สงครามไซเบอร์และพัฒนาการปฏิบัติการไซเบอร์ในอนาคต

นาวาเอก ดร.กรกช วิไลลักษณ์
นักศึกษาการวิจัย กองเอกสารการวิจัย
ฝ่ายวิชาการ กรมยุทธศึกษาทหารเรือ

บทคัดย่อ

ไซเบอร์สเปซ คือ ขอบเขตพื้นที่เสมือนที่ถูกนำมาใช้ประโยชน์ด้านความมั่นคงและการทหารเพิ่มขึ้นอย่างต่อเนื่อง เห็นได้จากการพัฒนาเสริมสร้าง และการแสดงขีดความสามารถทางไซเบอร์ของรัฐต่าง ๆ ซึ่งปรากฏให้เห็นอย่างเด่นชัดในรอบ ๒ ทศวรรษที่ผ่านมา อย่างไรก็ดี ความรู้ความเข้าใจในหลักการพื้นฐาน และหลักนิยมปฏิบัติการไซเบอร์ยังเป็นไปอย่างจำกัด จึงอาจส่งผลให้การดำเนินยุทธศาสตร์และนโยบายไม่สอดคล้องกับสภาพแวดล้อมด้านความมั่นคงบนไซเบอร์สเปซ ที่มีการเปลี่ยนแปลงไปอย่างรวดเร็วและต่อเนื่อง บทความนี้จึงนำเสนอหลักการพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์และศึกษาวิเคราะห์ปฏิบัติการไซเบอร์ครั้งสำคัญ ๆ เพื่อเชื่อมโยงให้เห็นความสัมพันธ์ของการป้องกันไซเบอร์และการรักษาความมั่นคงปลอดภัยของทรัพยากรและโครงสร้างพื้นฐานที่เกี่ยวข้องของกองทัพเรือให้พร้อมรองรับต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

คำสำคัญ

สงครามไซเบอร์ ปฏิบัติการไซเบอร์ ไซเบอร์สเปซ ความมั่นคงปลอดภัยไซเบอร์ และความมั่นคงปลอดภัยระบบสารสนเทศ

บทนำ

บทความนี้นำเสนอหลักการพื้นฐานที่เกี่ยวข้องกับสงครามไซเบอร์เพื่อรายงานสภาพแวดล้อม หลักการทั่วไปของปฏิบัติการไซเบอร์และแนวโน้มการเปลี่ยนแปลงปฏิบัติการไซเบอร์ โดยมีวัตถุประสงค์หลักเพื่อให้ผู้อ่านมีความรู้และความตระหนักรู้เพียงพอที่จะเข้าใจภัยคุกคามทางไซเบอร์ สามารถคาดการณ์แนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศซึ่งเป็นส่วนประกอบสำคัญของไซเบอร์ และกำหนดยุทธศาสตร์การป้องกันไซเบอร์สเปซ ได้อย่างเหมาะสม

๑. หลักการพื้นฐานสำคัญที่เกี่ยวข้องกับสงครามไซเบอร์[๑]

๑.๑ ไซเบอร์ หมายถึงอะไร

เครือข่ายอินเทอร์เน็ตซึ่งในระยะเริ่มแรกถูกพัฒนาขึ้นเพื่อตอบโจทย์เกี่ยวกับสงครามนิวเคลียร์จึงถูกออกแบบเป็นเครือข่ายที่มีความพร้อมใช้

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

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

อย่างไรก็ดี เครือข่ายอินเทอร์เน็ตตลอดจนเทคโนโลยีส่วนควบอื่น ๆ ที่เป็นโครงสร้างพื้นฐานที่สำคัญของไซเบอร์สเปซอาจถูกใช้ประโยชน์จาก

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

๑.๒ ภัยคุกคามทางไซเบอร์

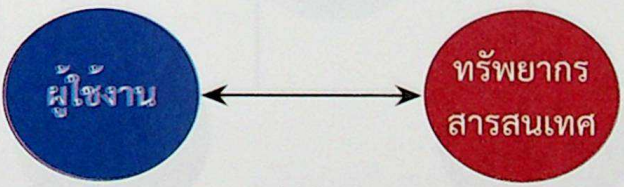
ภัยคุกคาม (Threats) หมายถึง บุคคล หรือเหตุการณ์ใด ๆ ก็ตามที่เป็นสาเหตุของการลดทอนความมั่นคงปลอดภัยของทรัพยากรสารสนเทศซึ่งประกอบด้วยโครงสร้างพื้นฐานฯ อันประกอบกันเป็นไซเบอร์สเปซ ตลอดจนข้อมูลข่าวสารที่รับ-ส่ง ผ่านช่องทางการสื่อสาร โดยภัยคุกคามดังกล่าวรวมไปถึงเหตุการณ์ที่เกิดขึ้นจากภัยธรรมชาติและอุบัติเหตุ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

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

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

๑.๓ ผลกระทบของภัยคุกคามทางไซเบอร์

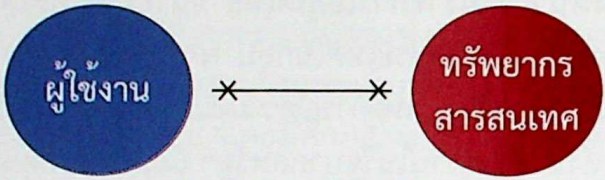
การเข้าถึงและใช้ประโยชน์จากทรัพยากรสารสนเทศและการสื่อสารของผู้ใช้งาน หากเป็นไปอย่างมั่นคงปลอดภัยสามารถแสดงได้ ดังภาพที่ ๑ โดยจะเห็นว่าผู้ใช้งานจะสามารถเข้าใช้งานทรัพยากรสารสนเทศได้โดยไม่มีบุคคลอื่นเข้าถึงทรัพยากรที่ผู้ใช้งานเข้าถึงอยู่โดยไม่มีสิทธิ์ ทั้งนี้ เมื่อจำแนกผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศ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



สภาวการณ์ที่มั่นคงปลอดภัย

ภาพที่ ๑ สภาวการณ์ที่มั่นคงปลอดภัย

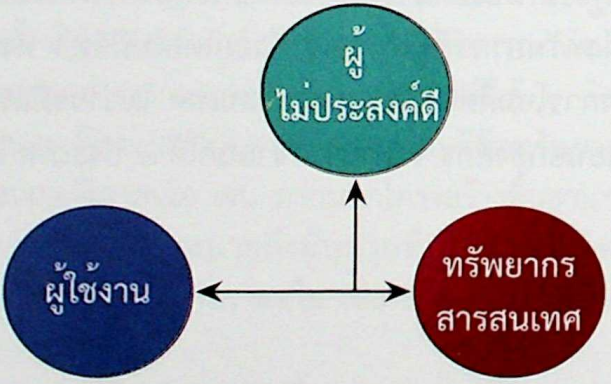
๑.๓.๑ การสกัดขัดขวาง (Interruption) คือ การทำให้ทรัพยากรสารสนเทศไม่สามารถให้บริการได้ เช่น การเข้ารหัสไฟล์หรือฮาร์ดดิสก์โดยซอฟต์แวร์เรียกค่าไถ่ การโจมตีแบบกระจาย (Distributed Denial of Service: DDoS) การขโมยอุปกรณ์ ดังแสดงในภาพที่ ๒ ยกตัวอย่าง การขโมยอุปกรณ์ย่อมส่งผลให้ผู้ใช้งานไม่สามารถเข้าถึงทรัพยากรนั้น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



Interruption

ภาพที่ ๒ การถูกสกัดขัดขวาง

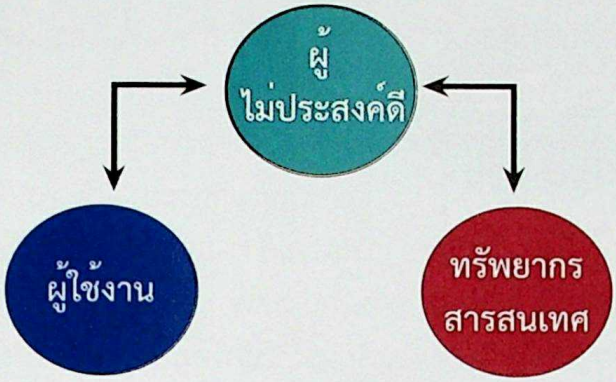
๑.๓.๒ การดักรับดักฟัง (Interception) คือ การเข้าถึงทรัพยากรสารสนเทศระหว่างที่กำลังถูกส่งผ่านระบบการสื่อสารหรือระบบเครือข่าย เช่น การใช้โปรแกรม Sniffer ดักรับดักฟังเครือข่าย หรือการดักรับสัญญาณที่แพร่กระจาย การคุ้ยขยะเพื่อค้นหาข้อมูลสำหรับเข้าใช้งานระบบ ดังแสดงในภาพที่ ๓ จะเห็นว่าทรัพยากรสารสนเทศเหล่านั้นจะถูกเข้าถึงได้จากผู้ไม่ประสงค์ดี ซึ่งถ้าหากปราศจากมาตรการป้องกันที่เหมาะสมผู้ไม่ประสงค์ดีย่อมทำความเข้าใจและล่วงรู้ถึงข้อมูลที่ รับ-ส่ง นั้น ๆ ได้



Interception

ภาพที่ ๓ การถูกดักรับดักฟัง

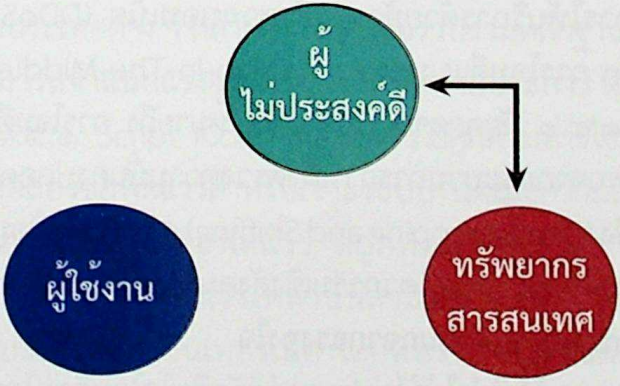
๑.๓.๓ การเปลี่ยนแปลงแก้ไข (Modification) คือ การทำให้ทรัพยากรสารสนเทศและการสื่อสารถูกเปลี่ยนสภาพไปโดยไม่มีสิทธิ์ หรือไม่ได้รับอนุญาต ดังแสดงในภาพที่ ๔ ยกตัวอย่างเช่น การเปลี่ยนแปลงแก้ไขข้อมูลเงินเดือนในระบบงานเงินเดือน การแก้ไขรายชื่อคำสั่งโดยไม่มีสิทธิ์ การแก้ไขหน้าเว็บโดยไม่ได้รับอนุญาต



Modification

ภาพที่ ๔ การเปลี่ยนแปลงแก้ไข

๑.๓.๔ การปลอมแปลง (Fabrication) คือ การสร้างทรัพยากรสารสนเทศและการสื่อสารเข้าสู่โครงสร้างพื้นฐานหรือระบบ เช่น การปลอมแปลงข้อมูล หรือการปลอมแปลงตัวตน ดังแสดงในภาพที่ ๕ ซึ่งหมายรวมถึงการส่งข้อมูลข่าวสารที่เป็นเท็จ (Misinformation) เพื่อสร้างผลกระทบต่อกระบวนการคิด การตัดสินใจ



Fabrication

ภาพที่ ๕ การปลอมแปลง

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

๑.๔ การจำแนกประเภทของภัยคุกคาม

เมื่อพิจารณาผลกระทบของภัยคุกคามที่ได้กล่าวมาแล้วจะพบว่าแนวทางการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารจะถูกแบ่งเป็น ๒ ลักษณะคือ ภัยคุกคามแบบแอคทีฟ (Active threats) และภัยคุกคามแบบพาสซีฟ (Passive threats)

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

๑.๔.๒ ภัยคุกคามแบบพาสซีฟ หมายถึง การโจมตีที่ผู้ไม่ประสงค์ดีจะไม่ถูกตรวจพบจากกระบวนการการเฝ้าตรวจความมั่นคงปลอดภัย เช่น OSINT การดักรับดักฟัง (Eavesdropping and Sniffing) การสืบค้นข้อมูลจาก Search Engine การโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม (Social Engineering) เป็นต้น

๑.๕ ภัยคุกคามจำแนกจากแรงจูงใจ

แรงจูงใจที่ทำให้ผู้ไม่ประสงค์ดีตัดสินใจโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารแตกต่างกันในแต่ละบุคคลและกลุ่มบุคคล

และด้วยแรงจูงใจที่แตกต่างกันย่อมส่งผลกระทบต่อพลังอำนาจแห่งชาติในระดับที่แตกต่างกันออกไป ภาพที่ ๖ แสดงเหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของประเทศซึ่งเกิดขึ้นอย่างต่อเนื่อง

ภาพที่ ๖ การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่เคยเกิดขึ้นในประเทศต่าง ๆ

จากการรวบรวมหลักฐานจากเหตุการณ์ที่ผ่านมาจะสามารถจำแนกแรงจูงใจที่ทำให้ผู้ไม่ประสงค์ดีตัดสินใจโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารแตกต่างกันในแต่ละบุคคลและกลุ่มบุคคล เหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของประเทศต่าง ๆ หลายประเทศ เมื่อรวบรวมหลักฐานจากเหตุการณ์ที่ผ่านมาจะสามารถจำแนกแรงจูงใจเหล่านั้นได้หลายประการ ดังนี้

๑.๕.๑ Script Kiddy หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ที่ชอบศึกษาทดลองซอฟต์แวร์สำหรับเจาะระบบ แต่ไม่มีความสามารถในการพัฒนาซอฟต์แวร์จึงต้องใช้ซอฟต์แวร์ ที่ถูกพัฒนาขึ้นมาจากแฮกเกอร์ที่มีความสามารถสูง โดยซอฟต์แวร์เหล่านั้นสามารถดาวน์โหลดได้จากแหล่งซอฟต์แวร์เปิดบนเครือข่ายอินเทอร์เน็ต โดยพบว่าเหตุการณ์ด้านความมั่นคงปลอดภัย ส่วนใหญ่เป็นผลจากการโจมตีกลุ่มคนในกลุ่มนี้และพบว่าผลเสียหายที่เกิดขึ้นไม่มีนัยสำคัญอย่างไรต่อพลังอำนาจแห่งชาติ

๑.๕.๒ Criminal หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากแรงขับเคลื่อนขององค์กรอาชญากรรมที่มุ่งหาประโยชน์จากการโจมตีโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร จากสถิติพบว่าปริมาณการโจมตีที่เกิดขึ้นจากกลุ่มนี้มีจำนวนมากรองลงมาจากการโจมตีของกลุ่มสคริปคิดดี้

๑.๕.๓ Hacker Groups หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินกิจกรรมของกลุ่มแฮกเกอร์ที่มีฝีมือ และเป็นผู้พัฒนาเครื่องมือสำหรับใช้โจมตีต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร โดยพบว่าผลกระทบของภัยคุกคามจากกลุ่มนี้มีมากถึงร้อยละ ๘๐ ของผลเสียหายทั้งหมด ลักษณะเฉพาะของภัยคุกคามจากกลุ่มนี้คือการกระทำเพื่อหวังผลประโยชน์ในรูปของตัวเงิน และเศรษฐกิจ

๑.๕.๔ Insider หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลการดำเนินการของกลุ่มคนภายในองค์กร ซึ่งเป็นจุดที่ได้รับการปกป้องต่ำกว่าโครงสร้างพื้นฐานที่เชื่อมต่อกับเครือข่ายภายนอก โดยมีแรงจูงใจในการกระทำส่วนใหญ่เพื่อแก้แค้นองค์กร หรือได้รับการสนับสนุนทางการเงินจากองค์กรคู่แข่ง

๑.๕.๕ Political/Religious หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินการจากบุคคลที่มีความเชื่อทางการเมืองตรงข้ามกันกระทำต่อกันเพื่อล้มล้างหรือสร้างสภาวะที่ฝ่ายตนต้องการ โดยมักไม่หวังผลความเสียหายต่อพลังอำนาจแห่งชาติ อย่างไรก็ดี เมื่อพิจารณาขอบเขตการใช้ความเชื่อทางศาสนาเป็นเครื่องมือจะพบว่าแนวโน้มการใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารในการปลูกฝังและขยายจำนวนผู้ร่วมอุดมการณ์ของกลุ่มก่อการร้ายเพิ่มขึ้นอย่างมีนัยสำคัญ

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

๑.๖ กำลังอำนาจแห่งชาติ

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

หลักการพื้นฐานที่ได้กล่าวมานี้เป็นพื้นฐานที่สำคัญในการทำความเข้าใจคุณลักษณะของพื้นที่ปฏิบัติการแนวทางการใช้กำลัง คุณลักษณะเฉพาะของปฏิบัติการไซเบอร์ และกรณีศึกษาได้อย่างถ่องแท้ในตอนถัดไป

๒. คุณลักษณะของสงครามไซเบอร์

ไซเบอร์สเปซเป็นพื้นที่เสมือนที่เกิดขึ้นจากความร่วมมือระหว่างกันในการพัฒนาเทคโนโลยีและบริการ ซึ่งผลักดันให้เกิดวิทยาการและความก้าวหน้าทางวิทยาศาสตร์จากการใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลข่าวสาร ดำเนินธุรกรรม พัฒนาเศรษฐกิจและสังคมร่วมกัน อย่างไรก็ดี เมื่อเกิดความขัดแย้งขึ้นระหว่างกัน ไซเบอร์สเปซก็ถูกใช้พื้นที่สนามรบ (Battlespace) เช่นเดียวกับโดเมนอื่น ๆ เพื่อดำรงรักษาไว้ซึ่งความมุ่งประสงค์แห่งชาติทางกายภาพเสมือนเป็นอาณาเขตอีกอาณาเขตหนึ่งของรัฐ การเข้าใจถึงคุณลักษณะเฉพาะ และแนวทางการใช้กำลังบนพื้นที่เสมือนแห่งนี้จึงมีความสำคัญอย่างยิ่งยวด

๒.๑ ลักษณะพื้นที่การรบและแนวทางการใช้กำลัง

หลักนิยมการใช้กำลังเป็นแนวคิดที่ใช้กำหนดทิศทางการใช้กำลังรบเพื่อบรรลุความมุ่งประสงค์ของชาติ (National Purpose) การพัฒนาหลักนิยมจึงต้องคำนึงถึงปัจจัยสำคัญ นับตั้งแต่ความมุ่งประสงค์ของชาติ ผลประโยชน์ของชาติ

วัตถุประสงค์ของชาติ นโยบายของชาติ นโยบายทางทหาร ยุทธศาสตร์ทหาร หลักนิยมพื้นฐาน และยุทธวิธีของหน่วย ร่วมกับองค์ความรู้ในประวัติศาสตร์การรบ บทเรียนจากการรบ ภัยคุกคาม ความเจริญก้าวหน้าด้านวิทยาศาสตร์และเทคโนโลยี และอาจกล่าวได้ว่า การใช้กำลังรบในแต่ละพื้นที่การรบ มีความต้องการและหลักนิยมการใช้กำลังที่แตกต่างกัน แม้ว่าจุดมุ่งหมายของการรบทางบก ทางทะเล และทางอากาศจะมีความคล้ายคลึงกัน โดยมีความต้องการหลัก ๆ เพื่อ ยึดพื้นที่ (Command) การควบคุมพื้นที่ (Control) หรือการปฏิเสธการใช้ประโยชน์ของพื้นที่นั้น ๆ จากฝ่ายตรงข้าม (Denial) โดยการก้าวเข้าสู่สภาวะสงครามในการรบทางบก ทางทะเล และทางอากาศมีความตรงไปตรงมา โดยมักเริ่มขึ้นเมื่อกำลังของแต่ละฝ่ายเคลื่อนเข้าหากัน เพื่อยึดครอง ควบคุม หรือปฏิเสธการใช้ประโยชน์เหนือพื้นที่นั้น ๆ จากฝ่ายตรงข้ามด้วยกองกำลังของตน บนหรือในยุทธบริเวณนั้น ๆ แต่สงครามไซเบอร์คุณลักษณะแตกต่างจากพื้นที่การรบอื่น ๆ อย่างมีนัยสำคัญ

๒.๑.๑ สงครามทางบก การดำเนินกลยุทธ์บนพื้นที่ทางบกมีมาควบคู่กับการวิวัฒนาการของมนุษย์ โดยอาวุธ ยุทธวิธี และการดำเนินกลยุทธ์ของการทำการรบทางบกได้รับการพัฒนามาอย่างต่อเนื่อง นับตั้งแต่ การขว้างปาหิน พัฒนาเป็นหอก ธนู เครื่องยิง ระเบิด ปืน ปืนใหญ่ ปืนกล รถถัง และกล่าวได้ว่าการพัฒนาของอาวุธชนิดต่าง ๆ ส่งผลโดยตรงต่อหลักนิยม ยุทธวิธี และการจัดกำลัง ซึ่งจะต้องถูกพัฒนาให้เหมาะสมกับอาวุธในแต่ละแบบ โดยมีแนวคิดพื้นฐานในการแบ่งมอบการบังคับบัญชาให้หน่วยรองและควบคุมการปฏิบัติ (Chain of Command and Span of Control) สำหรับการรบในยุคปัจจุบันจะพบว่าการใช้กำลังเพื่อทำการรบทางบก จะมีลักษณะเป็นการจัดกำลังผสมเหล่าที่ผนึกกำลังรบที่มีอำนาจการยิง และสามารถดำเนินกลยุทธ์ด้วยการจู่โจม รวดเร็ว รุนแรง สามารถเอาชนะกำลังรถถังและยานเกราะ มีส่วนยิงสนับสนุนจากอาวุธยิงสนับสนุน เช่น การจัดกองพันผสม ซึ่งประกอบด้วย กองร้อยรถถัง กองร้อยรถสายพาน กองร้อยรถสายพานลาดตระเวน และทหารราบ เพื่อปฏิบัติการรบด้วยวิธีรุก รับ และร่นถอยได้อย่างอ่อนตัวและมีประสิทธิภาพ และเมื่อพิจารณาประวัติศาสตร์สงครามที่ผ่านมาจะเห็นว่า การยุทธ์ในปัจจุบันต่างก็มีการใช้กองกำลังผสมเหล่าในการทำการรบ

๒.๑.๒ สงครามทางเรือ เมื่อพิจารณาพื้นที่ปฏิบัติการของการยุทธ์ทางเรือจะพบว่า พื้นที่การยุทธ์มีอาณาเขตกว้างขวางซึ่งเกื้อกูลต่อการเคลื่อนกำลัง โดยมีอุปสรรคเกี่ยวกับภูมิประเทศน้อยกว่าการยุทธ์ทางบก มีความเร็วในการเคลื่อนกำลังมากกว่าการรบทางบก โดยในหนึ่งวันอาจเคลื่อนที่ได้หลายสิบไมล์ ในขณะที่การรบทางบกอาจใช้ระยะเวลานานกว่าในการรุกคืบเข้าไปในภูมิประเทศ หลักนิยมการยุทธ์ทางเรือก็ได้รับอิทธิพลจากความก้าวหน้าของเทคโนโลยีเช่นเดียวกัน โดยเห็นได้จากการเปลี่ยนหลักนิยม ยุทธวิธีของกำลังทางเรือ เมื่อมีการพัฒนาเรือบรรทุกเครื่องบิน และกล่าวได้ว่าการยุทธ์ทางเรือในปัจจุบันขึ้นอยู่กับ ยุทธศาสตร์ในการใช้กำลังรบทางเรือ ระบบอำนวยการรบ การควบคุมบังคับบัญชา อันเป็นผลจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารของอุปกรณ์ตรวจจับและระบบอาวุธ โดยมักมีแนวคิดการจัดกำลังเข้าทำการรบแบบตามความสามารถ (Capability-Based)

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

๒.๑.๔ สงครามไซเบอร์ มีความคล้ายคลึงกับสงครามทางเรือและสงครามทางอากาศ เนื่องจากการไม่สามารถระบุขอบเขตทางกายภาพได้อย่างแน่นอน และการเชื่อมต่อกันเสมือนไร้พรมแดน ซึ่งในสงครามทางเรือและทางอากาศคู่ขัดแย้งสามารถเคลื่อนย้ายกำลังเข้าปะทะกันได้เมื่อเกิดความขัดแย้ง อย่างไรก็ดี ขอบเขตของสงครามไซเบอร์ไม่ได้ถูกจำกัดที่ทรัพยากรทางทหารหรือทรัพยากรของรัฐคู่กรณีแต่เพียงอย่างเดียว เนื่องจากเป้าหมายที่ถูกโจมตีอาจเป็นโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารอื่น ๆ

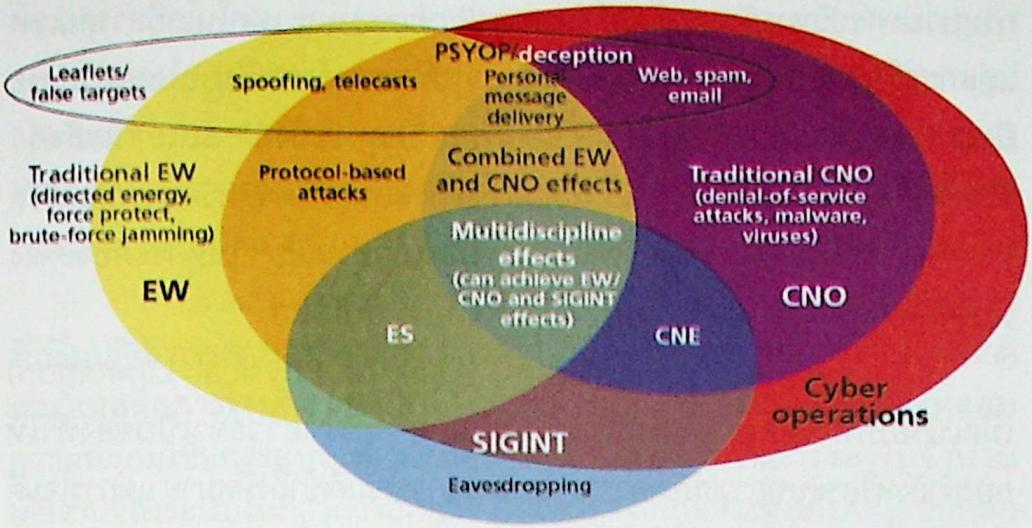
ที่อยู่นอกการควบคุมของหน่วยงานรัฐหรือกองทัพ อีกทั้งการระบุคู่ขัดแย้งในไซเบอร์สเปซก็กระทำได้อย่างไม่ชัดเจน ยกตัวอย่างเช่น โครงสร้างพื้นฐานของหน่วยงาน รัฐ B มีข้อบกพร่องด้านความมั่นคงปลอดภัยอย่างรุนแรง จึงถูกกองกำลังไซเบอร์รัฐ A โจมตีเพื่อใช้เป็นฐานสำหรับการโจมตีต่อโครงสร้างพื้นฐาน รัฐ C ซึ่งไม่มีความขัดแย้งใด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

๒.๒ คุณลักษณะของอาวุธที่ใช้ในสงครามไซเบอร์

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

๒.๓ ปฏิบัติการไซเบอร์

ในปัจจุบันสหรัฐฯ ยังไม่มีการกำหนดหลักนิยมสงครามไซเบอร์อย่างเป็นทางการ แต่มีการประยุกต์ใช้แนวทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารจนกล่าวได้ว่า แนวทางดังกล่าวเป็นปฏิบัติการเชิงรับ โดยหากกระทำสำเร็จจะมั่นใจได้ว่าทรัพยากรที่เกี่ยวข้องกับข้อมูล



ภาพที่ ๗ ภาพรวมการปฏิบัติการข้อมูลข่าวสาร

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

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

กระบวนการบริหารจัดการข้อมูลข่าวสาร (Process) และ เทคโนโลยีสารสนเทศและการสื่อสาร (Technology) ทั้งนี้ ปฏิบัติการทางทหารบนไซเบอร์สเปซมีแนวทางการปฏิบัติหลากหลายขึ้นอยู่กับ “วัตถุประสงค์” และ “ผลลัพธ์” ที่สอดคล้องกับความต้องการในระดับยุทธการและยุทธศาสตร์อย่างเห็นได้ชัด หากต้องการปฏิบัติการไซเบอร์ให้ได้ผล “ผู้มีส่วนได้ส่วนเสีย” ในทุกระดับจะต้องเข้าใจคุณลักษณะสำคัญของปฏิบัติการไซเบอร์[๒] อันได้แก่

๒.๓.๑ ความไร้พรมแดน (Lack of Physical Limitation) เมื่อเปรียบเทียบกับการโจมตีในโดเมนอื่น ๆ การใช้อาวุธจำเป็นต้องทำให้กองกำลังหรือระบบอาวุธมีขีดความสามารถในการโจมตีเข้าถึงที่หมาย แต่การโจมตีทางไซเบอร์แทบจะไม่มีข้อจำกัดในลักษณะนั้น ตราบที่การเชื่อมต่อของระบบเครือข่ายสามารถติดต่อสื่อสารระหว่างกัน หรือมีช่องทางสามารถส่งผ่านการโจมตีผ่านสื่อลักษณะอื่นได้ เช่น USB แฟลชไดรฟ์ หรือการแพร่กระจายของมัลแวร์จากอุปกรณ์ที่ได้รับความเชื่อถือ ตามที่ปรากฏในกรณี Stuxnet เป็นต้น

๒.๓.๒ ผลทางกายภาพ (Kinetic Effect) ผลสัมฤทธิ์ที่ต้องการสูงสุดของการปฏิบัติการไซเบอร์คือ การสร้างความเสียหายต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ แต่ส่งผลกระทบทางกายภาพ[๓] ดังเห็นได้จากกรณีศึกษาการโจมตีด้วยมัลแวร์ Stuxnet และ Downadup

๒.๓.๓ พฤติกรรมลับ (Stealth) ปฏิบัติการไซเบอร์โดยเฉพาะอย่างยิ่ง CNO จำเป็นต้องมีการซ่อนพลางการปฏิบัติอย่างเหมาะสม ดังกรณีการโจมตีศูนย์ข้อมูลกลาโหมสาธารณรัฐเกาหลี ซีเรีย Stuxnet และเหตุการณ์อื่น ๆ จะเห็นได้ว่าการค้นหาตัวตนที่แท้จริงของผู้ทำการโจมตีบนไซเบอร์สเปซกระทำได้อย่างจำกัด

๒.๓.๔ ความยืนหยุ่นสูง (Mutability and Inconsistency) จากกรณีศึกษาที่ได้กล่าวมาจะพบว่า ปฏิบัติการไซเบอร์ต้องการความอ่อนตัวและจะต้องปรับเปลี่ยนตนเองให้สอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงได้ ยกตัวอย่างเช่น การโจมตีด้วยเทคนิคหนึ่ง ๆ ต่อเป้าหมายที่แตกต่างกัน ผลลัพธ์ที่ได้อาจแตกต่างกันเนื่องจากปัจจัยของซอฟต์แวร์และฮาร์ดแวร์ที่เกี่ยวข้องเปลี่ยนไป

๒.๓.๕ การระบุตัวตนและสิทธิ์ (Identity and Privileges) ผลสำเร็จของปฏิบัติการไซเบอร์ขึ้นอยู่กับความสามารถในการได้รับฐานานุรูปและสิทธิ์ของบุคคลหรือระบบที่เกี่ยวข้องกับเป้าหมายการโจมตี ซึ่งแตกต่างจากการปฏิบัติการทางทหารโดยปกติ ซึ่งการรับรู้ถึงตัวตนและสิทธิ์นั้นไม่มีผลระหว่างการปฏิบัติการ

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

๒.๓.๗ การควบคุมโครงสร้างพื้นฐาน (Infrastructure Control) การควบคุมโครงสร้างพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์ได้อย่างเบ็ดเสร็จย่อมส่งผลดีต่อความสำเร็จของปฏิบัติการ คล้ายคลึงกับการเข้ายึดพื้นที่สำคัญทางทหารในการปฏิบัติทางทหารในโดเมนอื่น ๆ อย่างไรก็ดี การควบคุมโครงสร้างพื้นฐานที่เกี่ยวข้องกับปฏิบัติการไซเบอร์นั้น กระทำได้อย่างจำกัดในทางปฏิบัติ เนื่องจากคุณลักษณะเฉพาะของเครือข่ายอินเทอร์เน็ตที่การรับส่งข้อมูลไม่สามารถควบคุมเส้นทางได้อย่างสัมบูรณ์ และการโจมตีอาจเกิดขึ้นกับช่องโหว่ด้านการบริหารจัดการทรัพยากรที่เชื่อมต่อกันบนโครงสร้างพื้นฐานนั้น ๆ

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

๓. กรณีศึกษาจากปฏิบัติการไซเบอร์ในอดีต

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

กลาโหมสหรัฐฯ เช่น บริษัทล็อกฮีด มาติน (Lockheed Martin) ศูนย์การทดลองแห่งชาติซานเดีย (Sandia National Laboratories) เรดสโตนอาร์เซนอล (Redstone Arsenal) เป็นต้น โดยผลพิสูจน์หลักฐานคอมพิวเตอร์ (Computer Forensic) บ่งชี้ว่าการโจมตีมีจุดกำเนิดมาจากมณฑลกวางตุ้ง (Guangdong) สาธารณรัฐประชาชนจีน โดยมีข้อมูลบ่งชี้ว่า การโจมตีทางไซเบอร์เหล่านั้นเกิดขึ้นภายใต้การสนับสนุนจากรัฐบาลสาธารณรัฐประชาชนจีนอย่างลับ ๆ[๔] การโจมตีทางไซเบอร์ขนาดใหญ่ครั้งต่อมาเกิดขึ้นระหว่างปี ค.ศ.๒๐๐๗ - ๒๐๐๙ คู่ขัดแข้งในครั้งนี้คือ สาธารณรัฐเอสโตเนีย และสหภาพโซเวียต[๕] ซึ่งมีความขัดแย้งกันเนื่องจากสาธารณรัฐเอสโตเนียมีความต้องการเข้าร่วมกลุ่มสหภาพยุโรป

เป้าหมายสำคัญของการโจมตีคือ โครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารขององค์การภาครัฐ เช่น รัฐสภา กระทรวง องค์กรการเงิน การธนาคาร และองค์การสื่อต่าง ๆ ของสาธารณรัฐเอสโตเนีย ถูกโจมตีอย่างต่อเนื่องด้วยการโจมตีแบบกระจาย (DDoS) และการปรับเปลี่ยนหน้าเว็บเพจ (Web Defacement) ซึ่งเป็นการโจมตีแบบพื้นฐานและส่งผลเพียงเพื่อสกัดกั้นไม่ให้ผู้ใช้งานที่มีสิทธิ์สามารถเข้าใช้งานระบบที่ตกเป็นเป้าหมาย หรือเพียงเพื่อก่อกวน ไม่ได้สร้างความเสียหายให้กับโครงสร้างพื้นฐานอย่างหนักตั้งแต่วันที่ ๒๗ เมษายน ค.ศ.๒๐๐๗ อย่างไรก็ดี ผลกระทบที่เกิดขึ้นอย่างเห็นได้ชัดจากการโจมตีดังกล่าวคือ ความสับสนวุ่นวายและการเสียความเชื่อมั่นจากประชาชนในการบริหารจัดการภาวะวิกฤต ทั้งนี้ จากกรณีดังกล่าวส่งผลให้รัฐสภาแห่งสหภาพยุโรปร่วมกับ NATO ทำการตรวจประเมินความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญในประเทศกลุ่มสมาชิกและพัฒนาต่อเนื่องเป็นศูนย์ความร่วมมือป้องกันไซเบอร์สเปซของนาโต้ พร้อมกับบังคับใช้คู่มือ Tallinn[๖] ซึ่งเป็นกฎหมายระหว่างประเทศที่ใช้ในกลุ่มประเทศสหภาพยุโรป แต่ถูกนำมาใช้เป็นบรรทัดฐานอ้างอิงในระดับนานาชาติเมื่อจำเป็นต้องอ้างอิงประเด็นกฎหมายระหว่างประเทศในบริบทของสงครามไซเบอร์

ในช่วงเวลาเดียวกัน สาธารณรัฐอิสราเอลปฏิบัติการ Orchard สำเร็จเป็นอย่างดีในการโจมตีต่อเตาปฏิกรณ์นิวเคลียร์ Al Kibar ของสาธารณรัฐอาหรับซีเรียสำเร็จ โดยที่ไม่มีการต่อต้านจากระบบป้องกันภัยทางอากาศอันเป็นผลจากมัลแวร์ที่ถูกติดตั้งในโครงสร้างพื้นฐานฯ ที่เกี่ยวข้อง[๗]

ต่อมาในปี ค.ศ.๒๐๐๙ ระบบสารสนเทศและการสื่อสารขององค์กรการบินพลเรือนแห่งสหรัฐฯ ถูกโจมตี ส่งผลกระทบต่อการเดินอากาศของสายการบินและเที่ยวบินทางทหาร[๖] ในปีเดียวกันนั้น กองทัพเรือฝรั่งเศสจำเป็นต้องยกเลิกเที่ยวบินทางทหารของกองทัพเรือ โดยเป็นผลจากการแพร่ระบาดของมัลแวร์ Downadup[๗] ทั้งนี้ มัลแวร์ชนิดนี้ถูกปรับปรุงคุณสมบัติจากมัลแวร์ Conficker ที่แพร่ระบาดนับตั้งแต่ปี ค.ศ.๒๐๐๘ ให้มีขีดความสามารถในการซ่อนพรางและป้องกันตนเองได้เป็นอย่างดี โดยผลจากการวิเคราะห์ซอร์ซโค้ดบ่งชี้ว่ามัลแวร์มีต้นกำเนิดมาจากสาธารณรัฐยูเครนและสาธารณรัฐประชาชนจีน โดยการแพร่ระบาดของมัลแวร์ดังกล่าวเป็นไปอย่างต่อเนื่องจนถึงปี ค.ศ.๒๐๑๔ จะเห็นว่าพัฒนาการของรูปแบบการโจมตีนับตั้งแต่ปี ค.ศ.๒๐๐๓ จนถึงปี ค.ศ.๒๐๑๐ มีรูปแบบการโจมตีและเป้าหมายการโจมตีที่เปลี่ยนแปลงไป นอกจากนี้ยังแสดงให้เห็นถึงผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติของกองกำลังมากขึ้นอย่างเห็นได้ชัด

เป้าหมายการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานของรัฐเป็นการเฉพาะเริ่มเป็นรูปธรรมมากยิ่งขึ้นในเหตุการณ์ที่เตาปฏิกรณ์นิวเคลียร์ในเมือง Natanz สาธารณรัฐอิสลามอิหร่าน ซึ่งตกเป็นเป้าหมายของการโจมตีจากมัลแวร์ที่ถูกออกแบบมาสำหรับการโจมตีต่อระบบระบายความร้อนของเตาปฏิกรณ์ที่ควบคุมด้วยระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งเป็นระบบที่ใช้ในการตรวจสอบ เก็บข้อมูล และควบคุมกระบวนการผลิตต่าง ๆ จากระยะไกลที่ถูกใช้งานทั่วโลก มัลแวร์ Stuxnet[๑๐] เป็นมัลแวร์ที่ถูกพัฒนาขึ้นสำหรับปฏิบัติการนี้ เป็นหนอนอินเทอร์เน็ตที่มีความซับซ้อนและออกแบบให้โจมตีต่อระบบควบคุมเตาปฏิกรณ์นี้เป็นการเฉพาะ โดยถูกออกแบบให้แพร่กระจายตัวเองผ่าน USB แฟลชไดรฟ์ และระบบเครือข่ายและสร้างผลกระทบต่อระบบควบคุมเฉพาะที่ติดตั้งในระบบที่เมือง Natanz เท่านั้น ปฏิบัติการนี้ส่งผลให้เกิดความเสียหายทางกายภาพแก่อุปกรณ์และระบบควบคุมระบบปฏิกรณ์นิวเคลียร์ ทำให้อิหร่านจำเป็นต้องปิดระบบปฏิกรณ์นิวเคลียร์และชะลอโครงการพัฒนาขีดความสามารถทางนิวเคลียร์ไประยะหนึ่ง สหรัฐฯ และอิสลาเอลตกเป็นผู้ต้องสงสัยที่เกี่ยวข้องกับการพัฒนามัลแวร์และใช้มัลแวร์ดังกล่าวในการโจมตีต่อระบบปฏิกรณ์นิวเคลียร์ ซึ่งทั้งสหรัฐฯ และอิสราเอลปฏิเสธข้อกล่าวหาดังกล่าวอย่างสิ้นเชิง

ในปี ค.ศ.๒๐๑๒ มีนักวิจัยด้านความมั่นคงปลอดภัยรายงานตรวจพบช่องโหว่ที่ซ่อนอยู่ในโพรเซสเซอร์ Microsemi ProASIC3[๑๑] ซึ่งเป็นไมโครโปรเซสเซอร์สำคัญที่ถูกติดตั้งในอากาศยานหลากหลายชนิดนับตั้งแต่เครื่องบินขับไล่ของกองทัพอากาศสหรัฐฯ ไปจนถึงเครื่องบินโบอิ้ง 777 ของสายการบินพาณิชย์ อย่างไรก็ดี บริษัทผู้ผลิตปฏิเสธว่าช่องโหว่ดังกล่าวเป็นคุณสมบัติสำหรับการตรวจแก้ไขบั๊กของโพรเซสเซอร์นั้นที่ไม่ได้รับการเผยแพร่ด้วยความตั้งใจ เหตุการณ์ดังกล่าวสร้างความเคลือบแคลงใจในการใช้งานผลิตภัณฑ์ที่มีความซับซ้อนสูงเช่นนี้ โดยเฉพาะอย่างยิ่งการประยุกต์ใช้ในอุตสาหกรรมทางทหาร เนื่องจากช่องโหว่ลักษณะนี้อาจถูกใช้เป็นช่องทางในการโจมตีต่อระบบได้นั่นเอง สาธารณรัฐประชาธิปไตยประชาชนเกาหลีหรือเกาหลีเหนือ ทำการโจมตีต่อศูนย์ข้อมูลกระทรวงกลาโหมสาธารณรัฐเกาหลีสำเร็จ[๑๒] สามารถเข้าถึงเอกสารที่มีชั้นความลับที่มีขนาดรวมถึง ๒๓๕ กิกะไบต์ ซึ่งในจำนวนนั้นมีข้อมูลการวางแผนร่วมทางทหารระหว่างกองกำลังสหรัฐอเมริกาและสาธารณรัฐเกาหลี เมื่อปี ค.ศ.๒๐๑๖ โดยผลของการโจมตีในครั้งนั้นเป็นผลสำเร็จครั้งใหญ่ครั้งหนึ่งที่เกิดขึ้นจากความพยายามโจมตีต่อเป้าหมายทางทหาร และหน่วยงานเอกชนสำคัญของเกาหลีใต้อย่างต่อเนื่องนับตั้งแต่ปี ค.ศ.๒๐๐๙

จากกรณีศึกษาสำคัญ ๆ ที่กล่าวมาจะเห็นว่า ไซเบอร์สเปซถูกรัฐต่าง ๆ นำมาใช้ประโยชน์ด้านความมั่นคงเสมือนเป็นอาณาเขตหนึ่งของรัฐ ซึ่งผลสัมฤทธิ์ของปฏิบัติการไซเบอร์ที่ผ่าน ๆ มามีแนวโน้มที่จะส่งผลกระทบโดยตรงต่อยุทธศาสตร์ความมั่นคงและปฏิบัติการทางทหารในระดับยุทธการอย่างเห็นได้ชัด จึงส่งผลให้รัฐต่าง ๆ ดำเนินนโยบายเพิ่มขีดความสามารถในการควบคุมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานระบบสารสนเทศภายใน ตลอดจนความพยายามพัฒนาขีดความสามารถเชิงรุกเพื่อสร้างความได้เปรียบบนไซเบอร์เสปซ[๑๓]

๔. แนวโน้มการเปลี่ยนแปลงปฏิบัติการไซเบอร์

จากการพิจารณารูปแบบการโจมตีต่อระบบสารสนเทศและการสื่อสารในช่วงระยะเวลา ๑๐ ปีที่ผ่านมา สามารถอนุมานแนวโน้มการเพิ่มขีดความสามารถของการประยุกต์ใช้รูปแบบการโจมตีลักษณะดังกล่าวในปฏิบัติการไซเบอร์ได ดังนี้

แม้ว่าพัฒนาการการโจมตีที่มีความซับซ้อนและยากจะสามารถกระทำได้ในทางปฏิบัติ เช่น การโจมตีทางเครือข่ายต่อ UAV RQ-๑๗๐[๑๔] ของสหรัฐฯ ซึ่งบินเหนือน่านฟ้าสาธารณรัฐอิสลามอิหร่าน เพื่อเปลี่ยนเส้นทางและนำร่อนลงเพื่อทำการวิศวกรรมย้อนกลับ (Reverse Engineer) นั้น มีโอกาสเกิดขึ้นน้อยกว่าการโจมตีที่มีความซับซ้อนน้อยกว่า เช่น DDoS ที่หวังผลเพียงแค่ทำให้เป้าหมายไม่สามารถให้บริการต่อผู้ใช้งานได้ เช่นเดียวกับเทคนิคการโจมตีโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารผ่านมัลแวร์ซอฟต์แวร์เรียกค่าไถ่ซึ่งโจมตีต่อช่องโหว่ด้านความมั่นคงปลอดภัยที่ถูกเปิดเผยเป็นสาธารณะ เนื่องจากเป็นการโจมตีบรรลุวัตถุประสงค์และสร้างผลกระทบได้เร็ว ทันต่อสถานการณ์มากกว่า

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

ความก้าวหน้าของเทคโนโลยีปัญญาประดิษฐ์ (AI) จะส่งผลต่อขีดความสามารถของปฏิบัติการไซเบอร์ เช่น การพัฒนามัลแวร์หรือซอฟต์แวร์อัตโนมัติที่สามารถค้นหาและวิเคราะห์ช่องโหว่ รวมถึงทำการโจมตีต่อช่องโหว่ที่มีในระบบควบคุมบังคับบัญชา หรือการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ในการสร้างและเผยแพร่ข้อมูลข่าวสารที่เป็นเท็จ เพื่อสร้างผลกระทบต่อกระบวนการข่าวกรอง การลวงทางการข่าว ด้วยการสร้างข้อความหรือมัลติมีเดียที่ไม่มีอยู่จริงแต่ดูมีความน่าเชื่อถือ เนื่องจากสามารถผลิตซ้ำชุดข้อมูลดังกล่าวได้ในรูปแบบที่หลากหลายและมีแหล่งที่มาต่างกัน[๑๕]

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

ภาพที่ ๘ Soldier 4.0 Concept

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

๕. ขีดความสามารถที่พึงประสงค์สำหรับ Cyber Defense ของกองทัพเรือ

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

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

เอกสารอ้างอิง

๑ Andress J., Winterfeld S. (2013), Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners: Second Edition., Waltham, MA 02451, USA, ISBN 978-0-12-416672-1

๒ Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & Security, 49, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

๓ Wilailux, Korakoch, (2019), The Kinetic Effect of Cyberwar,

๔ Elliott C.. (2010), Botnets: To what extent are they a threat to information security? Information Security Technical Report, 15 (3), pp.79–103. https://doi.org/10.1016/j.istr.2010.11.003

๕ Koch, R., & Golling, M. (2018). The cyber decade: Cyber defence at a X-ing point. 2018 10th International Conference on Cyber Conflict (CyCon), 2018-May, pp.159–186, https://doi.org/10.23919/CYCON.2018.8405016

๖ S, Michael N (Gen. ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.

๗ S. Adee.(2008) , "The hunt for the kill switch", IEEE Spectrum, Vol.45 No.5, pp.34-39, https://doi.org/10.1109/MSPEC.2008.4505310

๘ Marks, P. (2011). "Air traffic system vulnerable to cyber-attack". New Scientist. Vol. 211 No. 2829, pp. 22-23.

๙ D. Cenciotti (2009). "French Navy Rafales grounded by a computer viru". The Aviationist. Available at https://theaviationist.com/2009/02/13/french-navy-rafales-grounded-bya-computer-virus/

๑๐ Shin, J., Son, H., Khalil ur, R., & Heo, G. (2015). Development of a cyber-security risk model using Bayesian networks. Reliability Engineering & System Safety, 134, 208–217. https://doi.org/10.1016/j.ress.2014.10.006

๑๑ Skorobogatov, S. and Woods, C. (2012). "Breakthrough silicon scanning discovers backdoor in military chip". International Workshop on Cryptographic Hardware and Embedded Systems. Available

๑๒ Kshetri, N. (2014). Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses. East Asia, 31(3), 183–201. https://doi.org/10.1007/s12140-014-9215-1

๑๓ Darko Galinec, Darko Možnik & Boris Guberina (2017) Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022

๑๔ Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J.C.H.; and Carter, Candice, (2018), «Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA›s Advanced Air Assets» NPP Book

๑๕ Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI:10.1080/03071847.2020.1765514