ที่ นร ๐๘๐๖/ว๑๒๒๕

ถึง หัวหน้าส่วนราชการที่เกี่ยวข้อง

กองความมั่นคงทางทะเล สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำเอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงทางทะเล (Maritime Security Focus) หรือ “MarSec Focus” ฉบับที่ ๕/๒๕๖๙ โดยมีหัวข้อ “Maritime Security Governance...กับวิวัฒนาการของภัยคุกคามความมั่นคงทางทะเล” (รายละเอียดตามที่แนบ) เพื่อเป็นการเสริมสร้างและเผยแพร่องค์ความรู้เกี่ยวกับความมั่นคงทางทะเลให้กับหน่วยงานที่เกี่ยวข้องพิจารณาใช้ประโยชน์ต่อไป

เรียน รองอธิการบดีฝ่ายแผนยุทธศาสตร์และนโยบาย

ด้วย กองความมั่นคงทางทะเล สำนักงานสภาความมั่นคงแห่งชาติ ขอส่งเอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงทางทะเล (Maritime Security Focus) หรือ “MarSec Focus” ฉบับที่ ๕/๒๕๖๙ โดยมีหัวข้อ "Maritime Security Governance...กับวิวัฒนาการของภัยคุกคามความมั่นคงทางทะเล"

สำนักงานสภาความมั่นคงแห่งชาติ
๕ มีนาคม ๒๕๖๙

จึงเรียนมาเพื่อ

๑. เพื่อโปรดทราบ

๒. เห็นควรเผยแพร่ให้ทราบโดยทั่วกันและสามารถดาวน์โหลดหนังสือได้ที่ https://docshare.buu.ac.th

กองความมั่นคงทางทะเล
๐๕ มี.ค. ๒๕๖๙
สำนักงานสภาความมั่นคงแห่งชาติ
โทร. ๐ ๒๖๒๙ ๘๐๐๐ ต่อ ๓๗๐๙
๐๕ มี.ค. ๒๕๖๙
โทรสาร ๐ ๒๖๒๙ ๘๐๕๘
ไปรษณีย์อิเล็กทรอนิกส์ saraban@nsc.go.th / nsc.maritime@gmail.com

ทราบ/ดำเนินการตามเสนอ

๐๕ มี.ค. ๒๕๖๙

MarSec Focus
Maritime Security Focus
สำนักงานสภาความมั่นคงแห่งชาติ
Office of the National Security Council
เอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงฯ ฉบับที่ 5/2569 วันที่ 1 มีนาคม 2569

Maritime Security Governance...กับวิวัฒนาการของภัยคุกคามความมั่นคงทางทะเล

วิวัฒนาการของภัยคุกคามความมั่นคงทางทะเลในยุคปัจจุบัน ได้มีการปรับเปลี่ยนรูปแบบและยุทธวิธีในการก่อเหตุที่มีลักษณะแบบไฮบริด (Hybrid) เพิ่มมากขึ้น โดยการนำเทคโนโลยีสมัยใหม่เข้ามาใช้เป็นเครื่องมือในการโจมตีเป้าหมาย ทั้งการปลอมแปลงสัญญาณนำทาง (GNSS Spoofing) การรบกวนสัญญาณ (Signal Jamming) รวมกับการใช้อากาศยานไร้คนขับ (UAV) เพื่อลดการสูญเสียของกำลังคน เพิ่มความแม่นยำในการโจมตี มีต้นทุนต่ำ ไร้ร่องรอยให้ติดตาม สามารถสั่นคลอนเสถียรภาพและความมั่นคงทางทะเลของรัฐชายฝั่งนั้น ๆ ได้อย่างกว้างขวาง

สถานการณ์

ในช่วงทศวรรษที่ผ่านมา พื้นที่ทะเลอาณาเขตของไทยต้องเผชิญกับภัยคุกคามความมั่นคงอย่างมีนัยสำคัญ ทั้งจากภัยคุกคามทางทหาร (แบบดั้งเดิม) จนไปสู่ความขัดแย้งในลักษณะที่คลุมเครือ (Gray-Zone Conflict) โดยฝ่ายตรงกันข้ามได้มีการนำเทคโนโลยีต้นทุนต่ำแต่ให้ผลกระทบเชิงยุทธศาสตร์สูงมาใช้เป็นเครื่องมือ อาทิ การใช้อากาศยานไร้คนขับร่วมกับการปลอมแปลงสัญญาณนำทาง (GNSS Spoofing) และการรบกวนสัญญาณ (Signal Jamming) เพื่อบ่อนทำลายหรือลดขีดความสามารถในการประเมินสถานการณ์และการตัดสินใจของฝ่ายไทย

กรณีข้อพิพาททางทะเลของไทยในพื้นที่ตะวันออกนั้น ที่ผ่านมาหน่วยงานภาครัฐและเอกชนได้มีการพึ่งพาระบบนำทางจากดาวเทียมและเครือข่ายสื่อสารดิจิทัลในการดำเนินกิจกรรมทางทะเล ส่งผลทำให้เรือพาณิชย์ แท่นขุดเจาะน้ำมัน และโครงสร้างพื้นฐานสำคัญ ๆ ตามแนวชายฝั่งมีความเปราะบางต่อการโจมตีของภัยคุกคามความมั่นคงรูปแบบใหม่เพิ่มมากขึ้น อาทิ การตรวจพบอากาศยานไร้คนขับของฝ่ายตรงกันข้ามในพื้นที่อ่าวไทย (บริเวณแท่นขุดเจาะน้ำมัน) ยิ่งสะท้อนให้เห็นถึงวิวัฒนาการของภัยคุกคามความมั่นคงทางทะเลที่มียุทธวิธีแตกต่างไปจากเดิม ฉะนั้น การพัฒนาระบบเฝ้าระวังป้องกันภัยคุกคามความมั่นคงทางทะเลจึงเป็นเรื่องที่สำคัญ โดยเฉพาะการพัฒนาองค์ความรู้ ทักษะ ยุทธวิธี เครื่องมือ และขีดความสามารถของบุคลากรในด้านต่าง ๆ ให้มีความพร้อมในการตอบสนองต่อสถานการณ์ที่เกิดขึ้นอย่างทันท่วงทีและเป็นระบบ

แนวคิดการกำกับดูแลความมั่นคงทางทะเล (Maritime Security Governance)

การปลอมแปลงตัวตน (Spoofing) ในบริบทความมั่นคงทางทะเลนั้นเป็นการสร้างชุดข้อมูลและสัญญาณดิจิทัลที่เกี่ยวข้องกับการนำทางและการรับรู้สถานการณ์ของเรือผู้ก่อเหตุ เพื่อทำให้ระบบการรับสัญญาณและประมวลผลข้อมูลของหน่วยงานรัฐไม่ตรงกับความเป็นจริง โดย Spoofing จะมุ่งเน้นการบ่อนทำลาย “ความเชื่อมั่นในข้อมูล” มากกว่าการทำให้ระบบหยุดทำงานอย่างสิ้นเชิง

โดย Spoofing สามารถจำแนกออกเป็น 3 รูปแบบ กล่าวคือ ***รูปแบบที่หนึ่ง*** GNSS Spoofing เป็นการปลอมแปลงสัญญาณตำแหน่งเวลา และพิกัดจากระบบนำทางด้วยดาวเทียม ส่งผลให้เรือเข้าใจว่าตนอยู่ในตำแหน่งอื่น ซึ่งไม่ตรงกับความเป็นจริง ***รูปแบบที่สอง*** AIS Spoofing เป็นการปลอมแปลงข้อมูลการระบุตัวตนเรือ ความเร็ว และทิศทางในระบบ AIS ซึ่งส่งผลทำให้เกิดปรากฏการณ์ “เรือผี” และลดประสิทธิภาพของระบบ การควบคุมการจราจรทางทะเล และ ***รูปแบบที่สาม*** Sensor/Data Spoofing เป็นการปลอมแปลงข้อมูลจากเซนเซอร์ภายในเรือ อาทิ Heading, Speed, Time, ETA และข้อมูลใน AIS ซึ่งส่งผลกระทบโดยตรงต่อการตัดสินใจของผู้ควบคุมเรือและระบบอัตโนมัติ

ฉะนั้น Spoofing จึงไม่ใช่เป็นเพียงปัญหาเชิงเทคนิค แต่เป็นภัยคุกคามความมั่นคงเชิงระบบ ที่สามารถบ่อนทำลายความปลอดภัยในการเดินเรือและเสถียรภาพของระบบการขนส่งทางทะเลในภาพรวมด้วย

บทวิเคราะห์

มิติทางด้านยุทธการ : การปลอมแปลงตัวตนของเรือพาณิชย์สามารถบ่อนทำลายขีดความสามารถในการรับรู้สถานการณ์ทางทะเลของเรือ และหน่วยงานควบคุมระบบการจราจร อันจะส่งผลต่อการตัดสินใจในการเดินเรือ การหลบหลีก และการขาดความแม่นยำในการติดต่อประสานงาน โดยเฉพาะในบริเวณพื้นที่ยุทธศาสตร์ทางทะเล อาทิ ช่องแคบ เส้นทางเดินเรือหลัก และที่ตั้งของโครงสร้างพื้นฐานทางด้านพลังงานในทะเล

มิติทางด้านเศรษฐกิจ : อาจก่อให้เกิดความล่าช้าในการขนส่ง การเกิดความเสียหายจากอุบัติเหตุทางทะเล การเสียค่าใช้จ่ายในการประกันภัยที่เพิ่มสูงขึ้น และการขาดความเชื่อมั่นในระบบการขนส่งทางทะเลในภาพรวม นอกจากนี้ Spoofing ยังสามารถถูกใช้เป็นเครื่องมือในกิจกรรมผิดกฎหมายอื่น ๆ อาทิ การหลีกเลี่ยงระบบการตรวจสอบการลักลอบขนส่งสินค้า การบิดเบือนข้อมูล และการหลีกเลี่ยงมาตรการกำกับดูแลจากหน่วยงานภาครัฐ ซึ่งส่งผลกระทบต่อเสถียรภาพและความมั่นคงทางเศรษฐกิจของประเทศต่าง ๆ

มิติทางด้านการรบกวนสัญญาณ : เป็นการโจมตีทางอิเล็กทรอนิกส์รูปแบบหนึ่ง ที่มีเป้าหมายเพื่อทำให้ระบบการรับสัญญาณไม่สามารถทำงานได้อย่างมีประสิทธิภาพ อาทิ การ “ตัดขาด” ขีดความสามารถในการรับรู้ข้อมูลอย่างสิ้นเชิง ผ่านการส่งสัญญาณรบกวนในย่านความถี่เดียวกัน ซึ่งจะส่งผลทำให้สัญญาณจริงถูกกลบ หรือสูญเสียความเสถียรจนทำให้เรือไม่สามารถยืนยันตำแหน่ง ทิศทาง ความเร็วของเรือ และไม่สามารถรับส่งข้อมูลระหว่างเรือหรือศูนย์ควบคุมได้ ซึ่งภาวะดังกล่าวอาจก่อให้เกิดอุบัติเหตุทางทะเลในลักษณะต่าง ๆ อาทิ การชนกันของเรือและเรือสูญเสียการควบคุมในสถานการณ์ฉุกเฉิน ทั้งนี้ สะท้อนให้เห็นว่าการรบกวนสัญญาณไม่ได้เป็นเพียงปัญหาเชิงเทคนิค แต่เป็นเครื่องมือสำคัญที่สามารถนำมาใช้เป็นภัยคุกคามความมั่นคงทางทะเลได้ด้วย

มิติทางด้านเทคโนโลยีด้านอาวุธ : อากาศยานไร้คนขับถือว่าเป็นภัยคุกคามความมั่นคงทางทะเลด้านไซเบอร์อีกรูปแบบหนึ่ง ซึ่งสามารถนำมาใช้เป็นเครื่องมือในกิจกรรมต่าง ๆ ทางทะเลได้หลากหลายลักษณะ ทั้งการคุกคามเรือพาณิชย์ การคุกคามโครงสร้างพื้นฐานทางด้านพลังงานและเศรษฐกิจ การใช้ลาดตระเวนและตรวจการณ์การสื่อสาร และการโจมตีทางอิเล็กทรอนิกส์ โดยข้อดีของอากาศยานไร้คนคือ สามารถปกปิดข้อมูลหรือตัวตนของผู้ก่อเหตุได้อย่างแนบเนียน สามารถเข้าใกล้เป้าหมาย ชี้เป้าหมาย ลดการใช้หรือการสูญเสียของกำลังคน และช่วยเพิ่มความแม่นยำในการโจมตี

จากเนื้อหาที่กล่าวมาข้างต้น เป็นเหตุผลที่ทำให้หน่วยงานความมั่นคงทางทะเลของไทย ต้องเร่งเสริมสร้างความตระหนักรู้ พัฒนาขีดความสามารถของเครื่องมือในการตรวจจับ เพิ่มประสิทธิภาพของระบบเฝ้าระวังป้องกันเพื่อรับมือกับภัยคุกคามความมั่นคง และกำหนดนโยบายความมั่นคงทางทะเลในลักษณะแบบองค์รวมที่ครอบคลุมในมิติทางไซเบอร์ด้วย เนื่องจากสิ่งเหล่านี้เป็นเงื่อนไขหรือปัจจัยที่สำคัญในการเฝ้าระวังป้องกันและการรักษาผลประโยชน์ของชาติทางทะเลของไทยในยุคปัจจุบัน ซึ่งภัยคุกคามความมั่นคงทางทะเลมีการปรับเปลี่ยนรูปแบบและยุทธวิธีในการก่อเหตุ/โจมตีเป้าหมาย โดยในปัจจุบันกลุ่มผู้ก่อเหตุไม่จำเป็นต้องใช้กำลังคนเพื่อก่อเหตุโดยตรง แต่สามารถสร้างความเสียหายหรือสั่นคลอนความมั่นคงทางทะเลของประเทศนั้น ๆ ผ่านเทคโนโลยีที่ทันสมัย มีต้นทุนต่ำ และไร้ร่องรอยในการติดตาม

บทส่งท้าย

เมื่อฝ่ายตรงกันข้ามเริ่มมีการนำระบบการปลอมแปลงตัวตน (Spoofing) และการรบกวนสัญญาณ (Jamming) มาใช้ร่วมกับอากาศยานไร้คนขับ ส่งผลทำให้หน่วยงานความมั่นคงของไทยเริ่มมีความตระหนักรู้ และค้นหาแนวทางเพื่อเร่งพัฒนาระบบเฝ้าระวังป้องกันภัยคุกคามความมั่นคงทางทะเลให้มีประสิทธิภาพเพิ่มมากขึ้น ทั้งนี้ เพื่อรักษาผลประโยชน์ของชาติทางทะเลและดูแลความสงบเรียบร้อยในการดำเนินกิจกรรมต่าง ๆ ในทะเลอาณาเขตของตน

ในอนาคตมีการคาดการณ์ว่า ไม่ใช่มีเพียงแค่ UAV เท่านั้นที่เป็นภัยคุกคาม แต่ยังมี USV และ UUV ที่จะเข้ามามีบทบาทใน Gray-Zone มากขึ้นด้วย ฉะนั้น ในบริบทของหน่วยงานความมั่นคงทางทะเล การนำเทคโนโลยีเข้ามาช่วยในการเฝ้าระวังป้องกันการโจมตีโครงสร้างพื้นฐานที่สำคัญ ๆ ในทะเลอาณาเขตของไทย จึงเป็นเรื่องที่หลีกเลี่ยงไม่ได้ โดยการดำเนินการภายใต้กรอบแนวคิดความมั่นคงแบบองค์รวม ที่ต้องบูรณาการการทำงานในทุกมิติ (ทั้งบนภาคพื้น ผิวน้ำ ใต้น้ำ อากาศ และไซเบอร์) ตามกรอบ Maritime Security Governance จะช่วยให้หน่วยงานความมั่นคงทางทะเลของไทย มีขีดความสามารถในการรับรู้สถานการณ์ การตัดสินใจ การกำกับดูแล และตอบสนองต่อภัยคุกคามความมั่นคงทางทะเลในภาพรวมได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

★อ้างอิง

- European Union Agency for Cybersecurity. (2019). Threat landscape for maritime transport. ENISA.
- International Maritime Organization. (2017). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3). IMO.
- International Maritime Organization. (2017). Maritime cyber risk management in safety management systems (Resolution MSC.428(98)). IMO.
- Klein, D., & O'Hanlon, M. (2020). Gray zone conflict and hybrid threats. Brookings Institution Press.
- Kraska, J., & Pedrozo, R. (2018). International maritime security law. Martinus Nijhoff Publishers.
- Maritime Executive. (2023). GNSS interference and spoofing threaten global shipping. The Maritime Executive.
- MarSec Focus. (2568). Maritime Cyber Security ความท้าทายใหม่ของโลกยุคดิจิทัล (ตอนที่ 2). กองความมั่นคงทางทะเล, สภาความมั่นคงแห่งชาติ.
- Pole Star Global. (2024). Maritime intelligence and GNSS disruption report. Pole Star Global.
- Royal United Services Institute. (2022). The use of drones in gray-zone operations. RUSI.
- United Nations Conference on Trade and Development. (2023). Review of maritime transport 2023. UNCTAD.
- United States Department of Homeland Security. (2021). Protecting critical infrastructure from unmanned aircraft systems. DHS.

วิเคราะห์โดย... ร.ต. อเนชา เผ่าพาณิชย์ และ นายกนกกฤษณ์ รักษาพรหมณ์

รายชื่อตามแนบ

๑. ปลัดกระทรวงกลาโหม

๒. ปลัดกระทรวงการต่างประเทศ

๓. ปลัดกระทรวงการท่องเที่ยวและกีฬา

๔. ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม

๕. ปลัดกระทรวงพลังงาน

๖. ปลัดกระทรวงมหาดไทย

๗. ปลัดกระทรวงศึกษาธิการ

๘. ปลัดกระทรวงคมนาคม

๙. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑๐. ปลัดกระทรวงยุติธรรม

๑๑. ปลัดกระทรวงเกษตรและสหกรณ์

๑๒. ปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

๑๓. เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

๑๔. ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

๑๕. เลขาธิการคณะกรรมการส่งเสริมการลงทุน

๑๖. เลขาธิการศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล

๑๗. ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

๑๘. ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ

๑๙. ผู้บัญชาการวิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

๒๐. ผู้อำนวยการสำนักการศึกษาทหาร สถาบันวิชาการป้องกันประเทศ

๒๑. ผู้บัญชาการทหารเรือ

๒๒. อธิบดีกรมเจ้าท่า

๒๓. อธิบดีกรมทรัพยากรทางทะเลและชายฝั่ง

๒๔. อธิบดีกรมประมง

๒๕. อธิบดีกรมศุลกากร

๒๖. อธิบดีกรมสนธิสัญญาและกฎหมาย

๒๗. อธิบดีกรมเชื้อเพลิงธรรมชาติ

๒๘. ผู้บังคับการตำรวจน้ำ

๒๙. เลขาธิการกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

๓๐. อธิการบดีมหาวิทยาลัยสุโขทัยธรรมาธิราช

๓๑. อธิการบดีมหาวิทยาลัยแม่โจ้

๓๒. อธิการบดีวิทยาลัยเทคโนโลยีทางทะเลแห่งเอเชีย

๓๓. อธิการบดีมหาวิทยาลัยบูรพา

๓๔. อธิการบดีมหาวิทยาลัยทักษิณ

๓๕. อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

๓๖. อธิการบดีมหาวิทยาลัยเกษตรศาสตร์

๓๗. อธิการบดีมหาวิทยาลัยราชภัฏสงขลา

๓๘. อธิการบดีมหาวิทยาลัยสงขลานครินทร์

๓๙. อธิการบดีจุฬาลงกรณ์มหาวิทยาลัย

๔๐. คณบดีคณะสิ่งแวดล้อมและทรัพยากรศาสตร์ มหาวิทยาลัยมหิดล

๔๑. อธิการบดีมหาวิทยาลัยราชภัฏภูเก็ต

๔๒. อธิการบดีมหาวิทยาลัยรามคำแหง

๔๓. อธิการบดีมหาวิทยาลัยธรรมศาสตร์

๔๔. อธิการบดีสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

๔๕. อธิการบดีมหาวิทยาลัยวลัยลักษณ์

3.2.1 เอกสารเรื่องเดิม

งานสารบรรณ สำนักงานอธิการบดี
หนังสือเข้าภายนอก
เลขรับ 01112
วันที่ 10/2/2569
เวลา 17:04

ที่ นร ๐๘๐๖/ว ๘๑๖

ถึง หัวหน้าส่วนราชการที่เกี่ยวข้อง

กองความมั่นคงทางทะเล สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำเอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงทางทะเล (Maritime Security Focus) หรือ “MarSec Focus” ฉบับที่ ๓/๒๕๖๙ โดยมีหัวข้อ “Cobra Gold 2026....กับการเสริมสร้างความมั่นคงทางทะเลของไทย” (รายละเอียดตามที่แนบ) เพื่อเป็นการเสริมสร้างและเผยแพร่องค์ความรู้เกี่ยวกับความมั่นคงทางทะเลให้กับหน่วยงานที่เกี่ยวข้อง พิจารณาใช้ประโยชน์ต่อไป

เรียน รองอธิการบดีฝ่ายแผนยุทธศาสตร์และนโยบาย

ด้วย กองความมั่นคงทางทะเล สำนักงานสภาความมั่นคงแห่งชาติ ขอส่งเอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงทางทะเล (Maritime Security Focus) หรือ “MarSec Focus” ฉบับที่ ๓/๒๕๖๙ โดยมีหัวข้อ "Cobra Gold 2026....กับการเสริมสร้างความมั่นคงทางทะเลของไทย"

จึงเรียนมาเพื่อ

๑. เพื่อโปรดทราบ

๒. เห็นควรเผยแพร่ให้ทราบโดยทั่วกันและสามารถดาวน์โหลดหนังสือได้ที่ https://docshare.buu.ac.th

สำนักงานสภาความมั่นคงแห่งชาติ
๑๐ กุมภาพันธ์ ๒๕๖๙

ปฏิบัติ
กองความมั่นคงทางทะเล ๑๐ ก.พ. ๒๕๖๙
สำนักงานสภาความมั่นคงแห่งชาติ ๑๐ ก.พ. ๒๕๖๙
โทร. ๐ ๒๖๒๙ ๘๐๐๐ ต่อ ๓๗๐๙
โทรสาร ๐ ๒๖๒๙ ๘๐๕๘
ไปรษณีย์อิเล็กทรอนิกส์ saraban@nsc.go.th / nsc.maritime@gmail.com

ทราบ/ดำเนินการตามเสนอ

๑๐ ก.พ. ๒๕๖๙