ความก้าวหน้าของขีดความสามารถด้านไซเบอร์และผลกระทบต่อสงครามทางเรือในอนาคต

(The Role of Advanced Cyber Capabilities and its Implication to Future Maritime War Fighting)

โดย นาวาเอก ดร.กรกช วิไลลักษณ์

กล่าวนำ

รัสเซียเริ่มสงครามรัสเซีย-ยูเครนด้วยกำลังทางบก เรือ และอากาศ เมื่อวันที่ ๒๒ กุมภาพันธ์ ค.ศ.๒๐๒๒ อย่างไรก็ดีพบกว่ารัสเซียได้เริ่มปฏิบัติการไซเบอร์ต่อเป้าหมายทางทหารและพลเรือนของยูเครนอย่างต่อเนื่องผ่านกลุ่มแฮคเกอร์ในสังกัดตั้งแต่เดือนมกราคม ค.ศ.๒๐๒๒ (Kramer, 2022) (Microsoft, 2022) โดยพบรายงานการโจมตีทางไซเบอร์ระหว่างกันอย่างต่อเนื่องจนถึงปัจจุบัน โดยพบว่าการโจมตีของรัสเซียจะมุ่งเน้นการโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารสำคัญ (Critical Information Infrastructure: CII) ของรัฐบาลและหน่วยทหารยูเครนโดยมุ่งประสงค์เพื่อลดทอนขีดความสามารถการปฏิบัติการของกองกำลังในทุก ๆ โดเมน ทั้งนี้แนวโน้มการประยุกต์ใช้ขีดความสามารถด้านไซเบอร์เชิงรุกได้รับการพัฒนาอย่างต่อเนื่องในกลุ่มประเทศนาโต เช่นเดียวกับการใช้ขีดความสามารถด้านไซเบอร์เพื่อสร้างความเกื้อกูลต่อการปฏิบัติการทางทหาร (Dowse, 2018) (Smeets, 2019) (Tangredi & Galdorisi, 2021) ทั้งนี้การโจมตี

ทางไซเบอร์ถูกพัฒนาขึ้นให้มีขีดความสามารถสูงขึ้นกว่าการโจมตีเพื่อ การเข้าถึงข้อมูลลับ การแก้ไขเปลี่ยนแปลงข้อมูล และการทำให้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารของเป้าหมายใช้การไม่ได้ โดยปัจจุบันพบว่ารัฐต่าง ๆ มีความพยายามประยุกต์ใช้เทคโนโลยีอื่น ๆ เช่น เอไอ ร่วมกับการโจมตีทางไซเบอร์เพื่อเพิ่มขีดความสามารถและปรับเปลี่ยนกลยุทธการโจมตีทางไซเบอร์ให้เกิดความได้เปรียบบนไซเบอร์โดเมนเพิ่มขึ้นอย่างเห็นได้ชัด โดยเฉพาะอย่างยิ่งการประยุกต์ใช้ในการปฏิบัติการทางเรือโดยปรากฏความพยายามเร่งพัฒนาแนวคิดการปฏิบัติและการเสริมสร้างขีดความสามารถด้านไซเบอร์ของกำลังรบทางเรือให้สอดรับกับภัยคุกคามที่เกิดขึ้นบนไซเบอร์โดเมนอย่างต่อเนื่อง

คำสำคัญ

Advanced Cyber Capabilities, Maritime Warfare, AI, CII, Network Centric Warfare

การปฏิบัติการทางเรือในอนาคตจำเป็นต้องมีขีดความสามารถด้านไซเบอร์ในระดับก้าวหน้า

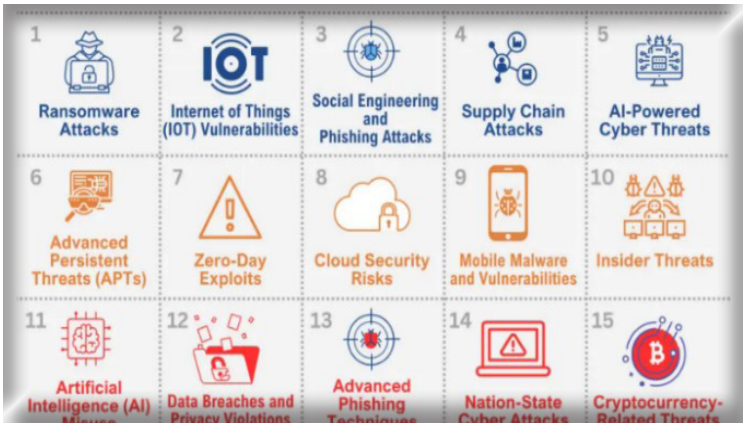
ไซเบอร์สเปซเป็นพื้นที่เสมือนที่มนุษย์รับรู้ได้จากการประยุกต์และใช้งานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารซึ่งประกอบด้วยระบบเครือข่าย อินเทอร์เน็ต ฮาร์ดแวร์และซอฟต์แวร์ซึ่งถูกเข้าถึงและใช้งานโดยมนุษย์ ในปัจจุบันพบว่าไซเบอร์สเปซเป็นพื้นที่ความขัดแย้งใหม่ที่รัฐต่างเร่งพัฒนาขีดความสามารถในการใช้โดเมนให้เกิดประโยชน์สูงสุดสำหรับการแลกเปลี่ยนข้อมูลข่าวสาร การดำเนินธุรกิจและธุรกรรม การพัฒนาเศรษฐกิจดิจิทัล ตลอดจนการพัฒนาสังคมผ่านการให้บริการแก่พลเมืองในรัฐนั้น ๆ สำหรับการประยุกต์ใช้งานในกิจการด้านความมั่นคงพบว่ารัฐมีแนวโน้มใช้ประโยชน์จากไซเบอร์โดเมนร่วมกับการปฏิบัติการทางทหารในโดเมนอื่น ๆ เพิ่มขึ้นอย่างต่อเนื่องโดยมีปฏิบัติการไซเบอร์ที่สำคัญเช่น

ปฏิบัติการไททันเรน (Titan Rain) โดยสาธารณรัฐประชาชนจีนใน ค.ศ.๒๐๐๓ โดยเป็นปฏิบัติการไซเบอร์เชิงรุกต่อโครงสร้างพื้นฐานสำคัญ (Critical Information Infrastructure: CII) ของสหรัฐอเมริกา เพื่อโจรกรรมข้อมูลด้านการทหาร และเทคโนโลยีจากโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของ บริษัทล๊อกฮีดมาติน (Lockheed Martin) และศูนย์การทดลองแห่งชาติ ซานเดีย (Sandia National Laboratories) ตลอดจนโครงสร้างพื้นฐาน สำคัญอื่น ๆ เช่นระบบบริหารจัดการพลังงานไฟฟ้าและน้ำมัน

ใน ค.ศ.๒๐๐๙ สาธารรัฐอิสราเอลดำเนินปฏิบัติการออร์ชาร์ด (Orchard) หรือ ปฏิบัติการเอาท์ไซด์เดอะบ๊อกซ์ (Outside the Box) เพื่อ โจมตีต่อเตาปฏิกรณ์นิวเคลียร์ในเมืองอาลคิบาร์ (Al Kibar Reactor) ของ สาธารณรัฐซีเรีย (วิไลลักษณ์, 2022) โดยส่งเครื่องบินF-15 จำนวน ๗ ลำ เข้าไปทิ้งระเบิดเป้าหมายทางทหาร ซึ่งปราศจากการต่อต้านจากระบบ ป้องกันภัยทางอากาศ โดยเป็นผลสืบเนื่องจากการโจมตีทางไซเบอร์ต่อ ระบบป้องกันภัยทางอากาศของซีเรีย การโจมตีทางไซเบอร์ในครั้งนั้น อิสราเอลสร้างภาพสถานการณ์บนระบบเรดาร์ตรวจการณ์ให้ไม่ปรากฏ อากาศยานที่รุกล้ำน่านฟ้าทำให้ซีเรียไม่ได้ดำเนินการตอบโต้ใด ๆ ต่อการ ละเมิดน่านฟ้า และกล่าวได้ว่าปฏิบัติการของอิสราเอลบรรลุวัตถุประสงค์ ทางทหารโดยไม่มีการสูญเสียอากาศยานเนื่องจากซีเรียไม่สามารถดำรง ขีดความสามารถด้านไซเบอร์ได้อย่างเพียงพอ

กล่าวได้ว่าปัจจุบันปฏิบัติการไซเบอร์เป็นเครื่องมือหนึ่งที่สำคัญในการ ช่วงชิงความได้เปรียบและสามารถสร้างผลกระทบต่อภูมิรัฐศาสตร์ของรัฐ ต่าง ๆ ได้ ทั้งนี้เนื่องจากปฏิบัติการไซเบอร์มีความสัมพันธ์กับข้อมูลข่าวสาร ที่ถูกผลิต ประมวลผล และส่งผ่านโครงสร้างพื้นฐานระบบสารสนเทศและ การสื่อสารซึ่งเป็นกำลังอำนาจหนึ่งของรัฐโดยเครื่องมือที่สำคัญคือการใช้ ประโยชน์ภัยคุกคามทางไซเบอร์เพื่อโจมตีต่อเป้าหมายสำคัญของคู่ขัดแย้ง เมื่อพิจารณาภัยคุกคามทางไซเบอร์ที่สำคัญใน ค.ศ.๒๐๒๔ ซึ่งแสดงในภาพที่ ๑

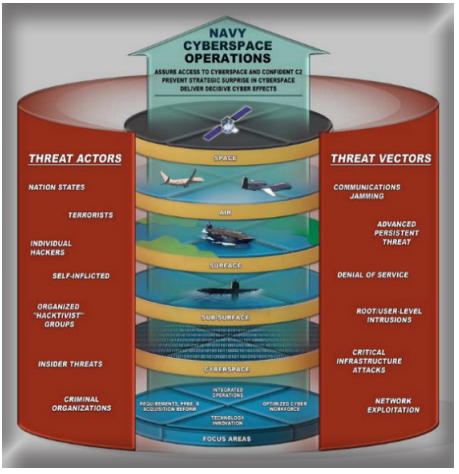
จะพบว่าภัยคุกคามทางไซเบอร์ส่วนใหญ่มีลักษณะเป็นภัยคุกคามแบบดั้งเดิม เช่น ซอฟต์แวร์เรียกค่าไถ่ (Ransomware Attacks) วิศวกรรมเชิงสังคม (Social Engineering and Phishing Attacks) การโจมตีจากภายใน (Insider Threats) และมีแนวโน้มการประยุกต์ใช้ภัยคุกคามที่มีผนวกรวมเทคโนโลยีปัญญาประดิษฐ์เพื่อขยายขีดความสามารถในการโจมตี (AI-Powered Cyber Threats) การใช้ปัญญาประดิษฐ์ในทางที่ผิด (Artificial Intelligence Misuse) และ เอพีที (Advanced-Persistent Threat: APT) ซึ่งมีความซับซ้อนสูงมากขึ้นมี และมีแนวโน้มที่จะถูกนำมาประยุกต์ใช้ในการโจมตีทางไซเบอร์ในระดับก้าวหน้า



ภาพที่ ๑ แนวโน้มภัยคุกคามสำคัญใน ค.ศ.๒๐๒๔ (Prajwal, 2023)

ทั้งนี้พัฒนาการการประยุกต์ใช้ขีดความสามารถทางไซเบอร์ได้รับการพัฒนาอย่างต่อเนื่องควบคู่ไปกับการพัฒนาขีดความสามารถทางทหาร โดยปรับเปลี่ยนจากรูปแบบของปฏิบัติการไซเบอร์แบบดั้งเดิม (Classical Cyber Operation) ซึ่งมุ่งเน้นการประยุกต์ใช้ขีดความสามารถด้านไซเบอร์ร่วมกับหลักนิยมสงครามผสมผสาน (Hybrid warfare) อันเป็นตามหลักนิยมของประเทศกลุ่มรัสเซีย จีน เกาหลีเหนือ และปฏิบัติการพิเศษ (Special Operations) และปฏิบัติการข่าวสาร (Information Operations) ของประเทศกลุ่มสหรัฐอเมริกาและนาโต้

โดยปฏิบัติการไซเบอร์แบบดั้งเดิมมุ่งเน้นการโจมตีต่อโครงสร้างพื้นฐานสำคัญที่เป็นเป้าหมายทางทหารเป็นหลัก และพัฒนาขีดความสามารถของภัยคุกคาม อย่างไรก็ดีปฏิบัติการไซเบอร์แบบก้าวหน้า (Advanced Cyber Operations) จากการต่อยอดวิธีการโจมตีแบบดั้งเดิมจากการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ชั้นสูงจึงส่งผลให้รูปแบบการโจมตี ความเสียหายและผลกระทบเปลี่ยนแปลงไปจากภัยคุกคามไซเบอร์ในระดับก้าวหน้าโดยผสมผสานเทคนิคการประมวลผลข้อมูลที่เกี่ยวข้อง ส่งผลให้เกิดรูปแบบการโจมตีแบบใหม่ ๆ ซึ่งเพิ่มประสิทธิภาพและสร้างผลลัพธ์เพิ่มเติมจากการปฏิบัติการไซเบอร์แบบดั้งเดิม โดยมีขีดความสามารถเกี่ยวกับ การก่อกวนให้เกิดข้อผิดพลาดของข้อมูล (DataMisclassification) การสังเคราะห์ปลอมแปลงข้อมูล (Synthetic Data Generation) และการวิเคราะห์ข้อมูลบนไซเบอร์โดเมน (Data Analysis) ซึ่งการกระทำดังกล่าวจะส่งผลกระทบต่อขีดความสามารถในการตัดสินใจให้สอดคล้องกับสภาพสนามรบในการตัดสินใจของผู้มีอำนาจตัดสินใจหรือความเสียหายต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารอย่างร้ายแรง และพบว่าการใช้ประโยชน์จากไซเบอร์โดเมนเป็นยุทธศาสตร์สำคัญ และในการสร้างการได้เปรียบทางไซเบอร์ และเพื่อสร้างสภาพแวดล้อมให้การปฏิบัติการทางเรือในทุก ๆ พื้นที่ปฏิบัติการทางเรือ ได้แก่ ผิวน้ำ ใต้น้ำ อากาศ อวกาศ และไซเบอร์ ดังแสดงในภาพที่ ๒



ภาพที่ ๒ การปฏิบัติการไซเบอร์ในบริบทของปฏิบัติการทางเรือ (Howard & de Arimateia da Cruz, 2017)

สำหรับการปฏิบัติการทางเรือซึ่งมีพลวัตรและความซับซ้อนของการปฏิบัติการสูงและมีการประยุกต์เทคโนโลยีชั้นสูงในระบบตรวจจับระบบสื่อสาร ระบบอาวุธและระบบเครื่องยนต์ อีกทั้งมีความต้องการการตัดสินใจอย่างแม่นยำสอดคล้องกับการเปลี่ยนแปลงของข้อมูลที่จำเป็นและเกี่ยวข้องกับการบรรลุภารกิจ เนื่องจากกองกำลังทางเรือในยุคปัจจุบันต่างประยุกต์ใช้โครงสร้างพื้นฐานการสื่อสารและเทคโนโลยีสารสนเทศและไซเบอร์สเปซในการเชื่อมโยงการสื่อสาร การสร้างความตระหนักรู้ถึงสถานการณ์ การรวบรวมและประมวลข่าวกรอง ตลอดจนการควบคุมบังคับบัญชาให้เป็นไปอย่างมีประสิทธิภาพ และกล่าวได้ว่าขีดความสามารถของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารและไซเบอร์สเปซเป็นเป้าหมายสำคัญที่จะถูกบั่นทอนขีดความสามารถหรือทำให้หมดสภาพ ทั้งนี้เมื่อพิจารณาคุณสมบัติเชิงระบบของยานรบทางเรือในยุคปัจจุบันจะพบว่ายานรบต่าง ๆ ประกอบด้วยระบบย่อย ๆ ซึ่งถูกพัฒนาขึ้นจากการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารที่มีขีดความสามารถในการประมวลผลข้อมูลดิจิทัลและมีขีดความสามารถในการเชื่อมต่อกับระบบเครือข่ายที่สามารถแลกเปลี่ยนข้อมูลกันระหว่างระบบย่อย ๆ ภายในยานรบและระหว่างยานรบ และศูนย์ปฏิบัติการ โดยกองกำลังทางเรือของประเทศในกลุ่มนาโตต่างกำหนดยุทธศาสตร์ในการเร่งพัฒนาขีดความสามารถด้านไซเบอร์ให้กับกองกำลังอย่างต่อเนื่องนับตั้งแต่ ค.ศ.๒๐๑๘ เป็นต้นมา (Thiele, 2018) และอาจกล่าวได้ว่าความสำเร็จของปฏิบัติการทางเรือในอนาคตขึ้นอยู่กับขีดความสามารถด้านไซเบอร์ในระดับก้าวหน้า

คุณลักษณะขีดความสามารถด้านไซเบอร์ในระดับก้าวหน้า

การปฏิบัติการไซเบอร์แบบดั้งเดิมจะเกี่ยวข้องกับการประยุกต์ใช้ขีดความสามารถเชิงเทคนิคของเจ้าหน้าที่ในระดับปฏิบัติเพื่อโจมตีต่อโครงสร้างพื้นฐานสำคัญของฝ่ายตรงข้าม เพื่อสร้างความได้เปรียบบนไซเบอร์โดเมนมักพบว่าแนวโน้มการโจมตีที่ส่งผลให้ระบบที่ตกเป็นเหยื่อ

ปฏิเสธการให้บริการเป็นผลกระทบพื้นฐานที่เกิดขึ้นจากการโจมตีทางไซเบอร์ อย่างไรก็ดีพัฒนาการของการโจมตีนับตั้งแต่ปี ค.ศ.๒๐๒๕ การประยุกต์ขีดความสามารถทางไซเบอร์ในระดับก้าวหน้ามีแนวโน้มถูกนำมาใช้ในการโจมตีทางไซเบอร์เพิ่มมากยิ่งขึ้น และสามารถจำแนกคุณลักษณะและขีดความสามารถด้านไซเบอร์ในระดับก้าวหน้าเป็นกลุ่ม ๆ ดังนี้

- การโจมตีทางไซเบอร์ที่สนับสนุนด้วยเทคโนโลยีเอไอ (AI-Driven Cyber Threats) โดยปฏิบัติการไซเบอร์เชิงรุกรูปแบบต่างๆ เช่น การเจาะระบบ (Penetration Testing) การโจมตีด้วยมัลแวร์ การเจาะระบบ และการโจมตีแบบเอพีที (Advanced Persistent Threats: APT) ต่อเป้าหมายสำคัญจะปฏิบัติร่วมกับการประยุกต์ใช้เทคโนโลยีเอไอ เพื่อโจมตีต่อเป้าหมายสำคัญเนื่องจากเทคโนโลยีเอไอมีขีดความสามารถในการลดขีดความสามารถในการตรวจจับและตอบสนองต่อการโจมตี หรือส่งผลให้ขีดความสามารถไซเบอร์เชิงรับของเป้าหมายเป็นไปอย่างจำกัด เทคโนโลยีที่เกี่ยวข้องได้แก่ เจนเนอร์เรทีฟเอไอ (Generative AI) ซึ่งอาจนำมาประยุกต์ใช้ในการโจมตีด้วยเทคโนโลยีกลุ่มดีปเฟค (Deepfake) ร่วมกันกับการโจมตีรูปแบบอื่น ๆ เช่น เอพีทีและวิศวกรรมเชิงสังคม (Social Engineering) โดยมีรายงานว่าสามารถขยายขีดความสำเร็จได้ถึงร้อยละ ๘๐ และอำนวยให้ผู้โจมตีสามารถโจมตีต่อเป้าหมายจำนวนมากพร้อม ๆ กัน จะเห็นได้ว่าการโจมตีที่ได้กล่าวมาส่งผลกับขีดความสามารถในการตรวจจับและบริหารจัดการเหตุการณ์การโจมตีของผู้ตกเป็นเหยื่อ อีกทั้งรองรับการโจมตีที่สนับสนุนด้วยเทคโนโลยีที่จำเป็น เช่นเดียวกับการปฏิบัติการเชิงรับซึ่งเกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ซึ่งประกอบด้วย การเฝ้าตรวจ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยก็จำเป็นต้องประยุกต์ใช้เทคโนโลยีเอไอในการปฏิบัติการเชิงรับได้เช่นเดียวกัน

- การเตรียมภูมิรัฐศาสตร์สำหรับสงครามไซเบอร์ (Geopolitical Cyber Warfare) จากรัฐที่มีขีดความสามารถในระดับก้าวหน้าเช่น สหรัฐ

รัสเซีย จีน และเกาหลีเหนือ มียุทธวิธีในการโจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญ โดยรัฐที่มีขีดความสามารถในการผลิตอุปกรณ์ฮาร์ดแวร์ เช่นสหรัฐ ไต้หวัน และจีน ต่างมีแนวโน้มประยุกต์ใช้การโจมตีต่อช่องโหว่ด้านความมั่นคงปลอดภัยที่มีบนไมโครชิปของอุปกรณ์ต่าง ๆ ซึ่งการโจมตีเหล่านั้นมีจะมีความซับซ้อนและสร้างผลกระทบในวงกว้างทั้งในระดับข้อมูลข่าวสารและกายภาพของโครงสร้างพื้นฐานที่ถูกโจมตี

- ความร่วมมือด้านอาชญากรรมบนไซเบอร์โดเมน (Global Cybercrime Collaboration and Expansion) ระหว่างรัฐพันธมิตรปรากฏให้เห็นเป็นรูปธรรมมากยิ่งขึ้นโดยเห็นได้จากพัฒนาการของกรอบการฝึกปฏิบัติการไซเบอร์ระหว่างกันในกลุ่มชาติยุโรปตะวันตกซึ่งเป็นพันธมิตรกับสหรัฐหรือการรวมตัวกันของกลุ่มประเทศที่เป็นพันธมิตรกลุ่มรัสเซีย จีน และเกาหลีเหนือ โดยพบว่ามัลแวร์ที่แพร่ระบาดตั้งแต่เดือนตุลาคม ค.ศ.๒๐๒๔ เป็นต้นมามีมัลแวร์จำนวนมากที่ได้รับการพิสูจน์ว่าเป็นมัลแวร์ที่ร่วมกันผลิตโดยกลุ่มจัมไป พิสซีส (Jumpy Pisces) ซึ่งเป็นกลุ่มแฮคเกอร์ที่ได้รับการสนับสนุนจากรัฐบาลเกาหลีเหนือ ทั้งนี้ มัลแวร์เหล่านี้จะเป็นเครื่องมือสำคัญที่สามารถนำมาใช้ในการโจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญ เพื่อลดหย่อนขีดความสามารถของฝ่ายตรงข้ามได้เป็นอย่างดี

- การโจมตีต่อห่วงโซ่อุปทาน (Supply Chain Attack Expansion) เป็นกลยุทธในการโจมตีต่อห่วงโซ่อุปทานที่เกี่ยวข้องกับการปฏิบัติการทางทหารโดยเฉพาะอย่างยิ่งการส่งกำลังบำรุง เพื่อลดหย่อน หรือบ่อนทำลายขีดความสามารถในการปฏิบัติของฝ่ายตรงข้าม โดยในบริบทของปฏิบัติการทางเรือจะเกี่ยวข้องกับการโจมตีต่อห่วงโซ่อุปทานที่เกี่ยวข้องกับการบริหารจัดการการส่งกำลังบำรุง การบริหารจัดการท่าเรือและโครงสร้างพื้นฐานสำคัญที่เกี่ยวข้อง เช่น ระบบบริหารจัดการอัตโนมัติของโรงไฟฟ้า ระบบบริหารจัดการการสื่อสารและโทรคมนาคม การสนับสนุนทางการแพทย์ เป็นต้น

ขีดความสามารถด้านไซเบอร์ในการปฏิบัติการทางเรือในอนาคต

การปฏิบัติการทางเรือในอนาคตจำเป็นต้องใช้ประโยชน์จากขีดความสามารถด้านไซเบอร์อย่างเต็มขีดความสามารถพร้อม ๆ กับการลดทอนประสิทธิภาพการใช้ประโยชน์ไซเบอร์สเปซของกองกำลังฝ่ายตรงข้ามด้วยการปฏิบัติการไซเบอร์เชิงรุกควบคู่กับไปกับการปฏิบัติการไซเบอร์เชิงรับ โดยในอนาคตขีดความสามารถด้านไซเบอร์จะเป็นแกนหลักที่สำคัญทั้งในการปฏิบัติการร่วมระหว่างกองกำลังในทุก ๆ มิติ ร่วมกับการปฏิบัติการร่วมของกำลังทางเรือด้วยการประยุกต์ใช้งานโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารบนแนวคิดการปฏิบัติการโดยใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare) ทั้งนี้ผลสัมฤทธิ์ของปฏิบัติการไซเบอร์เชิงรุกจะส่งผลต่อประสิทธิภาพและลดทอนขีดความสามารถในการค้นหาและการเข้าต่อตีต่อเป้าหมายทางการทหารของฝ่ายตรงข้าม ทั้งจากการสร้างข้อมูลปลอมหรือบิดเบือนข้อมูลข่าวสารที่ระบบค้นหาเป้าหมาย ศูนย์ยุทธการหรือระบบบริการจัดการข้อมูลภายในศูนย์ปฏิบัติการ โดยพบข้อมูลรายงานการโจมตีทางไซเบอร์เป็นส่วนหนึ่งของปฏิบัติการทางทหารอย่างต่อเนื่องในสงครามรัสเซีย-ยูเครน (Pinko, 2023) ซึ่งโครงสร้างพื้นฐานข้อมูลข่าวสารสำคัญของยูเครนถูกโจมตีอย่างต่อเนื่องก่อนที่รัสเซียจะเริ่มปฏิบัติการทางทหาร

สำหรับการโจมตีทางไซเบอร์ของคู่ขัดแย้งในสงครามรัสเซีย-ยูเครนในด้านที่เกี่ยวข้องกับปฏิบัติการทางเรือพบว่ามีความพยายามโจมตีต่อโครงสร้างพื้นฐานข้อมูลข่าวสารสำคัญของทั้งสองฝ่ายโดยหวังผลให้เกิดการรบกวนและหลอกลวงระบบกำหนดตำแหน่งบนพื้นโลก (GPS) ซึ่งใช้ในการนำเรือ นอกจากนี้ยังพบว่าโครงสร้างพื้นฐานที่เกี่ยวข้องกับการเดินเรือของพลเรือนเช่นระบบพิสูจน์ทราบเรืออัตโนมัติ (Automatic Identification System: AIS) ในพื้นที่ความขัดแย้งก็ตกเป็นเป้าหมายหนึ่งของการโจมตีทางไซเบอร์เช่นเดียวกัน เมื่อพิจารณาผลกระทบที่อาจเกิดขึ้นจากปฏิบัติการลักษณะนี้ อาจสร้างผลกระทบให้การประสานงานและการกู้ภัยทางทะเล

กระทำได้อย่างจำกัด และส่งผลต่อการวางแผนและการอำนวยการยุทธของฝ่ายที่ตกเป็นเป้าหมายของการโจมตี ทั้งนี้การโจมตีทางไซเบอร์ต่อปฏิบัติการทางเรือมีแนวโน้มส่งผลกระทบต่อความเสียหายทางกายภาพของยานรบและเรือในพื้นที่ปฏิบัติการ

นอกจากการโจมตีต่อโครงสร้างพื้นฐานสำคัญที่เกี่ยวข้องกับการเดินเรือซึ่งเป็นแหล่งข้อมูลข่าวสารหลักของการนำเรือแล้ว ระบบควบคุมบังคับบัญชาต่าง ๆ ยังเป็นเป้าหมายทางทหารที่สำคัญของปฏิบัติการไซเบอร์ที่จะเกิดขึ้นในอนาคต เนื่องจากเป็นขีดความสามารถสำคัญในการสร้างภาพสถานการณ์สำหรับการปฏิบัติการและอำนวยการยุทธในทุก ๆ ระดับ เนื่องจากระบบที่เป็นเป้าหมายของการโจมตีมักถูกพัฒนาขึ้นในลักษณะปิด แต่โมดูลย่อย ๆ ที่ทำงานร่วมกันจะถูกพัฒนาขึ้นจากเทคโนโลยี หรือผลิตภัณฑ์สำเร็จรูป (Commercial Off-the-Shelf: COTS) โดยระบบย่อย ๆ เหล่านั้นมักมีช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerabilities) ที่เปิดโอกาสให้ฝ่ายตรงข้ามโจมตีผ่านระบบเครือข่าย หรือช่องโหว่เกี่ยวกับการบริหารจัดการการเข้าใช้งานระบบได้ โดยเป็นผลจากการเชื่อมต่อกันเป็นระบบของทรัพยากรสารสนเทศและการสื่อสารที่หลอมรวมกันเพื่อสนับสนุนแนวคิดการปฏิบัติการโดยใช้เครือข่ายเป็นศูนย์กลาง ซึ่งการลดผลสำเร็จของการโจมตีที่อาจเกิดขึ้นของหน่วยต่าง ๆ ทำได้ด้วยการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการปฏิบัติการไซเบอร์เชิงรับของหน่วยนั้น ๆ ให้เป็นไปอย่างรัดกุม

การจัดการความมั่นคงปลอดภัยไซเบอร์จะคำนึงถึงการประยุกต์ใช้เทคโนโลยี กระบวนการ และทรัพยากรมนุษย์อย่างเหมาะสมสอดคล้องกับภัยคุกคามที่มีต่อทรัพยากรที่สนใจ โดยประยุกต์ใช้แนวคิดการป้องกันเชิงลึก (Defense in Depth) เพื่อเฝ้าตรวจและป้องกันทรัพยากรและข้อมูลข่าวสารที่ถูกสร้าง ประมวลผลและรับ-ส่งผ่านโครงสร้างพื้นฐานข้อมูลข่าวสารและระบบอำนวยการรบ โดยพบว่าการประยุกต์ใช้เทคโนโลยี

เพื่อการเฝ้าตรวจและป้องกันสามารถป้องกันการโจมตีและลดผลกระทบที่เกิดขึ้นทางเทคนิคต่าง ๆ ได้อย่างมีประสิทธิภาพ และพบว่ากองทัพเรือของชาติพัฒนาแล้วเช่น สหรัฐ แคนาดา ออสเตรเลียมีแนวคิดเพิ่มขีดความสามารถไซเบอร์เชิงรับให้กับหน่วยเรือให้กับผู้ปฏิบัติงานบนเรือในทุก ๆ ระดับ เนื่องจากช่องโหว่ด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์มักเกิดขึ้นจากการขาดความรู้ ทักษะและขีดความสามารถที่จำเป็นในการใช้ทรัพยากรสารสนเทศและการสื่อสารรวมถึงระบบควบคุมบังคับบัญชาต่างๆ ให้เป็นไปอย่างมั่นคงปลอดภัย (Meadors, 2022) นอกจากนี้กองทัพเรือในประเทศต่าง ๆ ที่ได้กล่าวมามีแนวคิดการจัดตั้งศูนย์ปฏิบัติการไซเบอร์บนเรือเพื่อให้การเฝ้าตรวจและบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสามารถดำเนินการได้พร้อม ๆ กับการปฏิบัติการทางเรือ เนื่องจากการปฏิบัติการทางเรือในอนาคตจำเป็นต้องใช้ศักยภาพด้านไซเบอร์ทั้งการปฏิบัติการไซเบอร์เชิงรุกและเชิงรับด้วยการประยุกต์ใช้ทรัพยากรมนุษย์และโครงสร้างพื้นฐานทรัพยากรสารสนเทศและการสื่อสารด้วยมาตรการควบคุมที่สอดรับกับภัยคุกคาม

บทสรุป

การประยุกต์ใช้ขีดความสามารถด้านไซเบอร์กับการปฏิบัติการทางทหารมีแนวโน้มเพิ่มขึ้นอย่างเห็นได้ชัดเนื่องจากไซเบอร์โดเมนมีขีดความสามารถในการประสานข้อมูลข่าวสารที่ถูกสร้าง บริหารจัดการและส่งผ่านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารที่หน่วยทหารบนโดเมนต่าง ๆ จำเป็นต้องใช้งานร่วมกัน โดยยอมรรับกันว่าไซเบอร์โดเมนเป็นโดเมนหนึ่งที่รัฐ หน่วยทหารและตัวแสดงที่ไม่ใช่รัฐต่างสร้างความเกื้อกูลในการปฏิบัติให้กับฝ่ายตนพร้อม ๆ กับพยายามลดขีดความสามารถบนไซเบอร์ของฝ่ายตรงข้าม สำหรับการปฏิบัติการทางเรือมีแนวโน้มการพึ่งพิงขีดความสามารถด้านไซเบอร์ทั้งเชิงรับและเชิงรุกมากยิ่งขึ้นเนื่อง โดยเห็นได้จากรัฐต่าง ๆ ต่างเร่งปรับปรุงขีดความสามารถการปฏิบัติการไซเบอร์

และบูรณาการขีดความสามารถทางไซเบอร์กับเทคโนโลยีต่าง ๆ รวมไปถึงการจัดตั้งหน่วยและแบ่งมอบภารกิจเพื่อสร้างขีดความสามารถในระดับก้าวหน้าสนับสนุนการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ จึงมีความจำเป็นอย่างยิ่งยวดที่กองทัพต้องปรับตัว และเสริมสร้างขีดความสามารถด้านไซเบอร์เพื่อพัฒนาขีดความสามารถที่จำเป็นสำหรับการปฏิบัติภารกิจในอนาคต

เอกสารอ้างอิง

Kramer, A. E. (2022). Hacker Bring Down Dovernment Sites in Ukaine. The New York Times.

Microsoft. (2022). Defending Ukeaine: Early Lessons from the Cyber War. Washington: Microsoft Corporation.

Tangredi, S., & Galdorisi, G. (2021). AI at War. USA: U.S. Naval Institute.

Bonnie Johnson, John M. Green, Gregory Burns, Todd Collier, Richard Cornish, Kyle Curley, . . . Jared Spears. (2023). Mapping Artificial Intelligence to the Naval Tactical Kill Chain. Naval Engineers Journal, 155-167.

Max Smeets. (2019). NATO members' Organizatioinal Path Towards Conducting Offensive Cyber Operation: A Framework for Analysis. 2019 11th International Conference on Cyber Conflict (หน้า 1-15). Tallinn: NATO CCD COE Publications.

Dowse, A. (2018). The Need for Trusted Autonomy in Military Cyber Security. Foundations of Trusted Autonomy, 203-213.

Meadors, T. B. (2022, September). Cyber Warfare Is a Navy Mission. Retrieved from U.S. Naval Institute: https://www.usni.org/magazines/proceedings/2022/september/cyber-warfare-navy-mission

กรกช วิไลลักษณ์. (2021). พัฒนาการช่วงชิงความได้เปรียบบนไซเบอร์โดเมน. ในนาวิกาธิปัตย์สาร (เล่ม ฉบับที่ 101 45-1).

กรกช วิไลลักษณ์. (2022). สงครามไซเบอร์และพัฒนาการการปฏิบัติการไซเบอร์ในอนาคต. นาวิกาธิปัตย์สาร, ฉบับที่ 102 45-2.

Ralph D. Thiele. (2018). Game Changer - Cyber Security in the Naval Domain. Strategy Series: Focus on Defense and International Security(530).

Ahmed, A. M., Hussaini, A., & Abdulhamid, A. (2022). Cyber Warfare And National Security: Imperative For Naval Operations. 2022 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE. doi: 10.1109/CSCI58124.2022.00176

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2.

Eyal Pinko. (2023). The Cyber Domain in the Russo-Ukraian War. The Begin-Sadat Center for Strategic Studies.

Prajwal. (2023, 08 10). Sprintzeal. Retrieved 01 25, 2025, from https://www.sprintzeal.com/blog/top-cybersecurity-threats

Andre Smit, และ Jamila Hammami. (2023). Cyberwarfare and the Maritime Domain. Korea Institute for Maritime Strategy.

กรกช วิไลลักษณ์. (2022). สงครามไซเบอร์และพัฒนาการการปฏิบัติการไซเบอร์ในอนาคต. นาวิกาธิปัตย์สาร, ฉบับที่ 102 45-2.

Howard, T., & de Arimateia da Cruz, J. (2017, 01 17). A Cyber Vulnerability Assessment of the U.S.Navy in the 21st Century. Retrieved 01 25, 2025, from CIMSEC: https://cimsec.org/cyber-vulnerability-assessment-u-s-navy-21st-century/