พัฒนาการ การช่วงชิงความได้เปรียบ บนไซเบอร์โดเมน

โดย นาวาเอก ดร.กรกช วิไลลักษณ์

บทคัดย่อ

ไซเบอร์โดเมนเป็นพื้นที่ปฏิบัติการสำคัญที่เชื่อมโยงปฏิบัติการทางทหารที่เกิดขึ้นบนโดเมนอื่น ๆ เข้าด้วยกันเนื่องจากการปฏิบัติการทางทหารเหล่านั้นต่างพึ่งพาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารบนไซเบอร์โดเมนในการแลกเปลี่ยนข้อมูลข่าวสาร ควบคุมบังคับบัญชา การช่วงชิงความได้เปรียบด้านข้อมูลข่าวสารสำหรับประกอบการตัดสินใจทั้งในระดับยุทธศาสตร์ ระดับปฏิบัติการ และระดับยุทธวิธี จนอาจกล่าวได้ว่าการได้เปรียบบนไซเบอร์โดเมนอาจส่งผลสำคัญต่อความมั่นคงของชาติทั้งในภาวะปกติไปจนถึงภาวะสงคราม ซึ่งสามารถศึกษาเปรียบเทียบได้จากกรณีสงครามรัสเซีย-ยูเครน ที่มีพัฒนาการมายาวนานต่อเนื่องก่อนการเริ่มรุกรานเข้าช่วงชิงพื้นที่ทางบกและทางทะเล บทความนี้วิเคราะห์รวบรวมผลการศึกษาการวิจัยและการพัฒนาขีดความสามารถที่เกี่ยวข้องกับสงครามไซเบอร์และนำเสนอข้อเสนอแนะเชิงยุทธศาสตร์เพื่อเสริมสร้างขีดความสามารถด้านไซเบอร์สำหรับกองทัพเรือเพื่อเตรียมความพร้อมให้สอดรับกับพัฒนาการของภัยคุกคามทางไซเบอร์ ที่มีแนวโน้มเปลี่ยนแปลงไปอย่างก้าวกระโดด

คำสำคัญ

สงครามไซเบอร์ ปฏิบัติการไซเบอร์ ปฏิบัติการข่าวสาร ไซเบอร์สเปซ การเรียนรู้ของเครื่อง

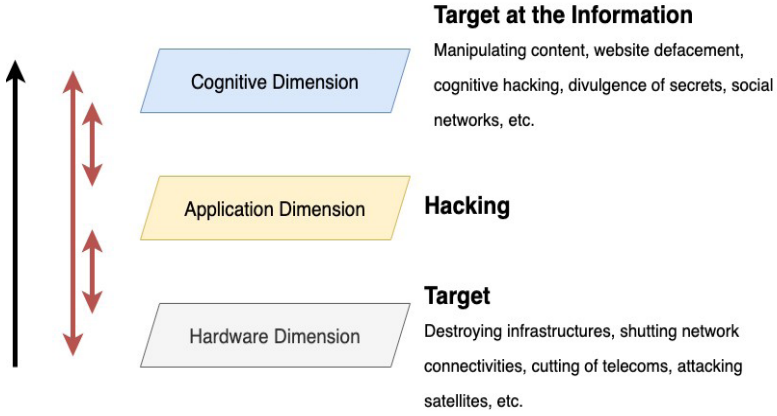
บทนำ

ปฏิบัติการไซเบอร์เป็นเครื่องมือหลักที่สำคัญในการช่วงชิงความได้เปรียบบนไซเบอร์โดเมนสืบเนื่องจากผลสำเร็จของปฏิบัติการไซเบอร์สามารถสร้างผลกระทบต่อภูมิรัฐศาสตร์ (Geopolitics) ของรัฐที่ตกเป็นเป้าหมาย และเมื่อพิจารณาความเปลี่ยนแปลงที่เกิดขึ้นกับสภาพภูมิรัฐศาสตร์

ของการเมืองระหว่างประเทศ นับตั้งแต่ปี ค.ศ.๒๐๐๐ เป็นต้นมา ไม่สามารถจะปฏิเสธได้ว่าสภาพแวดล้อมด้านความมั่นคงของรัฐต่าง ๆ มีความเกี่ยวเนื่องกับข้อมูลข่าวสารที่ถูกผลิต ประมวลผล และส่งผ่านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและเครือข่ายอินเทอร์เน็ตซึ่งเป็นโครงสร้างสำคัญที่ทำให้เกิดไซเบอร์โดเมน โดยพบว่ารัฐต่าง ๆ ดำเนินการพัฒนาขีดความสามารถด้านไซเบอร์ของตนอย่างต่อเนื่องโดยเฉพาะรัฐมหาอำนาจ เช่น สหรัฐอเมริกา สหพันธรัฐรัสเซีย และสาธารณรัฐประชาชนจีน โดยรัฐที่ได้กล่าวมาต่างช่วงชิงความได้เปรียบจากการพัฒนาขีดความสามารถเชิงรุกในการโจมตีต่อโครงสร้างพื้นฐานข้อมูลข่าวสารสำคัญ (Critical Information Infrastructure: CII) รวมถึงการพัฒนาขีดความสามารถเชิงรับในการป้องกันโครงสร้างพื้นฐานข่าวสารสำคัญของตน และตอบสนองต่อปฏิบัติการข่าวสาร (Information Operation: IO) เพื่อปกป้องและรักษาผลประโยชน์ของรัฐตนจากภัยคุกคามทั้งที่เป็นรัฐ (State Actor) และตัวแสดงที่ไม่ใช่รัฐ (Non-state Actor) ที่โจมตีที่สร้างผลกระทบต่อ Cognitive Dimension Application Dimension และ Hardware Dimension ของตัวแสดงต่าง ๆ ที่มีปฏิสัมพันธ์กันบนไซเบอร์เสปซ [1] ดังแสดงในภาพที่ ๑

จากภาพที่ ๑ จะพบว่าเป้าหมายของปฏิบัติการไซเบอร์ในแต่ละมิติจะแตกต่างกันออกไป เนื่องจากการโจมตีต่อเป้าหมายใน Hardware Dimension มุ่งประสงค์ให้บุคคลหรือระบบสารสนเทศและการสื่อสารที่ตกเป็นเหยื่อสูญเสียคุณสมบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลข่าวสารที่ถูกสร้าง จัดเก็บ ประมวลผลและส่งผ่านไปยังระบบสารสนเทศอื่น ๆ ที่เชื่อมต่อกับเหยื่อ ผลกระทบดังกล่าวอาจส่งผลให้ระบบที่ตกเป็นเหยื่อปฏิเสธการให้บริการต่อผู้ใช้งานที่มีสิทธิ์ ข้อมูลในระบบถูกปรับเปลี่ยนหรือถูกเข้าถึงและนำไปเผยแพร่หรือถูกจารกรรมข้อมูล เป็นต้น สำหรับ Application Dimension ซึ่งเปรียบเสมือนกรรมวิธีที่สามารถนำมาประยุกต์ใช้ในการโจมตี (Hacking) ต่อเป้าหมายแล้วละเมิดความมั่นคงปลอดภัย

ของทรัพยากรสารสนเทศและการสื่อสารซึ่งการกระทำดังกล่าวย่อมส่งผลต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร และ Cognitive Dimension ซึ่งเป็นมิติการรับรู้ถึงข้อมูลข่าวสารบนไซเบอร์สเปซของสังคม ทั้งนี้วิธีการดังกล่าวไม่จำเป็นต้องกระทำผ่านการโจมตีแต่เพียงอย่างเดียว เนื่องจากผู้ริเริ่มโจมตีอาจนำเข้าข้อมูลสามารถสร้างเรื่องราวให้เกิดความรู้สึกในด้านลบต่อสังคม เพื่อบรรลุวัตถุประสงค์ทางทหารแก่ผู้ริเริ่มได้เช่นเดียวกันโดยเห็นได้จากกรณีวิกิลีกส์ (Wikileaks) [2] เป็นต้น



ภาพที่ ๑ ผลกระทบและปฏิสัมพันธ์ระหว่างมิติและตัวแสดงบนไซเบอร์โดเมน [1]

การช่วงชิงความได้เปรียบเหนือไซเบอร์สเปซเกี่ยวข้องกับข้อมูลข่าวสารที่ถูกสร้าง ประมวลผล จัดเก็บและส่งต่อผ่านโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารที่เชื่อมต่อกันผ่านเครือข่ายอินเทอร์เน็ตหรือโครงข่ายการสื่อสารและโทรคมนาคมอื่น ๆ โดยการได้เปรียบเชิงข้อมูลข่าวสารบนไซเบอร์สเปซ สามารถจำแนกเป็นขีดความสามารถด้านการ

ปฏิบัติการข่าวสารหลัก ๆ ๖ ด้านได้แก่ การรับรู้และเข้าใจสถานการณ์ การควบคุมบังคับบัญชาและการสื่อสาร (Command and Control, and Communication) การยุทธ์ต่อระบบควบคุมบังคับบัญชา (Command and Control Warfare: C2W) การทำลายโครงสร้างการบังคับบัญชาด้วยปฏิบัติการข่าวสาร การเสริมสร้างโครงสร้างการบังคับบัญชาด้วยปฏิบัติการข่าวสาร และการสร้างอิทธิพลต่อตัวแสดงอื่น ๆ ด้วยปฏิบัติการข่าวสาร ไซเบอร์คิลเชน (Cyber Kill Chain)

แนวคิดไซเบอร์คิลเชนถูกพัฒนาขึ้นจากแนวทางการโจมตีเป้าหมายทางทหาร (Kill Chain) แบบพื้นฐานซึ่งประกอบด้วย ๔ ขั้นตอนได้แก่ การค้นหาและพิสูจน์ทราบเป้าหมาย (Identification of Target) การส่งกองกำลังไปยังเป้าหมาย (Dispatching of forces to Target) การโจมตีต่อเป้าหมาย (Initiation of attack to Target) และการทำลายเป้าหมาย (Destruction of Target) สำหรับแนวคิดไซเบอร์คิลเชนถูกพัฒนาขึ้นโดยบริษัทล๊อกฮีทมาร์ติน (Lockheed Martin) โดยมีวัตถุประสงค์หลักเพื่อระบุขั้นตอนการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสาร การค้นหาช่องโหว่ด้านความมั่นคงปลอดภัย และการยับยั้งการโจมตีที่เกิดขึ้นในทุกขั้นตอนการโจมตีของผู้ไม่ประสงค์ดี ไซเบอร์คิลเชน[3] มีขั้นตอนสำคัญ ๗ ขั้นตอนได้แก่ การค้นหาเป้าหมาย (Reconnaissance) การพัฒนาและคัดเลือกวิธีการโจมตี (Weaponization) การเริ่มการโจมตี (Delivery) การเจาะระบบ (Exploitation) การติดตั้งชุดคำสั่งซอฟต์แวร์ (Installation) การยึดและควบคุมเป้าหมาย (Command and Control) และการดำเนินการให้บรรลุวัตถุประสงค์ (Action of Objectives) ทั้งนี้ในแต่ละขั้นตอนอาจมีวิธีการดำเนินการให้บรรลุวัตถุประสงค์เฉพาะที่หลากหลายขึ้นอยู่กับคุณลักษณะของเป้าหมายโดยมีรายละเอียดดังที่แสดงในตารางที่ ๑

ตารางที่ ๑ วิธีการและวัตถุประสงค์เฉพาะในแต่ละขั้นตอนของไซเบอร์คิลเชน

ขั้นตอน	วัตถุประสงค์	วิธีการดำเนินการ
การค้นหาเป้าหมาย	เพื่อรวบรวมข่าวสารสำคัญของเป้าหมายที่อาจเป็นประโยชน์ต่อการโจมตี เช่น อีเมล์แอดเดรสของบุคคลในองค์กร หมายเลขโทรศัพท์ ไอพีแอดเดรสของเครื่องให้บริการต่าง ๆ ของเป้าหมาย ข้อมูลบุคลากรบนโซเชียลมีเดีย ฯลฯ	- การรวบรวมข้อมูลจากแหล่งข้อมูลเปิด เช่น Search engines ข้อมูลสาธารณะของเป้าหมายที่มีบนเว็บไซต์อันได้แก่ อีเมลแอดเดรสและข้อมูลอื่น ๆ ที่อาจเป็นประโยชน์ วิธีการนี้เป้าหมายจะไม่มีโอกาสทราบว่าข้อมูลของตนถูกรวบรวมโดยผู้ไม่ประสงค์ดี - การแสกนเครือข่ายและการค้นหาช่องโหว่ด้านความมั่นคงปลอดภัยบนโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารของเป้าหมาย ทั้งนี้วิธีการนี้เป้าหมายสามารถทราบได้ว่ากิจกรรมนี้เกิดขึ้นกับทรัพยากรของตนได้จากการติดตั้งและดำเนินการเฝ้าตรวจความมั่นคงปลอดภัยทรัพยากรของตน
การพัฒนาและคัดเลือกวิธีการโจมตี	เพื่อคัดเลือกวิธีการโจมตี (Attack Vector) ที่เหมาะสมสำหรับการโจมตีต่อเป้าหมายนั้น ๆ	-การพัฒนาชุดคำสั่งสำหรับโจมตีต่อช่องโหว่บนระบบงานเว็บของเป้าหมาย -การพัฒนามัลแวร์เพื่อโจมตีต่อเป้าหมาย -การสร้างอีเมลสำหรับการโจมตีต่อบุคลากรในองค์กรเป้าหมายสำหรับการโจมตีแบบฟิชชิ่งหรือเทคนิคด้านวิศวกรรมสังคม (Social engineer) เป็นต้น

การเริ่มการโจมตี	เพื่อส่งชุดคำสั่งหรือมัลแวร์เข้าสู่เป้าหมาย	-การส่งฟิชชิ่งอีเมล์ที่เหยื่อคลิ๊กลิงค์แล้วจะมีการดาวน์โหลดมัลแวร์เข้าสู่เครื่องคอมพิวเตอร์หรืออุปกรณ์ของเหยื่อ -การส่งชุดคำสั่งเพื่อโจมตีต่อช่องโหว่เกี่ยวกับ SQL Injection บนระบบงานเว็บของเป้าหมาย -การส่ง Removable Storage เช่น USB Disk ที่มีมัลแวร์แฝงตัวอยู่ให้กับบุคลากรในองค์กรเป้าหมาย -ฯลฯ
การเจาะระบบ	เพื่อทำการติดตั้งชุดคำสั่ง ซอฟต์แวร์ เปลี่ยนแปลงข้อมูลที่มีในเครื่องเป้าหมาย	-การเจาะระบบด้วยซอฟต์แวร์หรือชุดคำสั่งที่สามารถโจมตีต่อช่องโหว่ด้านการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการ ซอฟต์แวร์ระบบให้บริการต่างๆ เช่น Web server Database servers ฯลฯ -เมื่อโจมตีช่องโหว่ดังกล่าวสำเร็จ ผู้ไม่ประสงค์ดีอาจทำการฝังชุดคำสั่ง สั่งให้สคริปต์ทำงานตามที่ถูกออกแบบในขั้นที่ ๒ เพื่อทำการเปลี่ยนแปลงข้อมูลหรือปรับเปลี่ยนกระบวนการทำงานบนเครื่องเหยื่อ

การติดตั้งชุดคำสั่งซอฟต์แวร์	เพื่อติดตั้งซอฟต์แวร์จำพวกแบคดอร์ (Backdoor) โทรจัน (Trojan) รูทคิทส์ (Rootkits) ที่สามารถอนุญาตให้ผู้ไม่ประสงค์ดี สามารถเข้าถึงทรัพยากรบนเป้าหมายได้อย่างไม่จำกัด หรือปิดการทำงานของระบบตรวจจับผู้บุกรุกบนเครื่องเป้าหมายนั้น ๆ	-การดาวน์โหลดชุดคำสั่งซอฟต์แวร์และติดตั้งลงบนเครื่องเป้าหมาย -การล่อลวงให้เหยื่อคลิ๊กดาวน์โหลดและติดตั้งมัลแวร์ที่อนุญาตให้มีการเข้าถึงจากระยะไกลได้
การยึดและควบคุมเป้าหมาย	เพื่อควบคุมการปฏิบัติการของทรัพยากรสารสนเทศและเครือข่ายของเป้าหมาย	-การได้มาซึ่งสิทธิ์ในการบริหารจัดการทรัพยากรสารสนเทศและเครือข่ายที่เชื่อมต่อ โดยเป็นผลจากการเจาะระบบเป็นทอด ๆ
การดำเนินการให้บรรลุวัตถุประสงค์	เพื่อคัดลอกหรือโอนย้ายข้อมูลจากทรัพยากรสารสนเทศและการสื่อสารที่ตกเป็นเหยื่อ รวมไปถึงการเข้ารหัสลับอุปกรณ์จัดเก็บข้อมูล การคัดลอกกุญแจรหัสหรือชุดข้อมูลใบรับรองอิเล็กทรอนิกส์ สำหรับนำไปใช้ในการโจมตีต่อทรัพยากรอื่น ๆ ที่มีการเชื่อมต่อกับระบบที่ตกเป็นเหยื่อ	-การส่งผ่านข้อมูลไปยังผู้โจมตีผ่านซอฟต์แวร์ที่ใช้ในขั้นตอนที่ ๖ -การเข้ารหัสลับฮาร์ดดิสก์เพื่อเรียกค่าไถ่ -การลบหรือทำลายข้อมูลที่ถูกจัดเก็บบนเครื่องเป้าหมาย -การเปลี่ยนแปลงข้อมูลที่ถูกจัดเก็บบนเครื่องเป้าหมาย

เมื่อพิจารณาขั้นตอนต่าง ๆ ที่เกิดขึ้นบนไซเบอร์คิลเชนแล้วจะพบว่าการป้องกันทรัพยากรสารสนเทศและการสื่อสารจากการโจมตีของผู้ไม่หวังดี จำเป็นต้องมีเจ้าหน้าที่ ๆ มีขีดความสามารถเชิงเทคนิคและการบริหารจัดการในระดับผู้เชี่ยวชาญ เนื่องจากบุคลากรกลุ่มนี้เป็นกำลังสำคัญในการวิเคราะห์และออกแบบนโยบายด้านปฏิบัติการไซเบอร์เชิงป้องกัน (Defensive Cyber Operation) การประยุกต์ใช้เครื่องมือสำหรับการตรวจจับการบุกรุก ทั้งในระดับเครือข่ายและโฮสต์

(Network-based and Host-based Intrusion/Prevention System) การประยุกต์ใช้เทคนิคการเฝ้าตรวจความมั่นคงปลอดภัยของข้อมูลข่าวสาร (Enterprise Information Security Monitoring) และไซเบอร์คิลเชน จะถูกนำมาประยุกต์ใช้ในการป้องกันยับยั้งการโจมตีของผู้ไม่ประสงค์ดีได้ จากการจำแนกขั้นตอนเป็นลำดับชั้นดังที่ได้กล่าวมา ยกตัวอย่างเช่น เมื่อเจ้าหน้าที่เฝ้าตรวจความมั่นคงปลอดภัยรายงานความพยายามสแกนหาช่องโหว่ด้านความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ผ่านหน้าเว็บเพจ พร้อม ๆ กับตรวจพบความพยายามโจมตีต่อช่องรับข้อมูลบนหน้าเว็บเพจด้วยเทคนิค SQL Injection จากไอพีแอดเดรสเดียวกัน ผู้ที่มีหน้าที่รับผิดชอบได้รับข้อมูลที่บ่งชี้ความเป็นภัยในระดับสูงจึงบังคับใช้กฎบนไฟร์วอลในการระงับการเข้าถึงจากไอพีแอดเดรสนั้น จากนั้นจึงเริ่มปฏิบัติการตามระเบียบปฏิบัติประจำเพื่อตอบสนองต่อการโจมตี (Incident Response) เพื่อวิเคราะห์ผลสำเร็จและขอบเขตความเสียหาย เป็นต้น

ปฏิบัติการไซเบอร์ในภาวะสงคราม

สงครามไซเบอร์เป็นภัยคุกคามต่อรัฐอย่างไม่ต้องสงสัย โดยเห็นได้จากในสถานการณ์ความขัดแย้งระหว่างรัฐในยุคปัจจุบันจะพบว่ามีการปฏิบัติการไซเบอร์เป็นส่วนหนึ่งของปฏิบัติการทางทหารที่กระทำต่อเป้าหมายทางทหาร ทั้งในระดับยุทธศาสตร์และระดับยุทธการ เนื่องจากปฏิบัติการไซเบอร์สามารถขยายผลการปฏิบัติของปฏิบัติการทางทหารในทุก ๆ ระดับให้มีประสิทธิผลมากยิ่งขึ้น ยกตัวอย่างเช่นการโจมตีทางไซเบอร์ต่อระบบป้องกันภัยทางอากาศด้วยการเปลี่ยนแปลงหรือปลอมแปลงข้อมูลเป้าหมายที่ถูกตรวจจับโดยเรดาร์จะสามารถเพิ่มโอกาสความสำเร็จให้กับการปฏิบัติการทางอากาศ [4,5] ได้เป็นต้น และเมื่อพิจารณาการรุกรานยูเครนของรัสเซียเมื่อวันที่ ๒๔ กุมภาพันธ์ พ.ศ.๒๕๖๕ จะพบว่าการใช้ขีดความสามารถด้านไซเบอร์ของทั้งสองฝ่ายถูกนำมาใช้เพื่อสร้างความได้เปรียบทั้งในด้านปฏิบัติการทางทหาร และการดำเนินยุทธศาสตร์การป้องกัน

ประเทศของรัฐบาลทั้งสองฝ่าย สามารถกล่าวได้ว่าปฏิบัติการไซเบอร์ที่เกิดขึ้นระหว่างความขัดแย้งซึ่งเริ่มขึ้นตั้งแต่ พ.ศ.๒๕๕๗ เป็นต้นมานั้น เป็นปฏิบัติการไซเบอร์ทางการทหารที่มีขนาดใหญ่ที่สุดนับตั้งแต่มีการสร้างคำจำกัดความ “สงครามไซเบอร์” เป็นต้นมา [6]

ภัยคุกคามแบบดั้งเดิม (Classical Cyber Operations)

ขีดความสามารถด้านไซเบอร์ถูกนำมาใช้สนับสนุนปฏิบัติการทางทหารปรากฏในผลการวิจัยปฏิบัติการไซเบอร์ขนาดใหญ่ ๓ ครั้งที่เกิดขึ้นกับสาธารณรัฐจอร์เจียเมื่อปี ค.ศ.๒๐๐๗ สหรัฐอเมริกาในปี ค.ศ.๒๐๑๒ และยูเครนระหว่าง ค.ศ.๒๐๑๓ – ค.ศ.๒๐๑๕ [7] ซึ่งผู้วิจัยศึกษาเปรียบเทียบการประยุกต์ใช้ปฏิบัติการไซเบอร์ซึ่งเป็นส่วนหนึ่งของหลักนิยมสงครามผสมผสาน (Hybrid warfare) ซึ่งเป็นแนวคิดการประยุกต์ใช้ทั้งพลังอำนาจทั้งปวงในการช่วงชิงความได้เปรียบฝ่ายตรงข้ามตั้งแต่ก่อนการประกาศสงคราม และภายใต้ภาวะสงคราม [8] ซึ่งในความขัดแย้งระหว่างรัสเซีย-ยูเครนในช่วง ค.ศ.๒๐๑๓ ได้ปรากฏการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญของยูเครนจำนวนหลายครั้ง ซึ่งเป้าหมายการโจมตีส่วนใหญ่จะมุ่งโจมตีต่อเว็บไซต์หน่วยงานรัฐและเอกชนที่เป็นโครงสร้างพื้นฐานข่าวสารสำคัญ (Critical Information Infrastructure: CII) โดยมีมุ่งประสงค์สำคัญในการรบกวนและสกัดขัดขวางการประมวลผลข้อมูลของเป้าหมาย และสร้างความตระหนกให้กับพลเมืองของชาติที่ตกเป็นเหยื่อด้วยการโจมตีต่อโครงสร้างพื้นฐานด้านสาธารณูปโภค เช่น ระบบพลังงาน ระบบขนส่งมวลชน ซึ่งมักประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเพิ่มประสิทธิภาพการให้บริการต่อพลเมือง ทั้งนี้เมื่อพิจารณาเป้าหมายและวิธีการโจมตีแล้วจะพบว่ายุทธวิธีนี้ถูกนำมาใช้อย่างเป็นรูปธรรม ตั้งแต่เหตุการณ์ความขัดแย้งระหว่าง รัสเซีย-เอสโทเนีย ตั้งแต่ ค.ศ.๒๐๐๗ [9]

ในช่วงเหตุการณ์ความขัดแย้งระหว่าง รัสเซีย-เอสโทเนีย มีรายงานการโจมตีต่อระบบให้บริการโดเมน (DNS) ด้วยเทคนิคการโจมตีแบบดีดอส (Distributed Denial of Service: DDoS) โดยใช้เครือข่ายบอทเน็ต (Botnet) จากคอมพิวเตอร์ที่ตกเป็นเหยื่อของมัลแวร์ที่แพร่กระจายผ่านอีเมลที่แอบติดตั้งมัลแวร์โดยที่ผู้ใช้งานไม่รู้ตัว แนวทางการโจมตีนี้ถูกใช้งานเป็นครั้งแรกในปี ค.ศ.๑๙๙๘ [10] โดยมีรายงานกลุ่มทมิฬไทเกอร์ (Tamil Tiger) ซึ่งเป็นกลุ่มผู้มีอุดมการณ์ทางการเมืองแบ่งแยกดินแดนในศรีลังกา ทำการโจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญของรัฐบาลศรีลังกา ส่งผลให้เว็บไซต์หน่วยงานรัฐบาลไม่สามารถให้บริการแก่ผู้ใช้งาน จะเห็นได้ว่าปฏิบัติการไซเบอร์เชิงรุกสามารถกระทำการโจมตีต่อเป้าหมายได้ทั้งจากตัวแสดงที่เป็นรัฐและตัวแสดงที่ไม่ใช่รัฐ ซึ่งผู้ริเริ่มอาจมีขีดความสามารถเลือกการโจมตีที่เหมาะสมกับเป้าหมายได้หลากหลายวิธี นอกจากการโจมตีแบบดีดอสที่มีมุ่งประสงค์เพื่อทำให้เป้าหมายปฏิเสธการให้บริการ จึงกล่าวได้ว่าการใช้อาวุธทางไซเบอร์ (Cyber weapons) ของรัฐเป็นการใช้ขีดความสามารถด้านไซเบอร์ (Means) เพื่อสร้างผลกระทบ (Effects) ต่อเป้าหมายจนสามารถบรรลุวัตถุประสงค์ (Objectives) ของปฏิบัติการ และสามารถนำแนวคิดนี้มาวิเคราะห์ปฏิบัติการไซเบอร์ที่เคยเกิดขึ้นเพื่อชี้ให้เห็นถึงภัยคุกคามที่เกิดขึ้นจากปฏิบัติการไซเบอร์ที่เคยเกิดขึ้นในอดีต เช่น ปฏิบัติการออร์ชาร์ด (Operation Orchard) เป็นต้น

ความสำเร็จของปฏิบัติการออร์ชาร์ดเริ่มต้นจากความบังเอิญที่เจ้าหน้าที่ระดับสูงของซีเรียละเลยให้คอมพิวเตอร์ส่วนตัวถูกเข้าถึงได้ระหว่างการเข้าพักที่โรงแรมแห่งหนึ่งในลอนดอน ส่งผลให้สายลับของอิสราเอลสามารถติดตั้งมัลแวร์ที่แอบส่งข้อมูลทั้งหมดที่ถูกส่งเข้าและออกจากคอมพิวเตอร์เครื่องนั้น จากการวิเคราะห์ข้อมูลที่มีอยู่บนเครื่องหน่วยข่าวกรองของอิสราเอลวิเคราะห์ข้อมูลภาพของ นายจอน จีบู ซึ่งเป็นบุคคลสำคัญในโครงการพัฒนาขีดความสามารถด้านนิวเคลียร์ของเกาหลีเหนือ

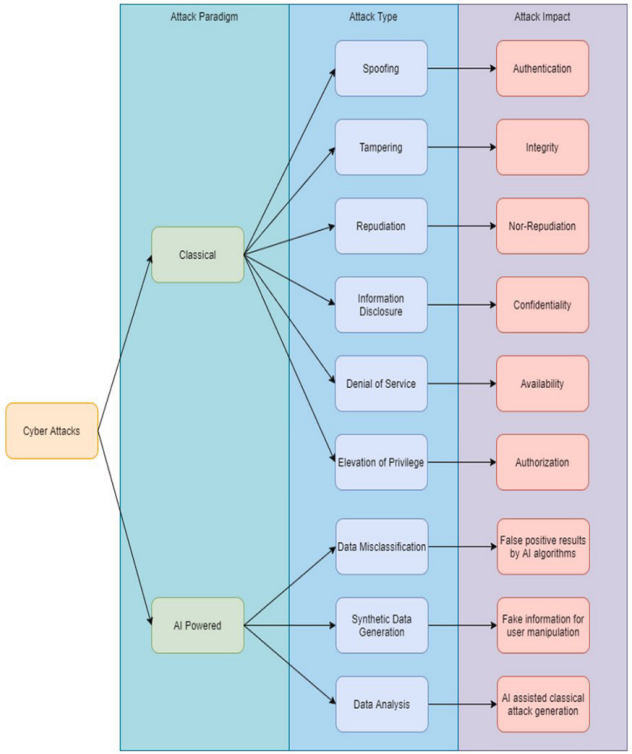
และ นายอิบราฮิม โอธมาน ซึ่งเป็นผู้อำนวยการคณะกรรมการพลังงานนิวเคลียร์ของซีเรียยืนคู่กันในซีเรีย นอกจากนี้ยังพบข้อมูลที่ทำให้เชื่อได้ว่าซีเรียกำลังดำเนินโครงการการพัฒนาคุณภาพพลูโตเนียมผ่านความร่วมมือกับเกาหลีเหนือเพื่อพัฒนาเป็นอาวุธนิวเคลียร์ [11] ซึ่งรัฐบาลอิสราเอลพิจารณาว่าเป็นภัยคุกคามระดับสูงต่อรัฐตนจึงตัดสินใจส่ง บ. F15I จำนวน ๗ ลำเข้าโจมตีต่อที่ตั้งโครงการพัฒนาขีดความสามารถดังกล่าวในวันที่ ๖ กันยายน ค.ศ.๒๐๐๗ ซึ่งอยู่ลึกเข้าไปในดินแดนของซีเรียโดยปราศจากการต้านทานจากระบบป้องกันภัยทางอากาศของซีเรียเนื่องจากระบบป้องกันภัยทางอากาศของซีเรียได้ถูกโจมตีทางไซเบอร์จนไม่สามารถรับรู้ภาพสถานการณ์ที่เกิดขึ้นบนห้วงอากาศของตนเองได้

ในปฏิบัติการออร์ชาร์ดเราคงไม่สามารถปฏิเสธได้ว่าความสำเร็จที่เกิดขึ้นเป็นผลจากความสำเร็จที่เริ่มต้นจากการฝังมัลแวร์ลงบนอุปกรณ์อิเล็กทรอนิกส์ของเป้าหมาย (ทั้งคอมพิวเตอร์ส่วนบุคคลและระบบป้องกันภัยทางอากาศ) จึงส่งผลกระทบทางตรงได้แก่ลวงทางข่าวสารอันเป็นผลสำเร็จจากการโจมตีระบบเรดาร์ และมีผลกระทบทางอ้อมทางกายภาพคือการเกิดความเสียหายร้ายแรงต่อโครงการพัฒนาอาวุธนิวเคลียร์ สำหรับเป้าหมายของปฏิบัติการนี้คือการลวงทางทหารต่อระบบป้องกันภัยทางอากาศและสามารถบรรลุวัตถุประสงค์ได้ทุกๆ ระดับคือในระดับยุทธศาสตร์สามารถทำลายขีดความสามารถด้านนิวเคลียร์ได้สำเร็จ ในระดับยุทธการสามารถบรรลุภารกิจได้โดยปราศจากการสูญเสียและใช้ทรัพยากรที่มีอย่างมีประสิทธิภาพ สำหรับระดับยุทธวิธีอิสราเอลสามารถสร้างภาพสถานการณ์ที่ได้ประโยชน์กับฝ่ายตนได้เป็นผลสำเร็จ และกล่าวได้ว่าพัฒนาการของขีดความสามารถด้านไซเบอร์ถูกนำมาใช้ประโยชน์ในปฏิบัติการทางทหารอย่างต่อเนื่องในหลาย ๆ ปฏิบัติการโดยขีดความสามารถดังกล่าวพัฒนาควบคู่ไปพร้อม ๆ กับขีดความสามารถด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐนั้น ๆ โดยจะเห็นได้จากแนวทางการโจมตีทางไซเบอร์

ที่ผ่าน ๆ มาอย่างเห็นได้ชัดเนื่องจากรัฐต่างมีความจำเป็นต้องช่วงชิงความได้เปรียบบนไซเบอร์โดเมนอย่างหลีกเลี่ยงไม่ได้ [12]

ภัยคุกคามแบบก้าวหน้า (Advanced Cyber Operations)

ความต้องการความได้เปรียบบนไซเบอร์โดเมนส่งผลให้รัฐต่าง ๆ พัฒนาขีดความสามารถด้านไซเบอร์อย่างต่อเนื่อง โดยพบว่าขีดความสามารถด้านไซเบอร์ที่ถูกพัฒนาขึ้นมีความเปลี่ยนแปลงไปจากขีดความสามารถพื้นฐานในยุคแรก ๆ โดยมีรายงานผลการศึกษาพัฒนาการของการโจมตีทางไซเบอร์ดังแสดงในภาพที่ ๒ [13]



ภาพที่ ๒ พัฒนาการของการโจมตีทางไซเบอร์ [13]

ผลการศึกษาของยามิน และคณะ [13] ชี้ให้เห็นว่าภัยคุกคามไซเบอร์แบบก้าวหน้าถูกขับเคลื่อนจากความก้าวหน้าของเทคโนโลยีปัญญาประดิษฐ์ และส่งผลให้ภัยคุกคามทางไซเบอร์มีขีดความสามารถที่สำคัญแตกต่างจากภัยคุกคามแบบดั้งเดิมได้แก่ การก่อกวนให้เกิดข้อผิดพลาดของข้อมูล (Data Misclassification) การสังเคราะห์ปลอมแปลงข้อมูล (Synthetic Data Generation) และการวิเคราะห์ข้อมูลบนไซเบอร์โดเมน (Data Analysis) จะเห็นได้ว่าแนวโน้มการโจมตีทางไซเบอร์จะมุ่งโจมตีต่อขีดความสามารถในการตัดสินใจของผู้มีอำนาจตัดสินใจในทุก ๆ ระดับ นอกจากนี้ผลการศึกษายังบ่งชี้ถึงแนวโน้มการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ ในการเพิ่มผลสำเร็จของการโจมตีจากภัยคุกคามแบบดั้งเดิม เนื่องจากการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์อย่างเหมาะสม จะช่วยลดโอกาสที่ปฏิบัติการไซเบอร์เชิงรุกจะถูกตรวจพบได้ในการโจมตีบางแบบ เช่น การปลอมแปลง (Spoofing) การดักรับเปลี่ยนแปลงข้อมูล (Tampering) และการทำให้ระบบปฏิเสธการให้บริการ (Denial of Service) โดยเป็นผลจากขีดความสามารถในการก่อกวนให้เกิดข้อมูลที่ผิดพลาดนั่นเอง

เทคโนโลยีปัญญาประดิษฐ์สามารถนำมาประยุกต์ใช้ในการโจมตีทางไซเบอร์ต่อบุคคล เช่น การโจมตีแบบวิศวกรรมเชิงสังคม (Social Engineering) จากการประยุกต์เทคโนโลยีปัญญาประดิษฐ์ในการวิเคราะห์คุณลักษณะจำเพาะของเหยื่อ (Target Profiling) ซึ่งจะช่วยให้การล่อลวงผู้ตกเป็นเหยื่อการโจมตีให้หลงเชื่อและปฏิบัติตามความตั้งใจของผู้โจมตีได้มากยิ่งขึ้น การประยุกต์ใช้เทคนิคการเรียนรู้ของเครื่อง (Machine learning) ในการจำลองหรือปลอมแปลงข้อมูลจะช่วยสร้างความน่าเชื่อถือให้กับปฏิบัติการข่าวสารในยุคปัจจุบันได้อย่างน่าเชื่อถือ โดยอาจสามารถสร้างแรงกระเพื่อมทางสังคมให้กับกลุ่มเป้าหมายได้เป็นอย่างดี โดยสามารถเห็นได้จากความสำเร็จของปฏิบัติการโฆษณาชวนเชื่อผ่านบล็อกเกอร์ (Blogger) ที่ถูกพัฒนาขึ้นจากเทคโนโลยีดีปเลินนิ่ง (Deep Learning) [14] ที่ถูกเผย

แพร่บนสังคมออนไลน์ที่ได้รับความนิยมสามารถสร้างกรอบความคิดจากการเผยแพร่ข้อมูลที่จูงใจให้สนับสนุนรัฐบาลรัสเซียต่อประชาชนยูเครนในช่วงก่อนการรุกล้ำพรมแดน เป็นต้น

ความต้องการการพัฒนาขีดความสามารถเชิงรุกของอาวุธทางไซเบอร์นับตั้งแต่ ค.ศ.๒๐๑๐ ของรัฐต่าง ๆ มีแนวโน้มเปลี่ยนแปลงจากการสร้างความเสียหายเชิงกายภาพให้กับเป้าหมายทางทหาร แต่เป็นการเสริมสร้างขีดความสามารถในการรวบรวมข่าวกรองและการต่อต้านข่าวกรองด้านความมั่นคง ด้วยการแสวงหาประโยชน์จากการเผยแพร่มัลแวร์ที่มีขีดความสามารถในการแพร่กระจายและมีฟังก์ชันการทำงานที่หลากหลาย เช่น การทำงานในลักษณะของซอฟต์แวร์เรียกค่าไถ่ (Ransomware) การทำงานในลักษณะของม้าโทรจัน (Trojan) การรบกวนระบบควบคุมบังคับบัญชา และการโจมตีต่อระบบปัญญาประดิษฐ์ที่ใช้ในการวิเคราะห์ข้อมูลข่าวสารฝ่ายตรงข้าม ฯลฯ โดยสังเกตได้จากขีดความสามารถของรัฐที่มีขีดความสามารถทางไซเบอร์เชิงรุกเช่น สหรัฐอเมริกา รัสเซีย อิสราเอล สาธารณรัฐประชาชนจีน สหราชอาณาจักร และฝรั่งเศสต่างมีโครงการพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารเพื่อรองรับการวิเคราะห์ข่าวกรองและการต่อต้านการโจมตีต่อระบบข่าวกรองอย่างต่อเนื่อง [13,14]

การป้องกันการโจมตีจากอาวุธทางไซเบอร์เชิงรุกจะขึ้นอยู่กับความสามารถในการบริหารจัดการความมั่นคงปลอดภัยของโครงสร้างพื้นฐานข่าวสารสำคัญ (Critical Information Infrastructure) และการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารซึ่งหลอมรวมกันเป็นอาณาเขตบนไซเบอร์โดเมนที่รัฐนั้น ๆ ดังนั้น การลดขีดความสามารถเชิงรุกของรัฐที่มุ่งประสงค์โจมตีจึงต้องประยุกต์ใช้เทคโนโลยีในการเฝ้าตรวจและบริหารจัดการความมั่นคงปลอดภัยและการสร้างขีดความสามารถเชิงป้องกันให้กับบุคลากรที่ปฏิบัติงานเกี่ยวข้องกับโครงสร้างพื้นฐานที่เกี่ยวข้อง

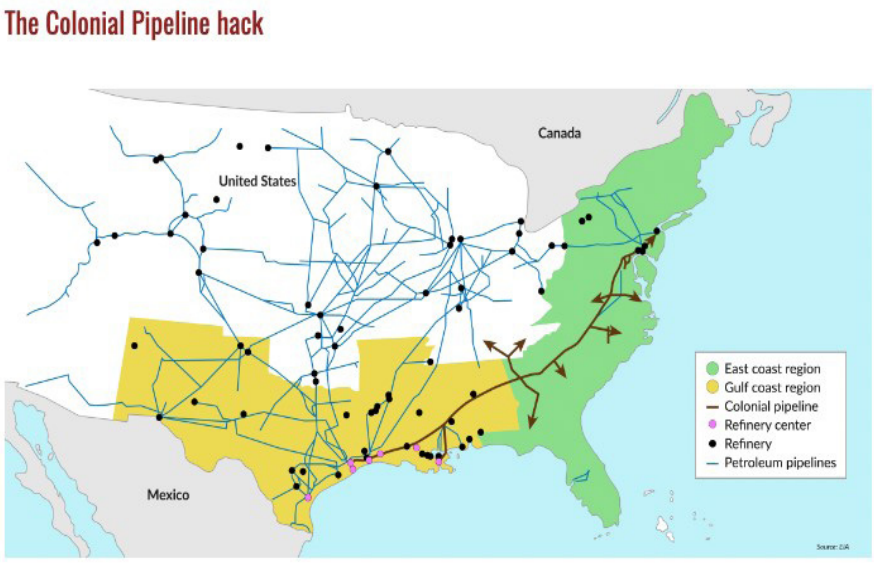
กับข่าวสารสำคัญ ควบคู่ไปกับการเสริมสร้างโครงสร้างพื้นฐานที่เกี่ยวข้องกับการเฝ้าตรวจและวิเคราะห์เหตุการณ์ด้านไซเบอร์ที่มีขีดความสามารถขั้นสูง เช่น มีความทนทานจากการพยายามโจมตี เพื่อการก่อกวนให้เกิดข้อผิดพลาดของข้อมูล (Data Misclassification) การสังเคราะห์ปลอมแปลงข้อมูล (Synthetic Data Generation) และการวิเคราะห์ข้อมูลบนไซเบอร์โดเมน (Data Analysis) เป็นต้น

กรณีศึกษาจากสงครามรัสเซีย-ยูเครน

รัสเซียดำรงยุทธศาสตร์การประยุกต์ใช้ขีดความสามารถด้านไซเบอร์ต่อคู่ขัดแย้งอย่างต่อเนื่อง นับตั้งแต่กรณีการละเมิดดินแดนและโจมตีทางไซเบอร์ต่อรัฐบาลเอสโตเนียเมื่อปี ค.ศ.๒๐๐๗ และใช้ขีดความสามารถนั้นโจมตีต่อยูเครนอย่างต่อเนื่อง ก่อนการเคลื่อนกำลังทหารเข้ารุกรานอธิปไตยในเดือนกุมภาพันธ์ ค.ศ.๒๐๒๒ โดยในปี ค.ศ.๒๐๑๕ มีผลสำเร็จของกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนโดยรัฐบาลรัสเซียทำการโจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญ (CII) ระบบพลังงานและระบบการให้บริการไฟฟ้าของยูเครนเป็นวงกว้าง [15] และมีรายงานว่าหน่วยงานรัฐบาลยูเครนตกเป็นเหยื่อการโจมตีทางไซเบอร์อย่างต่อเนื่องถึง ๖,๕๐๐ ครั้งในห้วงเดือนตุลาคมจนถึงเดือนพฤศจิกายน ค.ศ.๒๐๑๖ [13] ต่อเนื่องด้วยการโจมตีจากมัลแวร์ NotPetya ซึ่งถูกออกแบบให้โจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญทางด้านการเงินและการธนาคาร และโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารอื่น ๆ เหตุการณ์การแพร่กระจายมัลแวร์ดังกล่าว ส่งผลเป็นวงกว้าง และมีประมาณการมูลค่าความเสียหายที่เกิดขึ้นจากการแพร่กระจายของมัลแวร์ NotPetya ราว ๑๐,๐๐๐ ล้านดอลลาร์สหรัฐ

นับตั้งแต่ ค.ศ.๒๐๒๑ กลุ่มแฮกเกอร์โคซี่แบร์ (Cozy Bear, Nobelium, APT-29) ซึ่งเป็นกลุ่มแฮกเกอร์ที่โจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญของกลุ่มประเทศพันธมิตรนาโต้และสหรัฐอเมริกาอย่างต่อเนื่อง ตั้งแต่ปี ค.ศ.๒๐๒๐ เริ่มทำการโจมตีต่อเป้าหมายทางยุทธศาสตร์ของ

ยูเครนเพิ่มขึ้นอย่างเห็นได้ชัดในช่วงก่อนการเคลื่อนกำลังรุกล้ำเขตแดนยูเครนโดยพบว่ามีความพยายามโจมตีถึง ๑,๒๐๐ ครั้งในห้วงระยะเวลาเพียง ๒ เดือน ก่อนการโจมตีพร้อม ๆ กับการโจมตีต่อโครงสร้างพื้นฐานข่าวสารสำคัญของชาติที่เป็นพันธมิตรกับยูเครน เช่น การโจมตีต่อโครงสร้างพื้นฐานด้านการพลังงานของสหรัฐอเมริกาซึ่งส่งผลกระทบเป็นวงกว้าง ดังแสดงในภาพที่ ๓ [15]



ภาพที่ ๓ ผลกระทบจากการโจมตีของกลุ่มโคซี่แบร์ [15]

ในภาพรวมของปฏิบัติการไซเบอร์ที่เกิดขึ้นอย่างต่อเนื่องนับตั้งแต่การเคลื่อนกำลังเข้ารุกล้ำอธิปไตยยูเครน ในระดับยุทธศาสตร์จะพบว่ารัสเซียมียุทธศาสตร์ในการลดขีดความสามารถ สกัดขัดขวาง ทำลายหรือลดความน่าเชื่อถือของการบริหารประเทศของรัฐบาลยูเครนและชาติพันธมิตรผ่านกลุ่มแฮกเกอร์ที่ตนสนับสนุน อย่างไรก็ดีจากบทเรียนการ

ผนวกรวมไครเมียเมื่อ ค.ศ.๒๐๑๔ รัฐบาลยูเครนเรียนรู้และเร่งเตรียมความพร้อมเสริมสร้างขีดความสามารถด้านไซเบอร์อย่างต่อเนื่องพร้อมทั้งได้รับการสนับสนุนจากกลุ่มสหภาพยุโรป (EU) และไฟว์อายส์ (Five Eyes: FVEY) ซึ่งประกอบด้วยออสเตรเลีย แคนาดา นิวซีแลนด์ สหราชอาณาจักร และสหรัฐอเมริกา ในการพัฒนาโครงสร้างพื้นฐานและเตรียมบุคลากรให้มีขีดความสามารถพร้อมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ จึงสามารถต้านทานการโจมตีทางไซเบอร์ที่เกิดขึ้นและรักษาขีดความสามารถในการควบคุมบังคับบัญชาและการดำรงสภาพโครงสร้างพื้นฐานด้านการสื่อสารได้อย่างต่อเนื่อง

จนถึงปัจจุบันนับตั้งแต่การเริ่มสงครามรัสเซีย-ยูเครน มีรายงานการแพร่ระบาดของมัลแวร์จำนวนอย่างน้อย ๘ ชนิดได้แก่ WhisperGate/Whisperkill, FoxBlade (HermeticWiper), SonicVote (HermeticRansom), CaddyWiper, DesertBlade, Industroyer2, Lasainraw (IsaacWiper) and FiberLake (DoubleZero) มัลแวร์เหล่านี้ถูกออกแบบให้โจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารเพื่อลดขีดความสามารถด้านไซเบอร์ของยูเครน [16] และทำการโจมตีต่อโครงสร้างพื้นฐานด้านการสื่อสารและโทรคมนาคมเพื่อสนับสนุนปฏิบัติการข่าวสารของรัสเซียในหลายเหตุการณ์ เช่น การสร้างข่าวการยอมจำนนของประธานาธิบดียูเครน การรบกวนระบบดาวเทียม SpaceX’s Starlink โดยมีวัตถุประสงค์หลักเพื่อลดทอนขีดความสามารถด้านการสื่อสารของรัฐบาล รบกวนการควบคุมบังคับบัญชากำลังทหารของยูเครน เป็นต้น สามารถสรุปเหตุการณ์สำคัญที่เกี่ยวเนื่องกับปฏิบัติการไซเบอร์และผลกระทบระหว่างเดือน ก.พ. ๒๐๒๒ - เม.ย.๒๐๒๒ ดังตารางที่ ๒

ตารางที่ ๒ เหตุการณ์สำคัญที่เกี่ยวเนื่องกับปฏิบัติการไซเบอร์
และผลกระทบระหว่างเดือน ก.พ.๒๐๒๒ - เม.ย.๒๐๒๒

ห้วงเวลา	เหตุการณ์	เหตุการณ์ทางไซเบอร์
ก.พ. ๒๐๒๒	๒๔ ก.พ. การเคลื่อนกำลังเข้าสู่เมือง Sumy ของ กกล.รัสเซีย	๑๔ ก.พ. การโจมตีต่อ CII เมือง Odessa ๑๗ ก.พ. การโจมตีต่อ CII เมือง Sumy ๒๔ ก.พ. การโจมตีต่อโครงข่ายโทรคมนาคม KA-SAT ของสหภาพยุโรป
มี.ค. ๒๐๒๒	๑ มี.ค. การโจมตีด้วยอาวุธปล่อยนำวิถีต่อสถานีโทรทัศน์ในเมือง Kyiv ๓ มี.ค. การระเบิดของโรงงานไฟฟ้าหลายจุดที่เมือง Sumy ส่งผลให้มีไฟฟ้าดับเป็นวงกว้าง ๓ มี.ค. รัสเซียเข้ายึดพื้นที่โรงไฟฟ้าพลังงานนิวเคลียร์ที่มีขนาดใหญ่ที่สุดในยูเครน ๖ มี.ค. รัสเซียโจมตีต่อสนามบิน Vinnytsia ด้วยอาวุธปล่อยนำวิถี ๑๑ มี.ค. รัสเซียโจมตีต่อที่ทำการเมือง Dnipro ๑๖ มี.ค. รัสเซียโจมตีต่อสถานีโทรทัศน์เมือง Vinnytsia	๑ มี.ค. ธุรกิจสื่อสำคัญถูกโจมตีมีการเปลี่ยนหน้าเพจ และขโมยข้อมูลจากระบบ ๒ มี.ค. การโจมตีต่อเครือข่ายคอมพิวเตอร์ของกลุ่มธุรกิจไฟฟ้าพลังงานนิวเคลียร์ ๔ มี.ค. กลุ่ม APT28 โจมตีต่อระบบเครือข่ายคอมพิวเตอร์ของรัฐบาลที่เมือง Vinnytsia สำเร็จ ๑๑ มี.ค. การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานในเมือง Dnipro ๒๘ มี.ค. การโจมตีต่อกลุ่มธุรกิจโทรคมนาคม ส่งผลให้ไม่สามารถใช้โครงสร้างพื้นฐานด้านโทรคมนาคมเป็นวงกว้าง
เม.ย. ๒๐๒๒	๓ เม.ย. กกล.รัสเซียเข้ายึดพื้นที่อุตสาหกรรมน้ำมันในเมือง Odesa ๘ เม.ย. รัสเซียโจมตีระบบรางรถไฟด้วยอาวุธปล่อยนำวิถี ๑๐ เม.ย. รัสเซียทำลายสนามบินนานาชาติ Dnipro ๑๙ เม.ย. รัสเซียโจมตีด้วยอาวุธปล่อยต่อเมือง Kyiv และ Lviv	๘ เม.ย. การโจมตีของมัลแวร์ Sandworm ต่อโครงสร้างพื้นฐานพลังงานไฟฟ้า ๒๒ เม.ย. การโจมตีต่อหน่วยงานรัฐบาลด้วยเทคนิคดีดอส (Distributed Denial of Service: DDoS)

การโจมตีทางไซเบอร์ของรัสเซียในสงครามรัสเซีย-ยูเครนที่กำลังดำเนินอยู่ในขณะนี้แม้ว่าจะมีการควบคุมให้เป็นการโจมตีต่อเป้าหมายทางทหารในประเทศยูเครน แต่ผลกระทบที่เกิดขึ้นจากการใช้ขีดความสามารถเชิงรุกได้แพร่กระจายผ่านเครือข่ายอินเทอร์เน็ตไปยังภูมิภาค และประเทศอื่น ๆ ในหลายพื้นที่ เช่น การโจมตีต่อโครงข่ายโทรคมนาคม KA-SAT ซึ่งแม้ว่าจะมีวัตถุประสงค์เพื่อสกัดขัดขวางขีดความสามารถด้านการสื่อสารของกองกำลังยูเครน แต่โครงข่ายโทรคมนาคมดังกล่าวเป็นสินทรัพย์ของกลุ่มประเทศที่ไม่เกี่ยวข้องกับคู่สงคราม นอกจากนี้ยังมีรายงานการโจมตีของกลุ่มแฮกเกอร์ที่สนับสนุนรัสเซียได้ทำการโจมตีต่อโครงสร้างพื้นฐานสำคัญของหลายประเทศเช่น เชชเนีย เอสโตเนีย แลทเวีย โปแลนด์ สหราชอาณาจักร และสหรัฐอเมริกาในระหว่างวันที่ ๑๕-๒๒ เม.ย.

จากสรุปเหตุการณ์ที่ได้กล่าวมาจะเห็นได้ว่าการช่วงชิงการใช้ประโยชน์บนไซเบอร์โดเมนเป็นยุทธศาสตร์สำคัญในการทำสงคราม และการได้เปรียบทางไซเบอร์มีแนวโน้มส่งผลให้การปฏิบัติการทางทหารสามารถกระทำได้อย่างมีประสิทธิภาพมากขึ้นเนื่องจากผู้บังคับหน่วยทหารและผู้มีอำนาจตัดสินใจสามารถดำเนินการตามภาระหน้าที่ของตนได้อย่างถูกต้องเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไปอย่างต่อเนื่อง ซึ่งในกรณีของสงครามรัสเซีย-ยูเครนที่กำลังเป็นไปอยู่นี้แม้ว่าศักย์สงครามของยูเครนจะต่ำกว่าประเทศที่ริเริ่มสงครามเป็นอย่างมาก แต่ก็สามารถต้านทานการรุกด้วยวงรอบการตัดสินใจที่รวดเร็วแม่นยำ เนื่องจากยูเครนได้รับและดำรงค์ขีดความสามารถทางไซเบอร์ซึ่งเป็นโครงสร้างพื้นฐานสำคัญในการรวบรวมข่าวสารและสร้างภาพสถานการณ์จากพื้นที่การรบได้อย่างต่อเนื่อง อันเป็นผลจากการพัฒนาขีดความสามารถเชิงรับอย่างต่อเนื่องจากบทเรียนจากเหตุการณ์การผนวกรวมไครเมียของรัสเซียนับตั้งแต่ ค.ศ.๒๐๑๔ ผลกระทบที่เกิดขึ้นและข้อเสนอแนะ

ภัยคุกคามบนไซเบอร์โดเมนเป็นภัยคุกคามต่อความมั่นคงของชาติ และเป็นเครื่องมือที่สำคัญของการบรรลุวัตถุประสงค์ของสงคราม เห็นได้จากกรณีศึกษาจากสงครามรัสเซีย-ยูเครน จะพบว่าแนวโน้มการประยุกต์ใช้เทคโนโลยีขั้นสูงเพื่อขับเคลื่อนการโจมตีทางไซเบอร์มีพัฒนาการแบบก้าวกระโดด ทั้งด้านการโจมตีและการป้องกันซึ่งเป็นผลมาจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร การพัฒนาขีดความสามารถด้านไซเบอร์และการเสริมสร้างความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ให้กับพลเมืองและกำลังพลที่ปฏิบัติราชการในกองทัพย่อมเป็นส่วนสำคัญในการพัฒนาขีดความสามารถเชิงรับ (Defensive Capabilities) ให้กับพื้นที่รับผิดชอบด้านไซเบอร์ที่กองทัพเรือดูแลได้เป็นอย่างดี

การกำหนดยุทธศาสตร์การพัฒนาขีดความสามารถด้านไซเบอร์ให้กับกองทัพเรือ และการนำยุทธศาสตร์ไปสู่การปฏิบัติจะเป็นกุญแจสำคัญที่นำพาให้กองทัพเรือมีขีดความสามารถที่จำเป็น ในการปฏิบัติการและควบคุมบังคับบัญชากองกำลังในการปฏิบัติภารกิจในสาขาปฏิบัติการต่าง ๆ ที่มีในกองทัพเรือ ทั้งนี้สมรรถนะที่จำเป็นสามารถพิจารณาปัจจัยที่เกี่ยวข้องสำคัญ ๓ ประการ ได้แก่ การประยุกต์ใช้และพัฒนาเทคโนโลยีที่เหมาะสมต่อการปฏิบัติการไซเบอร์เชิงรุกและเชิงรับให้สอดคล้องกับสภาพแวดล้อมที่พัฒนาอย่างต่อเนื่องของไซเบอร์โดเมน การพัฒนาขีดความสามารถให้กับหน่วยงานที่มีหน้าที่รับผิดชอบหรือมีความเกี่ยวข้องกับโครงสร้างพื้นฐานข่าวสารสำคัญ และโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารที่ใช้งานในกองทัพเรือมีความมั่นคงปลอดภัย ซึ่งจะส่งผลให้การปฏิบัติการไซเบอร์เชิงรับเป็นไปอย่างมีประสิทธิภาพมากขึ้น การสร้างความตระหนักรู้และสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ให้กับกำลังพลในทุกระดับโดยเฉพาะอย่างยิ่งระดับผู้บริหารซึ่งเป็นกลจักรสำคัญในการกำหนดและขับเคลื่อนยุทธศาสตร์จะเป็นหลักประกันความสำเร็จของการสร้างความได้เปรียบในการปฏิบัติการไซเบอร์ของกองทัพเรือ

เอกสารอ้างอิง

[1] D. Ventre, “Information Warfare”, 2nd Edition., (2016) pp-263 ISBN: 978-1-848-21660-0

[2] Cornut J, de Zamaróczy N. How can document speak about practices? Practice tracing, the Wikileaks cables, and diplomatic culture. Cooperation and Conflict. (2021) ;56(3): 328-345. doi:10.1177/0010836720972426

[3] Henry Dalziel, Chapter 2 - Cyber Kill Chain, Securing Social Media in the Enterprise, Syngress, (2015), pp. 7-15, ISBN 9780128041802, doi:10.1016/B978-0-12-804180-2.00002-6.

[4] J. Toepher, “Sead from the group up: Sof’s role in the suppression of enemy air defense”, Thesis, Naval Postgraduate School (2019), Monterey CA 93943-500, USA, pp.36-41

[5] D. Fulghum, R. Wall, A. Butler, “Cyber-combat’s First Shot”, Aviation Week and Space Technology, November 26, 2007, pp.29-30

[6] J. A. Lewis, “Cyberwar and Ukraine”, Center for Strategic and International Studies, June 2022

[7] K. Boyte, “ The Evolution of Cyber Warfare in Information Operations Targeting Estonia, the U.S., and Ukraine, Developments in Information Security and Cybernetic War, (2019), IGI Global, DOI: 10.4018/978-1-5225-8304-2

[8] A. Giles, “Valery Gerasimov’s Doctrine”, Special Report, Universitat Potsdam, DOI: 10.13140/RG.2.2.10944.35848

[9] Evron G., “Battling botnet and online mob: Estonia’s defense efforts during the Internet war”, Georgetown Journal of International Affairs, 9(1), (2008), pp.121-126

[10] C. Easttom, J. Taylor., “Computer crime, investigation and the law”, Course Technology (2011), Boston MA

[11] P.W. Singer, A. Friedman, “Cybersecurity: What every one needs to know”, (2014), Oxford University Press, Oxford

[12] P. Christopher, “Understanding and Pursuing Information Advantage”, The Cyber Security Review, (2020), pp.109-121
[13] M. M. Yamin, M. Ullah, H. Ullah, B. Katt, “Weaponized AI for cyber attacks”, Journal of Information Security and Application, 57, (2021) DOI: 10.1016/j.jisa.2020.102722Get, pp.1-14
[14] European Digital Media Observation, “War in Ukraine”, (2022) Available at: https://edmo.eu/war-in-ukraine-the-fact-checked-disinformation-detected-in-the-eu/ (Accessed: July 23, 2022)
[15] F. Umbach, “Rissia’s cyber fog in the Ukraine war”, (2022), Available at: https://www.gisreportsonline.com/r/russia-cyber/ (Access: (Accessed: July 23, 2022)
[16] T. Burt, “The hybrid war in Ukrain”,(2022), https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/”(Access: (Accessed: July 23, 2022)