance Distributed Lethality, A CIMSEC Compendium, Feb 22, 2016
- ๑๐ Daniel Stefanus, ENS, Reviseing Operational & Promotion Paradigms, A CIMSEC Compendium, Feb 22, 2016
- ๑๑ US Navy and US Marine Corps, Littoral Operation in a Contested Environment, 2017.
- ๑๒ Papa et al 2018, DMO and Unmanned System Tactical Deployment, US Naval Post Graduate School, p.33
- ๑๓ Rajesh Uppal 2021, "US Navy Operating DMO, Strategy Integrating Diverse Autonomous Unmanned Vehicles UUV, USVs, UAVs",
- ๑๔ Renberg Carl and Gunzinger Mark, Air and Missile Defense at Crossroad: New Concepts and Technologies to defense America Oversea Bases, CSBA 2018
- ๑๕ Gardner Nikolas, "Military Lesson of the First World War," International Encyclopedia of WW I, 2018, p.3.
- ๑๖ นเรศร วงศ์ตระกูล, พล.ร.ต., "ปฏิบัติการข้อมูลข่าวสาร," เอกสารประกอบการสอน วทร. ๕๓, ๒๕๖๔
- ๑๗ Sebastien, No More Stealth Submarine: Could Quantum 'Radar' The National Interest, April 2019, pp.1-9.

- ๒๘ Stuger R. Stuger, Lt. Col, USAF, “Space Base ISR to Global Strike 2035”
- ๒๙ Mahnken G. Thomas, et al, 2020, Deterrence by Detection, CSBA, pp.1-56.
- ๓๐ Westra Arend G., “Radar Versus Stealth”, Ndupress, IFQ, Issue 55, 4th Quarter 2009, pp.1-9.
- ๓๑ Ahmed Ashik, et al, “Counter Stealth with Quantum Radar,” International of Advanced Engineering Research and Science, V.1 Issue 5, Oct 2014, pp.1-3.
- ๓๒ Clark Bryan, 2015, The Future of Warfare, CSBA, p.1-6.
- ๓๓ US Navy, A Design for Maintaining Maritime Superiority, Version 2.0 Dec 2018, p.4.
- ๓๔ US Navy ISR Roadmap, Industry Day, 2010.
- ๓๕ US Navy Information Warfare, Information Warfare Community, CNO, Pentagon
- ๓๖ Gunzinger Mark et al, 2017, Force Planning for the Era of Great Power Competition, CSBA, p.IV
- ๓๗ US DOD 2019, Military and Security Developments Involving the PRC, Annual Report to Congress, pp.14.
- ๓๘ US Defense Intelligence Agency, China Military Power: Modernizing a Force to Fight and Win, 201, p.11.
- ๓๙ Clark Bryan et al, 2017, Winning the Gray Zone: Using EM Warfare to Regain Escalation Dominance, p.5
- ๓๐ Gunzinger Mark et al, 2017, Force Planning for the Era of Great Power Competition, CSBA, p.15.
- ๓๑ US DOD 2020, “Military and Security Developments Involvements PRC”, Annual Report to Congress, p.5-6
- ๓๒ US CSIS, Cordesman Antony H., China New 2019 Defense White Paper, 2019.
- ๓๓ US DOD, 2020, ibid, p.
- ๓๔ Clark Bryan, Mosaic Warfare p.IV-V
- ๓๕ Sapaty Simon Peter, “Mosaic Warfare: From Philosophy to Model to Solutions,” MedCrave, International & Automation Journal, Volume 5 Issue 5-2109, pp.157 – 166.
- ๓๖ Chang Mengxiong, The Revolution in Military Affairs: Weapons of 21st Century, p2.

ขอขอบคุณ

บริษัท มาร์ชชีน จำกัด (มหาชน)

บริษัท อู่กรุงเทพ จำกัด

บริษัท ปตท.สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน)

ที่กรุณาให้การสนับสนุนเป็นสมาชิกกิตติมศักดิ์ของวารสารนาวิกานุสาริต
ซึ่งมีส่วนสำคัญให้การจัดทำวารสารนาวิกานุสาริตดำเนินการต่อไป
คุณภาพและยั่งยืน ตามวัตถุประสงค์

คณะกรรมการจัดทำวารสารนาวิกานุสาริต

ជំនាញ ៤.០ : គុណសម្បត្តិក៏ជាប់តំបង់

អនុវត្ត ប្រែប្រួល ក្នុងការ

บทนำ

องค์กรต่าง ๆ ไม่ว่าจะอยู่ในภาคส่วนใดของสังคมล้วนปรารถนาผู้บริหารที่มีภาวะผู้นำสูง สามารถครองตน ครองคน และครองงาน ได้เป็นอย่างดี นำมาซึ่งความสุข ความเจริญ และความสำเร็จอย่างยั่งยืนของส่วนรวม ซึ่งมีใช้เรื่องที่สามารถเกิดขึ้นได้โดยง่าย สาเหตุสำคัญประการหนึ่งก็คือ ผู้บริหารระดับต่าง ๆ มีความก้าวหน้าในอาชีพตนตามกฎเกณฑ์ขององค์กร โดยเฉพาะในภาครัฐ มีการกำหนดคุณสมบัติพื้นฐานสำหรับตำแหน่งสำคัญไว้ค่อนข้างตายตัว ที่เห็นได้ชัดคือ การบริหารงานบุคคลในกองทัพ ไซยศและอาวุโสทางทหาร เป็นต้น ในการพิจารณาบรรจุคนให้ดำรงตำแหน่งหลักต่าง ๆ การคำนึงถึงภาวะผู้นำของแต่ละคนอาจมีอยู่บ้าง โดยการใช้ดุลพินิจของผู้มีอำนาจแต่งตั้ง ซึ่งมีใช้หลักประกันที่เชื่อถือได้เสมอไป มักมีเรื่องของความสัมพันธ์ส่วนตัวเข้าไปเกี่ยวข้องอยู่เสมอ ในระบบราชการโดยรวมจึงเต็มไปด้วยผู้บริหารที่อ่อนด้อยด้านภาวะผู้นำ สร้างความสูญเสียที่ไม่จำเป็นให้แก่ประเทศชาติอย่างมากมายมหาศาล

โดยหลักการพื้นฐานแล้ว คุณสมบัติที่ผู้นำทั่วไปจำเป็นต้องมี พอสรุปได้ดังนี้

๑. ความมีวิสัยทัศน์

เจ้าประคุณ สมเด็จพระพุทธโฆษาจารย์ (ประยุทธ์ ปยุตฺโต) ท่านได้ให้ความหมายไว้ว่า เป็นผู้ที่มีคิดกว้าง มองไกล และใฝ่สูง กล่าวคือ มีความรู้ความเข้าใจในความเป็นไปต่าง ๆ อย่างรอบด้าน เพื่อนำมาพิจารณาถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรที่ตนสังกัด โดยเฉพาะต่อหน้าที่รับผิดชอบของตน เพื่อหาทางเอาประโยชน์ให้ได้อย่างเต็มที่จากผลดีอันพึงได้ และหลีกเลี่ยงผลร้ายที่อาจเกิดขึ้นให้กระทบน้อยที่สุด สำหรับการมองไกลนั้นท่านหมายถึง การเห็นความเชื่อมโยงจากอดีตถึงปัจจุบัน เพื่อนำมาวิเคราะห์/สังเคราะห์ ทำนายสภาวะการณ์ที่จะเกิดตามมาในอนาคตให้ได้ใกล้เคียงความเป็นจริงมากที่สุด ส่วนความใฝ่สูง ท่านได้เมตตาสอนว่า คือความมุ่งมั่นที่จะทำทุกเรื่องให้ดีที่สุด โดยรวมแล้วความมีวิสัยทัศน์ที่ดีจำเป็นต้องมีทั้งสติปัญญาและอุดมการณ์ในการทำงานที่เข้มแข็งแรงกล้าพอนั่นเอง

๒. แผนงาน

นับเป็นเรื่องจำเป็นในการทำงานต่าง ๆ เมื่อมีวิสัยทัศน์และจุดมุ่งหมาย ในอนาคตที่แจ่มชัดแล้วต้องนำมาจัดทำแผนงานที่เหมาะสม แบ่งงานออกเป็น ส่วนย่อย ๆ มีผู้รับผิดชอบแต่ละส่วนอย่างชัดเจน แจกแจงรายละเอียด ในการดำเนินงาน โดยเฉพาะทรัพยากรที่จำเป็นต้องใช้ อันได้แก่ คน เงิน วัสดุ เทคโนโลยี และเวลา เป็นต้น แผนงานที่ดีคือ หลักประกันความสำเร็จของงาน เป็นเครื่องยืนยันในความเป็นไปได้ของวิสัยทัศน์ที่ตั้งไว้ มิใช่เป็นเพียงจินตนาการ หรือความฝันอันเลื่อนลอย

๓. การมีทีมงานที่ดี

หมายถึง การใช้คนให้เหมาะกับงานนั่นเอง เมื่อแยกงานทั้งหมด ออกเป็นส่วนย่อย ๆ แล้ว แต่ละส่วนจำเป็นต้องมีผู้รับผิดชอบที่เหมาะสมคือ มีความรู้และประสบการณ์มากพอที่จะทำงานนั้นได้ดี มีทั้งประสิทธิภาพและ ประสิทธิภาพสูง ทุกคนในทีมมีความเป็นอันหนึ่งอันเดียวกัน เข้าใจในหน้าที่ของตน และเป้าหมายของส่วนรวม พร้อมให้ความช่วยเหลือเพื่อนร่วมทีมตามโอกาส ที่เหมาะสม ไม่เกี่ยงว่ามีใช้หน้าที่ตน แต่ก็ไม่ก้าวร้าวหรือรบกวนงานของ ผู้อื่นจนเกินความพอดี

๔. การสื่อสารที่ดี

นับเป็นคุณสมบัติสำคัญอีกประการหนึ่งที่ผู้นำพึงมี เป็นกลไก สร้างความรู้ความเข้าใจที่ถูกต้อง ทั้งภายในทีม ภายในองค์กร และกับสังคม ภายนอก การสื่อสารที่ผิดพลาดมักเกิดขึ้นได้เสมอ อาจนำมาซึ่งความเสียหาย อันใหญ่หลวงได้ จำเป็นที่ผู้นำต้องรู้เท่าทันและรีบแก้ไขทันที การปรึกษาหารือกัน และการมีส่วนร่วมอย่างทั่วถึงของทุกคนในทีม คือพื้นฐานของการสื่อสารที่ดี

๕. ความทรหดอดทน

การทำงานโดยทั่วไปคือ การแก้ปัญหา กว่าจะบรรลุเป้าหมาย ทั้งในระยะสั้นและระยะยาวที่ตั้งไว้ ย่อมผ่านพบอุปสรรคต่าง ๆ หนักบ้าง เบาบ้าง ผู้นำที่ดีต้องมีความเข้มแข็งทั้งกายใจ ไม่ท้อแท้หรือยอมจำนนโดยง่าย ใช้ความพยายามอย่างเต็มที่เพื่อต่อสู้กับความยากลำบากทั้งหลาย ในที่สุด ก็จะสามารถประสบความสำเร็จ อาจมีบ้างในบางกรณีที่ทำอย่างไรก็ไม่สามารถคลี่คลาย

ปัญหาได้ ซึ่งมักเกิดจากการตั้งเป้าหมายไว้สูงเกินไป หรือใช้วิธีดำเนินงานที่ไม่ถูกต้อง จึงจำเป็นต้องมีการวิเคราะห์และประเมินตามห้วงเวลาที่เหมาะสม เพื่อปรับปรุงแก้ไขการปฏิบัติให้ได้ผลดีขึ้น หรือทบทวนและปรับเปลี่ยนเป้าหมายให้สามารถทำได้จริงมากยิ่งขึ้น

๖. การยึดผลประโยชน์ของส่วนรวมเป็นหลักในการทำงาน

ผู้นำที่ดีต้องมีความมุ่งมั่นในการทำหน้าที่เพื่อองค์กร ไม่มีวาระซ่อนเร้นเกี่ยวกับประโยชน์ส่วนตนและพวกพ้อง ความมีใจให้สังคมอย่างชัดเจน ช่วยให้ได้รับความร่วมมืออย่างเต็มที่จากผู้ร่วมงาน นำมาซึ่งความสำเร็จอันยิ่งใหญ่ แม้จะต้องเผชิญกับความยากลำบากมากมายเพียงใดก็ตาม

๗. การประพฤติ ศิล ๕

คือ การรักษาความเป็นปกติทางกายและวาจา เป็นหลักประกันในการครองตนให้มีความมั่นคงและปลอดภัยในชีวิต ทรัพย์สิน และฐานะทางสังคม นับเป็นพื้นฐานต่ำสุดในทางธรรมที่ทุกคนพึงมี

๘. ความมีพรหมวิหาร ๔

อันประกอบด้วย เมตตา กรุณา มุทิตา และอุเบกขา

“เมตตา” คือ ความรักและปรารถนาดีอยากให้ผู้อื่นมีความสุข

“กรุณา” คือ ความสงสารเห็นใจ ลงมือช่วยเหลือให้ผู้อื่นพ้นทุกข์

“มุทิตา” หมายถึง ความพลอยยินดีในความสุข ความเจริญ ความสำเร็จ และการทำความดีของผู้อื่น

“อุเบกขา” หมายถึง การวางใจเป็นกลาง ยึดมั่นในความยุติธรรม ไม่มีอคติหรือความลำเอียงต่อผู้ใด และยอมรับในผลจากการกระทำของตน เป็นต้น

๙. มีสัมปยุตธรรม ๗

ได้แก่ รู้เหตุ รู้ผล รู้ตน รู้ประมาณ รู้กาล รู้ชุมชน และรู้บุคคล

“รู้เหตุ” คือ การรู้ชัดในเรื่องที่ต้องทำ เพื่อให้บรรลุผลตามเป้าหมายที่ตั้งไว้

“รู้ผล” มีความหมายในทางตรงกันข้ามคือ รู้ว่าเหตุที่ตนกำลังทำอยู่นั้นจะนำผลอย่างไรมาให้ในอนาคต หากเป็นเรื่องที่ดีมีคุณค่าก็เร่งทำ

ให้มากขึ้น แต่ถ้าพิจารณาอย่างละเอียดรอบคอบแล้วพบว่า จะเกิดผลเสียมากกว่า ก็จำเป็นต้องลด ละ หรือเลิกการกระทำเช่นนั้นเสีย

“**รู้ตน**” คือ การวิเคราะห์ตัวเองด้วยใจที่เป็นกลาง เพื่อให้เห็นชัดในธาตุแท้ของตน รู้จุดอ่อน จุดแข็งที่ตนมี อันจะนำไปสู่การพัฒนาและใช้ศักยภาพตนได้อย่างเหมาะสม

“**รู้ประมาณ**” หมายถึง การยึดหลักความพอเหมาะพอดี ในการกระทำต่าง ๆ ไม่สุมเสียงหรือระแวงระวังจนเกินควร การใช้ทรัพยากร เพื่อดำเนินการใด ๆ ก็คำนึงถึงความคุ้มค่า ไม่สุรุ่ยสุร่ายหรือตระหนี่ถี่เหนียว จนทำให้งานล้มเหลว เป็นต้น

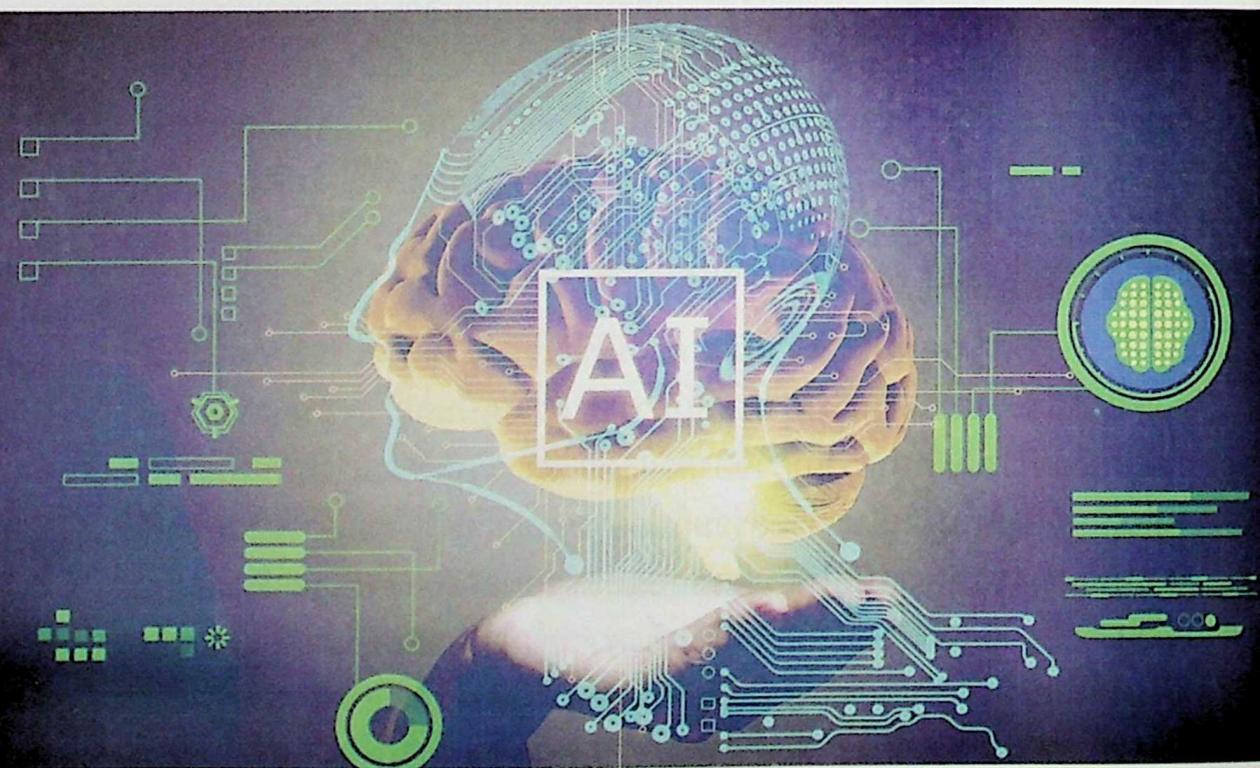
“**รู้กาล**” คือ รู้คุณค่าของเวลา มีหลักการบริหารเวลาที่ดี ควรทำอะไรในช่วงเวลาใดจึงจะเกิดประโยชน์สูงสุด เช่น การกิน การนอน การทำงาน และการออกกำลังกายตามห้วงเวลาที่เหมาะสม เพื่อการมีสุขภาพ แข็งแรงสมบูรณ์ทั้งกายใจ มีการกำหนดแบบแผนที่ชัดเจนและพยายามปฏิบัติ ให้ได้อย่างสม่ำเสมอ

“**รู้ชุมชน**” หมายถึง คนแต่ละหมู่เหล่ามักมีลักษณะเฉพาะที่ผิดแผก กันไปจากกลุ่มอื่น ๆ มากบ้างน้อยบ้าง โดยเฉพาะในเรื่องวัฒนธรรม ประเพณี และความเชื่อถือศรัทธาในเรื่องต่าง ๆ ซึ่งมักมีอิทธิพลมาจากเชื้อชาติและศาสนา ที่ต่างนับถือสืบทอดกันมาอย่างยาวนาน ผู้นำที่ดีจำเป็นต้องรู้และเข้าใจคนที่อยู่ในความปกครองดูแลของตนในเรื่องดังกล่าว เพื่อให้สามารถปฏิบัติต่อพวกเขา อย่างถูกต้องเหมาะสม

“**รู้บุคคล**” หมายถึง ความเข้าใจอย่างชัดเจนในลักษณะนิสัย ใจคอ ความรู้ความสามารถ ประสบการณ์ ความเป็นอยู่ และปัญหาส่วนตัว เป็นต้น ของแต่ละคนที่เราเกี่ยวข้องกับ โดยเฉพาะผู้ที่ทำงานร่วมกันในองค์กร เพื่อเป็นข้อมูลพื้นฐานในการอยู่ร่วมกันอย่างกลมกลืน มีความเข้าใจอันดีต่อกัน มอบหมายงานที่เขาถนัดให้รับผิดชอบและช่วยปลดเปลื้องปัญหาที่แต่ละคน มีอยู่เท่าที่สามารถทำได้ อันจะนำมาซึ่งความรักใคร่กลมเกลียวกันและความ เข้มแข็งของทีม รวมทั้งความสำเร็จขององค์กรด้วย

ทั้ง ๙ ประการ ที่กล่าวมานี้ นับเป็นคุณสมบัติพื้นฐานที่ผู้นำทุกยุค ฟังมี แต่ในยุค ๔.๐ มีความเปลี่ยนแปลงต่าง ๆ เกิดขึ้นมากมายอย่างรวดเร็ว แบบพลิกผันทีเดียว อันเป็นผลสืบเนื่องมาจากวิวัฒนาการด้านสื่อสารโทรคมนาคม

และคอมพิวเตอร์ ซึ่งมีความก้าวหน้าในอัตราสูงอย่างไม่หยุดยั้ง และได้มาเชื่อมต่อกันอย่างลงตัวในลักษณะของ Cyber Physical System มี Digital Technology และ Internet เป็นองค์ประกอบพื้นฐาน สร้างนวัตกรรมหลากหลายรูปแบบ ขึ้นทำงานแทนคน เช่น ปัญญาประดิษฐ์ (AI : Artificial Intelligence) อินเทอร์เน็ตแห่งสรรพสิ่ง (IoT : Internet of Things) Drone และยานไร้คนขับต่าง ๆ การพิมพ์สามมิติ (3D-Printing) และเทคโนโลยีด้านการเงิน (Fin Tech : Financial Technology) ส่งผลกระทบทั้งด้านบวกและลบเป็นวงกว้างต่อการดำเนินชีวิตของคนเราในปัจจุบันและอนาคต ไม่ว่าจะเป็นเรื่องการบริหารองค์กรทั้งภาครัฐและเอกชน การประกอบสัมมาอาชีพต่าง ๆ รวมทั้งการดำเนินชีวิตโดยทั่วไป จำเป็นที่ทุกคนต้องตระหนักรู้ ติดตามให้ทันความแปรเปลี่ยนที่เกิดขึ้นอย่างฉับพลัน เพื่อศึกษาวิเคราะห์ให้เห็นชัดถึงผลกระทบที่เกิดขึ้นต่อตนเองและส่วนรวม นำมาพิจารณากำหนดแนวทางตั้งรับ ปรับวิธีคิดและการประพฤติปฏิบัติต่าง ๆ ให้เป็นไปในทางที่สอดคล้องกับความเป็นไปในยุค ๔.๐ นี้



ที่มา : <https://www.transtimenews.co/3325/>

คำว่า ยุค ๔.๐ ในที่นี้ หมายถึง ยุคของการปฏิวัติอุตสาหกรรม ครั้งที่ ๔ ซึ่งเริ่มในราวยี่สิบกว่าปีที่ผ่านมา การเชื่อมต่อกันเป็น Cyber Physical System ระหว่างเทคโนโลยีด้านการสื่อสารและคอมพิวเตอร์ ทำให้มนุษย์สามารถติดต่อกันได้ทุกที่ทุกเวลาแทบจะไม่มีข้อจำกัด ในสารพัดรูปแบบของสารที่รับ-ส่งถึงกัน ทั้งเสียง ข้อความ ภาพนิ่งและภาพยนตร์ ด้วยอัตราความเร็วที่สูงมากอย่างไม่น่าเชื่อ โดยผ่าน Smart Phone ที่มีขนาดเพียงอุ้งมือเรา การค้นคว้าหาความรู้จากแหล่งต่าง ๆ ทั่วโลกก็สามารถทำได้ทำนองเดียวกัน

ความเปลี่ยนแปลงเช่นนี้มีส่วนหล่อหลอมนิสัยใจคอและพฤติกรรมของคนที่เกิดในยุค ๔.๐ (ราว พ.ศ.๒๕๔๐ เป็นต้นมา) หรือที่เรียกว่า Gen Z มีความผิดแผกจากคนรุ่นก่อน ๆ (Gen X และ Gen Y) อย่างมีนัยสำคัญ เช่น มีความอดทนต่ำในการคิดและทำเรื่องที่ตนไม่สนใจ ใช้ความพอใจเป็นเกณฑ์ตัดสินในการเลือกวิถีชีวิตตน ไม่ว่าจะเป็นเรื่องการศึกษาหาความรู้ และการประกอบอาชีพ ไม่ให้คุณค่ากับปริญญาบัตรและความนิยมยกย่องจากคนในสังคมมากเช่นในอดีต พอใจที่จะทำงานอิสระมากกว่าการเป็นมนุษย์เงินเดือน พร้อมทั้งจะเปลี่ยนอาชีพเมื่อรู้สึกว่ามีใจ คน Gen Z จำนวนไม่น้อยเลือกที่จะทำหลายอาชีพในเวลาเดียวกัน ซึ่งมีทั้งผู้ที่ประสบความสำเร็จอย่างสูงตั้งแต่อายุน้อย และพวกที่ค้นหาทางใหม่แบบลองถูกลองผิดไปเรื่อย ๆ ในด้านการสร้างครอบครัวนั้น คน Gen Z รวมทั้ง Gen Y (เกิดระหว่างราว พ.ศ. ๒๕๒๑ - ๒๕๓๙) ช่วงปลาย ๆ ไม่จริงจังเรื่องการมีคู่ครองเมื่อถึงวัยอันควร ไม่กังวลใจนักถ้าจะต้องครองโสดไปตลอดชีวิต การแต่งงานมิใช่เรื่องสำคัญมากสำหรับพวกเขา พอใจที่จะอยู่กินกันโดยไม่ต้องมีพิธีทองอะไรก็มีอยู่ไม่น้อย แม้มีคู่ครองแล้วก็เลือกที่จะไม่มีบุตรกันเป็นจำนวนมาก

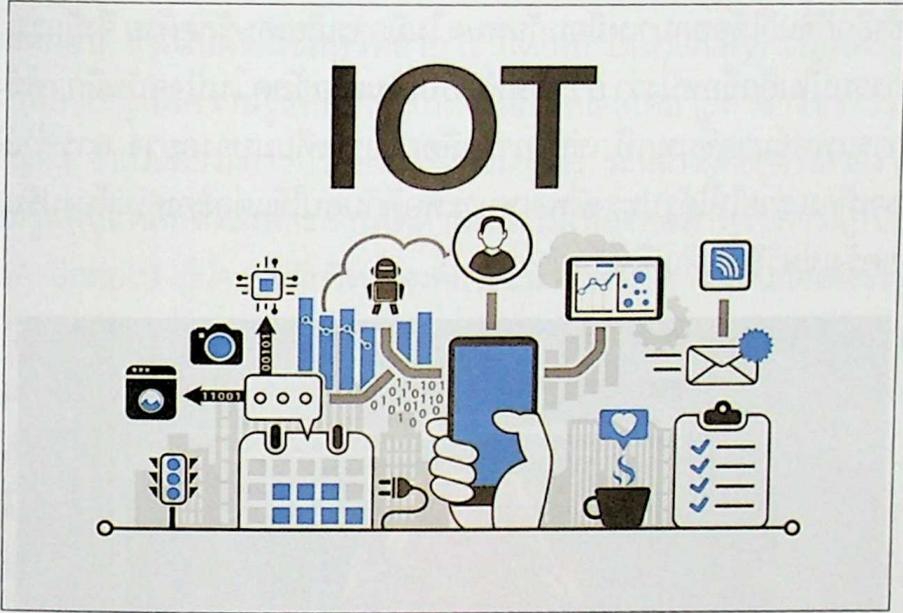
พฤติกรรมของคนในยุค ๔.๐ ที่เปลี่ยนแปลงไปดังที่ยกตัวอย่างข้างต้น จำเป็นอย่างยิ่งที่ผู้นำและผู้บริหารองค์กรต่าง ๆ ต้องตระหนักรู้อย่างละเอียดชัดเจน นำมาปรับพื้นฐานความคิดและจิตใจ (Mind Set) ของตน ให้สอดคล้องกับนิสัยใจคอของคนในยุคปัจจุบันและอนาคต ด้วยการเปิดใจกว้างยอมรับความแตกต่างให้ได้มากยิ่งขึ้น เพื่อให้สามารถปกครองดูแลและใช้งานพวกเขาได้อย่างมีประสิทธิภาพและประสิทธิผลสูง รวมทั้งการพัฒนาศักยภาพด้านต่าง ๆ ให้แก่เขาในแนวทางที่ถูกต้องด้วย

เรื่องที่เราควรรู้เกี่ยวกับนิสัยใจคอของคนยุค ๔.๐ นี้ อีกประการหนึ่งก็คือ พวกเขามีความผูกพัน (Engagement) และความภักดี (Loyalty) ต่อบริษัท ไม่มากเท่ากับคนรุ่นก่อน ๆ นับเป็นปัญหาสำคัญขององค์กรภาครัฐ ที่พยายามสรรหาและรักษาคนเก่งคนดีไว้ในระบบราชการ ซึ่งกำลังพัฒนาให้มีความทันสมัย นำเทคโนโลยียุค ๔.๐ เข้ามาใช้ในการบริหารงานมากขึ้นทุกขณะ หากผู้มีอำนาจหน้าที่ในการพัฒนาทรัพยากรมนุษย์ (Human Resource Development) มีความเข้าใจไม่ดีพอในเรื่องดังกล่าว คงยากที่จะประสบความสำเร็จตามเป้าหมายที่ตั้งใจไว้ เมื่อไม่สามารถสรรหาและรักษาคนดีคนเก่งไว้ได้มากเท่าที่ควร การพัฒนาด้านองค์ความรู้และระบบการบริหารจัดการต่าง ๆ ภายในองค์กรด้วยเทคโนโลยีสมัยใหม่ก็ย่อมต้อยค่าลง มีความสูญเปล่าเกิดขึ้นอย่างน่าเสียดายยิ่ง

เกี่ยวกับนวัตกรรมยุค ๔.๐ ที่ได้กล่าวถึงในตอนต้น นับเป็นเรื่องที่ผู้นำยุคใหม่ควรมีความรู้พอประมาณด้วยเช่นกัน ไม่จำเป็นต้องลึกซึ้งทางเทคนิคมากมายนัก นอกจากผู้ที่มีพื้นฐานเพียงพออยู่ก่อน รู้เพียงหลักการของระบบ และลักษณะการใช้ประโยชน์จากสิ่งเหล่านั้นในภาพกว้างก็น่าจะเพียงพอแล้ว หากต้องการความรู้ในเชิงลึกก็สามารถศึกษาค้นคว้าและไต่ถามผู้ที่มีความรอบรู้ในแต่ละเรื่องได้ จึงใคร่ขอขยายความโดยสังเขปในผลผลิตจากเทคโนโลยียุค ๔.๐ บางส่วน ดังต่อไปนี้

AI หรือปัญญาประดิษฐ์ ได้รับการพัฒนาต่อยอดมาจาก หุ่นยนต์ (Robot) ซึ่งในอดีตถูกใช้ในโรงงาน เพื่อทำหน้าที่แทนคนในเรื่องที่มีลักษณะไม่ซับซ้อนมากนัก แต่มีการทำซ้ำ ๆ ให้เกิดผลผลิตจำนวนมากในเวลาสั้น ๆ หากใช้แรงงานคนตามปกติก็จะทำได้ช้ากว่าและมีโอกาสผิดพลาดสูง จึงใช้ระบบอัตโนมัติในรูปของหุ่นยนต์เข้าทำแทน แต่ปัญญาประดิษฐ์หรือ AI ในปัจจุบันมีรูปแบบที่ผิดแผกไปมาก รวมทั้งประโยชน์ทางการใช้งานที่หลากหลายด้วย เช่น การเป็นพนักงานต้อนรับตามสถานบริการบางประเภท การเป็นผู้ประกาศข่าวงานด้านการแพทย์ ทั้งการดูแลผู้ป่วยในบางลักษณะและการผ่าตัด แม้กระทั่งการแข่งขันหมากรุกหมากล้อมกับผู้เล่นระดับแชมป์โลก ก็สามารถเอาชนะอย่างเด็ดขาดมาแล้ว ทั้งนี้เพราะ AI ในปัจจุบันได้รับการป้อนข้อมูลและโปรแกรมในการคิดอย่างละเอียด จึงมีความสามารถสูงกว่าคนเก่งเพียงคนเดียว ซึ่งมีวิธีคิดที่ไม่ว่างขวางลึกซึ้งเท่า AI

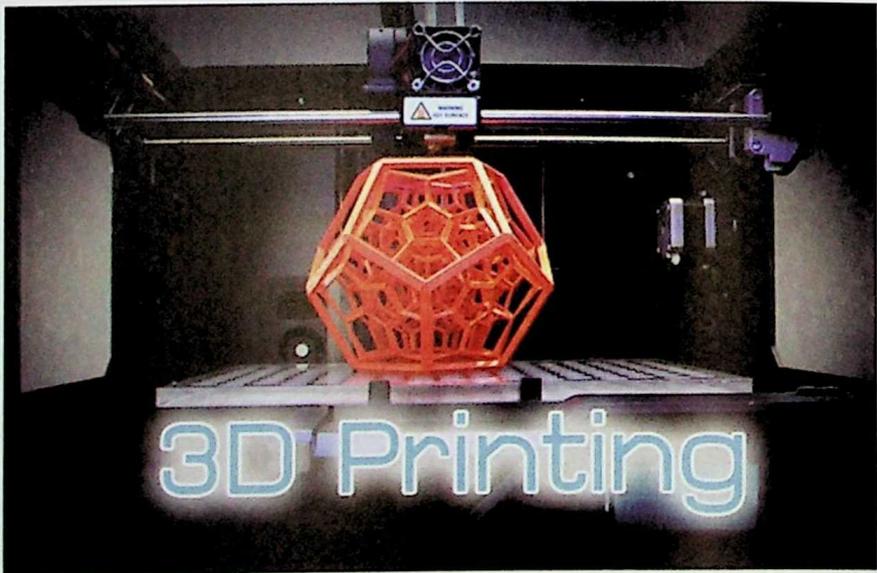
IoT หรืออินเทอร์เน็ตแห่งสรรพสิ่ง คือตัวอย่างที่เห็นได้ชัดเจนของความเป็น Cyber Physical System คือการใช้สัญญาณดิจิทัลผ่านระบบคอมพิวเตอร์และอินเทอร์เน็ต ไปบังคับควบคุมระบบหรืออุปกรณ์อื่นให้ทำงานตามที่ต้องการ เช่น การเปิดปิดระบบปรับอากาศหรือไฟฟ้าแสงสว่างภายในบ้านในระยะไกล โดยใช้การควบคุมด้วย Smart Phone และการควบคุม Drone รวมทั้งยานไร้คนขับอื่น ๆ ผ่านทางระบบคอมพิวเตอร์และอินเทอร์เน็ต



ที่มา : <https://www.allmobilerobotics.com/category/9/internet-of-things-iot>

Drone ในอดีตย้อนหลังไปไม่นานนัก มีการใช้งานในวงแคบกว่าปัจจุบัน ส่วนใหญ่ใช้ในการถ่ายภาพมุมสูงเพื่อเสริมงานด้านสื่อสารมวลชนและการสอดแนมทางทหาร แต่ทุกวันนี้ Drone มีบทบาทกว้างขวางขึ้นมาก เช่น ใช้ในการติดตามคนร้าย ช่วยเหลืองานดับไฟป่า ส่งคนและของในลักษณะของแท็กซี่อากาศ รวมทั้งการก่อวินาศกรรม ดังที่เกิดขึ้นในปีที่ผ่านมา การทิ้งระเบิดทำลายโรงกลั่นน้ำมันขนาดใหญ่ของประเทศซาอุดีอาระเบียและการสังหารนายพล Kasem Sulaimani ผู้บัญชาการกองกำลังคุดส์ (Quds Force) แห่งกองกำลังพิทักษ์การปฏิวัติอิสลามของอิหร่านก็ใช้ Drone เป็นอาวุธ สามารถบินหลบหลีกการตรวจจับของระบบการป้องกันภัยทางอากาศที่ทันสมัยเข้าทำลายเป้าหมายได้อย่างน่าอัศจรรย์ทีเดียว

3D-Printing หรือการพิมพ์สามมิติ คือการใช้ Computer Graphic ออกแบบรูปทรงที่ต้องการ อาจเป็นชิ้นส่วนเล็ก ๆ ของอัญมณี หรือส่วนประกอบงานก่อสร้างขนาดใหญ่ก็ได้ แล้วส่งสัญญาณภาพผ่านอินเทอร์เน็ตไปควบคุมระบบการผลิต ซึ่งมีการเตรียมวัสดุที่ต้องการใช้ล่วงหน้าไว้แล้ว เมื่อสั่งเริ่มการผลิต ทุกอย่างก็ดำเนินไปตามโปรแกรมที่กำหนด วัสดุแต่ละชนิดจะถูกเติมจนเต็มตามแบบที่เขียนไว้ในคอมพิวเตอร์ ผลผลิตที่ได้มีความสมบูรณ์ทุกส่วนผลิตซ้ำอีกกี่ชิ้นก็ได้ออกมาเหมือนกันหมด ไม่มีการเสียเศษวัสดุด้วย จึงมีการเรียกนวัตกรรมนี้ในอีกชื่อหนึ่งว่า การพิมพ์แบบเติมเนื้อวัสดุ ในปัจจุบันมีการใช้งานทางการแพทย์มากขึ้นทุกที เช่น การผลิตอวัยวะเทียมบางอย่าง การทำเฝือกและขาเทียม ช่วยให้ผู้ป่วยที่พอเหมาะพอดีกับคนไข้แต่ละคน ไม่ต้องปรับแต่งหลายครั้งเช่นวิธีดั้งเดิมที่ใช้กันมา



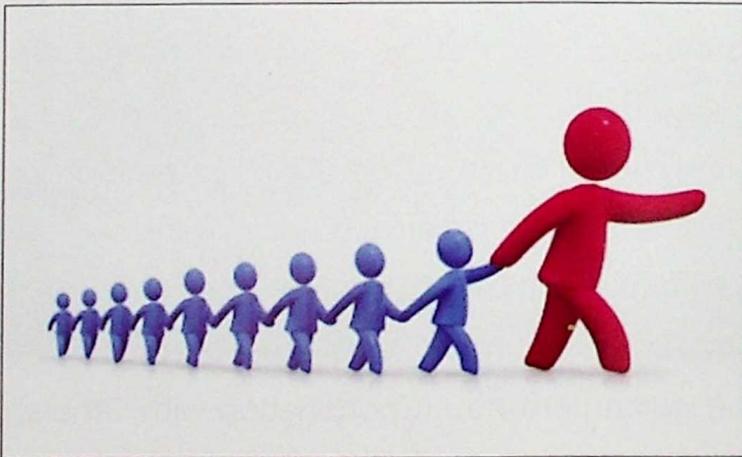
ที่มา : <https://www.smile-digital.com/blog/3d-printing/>

Financial Technology หรือ Fin Tech คืออีกนวัตกรรมหนึ่งซึ่งคนทั่วไปในปัจจุบันคุ้นเคยกันดี ธุรกิจทางการเงินหลายประเภทสามารถทำผ่าน Smart Phone ได้ เช่น การโอนเงินและการชำระค่าบริการต่าง ๆ ไม่จำเป็นต้องไปพบพนักงานที่สถาบันการเงินเช่นแต่ก่อน

อีกประการหนึ่งที่ผู้นำยุค ๔.๐ ควรรู้จักคือ ลักษณะของปัญหาที่เกิดขึ้นในปัจจุบันและอนาคต มีความผิดแผกแตกต่างไปจากสภาพเดิม ๆ มาก กล่าวคือ มีความผันผวน (Volatility) ความไม่แน่นอน (Uncertainty) ความซับซ้อน (Complexity) และความคลุมเครือกำกวม (Ambiguity) สูงกว่าที่เคยเป็นมา มีผู้สรุปเป็นคำย่อว่า VUCA เป็นผลให้การวิเคราะห์/สังเคราะห์ปัญหาเพื่อหาหนทางแก้ไขที่ดีที่สุดไม่อาจใช้หลักคิดหรือทฤษฎีเดิม ๆ ให้ได้ผลดีเช่นแต่ก่อน จำเป็นต้องใช้สหวิทยาการ (Multi Disiplinary) เป็นเครื่องมือ กล่าวคือ ใช้ผู้ที่มีความรู้และประสบการณ์ในหลากหลายสาขาวิชา ร่วมกันแก้ปัญหา จำเป็นต้องมีการปรึกษาหารือกันมากขึ้น ระหว่างผู้ที่อยู่ต่างสายงานกัน ความรู้แคบแต่ลึกซึ่งเฉพาะด้านใดด้านหนึ่งไม่เพียงพอสำหรับการแก้ปัญหา VUCA อีกต่อไป ผู้นำและผู้บริหารองค์กรในระดับต่าง ๆ จำเป็นต้องตระหนักรู้ในความจริงเช่นนี้ ความสัมพันธ์ที่ดีระหว่างคนในองค์กร ไม่ว่าจะอยู่ฝ่ายหรือแผนกใดก็ตามมีความสำคัญยิ่ง ช่วยให้การประสานงานหรือร่วมกันแก้ปัญหาของส่วนรวมมีความราบรื่น เพื่อเป็นแนวทางในการแก้ปัญหาที่มีลักษณะ VUCA ให้ได้ผลดี สภาเศรษฐกิจโลก (World Economic Forum: WEF) ได้สรุปความสามารถที่จำเป็นสำหรับคนในยุค ๔.๐ ไว้ ๑๐ ประการ เรียงตามลำดับความสำคัญ ดังต่อไปนี้

- ๑) การแก้ปัญหาซับซ้อน (Complex Problem Solving)
- ๒) การคิดอย่างมีวิจารณ์ญาณ (Critical Thinking)
- ๓) ความคิดสร้างสรรค์ (Creativity)
- ๔) การบริหารจัดการคน (People Management)
- ๕) ความร่วมมือกับผู้อื่น (Coordination with Others)
- ๖) ความฉลาดทางอารมณ์ (Emotional Intelligence)
- ๗) การประเมินและตัดสินใจ (Judgment and Decision Making)
- ๘) การมีจิตมุ่งบริการ (Service Orientation)
- ๙) การเจรจาต่อรอง (Negotiation)
- ๑๐) การวิเคราะห์อย่างยืดหยุ่น (Cognitive Flexibility)

โดยภาพรวมแล้วอาจกล่าวได้ว่า คุณสมบัติสำคัญที่ผู้นำยุค ๔.๐ พึ่งมีได้แก่ การมีคุณลักษณะพื้นฐานทั้ง ๙ ประการ ดังที่กล่าวไว้ในตอนต้น ความรู้ความเข้าใจในนิสัยใจคอและพฤติกรรมของคน Gen Y และ Gen Z ตระหนักรู้ในความเปลี่ยนแปลงแบบพลิกผันและการเกิดนวัตกรรมใหม่ ๆ อยู่ตลอดเวลาจาก Digital Technology และ Internet ด้วยการศึกษาดูตัวอย่างผู้ไม่รู้ไม่เรียนตลอดชีวิต (Life Long Learning) รวมทั้งการพัฒนาตนเองให้มีความสามารถที่จำเป็นสำหรับคนยุค ๔.๐ ปรับเปลี่ยน Mind Set ลดการใช้อำนาจแบบควบคุมสั่งการตามลำดับชั้น เป็นการสร้างเครือข่ายการประสานงานและความร่วมมือจากทุกภาคส่วนในองค์กร เน้นการมีส่วนร่วมอย่างทั่วถึงของคนทุกระดับ เพื่อแก้ปัญหาที่มีลักษณะ VUCA คือ มีความผันผวน (Volatility) ไม่แน่นอน (Uncertainty) ซับซ้อน (Complexity) และคลุมเครือกำกวม (Ambiguity) หากทำได้ครบถ้วนเช่นที่กล่าวแม้จะไม่สมบูรณ์ในทุกส่วน ย่อมมั่นใจได้ในความมีภาวะผู้นำที่เข้มแข็ง เป็นที่ศรัทธาเชื่อถือของผู้ร่วมงานในทุกระดับไม่ว่าจะเป็นคนยุคใดก็ตาม



ที่มา : <https://www.softbankthai.com/Article/Detail/17096>



ผู้นำ

เป็นผู้นำ ทำการใด ให้ยึดหลัก
สร้างความรัก สามัคคี มีถ้วนทั่ว
ถือคลองธรรม นำจิต ไม่คิดกลัว
รังสรรค์ตัว ดีทั่วพร้อม ย่อมยั่งยืน

ใฝ่พากเพียร เรียนรู้ อยู่เสมอ
อย่าละเมอ เผลอไผล จนไหลหลง
รักษศีลสัตย์ ตัดกิเลส เหตุเสื่อมลง
ถือความตรง คงมั่น ทุกวันคืน

จิตพร้อมให้ ใจพร้อมช่วย ด้วยแรงรัก
แม่เหนี่ยวหนัก จักสู้ได้ ไม่สุดฝืน
วันนี้รุ่ง พรุ่งนี้หล่น ทนกล้ากลืน
หลับเต็มตื่น กลับชื่นแจ่ม แจ่มใสพลัน

คตินำคน พันทางต่ำ ทำให้เห็น
ข้ามผ่านทุกข์ พบสุขเย็น เช่นที่ฝัน
รักส่วนรวม ร่วมหล่อหลอม พร้อมเพรียงกัน
เดินตามทาง ที่สร้างสรรค์ นิรันดร

นรชาติ

๑๔ กุมภาพันธ์ ๒๕๖๔

วารสารนาวิกาธิปัตย์สาร

ขอขอบคุณ

คุณหญิงศรีศิริ กฤษณจันทร์

ประธานมูลนิธิกองทุน

พลเรือเอก ประพัฒน์ - คุณหญิง ศรีศิริ กฤษณจันทร์

ผู้ให้การอุปถัมภ์โครงการพัฒนาและปรับปรุง

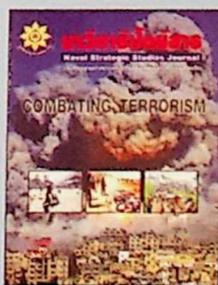
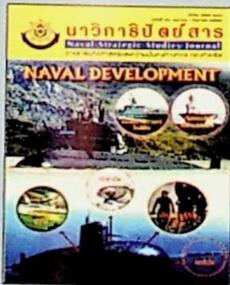
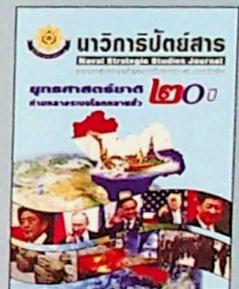
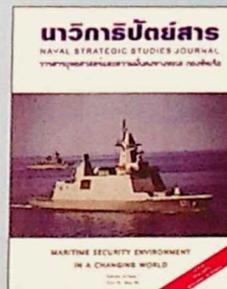
คุณภาพวารสารนาวิกาธิปัตย์สาร





นาวีกาธิปัตย์สาร

กำหนดตีพิมพ์รายหกเดือน ฉบับประจำเดือน ตุลาคม - มีนาคม และ
ฉบับประจำเดือน เมษายน - กันยายน ราคาฉบับละ ๑๒๐ บาท
ค่าสมาชิกรายปี ๒๒๐ บาท (๒ ฉบับ)



ผู้สนใจสมัครเป็นสมาชิกรายปี

- ติดต่อได้ที่ กองบรรณาธิการนาวีกาธิปัตย์สาร

ศูนย์ศึกษายุทธศาสตร์ทหารเรือ กรมยุทธศึกษาทหารเรือ

ต.ศาลายา อ.พุทธมณฑล จ.นครปฐม ๗๓๑๗๐

โทร. ๐ ๒๔๗๕ ๓๔๗๖ , ๐ ๒๔๗๕ ๓๔๕๒ หรือ

www.tnssc.navy.mi.th/journal

- โอนเงินเข้าบัญชีออมทรัพย์ ธนาคารทหารไทยธนชาติ

สาขาพุทธมณฑล เลขที่บัญชี ๐๗๙ - ๒ - ๑๔๓๙๔ - ๓

ชื่อบัญชี นาวีกาธิปัตย์สาร พร้อมทั้งส่งหลักฐานการโอนเงิน

Email : nssc.journal@gmail.com หรือ

โทรสาร ๐ ๒๔๗๕ ๓๔๔๐

