การป้องกันภัยคุกคามด้านไซเบอร์ทางทะเลต่อภัยคุกคามจากการปลอมแปลงและการรบกวนสัญญาณ: กรอบแนวคิดเสนอระบบการตระหนักรู้ทางทะเลแบบบูรณาการหลายมิติทางทะเล

Maritime Cyber Defense against Spoofing and Jamming Threats: Integrated Multi-Domain Maritime Awareness Framework: IMMAF

โดย ร้อยตรี อเนชา เผ่าพานิชย์

บทคัดย่อ

การเปลี่ยนผ่านสู่ยุคดิจิทัลได้ยกระดับประสิทธิภาพของระบบการเดินเรือและการบริหารจัดการทางทะเล ขณะเดียวกันก็เพิ่มความเปราะบางของโครงสร้างพื้นฐานทางทะเลต่อภัยคุกคามด้านไซเบอร์ โดยเฉพาะการปลอมแปลงสัญญาณ (Signal Spoofing) และการรบกวนสัญญาณ (Signal Jamming) ซึ่งส่งผลกระทบต่อความน่าเชื่อถือของระบบกำหนดตำแหน่ง การสื่อสาร และการตระหนักรู้สถานการณ์ทางทะเล อันเป็นปัจจัยสำคัญต่อการรักษาผลประโยชน์ของชาติทางทะเล บทความนี้มีวัตถุประสงค์เพื่อวิเคราะห์ลักษณะ กลไก และผลกระทบของภัยคุกคามจากการปลอมแปลงสัญญาณและการรบกวนสัญญาณภายใต้บริบทความมั่นคงไซเบอร์ทางทะเล โดยใช้การวิเคราะห์เอกสารเชิงยุทธศาสตร์และกฎหมายที่เกี่ยวข้อง ประกอบด้วย UNCLOS 1982 แผนความมั่นคงแห่งชาติทางทะเล พ.ศ.๒๕๖๖ – ๒๕๗๐) และพระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ ผลการวิเคราะห์ชี้ให้เห็นว่าการบูรณาการข้อมูลจากหลายมิติผ่านแนวคิดการตระหนักรู้และรับรู้สถานการณ์แบบหลายมิติ (**Multi-Domain Awareness: MDA**) ร่วมกับการจัดตั้งศูนย์ควบคุมสั่งการไซเบอร์ทางทะเล

Maritime Cyber Command และการพัฒนาระบบ ศูนย์การข่าวไซเบอร์ทางทะเล **Maritime Cyber Intelligence** จะช่วยยกระดับขีดความสามารถในการตรวจจับ ป้องกัน และตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างเป็นระบบ อันนำไปสู่การเสริมสร้างความมั่นคงทางทะเล การคุ้มครองโครงสร้างพื้นฐานที่สำคัญ และการรักษาเสถียรภาพของผลประโยชน์แห่งชาติภายใต้สภาพแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลงอย่างรวดเร็ว

คำสำคัญ ความมั่นคงด้านไซเบอร์ทางทะเล, การปลอมแปลงสัญญาณ, การรบกวนสัญญาณ, การตระหนักรู้หลายมิติ, ยุทธศาสตร์ความมั่นคงทางทะเล

Abstract

The transition to the digital era has significantly enhanced the efficiency of navigational systems and maritime management. At the same time, however, it has increased the vulnerability of maritime infrastructure to cyber threats, particularly signal spoofing and signal jamming. These threats can undermine the reliability and integrity of positioning, navigation, communication, and maritime situational awareness systems, all of which are critical to the protection of national maritime interests.

This article aims to analyze the characteristics, mechanisms, and strategic implications of signal spoofing and signal jamming within the broader context of maritime cybersecurity. The study employs a qualitative documentary analysis of relevant strategic and legal frameworks, including the United Nations Convention on the Law of the Sea 1982, Thailand's National Maritime Security Plan 2023–2027, and the Maritime National Interest Protection Act B.E. 2562 (2019).

The findings indicated that the integration of multidimensional information through a Multi-Domain Awareness framework, together with the establishment of a Maritime Cyber Command and the development of a Maritime Cyber Intelligence system, would significantly strengthen national capabilities to detect, prevent, respond to, and recover from maritime cyber threats in a systematic and coordinated manner. Such measures would enhance maritime security resilience, protect critical maritime infrastructure, and safeguard the continuity and stability of national maritime interests.

The article therefore argues that maritime cybersecurity should be elevated from a predominantly technical concern to a strategic national security priority. An integrated institutional framework, supported by intelligence fusion, interagency coordination, technological capability development, and clearly defined command-and-control mechanisms, is essential for maintaining maritime security and strategic stability amid a rapidly evolving and increasingly complex security environment.

Keywords: Maritime Cybersecurity; Signal Spoofing; Signal Jamming; Multi-Domain Awareness; Maritime Security Strategy

บทนำ (Introduction)

การปฏิวัติเทคโนโลยีดิจิทัลได้เปลี่ยนแปลงรูปแบบการดำเนินกิจกรรมทางทะเลจากการพึ่งพาระบบนำร่องแบบดั้งเดิมที่ใช้มนุษย์และการเดินเรือชายฝั่งอาศัยหลักนำและศาสตร์และศิลป์ของการหาตำบลที่เรือจากที่หนึ่งไปยังอีกที่หนึ่งอย่างปลอดภัยของนักเดินเรือโดยการนำร่อง (เจียม อัมระปาล, ๒๔๙๓) ในยุคที่เทคโนโลยีดิจิทัลเป็นโครงสร้างพื้นฐานสำคัญ

ของกิจกรรมทางทะเล ระบบนำร่อง การสื่อสาร การควบคุมการจราจร และการเฝ้าระวังพื้นที่ทางทะเลต่างพึ่งพาการเชื่อมโยงข้อมูลและสัญญาณอิเล็กทรอนิกส์อย่างต่อเนื่อง ระบบสำคัญ ได้แก่ ระบบระบุอัตโนมัติของเรือ (Automatic Identification System: AIS) ระบบกำหนดตำแหน่งและการนำร่องผ่านดาวเทียม (Global Navigation Satellite System: GNSS) ระบบแผนที่เดินเรืออิเล็กทรอนิกส์และสารสนเทศ (Electronic Chart Display and Information System: ECDIS) และระบบสื่อสารวิทยุทางทะเลย่านความถี่สูงมาก (Very High Frequency: VHF) ระบบดังกล่าวมีบทบาทต่อการสร้างการตระหนักรู้สถานการณ์ทางทะเล (Maritime Situational Awareness: MSA) ซึ่งเป็นพื้นฐานของการเดินเรืออย่างปลอดภัย การควบคุมพื้นที่ทางทะเล การคุ้มครองเส้นทางคมนาคม และการสนับสนุนการตัดสินใจของหน่วยงานด้านความมั่นคง International Maritime Organization (IMO) ได้ผลักดันแนวคิด e-Navigation เพื่อบูรณาการข้อมูลการเดินเรือ การสื่อสาร และการตัดสินใจของผู้ควบคุมเรือ (Master) ทำให้ระบบ Positioning, Navigation and Timing (PNT) กลายเป็นโครงสร้างพื้นฐานสำคัญของการเดินเรือสมัยใหม่ แต่ในขณะเดียวกันก็เพิ่มพื้นผิวการโจมตี (Attack Surface) ของระบบทางทะเล IMO (2021) และ International Association of Marine Aids to Navigation and Lighthouse Authorities (สมาคมระหว่างประเทศด้านอุปกรณ์ช่วยการเดินเรือและประภาคาร) IALA (2023) (กรมอุทกศาสตร์ กองทัพเรือ, ๒๕๕๗; กองทัพเรือ, ๒๕๔๑; International Maritime Organization [IMO], 2021) อย่างไรก็ตาม การเพิ่มขึ้นของการพึ่งพาเทคโนโลยีดังกล่าวได้สร้างความเปราะบางของโครงสร้างพื้นฐานทางทะเลต่อภัยคุกคามไซเบอร์ โดยเฉพาะการปลอมแปลงสัญญาณ (Signal Spoofing) และการรบกวนสัญญาณ (Signal Jamming) ซึ่งสามารถบิดเบือนข้อมูลตำแหน่ง ขัดขวางการสื่อสาร และลดทอนประสิทธิภาพของระบบบัญชาการและควบคุม

(Command and Control: C2) ตลอดจนส่งผลกระทบต่อการรับรู้สถานการณ์ทางทะเลในระดับยุทธวิธี ยุทธการ และยุทธศาสตร์ (U.S. Department of Defense, 2020, IMO, 2021) ในเชิงยุทธศาสตร์ ความถูกต้อง ความต่อเนื่อง และความน่าเชื่อถือของข้อมูลทางทะเลจึงมิใช่เพียงเงื่อนไขทางเทคนิค แต่เป็นองค์ประกอบของขีดความสามารถของรัฐในการรับรู้ ตัดสินใจ และใช้อำนาจทางทะเลอย่างมีประสิทธิภาพ

สำหรับประเทศไทย ซึ่งมีพื้นที่ทางทะเลคิดเป็นสัดส่วนสำคัญของเศรษฐกิจ การค้าระหว่างประเทศ และความมั่นคงแห่งชาติ การรักษาความมั่นคงของโครงสร้างพื้นฐานดิจิทัลทางทะเลจึงมิใช่เพียงประเด็นด้านเทคนิค หากแต่เป็นองค์ประกอบสำคัญของการคุ้มครองผลประโยชน์ของชาติทางทะเลตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐ มาตรา ๕๒ และพระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ จากมุมมองเชิงยุทธศาสตร์ ภัยคุกคามไซเบอร์ทางทะเลมิได้เป็นเพียงความเสี่ยงต่อระบบสารสนเทศ แต่เป็นความท้าทายต่อขีดความสามารถของรัฐในการรักษาอำนาจทางทะเล การคุ้มครองโครงสร้างพื้นฐานที่สำคัญ และการธำรงเสถียรภาพของผลประโยชน์แห่งชาติในสภาพแวดล้อมด้านความมั่นคงที่มีความซับซ้อนมากขึ้น

บทความนี้ใช้การวิเคราะห์เอกสารเชิงคุณภาพ โดยสังเคราะห์ข้อมูลจากกฎหมาย นโยบายความมั่นคงทางทะเล แนวทางการบริหารความเสี่ยงไซเบอร์ และเอกสารวิชาการที่เกี่ยวข้อง ประกอบกับข้อมูลจากผู้ปฏิบัติงานด้านการเดินเรือ เพื่อเปรียบเทียบลักษณะ กลไก ผลกระทบ และมาตรการตอบสนองต่อการปลอมแปลงและการรบกวนสัญญาณในระดับเทคนิค ระดับปฏิบัติการ และระดับยุทธศาสตร์

ภูมิทัศน์ภัยคุกคามไซเบอร์ทางทะเล (Maritime Cyber Threat Landscape)

การพึ่งพาเครือข่ายดิจิทัลและระบบอัตโนมัติทำให้ระบบทางทะเล

มีลักษณะเป็นระบบเชื่อมโยงระหว่างเทคโนโลยีสารสนเทศ เทคโนโลยีปฏิบัติการ ระบบสื่อสาร และอุปกรณ์นำร่อง ความเสียหายที่เกิดขึ้นในระบบหนึ่งจึงสามารถส่งผลกระทบต่อระบบอื่นเป็นลูกโซ่ ตั้งแต่ระดับเรือ ท่าเรือ ศูนย์ควบคุม ไปจนถึงระบบโลจิสติกส์และห่วงโซ่อุปทาน ภัยคุกคามไซเบอร์ทางทะเลจึงควรถูกพิจารณาในฐานะภัยคุกคามเชิงยุทธศาสตร์ (Strategic Threat) มากกว่าปัญหาทางเทคนิค เนื่องจากสามารถลดทอนขีดความสามารถของรัฐในการควบคุมพื้นที่ทางทะเลและคุ้มครองผลประโยชน์แห่งชาติได้อย่างมีนัยสำคัญ ด้วยแนวคิดด้านความมั่นคงทางทะเลร่วมสมัยได้เปลี่ยนจากการมุ่งเน้นภัยคุกคามทางทหารแบบดั้งเดิมไปสู่ภัยคุกคามแบบผสมผสาน (Hybrid Threats) ซึ่งผสานการโจมตีทางไซเบอร์ สงครามอิเล็กทรอนิกส์ การบิดเบือนข้อมูล และการปฏิบัติการข่าวสารเข้าด้วยกัน (NATO, 2023; Tam & Jones, 2019)

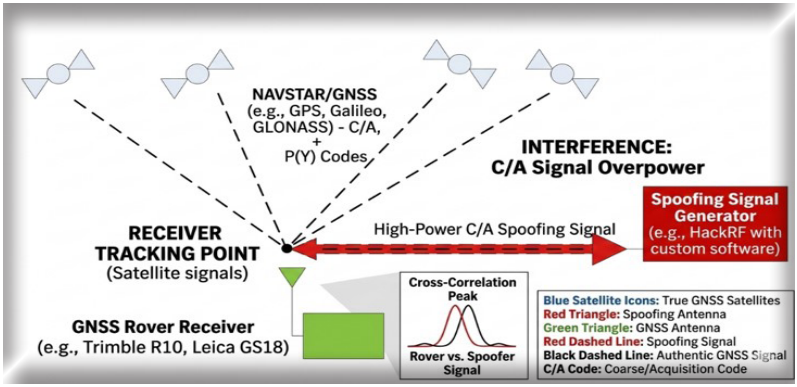
ในบริบทดังกล่าว ระบบนำร่องและระบบสื่อสารทางทะเลได้กลายเป็นเป้าหมายสำคัญของการโจมตี เนื่องจากเป็นโครงสร้างพื้นฐานที่สนับสนุนการสร้าง Maritime Common Operational Picture (MCOP) และการตัดสินใจของหน่วยงานด้านความมั่นคง การโจมตีต่อระบบเหล่านี้จึงส่งผลกระทบโดยตรงต่อความสามารถในการเฝ้าระวัง การข่าวกรอง และการบัญชาการควบคุมของรัฐ

ตัวแสดงที่ก่อภัยคุกคามมีเป้าหมายแตกต่างกัน โดยตัวแสดงที่มิใช่รัฐอาจมุ่งแสวงหาผลประโยชน์ทางเศรษฐกิจ ปกปิดกิจกรรมผิดกฎหมาย หรือสร้างความเสียหายต่อระบบ ขณะที่ตัวแสดงที่เป็นรัฐอาจใช้การปลอมแปลงและการรบกวนสัญญาณเป็นเครื่องมือในการปฏิบัติการพื้นที่สีเทา การข่าวกรอง สงครามอิเล็กทรอนิกส์ หรือการเตรียมสภาพแวดล้อมก่อนเกิดความขัดแย้ง ด้วยเหตุนี้ การวิเคราะห์ภัยคุกคามจึงต้องพิจารณาทั้งขีดความสามารถ เจตนา รูปแบบพฤติกรรม และบริบททางภูมิรัฐศาสตร์ควบคู่กันไป ความคลุมเครือในการระบุตัวผู้กระทำทำให้ภัยคุกคามลักษณะนี้มีคุณค่าทางยุทธศาสตร์ต่อฝ่ายโจมตี เพราะสามารถสร้างผลกระทบได้โดยลดความเสี่ยงจากการถูกตอบโต้โดยตรง

การปลอมแปลงสัญญาณในระบบทางทะเล (Signal Spoofing in Maritime Systems)

จากข้อมูลของกัปตันเรือพาณิชย์ในกองเรือของผู้เขียนสะท้อนว่า การปลอมแปลงสัญญาณ GNSS มิได้ส่งผลเฉพาะต่อตำบลที่เรือ แต่สามารถกระทบต่ออุปกรณ์ที่รับข้อมูลตำแหน่งและเวลาอ้างอิงจากระบบเดียวกัน เช่น ECDIS ระบบ AIS ระบบถือท้ายอัตโนมัติ และอุปกรณ์สื่อสารหรือบันทึกข้อมูลอื่นที่เชื่อมโยงกับ GNSS (กัปตันเรือพาณิชย์, การสื่อสารส่วนบุคคล, ๒๑ มกราคม ๒๕๖๙) ผลกระทบจึงอาจเกิดในลักษณะเชื่อมโยงระหว่างหลายระบบ มากกว่าจะจำกัดอยู่ที่เครื่องรับสัญญาณเพียงอุปกรณ์เดียว

ในเชิงยุทธศาสตร์ การปลอมแปลงสัญญาณเป็นการโจมตีต่อ “ความจริงที่ระบบใช้ตัดสินใจ” เพราะแม้หน่วยงานยังสามารถสื่อสารและปฏิบัติการได้ แต่การตัดสินใจนั้นอาจตั้งอยู่บนข้อมูลที่ถูกบิดเบือน ส่งผลให้ฝ่ายโจมตีสามารถชี้นำการรับรู้และพฤติกรรมของฝ่ายตรงข้ามโดยไม่จำเป็นต้องทำลายระบบโดยตรง



รูปที่ ๑ การจำลองผลกระทบของการปลอมแปลงสัญญาณต่อเครื่องรับ GNSS บนเรือพาณิชย์ แผนภาพแสดงกรณีที่แหล่งกำเนิดสัญญาณปลอมส่งข้อมูลตำแหน่งหรือเวลาอ้างอิงที่มีลักษณะใกล้เคียงกับสัญญาณจริง ทำให้เครื่องรับ GNSS ประมวลผลข้อมูลคลาดเคลื่อน ผลกระทบอาจส่งต่อไปยัง ECDIS, AIS และระบบอื่นที่ใช้ข้อมูลตำแหน่งร่วมกัน

ที่มา: สังเคราะห์และจัดทำโดยผู้เขียนด้วยเทคโนโลยีปัญญาประดิษฐ์ DALL-E ผ่าน ChatGGPT (OpenAI,2026)

การปลอมแปลงสัญญาณ (Signal Spoofing)

Signal Spoofing เป็นการสร้างหรือดัดแปลงสัญญาณให้เครื่องรับเชื่อว่าข้อมูลปลอมเป็นข้อมูลจริง ส่งผลให้ระบบ GNSS, AIS และ ECDIS แสดงตำแหน่งเรือคลาดเคลื่อนจากความเป็นจริง (ETSI, 2020; IMO, 2022) ผลกระทบมิได้จำกัดอยู่เพียงความผิดพลาดในการเดินเรือ แต่ยังส่งผลต่อการสร้าง Maritime Operating Picture และการวิเคราะห์ข่าวกรอง ซึ่งอาจนำไปสู่การตัดสินใจเชิงยุทธศาสตร์ที่คลาดเคลื่อน

การปลอมแปลงสัญญาณจึงเป็นการโจมตีต่อ “ความน่าเชื่อถือของข้อมูล” (Integrity of Information) ซึ่งถือเป็นศูนย์กลางของการตัดสินใจด้านความมั่นคงทางทะเลในยุคดิจิทัล

การรบกวนสัญญาณในระบบทางทะเล (Signal Jamming in Maritime Systems)

การรบกวนสัญญาณ (Signal Jamming)

เนื่องจากระบบ GNSS ให้ข้อมูลทั้งตำแหน่ง การนำร่อง และเวลา หรือ Positioning, Navigation and Timing: PNT การรบกวนสัญญาณจึงอาจส่งผลมากกว่าการสูญเสียตำบลที่เรือ โดยอาจกระทบต่อการเทียบเวลา การบันทึกข้อมูล การประสานระบบสื่อสาร และอุปกรณ์ที่ต้องใช้เวลาอ้างอิงร่วมกัน ความเสี่ยงจึงมีลักษณะเป็นผลกระทบต่อระบบเครือข่ายมากกว่าความขัดข้องของอุปกรณ์นำร่องเพียงจุดเดียว

Signal Jamming มีวัตถุประสงค์เพื่อทำให้ระบบสื่อสารและระบบนำร่องไม่สามารถใช้งานได้ โดยการปล่อยคลื่นรบกวนในย่านความถี่เดียวกัน ส่งผลให้การสื่อสาร การนำร่อง และการประสานการปฏิบัติการของกำลังทางเรือหยุดชะงัก (Mukherji & Chandele, n.d.; SGM, 2020)

แม้ Signal Jamming จะไม่บิดเบือนข้อมูลเหมือน Signal Spoofing แต่ผลกระทบต่อความต่อเนื่องของการบัญชาการและควบคุมอาจรุนแรงกว่าในสถานการณ์วิกฤติ เนื่องจากทำให้หน่วยปฏิบัติการสูญเสียความ

สามารถในการติดต่อสื่อสารและประสานงานและติดตามภาพสถานการณ์โดยรวมในการเฝ้าระวังและตระหนักถึงภัยความมั่นคงทางทางทะเล

เมื่อพิจารณาตามหลักการบริหารความเสี่ยงไซเบอร์ ภัยคุกคามทั้งสองรูปแบบมีเป้าหมายแตกต่างกัน กล่าวคือ การปลอมแปลงสัญญาณมุ่งทำลายความสมบูรณ์และความน่าเชื่อถือของข้อมูล (Integrity) โดยทำให้ระบบรับข้อมูลที่ผิดพลาดเสมือนเป็นข้อมูลจริง ขณะที่การรบกวนสัญญาณมุ่งลดทอนความพร้อมใช้ของระบบ (Availability) โดยทำให้เครื่องรับไม่สามารถเข้าถึงหรือประมวลผลสัญญาณที่จำเป็นได้ ความแตกต่างดังกล่าวมีนัยสำคัญต่อการออกแบบมาตรการป้องกัน เนื่องจากระบบที่ “ยังทำงานแต่ให้ข้อมูลผิด” อาจสร้างความเสี่ยงเชิงยุทธศาสตร์มากกว่าระบบที่หยุดทำงานอย่างชัดเจน (IMO, 2021; Tam & Jones, 2019)

ดังนั้น การรับมือกับภัยคุกคามไซเบอร์ทางทะเลจึงต้องครอบคลุมทั้งการพิสูจน์ความถูกต้องของข้อมูลและการรักษาความต่อเนื่องของระบบ ไม่ใช่มุ่งเพียงการป้องกันการหยุดชะงักของอุปกรณ์เท่านั้น

ในระดับปฏิบัติการเดินเรือ การเสริมสร้างความยืดหยุ่นด้านการเดินเรือ (Navigational Resilience) จำเป็นต้องรักษาขีดความสามารถในการใช้วิธีหาตำบลที่เรือที่เป็นอิสระจากระบบดาวเทียม เช่น การใช้เรดาร์และวัตถุชายฝั่ง การตรวจสอบตำบลที่ด้วยแผนที่เดินเรือ การเดินเรือดาราศาสตร์ และการใช้วิธีการเดินเรือชายฝั่ง ทั้งนี้เพื่อให้เรือสามารถดำรงความปลอดภัยและความต่อเนื่องของภารกิจได้เมื่อข้อมูลจาก GNSS เกิดความผิดปกติหรือไม่น่าเชื่อถือ

มาตรการรับมือควรใช้หลักความหลากหลายและความเป็นอิสระของระบบสำรอง ได้แก่ การมีช่องทางสื่อสารหลายรูปแบบ การใช้ระบบนำร่องด้วยการหาที่เรือชายฝั่ง การตรวจสอบตำบลที่ด้วยเรดาร์และวัตถุชายฝั่ง การบริหารคลื่นความถี่ การตรวจจับแหล่งกำเนิดสัญญาณรบกวน ตลอดจนการกำหนดขั้นตอนปฏิบัติเมื่อสูญเสียข้อมูล **Positioning, Navigation and Timing** (PNT) ระบบ ECDIS, AIS, GMDSS, VDR,

Radar Tracking และระบบ Autopilot ต่างใช้ข้อมูลเวลาและตำแหน่งจาก GNSS ร่วมกัน ดังนั้นการโจมตี PNT จึงมีผลกระทบแบบ Cascading Effect ต่อระบบเรือทั้งหมดทั้งนี้ ระบบสำรองต้องไม่พึ่งพาแหล่งข้อมูลหรือโครงสร้างพื้นฐานเดียวกับระบบหลัก

หากการปลอมแปลงสัญญาณทำลายความน่าเชื่อถือของข้อมูล การรบกวนสัญญาณย่อมทำลายความต่อเนื่องของการปฏิบัติการ ดังนั้นความพร้อมรบและความปลอดภัยทางทะเลจึงขึ้นอยู่กับความสามารถของหน่วยงานในการดำรงภารกิจภายใต้สภาวะที่ข้อมูลและการสื่อสารไม่สมบูรณ์

ความสัมพันธ์กับ Signal Spoofing และ Signal Jamming

ประเด็น	Signal Spoofing การปลอมแปลงสัญญาณ	Signal Jamming การรบกวนสัญญาณ
Positioning	ตำแหน่งผิด	ไม่ทราบตำแหน่ง
Navigation	นำร่องผิดเส้นทาง	ไม่สามารถนำร่องได้
Timing	เวลาอ้างอิงผิด	สูญเสียเวลาอ้างอิง
ผลกระทบ	ระบบทำงานแต่ข้อมูลผิด	ระบบไม่สามารถใช้งานได้

ตารางที่ ๑ ความสัมพันธ์กับ การปลอมแปลงสัญญาณSignal Spoofing และ การรบกวนสัญญาณSignal Jamming

ความแตกต่างดังกล่าวสะท้อนให้เห็นว่า Signal Spoofing มีผลกระทบต่อ Information Integrity ขณะที่ Signal Jamming ส่งผลต่อ System Availability ซึ่งสอดคล้องกับหลักการ CIA Triad ของความมั่นคงปลอดภัยสารสนเทศ (NIST, 2024)

ภัยคุกคามจาก GNSS Jamming และ Spoofing ต่อการเดินเรือ

ระบบดาวเทียมนำทางโลก (GNSS) เป็นโครงสร้างพื้นฐานสำคัญ

ของการเดินเรือสมัยใหม่ แต่กำลังเผชิญภัยคุกคามจาก **การรบกวนสัญญาณ (Jamming)** และ **การปลอมแปลงสัญญาณ (Spoofing)** โดยเฉพาะในพื้นที่ความขัดแย้งทางภูมิรัฐศาสตร์ ซึ่งอาจทำให้เรือสูญเสียตำแหน่งหรือได้รับข้อมูลพิกัดที่ผิดพลาด ส่งผลต่อความปลอดภัยของการเดินเรือและการตัดสินใจของเจ้าหน้าที่ประจำเรือ

Jamming คือการส่งคลื่นรบกวนเพื่อปิดกั้นสัญญาณดาวเทียม ทำให้ระบบไม่สามารถระบุตำแหน่งได้ ส่วน **Spoofing** เป็นการส่งสัญญาณเท็จหลอกให้ระบบคำนวณตำแหน่งผิด โดยผู้ปฏิบัติงานอาจไม่ทราบว่าข้อมูลที่ได้รับเป็นข้อมูลปลอม จึงมีความอันตรายมากกว่า

หลักการสำคัญในการลดความเสี่ยงคือ **ไม่พึ่งพา GNSS เพียงแหล่งเดียว** แต่ต้องตรวจสอบตำแหน่งเรือด้วยวิธีอื่นร่วมกัน เช่น Radar, Visual Navigation, Physical Aids to Navigation, Depth Sounder และ Dead Reckoning (DR) พร้อมเฝ้าระวังสัญญาณผิดปกติ เช่น ค่า HDOP สูง ระบบ RAIM แจ้งเตือน หรือข้อมูลตำแหน่งไม่สอดคล้องกับสภาพจริง

กรณีศึกษาจริงสะท้อนให้เห็นผลกระทบอย่างชัดเจน ได้แก่ เรือสินค้าชนแนวปะการังในทะเลแดงหลังเชื่อพิกัด Estimated Position (EP) บน ECDIS โดยไม่ตรวจสอบกับสภาพแวดล้อมจริง ทำให้ตำแหน่งคลาดเคลื่อนกว่า **๔๐ ไมล์ทะเล** และอีกกรณีหนึ่ง ระบบ GPS แสดงตำแหน่งเรืออยู่บนบกกลางทะเลทราย ส่งผลให้นายเรือต้องระงับการออกเรือและเกิดข้อพิพาททางการค้าตามมา

บทเรียนสำคัญ คือ ความปลอดภัยของการเดินเรือไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่ขึ้นอยู่กับการประเมินสถานการณ์ การตรวจสอบข้อมูลจากหลายแหล่ง (Cross-check) และการตัดสินใจของกำลังพลบนสะพานเดินเรือภายใต้หลักการนำเรือที่ปลอดภัย (Safe Navigation) และการบริหารความเสี่ยงเชิงรุก (Proactive Risk Management) เพื่อรับมือกับภัยคุกคามไซเบอร์ทางทะเลที่มีแนวโน้มเพิ่มสูงขึ้น

ผลกระทบเชิงยุทธศาสตร์ต่อความมั่นคงทางทะเลของประเทศไทย (Strategic Implications for Thailand's Maritime Security)

สำหรับประเทศไทย พื้นที่ทางทะเลเป็นฐานสำคัญของการค้า การขนส่งพลังงาน การประมง และความมั่นคงแห่งชาติ การคุ้มครองระบบนำร่องและโครงสร้างพื้นฐานสารสนเทศทางทะเลจึงเป็นภารกิจที่มีนัยสำคัญเชิงยุทธศาสตร์ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐ มาตรา ๕๒ กำหนดให้รัฐจัดให้มีการทหาร การทูต และการข่าวกรองที่มีประสิทธิภาพเพื่อพิทักษ์รักษาความมั่นคงของรัฐและผลประโยชน์ของชาติ ขณะที่พระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ และแผนความมั่นคงแห่งชาติทางทะเล พ.ศ.๒๕๖๖ – ๒๕๗๐ เน้นการบูรณาการการปฏิบัติงานและข้อมูลระหว่างหน่วยงานที่เกี่ยวข้อง ดังนั้น ความมั่นคงไซเบอร์ทางทะเลจึงควรถูกพิจารณาเป็นส่วนหนึ่งของกลไกการรักษาผลประโยชน์ของชาติทางทะเล มิใช่เป็นภารกิจเฉพาะด้านเทคโนโลยีสารสนเทศเท่านั้น (รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐, ๒๕๖๐, มาตรา ๕๒; สำนักงานสภาความมั่นคงแห่งชาติ, ๒๕๖๖) ประเทศไทยตั้งอยู่บนเส้นทางคมนาคมทางทะเลที่สำคัญของภูมิภาคอินโด–แปซิฟิก ซึ่งมีความสำคัญทางนัยภูมิศาสตร์ และภูมิรัฐศาสตร์ หากการหยุดชะงักของระบบนำร่องและระบบสื่อสารจึงอาจส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจ พลังงาน และการคุ้มครองอธิปไตยทางทะเล (สำนักงานสภาความมั่นคงแห่งชาติ, ๒๕๖๖; UNCLOS, 1982) ความมั่นคงไซเบอร์ทางทะเลจึงควรถูกบูรณาการเป็นส่วนหนึ่งของยุทธศาสตร์ความมั่นคงแห่งชาติ ไม่ใช่เป็นภารกิจเฉพาะของหน่วยงานด้านเทคโนโลยีสารสนเทศ เนื่องจากมีผลกระทบโดยตรงต่อการรักษาอำนาจทางทะเลของรัฐ

การพัฒนาเทคโนโลยีดิจิทัลและระบบการนำร่องผ่านดาวเทียมได้กลายเป็นองค์ประกอบสำคัญของกิจกรรมทางทะเลสมัยใหม่ ไม่ว่าจะเป็นการเดินเรือพาณิชย์ การบริหารจัดการท่าเรือ หรือการปฏิบัติการทางทหาร

ของกองทัพเรือ อย่างไรก็ตาม ภัยคุกคามจากการปลอมแปลงสัญญาณ (Signal Spoofing) และการรบกวนสัญญาณ (Signal Jamming) ได้ก่อให้เกิดความท้าทายใหม่ต่อความมั่นคงทางทะเล เนื่องจากภัยคุกคามดังกล่าวสามารถบ่อนทำลายความน่าเชื่อถือของระบบนำร่อง ระบบติดตามเรือ และระบบสื่อสารทางทะเล ซึ่งเป็นโครงสร้างพื้นฐานสำคัญของการตระหนักรู้สถานการณ์ทางทะเล (Maritime Situational Awareness) และการควบคุมการปฏิบัติการของกำลังทางเรือ

พื้นที่ทางทะเลของประเทศไทย มีความสำคัญต่อเศรษฐกิจและความมั่นคงของชาติ การรักษาความปลอดภัยของระบบนำร่องและระบบสื่อสารทางทะเลจึงเป็นประเด็นที่มีความสำคัญเชิงยุทธศาสตร์ ทะเลไทยเป็นส่วนหนึ่งของเส้นทางคมนาคมทางทะเลที่สำคัญของภูมิภาคอินโด-แปซิฟิก โดยเฉพาะบริเวณอ่าวไทยและทะเลอันดามัน ผลกระทบต่อประเทศไทยสามารถพิจารณาได้อย่างน้อยสี่ระดับ ได้แก่

๑. ระดับความปลอดภัยในการเดินเรือ ซึ่งเกี่ยวข้องกับความเสี่ยงต่อชีวิต เรือ และสิ่งแวดล้อม

๒. ระดับเศรษฐกิจและโลจิสติกส์ ซึ่งเกี่ยวข้องกับท่าเรือ การขนส่งพลังงาน และห่วงโซ่อุปทาน

๓. ระดับความมั่นคงและการบังคับใช้กฎหมาย ซึ่งเกี่ยวข้องกับการตรวจจับการประมงผิดกฎหมาย การลักลอบขนส่ง และกิจกรรมในพื้นที่สีเทา และ

๔. ระดับยุทธศาสตร์ ซึ่งเกี่ยวข้องกับความสามารถของรัฐในการรักษาภาพสถานการณ์ร่วม การควบคุมพื้นที่ และการตัดสินใจในภาวะวิกฤติ

หากพื้นที่ทางทะเลที่มีการขนส่งสินค้าระหว่างประเทศ การประมงและกิจกรรมทางเศรษฐกิจทางทะเลจำนวนมาก ถูกการบิดเบือนข้อมูลตำแหน่งเรือหรือการหยุดชะงักของระบบสื่อสารทางทะเลจึงอาจส่งผลกระทบต่อทั้งความมั่นคงทางเศรษฐกิจ ความปลอดภัยในการเดินเรือ และความสามารถในการควบคุมพื้นที่ทางทะเลของรัฐ

ในมิติของกฎหมายระหว่างประเทศ การบริหารจัดการและการรักษาความมั่นคงของพื้นที่ทางทะเลต้องดำเนินการภายใต้กรอบของอนุสัญญาสหประชาชาติว่าด้วยกฎหมายทะเล ค.ศ.๑๙๘๒ (United Nations Convention on the Law of the Sea: UNCLOS 1982) ซึ่งกำหนดสิทธิและหน้าที่ของรัฐชายฝั่งในการบริหารจัดการพื้นที่ทางทะเลและทรัพยากรทางทะเล ภายใต้อนุสัญญาดังกล่าว รัฐชายฝั่งมีสิทธิอธิปไตยในการใช้ประโยชน์ การสำรวจ และการอนุรักษ์ทรัพยากรธรรมชาติภายในเขตเศรษฐกิจจำเพาะ (Exclusive Economic Zone: EEZ) รวมถึงมีหน้าที่ในการรักษาความปลอดภัยและความเป็นระเบียบของกิจกรรมทางทะเลภายในเขตอำนาจของตน

แม้ UNCLOS 1982 มิได้กำหนดหลักเกณฑ์เกี่ยวกับการปลอมแปลงหรือการรบกวนสัญญาณไซเบอร์โดยตรง แต่อานุภาพของภัยคุกคามดังกล่าวอาจกระทบต่อการใช้สิทธิในการเดินเรือ ความปลอดภัยในการเดินเรือ และการปฏิบัติหน้าที่ของรัฐชายฝั่งภายใต้กฎหมายทะเลระหว่างประเทศ ประเด็นสำคัญจึงอยู่ที่การระบุตัวผู้กระทำ การกำหนดเขตอำนาจ และการพิจารณาว่าการกระทำนั้นเป็นอุบัติการณ์ทางเทคนิค การกระทำที่มิชอบหรือส่วนหนึ่งของปฏิบัติการทางทหาร นอกจากนี้ UNCLOS 1982 ยังเน้นย้ำถึงความสำคัญของความปลอดภัยในการเดินเรือ (Safety of Navigation) และการป้องกันอันตรายที่อาจเกิดขึ้นต่อการใช้ทะเลเพื่อการเดินเรือระหว่างประเทศ ภัยคุกคามที่ส่งผลต่อระบบนำร่อง เช่น การปลอมแปลงสัญญาณหรือการรบกวนสัญญาณ จึงอาจส่งผลกระทบต่อเสถียรภาพของระบบการเดินเรือระหว่างประเทศ และอาจก่อให้เกิดความเสี่ยงต่อความปลอดภัยของเรือและลูกเรือในพื้นที่ทะเลที่มีการจราจรหนาแน่น

จากมุมมองเชิงยุทธศาสตร์ ความเสี่ยงสำคัญที่สุดมิได้อยู่ที่การสูญเสียสัญญาณเป็นการชั่วคราว แต่อยู่ที่การสูญเสียความเชื่อมั่นต่อภาพสถานการณ์ร่วม ซึ่งอาจทำให้รัฐไม่สามารถแยกแยะจากเหตุการณ์ปกติ ออกจาก อุบัติเหตุ อาชญากรรม และการกระทำเชิงปรปักษ์ได้อย่างทันท่วงที

ในเชิงยุทธศาสตร์ ความสามารถของรัฐในการเฝ้าระวังและควบคุมกิจกรรมทางทะเล หรือที่เรียกว่า Maritime Domain Awareness (MDA) ถือเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงทางทะเล ระบบการติดตามเรือ เช่น AIS และระบบนำร่องผ่านดาวเทียม เป็นเครื่องมือหลักในการสร้างภาพรวมของสถานการณ์ทางทะเล (Maritime Operating Picture) หากระบบดังกล่าวถูกบิดเบือนหรือถูกทำให้ไม่สามารถใช้งานได้ ความสามารถของรัฐในการตรวจจับกิจกรรมที่ผิดปกติ เช่น การลักลอบขนส่งสินค้า การทำประมงผิดกฎหมาย หรือกิจกรรมทางทหารที่ไม่พึงประสงค์ อาจลดลงอย่างมีนัยสำคัญ

สำหรับหน่วยงานความมั่นคงทางทะเล และภาคเอกชนอุตสาหกรรมพานิชย์นาวี ภัยคุกคามจากการโจมตีระบบสัญญาณและระบบสื่อสารทางทะเลจึงไม่ใช่เพียงปัญหาทางเทคนิคเท่านั้น แต่ยังเป็นประเด็นเชิงยุทธศาสตร์ที่เกี่ยวข้องกับความสามารถในการควบคุมพื้นที่ทางทะเล การป้องกันผลประโยชน์ของชาติ และการรักษาเสถียรภาพของเส้นทางคมนาคมทางทะเล การบูรณาการข้อมูลจากหลายแหล่ง เช่น ระบบเรดาร์ชายฝั่ง ดาวเทียม และระบบติดตามเรือ จึงเป็นแนวทางสำคัญในการเสริมสร้างความน่าเชื่อถือของระบบการรับรู้สถานการณ์ทางทะเล

นอกจากนี้ การพัฒนาขีดความสามารถด้านความมั่นคงไซเบอร์ทางทะเลยังเป็นองค์ประกอบสำคัญของยุทธศาสตร์การป้องกันประเทศในยุคดิจิทัล การเสริมสร้างศักยภาพของหน่วยงานด้านการข่าวกรอง การพัฒนาระบบตรวจจับการโจมตีทางไซเบอร์ และการฝึกอบรมบุคลากรด้านความมั่นคงไซเบอร์ทางทะเล จะช่วยเพิ่มความสามารถของประเทศไทยในการป้องกันและรับมือกับภัยคุกคามที่อาจส่งผลกระทบต่อโครงสร้างพื้นฐานทางทะเลและการปฏิบัติการของกำลังทางเรือ

ดังนั้น ภัยคุกคามจากการปลอมแปลงสัญญาณและการรบกวนสัญญาณจึงควรถูกพิจารณาในกรอบของยุทธศาสตร์ความมั่นคงทางทะเล

ของประเทศ โดยการพัฒนาระบบเฝ้าระวัง การบูรณาการข้อมูล และการเสริมสร้างขีดความสามารถด้านไซเบอร์ของกองทัพเรือ จะช่วยให้ประเทศไทยสามารถรักษาความมั่นคงของพื้นที่ทางทะเลและปกป้องผลประโยชน์ของชาติได้อย่างมีประสิทธิภาพภายใต้บริบทของกฎหมายทะเลระหว่างประเทศและสภาพแวดล้อมด้านความมั่นคงที่เปลี่ยนแปลงไป

ช่องว่างสำคัญของประเทศไทยจึงมิได้อยู่เพียงที่การขาดเทคโนโลยีตรวจจับ หากแต่อยู่ที่การเชื่อมโยงอำนาจหน้าที่ ข้อมูล ข่าวกรอง และกระบวนการตัดสินใจระหว่างหน่วยงานให้สามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

ผลการวิเคราะห์แสดงให้เห็นว่าการรับมือกับภัยคุกคามไซเบอร์ทางทะเลจำเป็นต้องดำเนินการในลักษณะบูรณาการ ทั้งด้านโครงสร้างองค์กร เทคโนโลยี การข่าวกรอง กฎหมาย และความร่วมมือระหว่างประเทศ ดังนั้น ข้อเสนอเชิงนโยบายต่อไปนี้จึงมุ่งเสริมสร้างความยืดหยุ่นของระบบความมั่นคงทางทะเลของประเทศไทยในทุกมิติ

การบูรณาการการตระหนักรู้หลายมิติ (Multi-Domain Awareness)

แนวคิด Multi-Domain Awareness เป็นการประยุกต์แนวคิดจาก Multi-Domain Operations (MDO) ของกองทัพสมัยใหม่ มุ่งบูรณาการข้อมูลจากมิติทางทะเล อากาศ อวกาศ ไซเบอร์ และข่าวกรอง เพื่อสร้างภาพสถานการณ์ร่วม (Common Operational Picture: COP) ที่สนับสนุนการตัดสินใจเชิงยุทธศาสตร์ (U.S. Department of Defense, 2022)

สำหรับประเทศไทย การประยุกต์ใช้ Multi-Domain Awareness จะช่วยยกระดับการบูรณาการข้อมูลระหว่างกองทัพเรือ ศรชล. หน่วยงานด้านข่าวกรอง หน่วยงานความมั่นคงทางทะเลและภาคเอกชน ทำให้สามารถตรวจจับและตอบสนองต่อภัยคุกคามแบบผสมผสานได้อย่างมีประสิทธิภาพมากขึ้น

ข้อเสนอเชิงนโยบายเพื่อเสริมสร้างความมั่นคงไซเบอร์ทางทะเล (Policy Recommendations for Strengthening Maritime Cyber Security)

จากการวิเคราะห์ภัยคุกคามด้านการปลอมแปลงสัญญาณ (Signal Spoofing) และการรบกวนสัญญาณ (Signal Jamming) พบว่า ภัยคุกคามทั้งสองรูปแบบมิได้ส่งผลกระทบเฉพาะต่อระบบนำร่องหรือการสื่อสารทางทะเล หากแต่กระทบต่อขีดความสามารถของรัฐในการรับรู้สถานการณ์ การบัญชาการและควบคุม การข่าวกรอง ตลอดจนการคุ้มครองผลประโยชน์ของชาติทางทะเลในภาพรวม ภัยคุกคามดังกล่าวจึงควรถูกพิจารณาเป็น **ภัยคุกคามเชิงยุทธศาสตร์ (Strategic Maritime Cyber Threats)** มากกว่าปัญหาทางเทคนิคของระบบสารสนเทศเพียงอย่างเดียว

ผลการวิเคราะห์ยังสะท้อนให้เห็นว่า การรับมือกับภัยคุกคามไซเบอร์ทางทะเลไม่สามารถอาศัยมาตรการด้านเทคโนโลยีหรือการดำเนินงานของหน่วยงานใดหน่วยงานหนึ่งได้ เนื่องจากภัยคุกคามมีลักษณะเชื่อมโยงหลายมิติ ทั้งด้านเทคโนโลยี การปฏิบัติการ ข่าวกรอง กฎหมาย และความสัมพันธ์ระหว่างประเทศ ดังนั้น การกำหนดนโยบายจึงจำเป็นต้องอยู่บนพื้นฐานของ **การบูรณาการ (Integration)** และ **ความยืดหยุ่นของระบบ (Resilience)** เพื่อให้สามารถป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูการปฏิบัติการได้อย่างต่อเนื่อง แม้อยู่ภายใต้สภาวะที่ระบบนำร่องหรือระบบสื่อสารถูกลดทอนประสิทธิภาพ

ในบทความนี้ ผู้เขียนเสนอกรอบนโยบายเพื่อเสริมสร้างความมั่นคงไซเบอร์ทางทะเลของประเทศไทยบนพื้นฐานของ **สี่เสาหลัก (Four Strategic Pillars)** ได้แก่ (๑) การกำกับดูแลและโครงสร้างองค์กร (Governance and Organizational Structure) (๒) เทคโนโลยีและการบูรณาการข้อมูล (Technology and Data Integration) (๓) การพัฒนากำลังคนและขีดความสามารถ (Human Capital and Capability Development) และ

(๔) กฎหมาย ความร่วมมือ และธรรมาภิบาลระหว่างประเทศ (Legal Framework and International Cooperation) เพื่อรองรับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว

กรอบแนวคิดในการพัฒนาความมั่นคงไซเบอร์ทางทะเล

การกำหนดข้อเสนอเชิงนโยบายจำเป็นต้องอาศัยความเข้าใจความแตกต่างของแนวคิดที่เกี่ยวข้องกับการรับรู้และการบูรณาการข้อมูลทางทะเล ซึ่งมีพัฒนาการจากการรับรู้สถานการณ์เชิงพื้นที่ไปสู่การรับรู้หลายมิติที่เชื่อมโยงข้อมูลจากทุกโดเมนการปฏิบัติการ

การตระหนักรู้สถานการณ์ทางทะเล (Maritime Situational Awareness: MSA) หมายถึง ความสามารถในการรับรู้ ติดตาม และประเมินสถานการณ์ที่เกิดขึ้นในพื้นที่ทางทะเล ณ ช่วงเวลาใดช่วงเวลาหนึ่ง เพื่อสนับสนุนการตัดสินใจของผู้ปฏิบัติและผู้บังคับบัญชาในระดับยุทธวิธีและยุทธการ โดยมุ่งเน้นการรวบรวมข้อมูลจากระบบนำร่อง ระบบตรวจจับ และระบบสื่อสาร เพื่อสร้างภาพสถานการณ์ที่สะท้อนสภาพแวดล้อมการปฏิบัติการในเวลาจริง (Real-time Operational Picture) ข้อมูลดังกล่าวครอบคลุมตำแหน่ง การเคลื่อนที่ สภาพอากาศ การจราจรทางทะเล ตลอดจนเหตุการณ์ผิดปกติที่อาจส่งผลต่อความปลอดภัยในการเดินเรือหรือการปฏิบัติการทางทะเล (International Maritime Organization [IMO], 2021)

ในบริบทของความมั่นคงทางทะเล MSA เป็นองค์ประกอบพื้นฐานของระบบบัญชาการและควบคุม (Command and Control: C2) เนื่องจากช่วยให้หน่วยงานสามารถรับรู้และตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที อย่างไรก็ตาม MSA มุ่งเน้นการรับรู้ “สถานการณ์ที่กำลังเกิดขึ้น” ในพื้นที่และช่วงเวลาที่กำหนด จึงมีขอบเขตจำกัดในด้านการวิเคราะห์ความเชื่อมโยงเชิงยุทธศาสตร์ระหว่างกิจกรรมต่าง ๆ หรือการคาดการณ์ภัยคุกคามในระยะยาว

ดังนั้น MSA จึงเป็นพื้นฐานสำคัญของการปฏิบัติการทางทะเลในระดับยุทธวิธีและยุทธการ โดยมีบทบาทในการสนับสนุนการตัดสินใจแบบทันต่อเหตุการณ์ (Real-time Decision Making) มากกว่าการวิเคราะห์เชิงยุทธศาสตร์หรือการประเมินภัยคุกคามในภาพรวม

การตระหนักรู้ในมิติทางทะเล (Maritime Domain Awareness: MDA) เป็นแนวคิดที่มีขอบเขตกว้างกว่า MSA โดยหมายถึง ความเข้าใจอย่างครอบคลุมต่อกิจกรรม สภาพแวดล้อม และปัจจัยทั้งหมดที่เกิดขึ้นในมิติทางทะเล ซึ่งอาจส่งผลกระทบต่อความมั่นคง ความปลอดภัย เศรษฐกิจ สิ่งแวดล้อม หรือผลประโยชน์แห่งชาติ (U.S. Department of Homeland Security, 2005) แนวคิดดังกล่าวครอบคลุมทั้งกิจกรรมของเรือ การใช้ทรัพยากรทางทะเล โครงสร้างพื้นฐานทางทะเล พื้นที่ชายฝั่ง ห่วงโซ่อุปทาน และกิจกรรมของตัวแสดงที่เป็นรัฐและมิใช่รัฐ

การพัฒนา MDA จำเป็นต้องอาศัยการบูรณาการข้อมูลจากหลายแหล่ง ได้แก่ ระบบระบุอัตโนมัติของเรือ (AIS) ระบบติดตามเรือประมง (VMS) เรดาร์ชายฝั่ง ภาพถ่ายดาวเทียม ข่าวกรองทางทะเล และฐานข้อมูลระหว่างประเทศ เพื่อสร้าง **Maritime Common Operational Picture (MCOP)** ที่ช่วยให้หน่วยงานด้านความมั่นคงสามารถตรวจจับกิจกรรมผิดปกติ วิเคราะห์แนวโน้ม และประเมินผลกระทบต่อผลประโยชน์ของชาติได้อย่างเป็นระบบ

สำหรับประเทศไทย แนวคิด MDA มีความสอดคล้องกับพระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ ซึ่งมุ่งเน้นการบูรณาการข้อมูลและการปฏิบัติงานระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อยกระดับประสิทธิภาพในการเฝ้าระวัง การบังคับใช้กฎหมาย และการคุ้มครองผลประโยชน์ของชาติทางทะเล

MDA จึงเป็นกรอบการบริหารจัดการความมั่นคงทางทะเลในระดับยุทธศาสตร์ ที่เชื่อมโยงการรับรู้สถานการณ์เข้ากับการวิเคราะห์ข่าวกรอง

การบริหารความเสี่ยง และการกำหนดนโยบาย เพื่อให้รัฐสามารถรักษาผลประโยชน์ของชาติทางทะเลได้อย่างยั่งยืน

บทสรุป (Conclusion)

การเปลี่ยนผ่านสู่ยุคดิจิทัลทำให้ระบบดาวเทียมนำทาง การสื่อสาร และโครงสร้างพื้นฐานดิจิทัลทางทะเลกลายเป็นปัจจัยสำคัญของความมั่นคงทางทะเล ขณะเดียวกันก็เพิ่มความเปราะบางต่อภัยคุกคามไซเบอร์ โดยเฉพาะ **การปลอมแปลงสัญญาณ (Signal Spoofing)** และ **การรบกวนสัญญาณ (Signal Jamming)** ซึ่งส่งผลกระทบโดยตรงต่อความถูกต้องของข้อมูลการตระหนักรู้สถานการณ์ทางทะเล (Maritime Situational Awareness: MSA) การตระหนักรู้มิติทางทะเล (Maritime Domain Awareness: MDA) และการสร้างภาพสถานการณ์ร่วม (Common Operational Picture: COP) อันเป็นพื้นฐานของการบัญชาการและการตัดสินใจในทุกระดับ

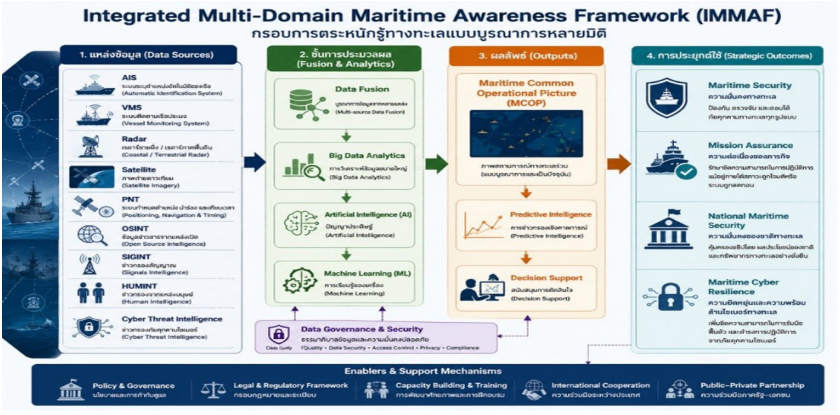
บทความชี้ให้เห็นว่า ภัยคุกคามดังกล่าวได้พัฒนาเป็นส่วนหนึ่งของ **สงครามลูกผสม (Hybrid Warfare)** ที่เชื่อมโยงการปฏิบัติการไซเบอร์ สงครามอิเล็กทรอนิกส์ และการปฏิบัติการข่าวสารเข้าด้วยกัน จึงจำเป็นต้องเปลี่ยนแนวคิดจากการป้องกันระบบเฉพาะส่วน ไปสู่การพัฒนาระบบ **ความมั่นคงไซเบอร์ทางทะเลแบบบูรณาการ (Integrated Maritime Cyber Security System)** ที่เชื่อมโยงข้อมูล ข่าวกรอง เทคโนโลยี บุคลากร และการตัดสินใจระหว่างทุกภาคส่วน

ข้อเสนอสำคัญของบทความ คือ **กรอบการตระหนักรู้ทางทะเลแบบบูรณาการหลายมิติ (Integrated Multi-Domain Maritime Awareness Framework: IMMAF)** ซึ่งผู้เขียนพัฒนาขึ้นจากการบูรณาการแนวคิด Maritime Domain Awareness (MDA) กับ Multi-Domain Operations (MDO) เพื่อเชื่อมโยงข้อมูลจากมิติทางทะเล อากาศ อวกาศ ไซเบอร์ คลื่นแม่เหล็กไฟฟ้า และข่าวกรองเข้าสู่กระบวนการวิเคราะห์เดียวกัน ช่วยยกระดับจากการรับรู้สถานการณ์แบบเรียลไทม์ไปสู่ **การข่าวกรอง**

เชิงคาดการณ์ (Predictive Intelligence) และการสนับสนุนการตัดสินใจเชิงยุทธศาสตร์ (Strategic Decision Support)

ในเชิงนโยบาย ประเทศไทยควรเร่งพัฒนาระบบนิเวศด้านความมั่นคงไซเบอร์ทางทะเล (Maritime Cyber Security Ecosystem) ภายใต้กรอบพระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ แผนความมั่นคงแห่งชาติทางทะเล พ.ศ.๒๕๖๖ – ๒๕๗๐ และ UNCLOS 1982 เพื่อเสริมสร้าง **Cyber Resilience** และเพิ่มขีดความสามารถในการป้องกัน ตอบสนอง และฟื้นฟูจากภัยคุกคามที่ซับซ้อนในภูมิภาคอินโด–แปซิฟิก

ท้ายที่สุด ความมั่นคงไซเบอร์ทางทะเลมิใช่เพียงประเด็นด้านเทคโนโลยีสารสนเทศ แต่เป็นองค์ประกอบสำคัญของ **กำลังอำนาจทางทะเล (Sea Power)** และความมั่นคงแห่งชาติ การบูรณาการข้อมูล ข่าวกรอง และเทคโนโลยีผ่านกรอบ IMMAF จะเป็นรากฐานสำคัญในการสร้างความได้เปรียบเชิงยุทธศาสตร์ เพิ่มความยืดหยุ่นของระบบ และเสริมสร้างศักยภาพของประเทศไทยในการรักษาอธิปไตย ผลประโยชน์ของชาติ และความมั่นคงทางทะเลในยุคดิจิทัลอย่างยั่งยืน.



รูปที่ ๒ Integrated Multi-Domain Maritime Awareness Framework (IMMAF) การบูรณาการกรอบแนวคิดเชิงยุทธศาสตร์ที่บูรณาการข้อมูล ข่าวกรอง และเทคโนโลยีจากทุกมิติของการปฏิบัติการ เพื่อสนับสนุนการตัดสินใจ

ที่มา: วิเคราะห์และจัดทำโดยผู้เขียนด้วยเทคโนโลยีปัญญาประดิษฐ์ DALL-E ผ่าน ChatGGPT (OpenAI,2026)

เอกสารอ้างอิง

กรมอุทกศาสตร์ กองทัพเรือ. (๒๕๕๗). ระบบควบคุมติดตามระยะไกลและสารสนเทศเครื่องหมายทางเรือในน่านน้ำไทย (Automatic Identification System: AIS). กองเครื่องหมายทางเรือ ศูนย์สนับสนุนการเดินเรือ กรมอุทกศาสตร์.

กองทัพเรือ. (๒๕๔๑). คำแนะนำระบบการหาตำบลที่เรือด้วยดาวเทียม จี พี เอส (อทร. ๗๗๐๖). คณะทำงานพิจารณาและจัดทำ อทร.ด้านการศึกษาชั้นพื้นฐาน.,

กองทัพเรือ. (๒๕๔๓). หลักการและทฤษฎีการทำสงคราม (อทร. ๘๐๐๔). คณะทำงานพิจารณาและจัดทำ อทร.ด้านการศึกษาชั้นสูง.

กองทัพเรือ. (๒๕๔๔). การป้องกันและรักษาผลประโยชน์ของชาติทางทะเล (อทร. ๘๐๐๒). คณะทำงานพิจารณาและจัดทำ อทร.ด้านการศึกษาชั้นสูง.

กองทัพเรือ. (๒๕๔๖). หลักนิยมทางทะเลของกองทัพเรือ (อทร. ๘๐๐๑). คณะทำงานพิจารณาและจัดทำ อทร.ด้านการศึกษาชั้นสูง.

โกมุท กมลนาวิน. (๒๕๒๒). ลักษณะของสงครามและหลักการสงคราม [เอกสารประกอบการบรรยาย]. โรงเรียนเสนาธิการทหารเรือ.,

ชาติ นาวาวิจิต. (๒๕๓๙). การกำหนดยุทธศาสตร์และกำลังรบของกองทัพเรือ [เอกสารประจำภาค]. วิทยาลัยการทัพเรือ.,

นิตย์ ศรีสมวงษ์. (๒๕๔๐). จากน่านน้ำชายฝั่งสู่ทะเลลึก. สถาบันวิชาการทหารเรือชั้นสูง.,

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐. (๒๕๖๐, ๖ เมษายน). ราชกิจจานุเบกษา. เล่ม ๑๓๔ ตอนที่ ๔๐ ก. หน้า ๑-๙๐.

สถาบันวิชาการทหารเรือชั้นสูง. (๒๕๔๐). ปัญหาในทะเลจีนใต้กับผลกระทบต่อยุทธศาสตร์และโครงสร้างกำลังรบของไทย [การศึกษาปัญหาระดับยุทธศาสตร์และนโยบายกองทัพเรือ].,

สถาบันวิชาการทหารเรือชั้นสูง. (๒๕๔๐). ปัญหาประมงในเขตเศรษฐกิจจำเพาะ [การศึกษาปัญหาระดับยุทธศาสตร์และนโยบายกองทัพเรือ].,

สถาบันวิชาการทหารเรือชั้นสูง. (๒๕๔๐). เศรษฐกิจทางทะเล [การศึกษาปัญหาระดับยุทธศาสตร์และนโยบายกองทัพเรือ].,

สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ. (๒๕๖๕). แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๓. สำนักนายกรัฐมนตรี.

สำนักงานสภาความมั่นคงแห่งชาติ. (๒๕๕๘). แผนความมั่นคงแห่งชาติทางทะเล (พ.ศ.๒๕๕๘ - ๒๕๖๔). สำนักนายกรัฐมนตรี.

สำนักงานสภาความมั่นคงแห่งชาติ. (๒๕๖๖). แผนความมั่นคงแห่งชาติทางทะเล (พ.ศ.๒๕๖๖ - ๒๕๗๐). บริษัท ซีดี มีเดีย ไกด์ จำกัด.

หรรษา จรรย์แสง. (๒๕๔๐). การอนุรักษ์สิ่งแวดล้อมและทรัพยากรมีชีวิตในทะเลและบทบาทกองทัพเรือ [เอกสารประจำภาค]. วิทยาลัยการทัพเรือ.,

เอกสารอ้างอิงภาษาต่างประเทศ

The Navigator (ฉบับเดือนตุลาคม ค.ศ. 2025)

The Royal Australian Air Forces. (n.d.). The condensed air power manual. Air Power Studies Centre.

The Royal Navy. (1996). The fundamentals of British maritime doctrine (BR 1806). The Stationary Office.

The Royal New Zealand Navy. (1997). Maritime doctrine for the Royal New Zealand Navy.,

The United States Navy. (1994). Naval doctrine publication 1: Naval warfare. Naval Doctrine Command.

US Naval War College. (1996). Operational arts.

US Naval Warfare Development Command. (1998). Multinational maritime operations (MMOPs).

US Naval Warfare Development Command. (1998). Use of force manual (UFM).

Department of Treaties and Legal Affairs. (2005). United Nations Con vention on the Law of the Sea 1982 (UNCLOS). Ministry of Foreign Affairs.

International Maritime Organization. (2021). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3 Rev.1). IMO.

National Security Council. (2023). Thailand maritime security plan (2023–2027). Office of the National Security Council.

Journal of Marine Engineering & Technology ISSN: 2046-4177 (Print) 2056-8487 (Online) Journal homepage: www.tandfonline.com/journals/tmar20

Office of the Attorney General. (2019). Maritime national interests pro tection act B.E. 2562 (2019). Government of Thailand.

Royal Thai Navy. (2001). Naval reference document 8002: Protection of national maritime interests. Naval Education Department.

Tam, K., & Jones, K. (2019). Maritime cybersecurity: A growing threat goes unanswered. Journal of Transportation Security, 12(3–4), 205–220. https://doi.org/10.1007/s12198-019-00217-3

United Nations. (1982). United Nations Convention on the Law of the Sea. United Nations.

U.S. Department of Defense. (2020). Cyber strategy of the United States Department of Defense. Department of Defense.

รายการอ้างอิงเว็บไซต์ (ภาษาไทย)

สำนักงานสภาความมั่นคงแห่งชาติ. (๒๕๖๖). แผนความมั่นคงแห่งชาติทางทะเล (พ.ศ.๒๕๖๖ - ๒๕๗๐). https://www.nsc.go.th

Marsefocus

รายการอ้างอิงเว็บไซต์ (ภาษาต่างประเทศ) โดยสืบค้นวันที่ ๕ มีนาคม ๒๕๖๙

European Telecommunications Standards Institute (ETSI). (2020). ETSI TS 103 246-5 V1.1.1 (2016-01) and V1.3.1 (2020-10). Satellite Earth Stations and Systems (SES). GNSS-Based Location Systems, Part 5: Performance Test Specification. https://portal.etsi.org/Services/editHelp/Search/FAQs/TEDDI

International Organization for Standardization (ISO). (2022). ISO 24246:2022(en); Space Systems—Requirements for Global Navigation Satellite System (GNSS) Positioning Augmentation Centers. https://www.iso.org/obp/ui#home

Mukherji, V., & Chandele, A. K. S. (n.d.). GNSS Jamming: An Omnipresent Threat. Geospatial World. https://www.geospatialworld.net/prime/special-features/gnss-jamming-an-omnipresent-threat/

Novatel. (n.d.). What Are Global Navigation Satellite Systems?. https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss

SGM. (2020). Jamming and spoofing.