- **เพื่อการศึกษา** -

ที่ กห ๐๑๓๔.๑/๖๘

คณะเจ้าหน้าที่ทำงานกลุ่มที่ ๖
สายไหม กทม. ๑๐๒๒๐

มี.ค.๖๘

เรื่อง รายงานผลการดำเนินการ เรื่อง แนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศ ต่อคณะกรรมการบริหาร ทอ.(สมมติเพื่อการศึกษา)

เรียน ประธานคณะกรรมการบริหาร ทอ.(สมมติเพื่อการศึกษา)

อ้างถึง คำสั่งโรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ (เฉพาะ) ที่ ๓/๖๗ ลง ๒๖ พ.ย.๖๗ เรื่อง แต่งตั้งคณะกรรมการเพื่อการฝึกงานในหน้าที่ฝ่ายอำนวยการ

สิ่งที่ส่งมาด้วย ๑. ผนวก ก คำอธิบายเพิ่มเติมลำดับข้อไขที่เป็นไปได้
๒. ผนวก ข อธิบายความเสี่ยงที่ควรนำมาพิจารณาข้อไข
๓. ผนวก ค ผลการทดสอบข้อไขกับเกณฑ์การพิจารณา
๔. ผนวก ง คำอธิบายข้อพิจารณาเพิ่มเติมประกอบการเลือกข้อไขที่ ๒
๕. ผนวก จ ขั้นตอนการโจมตีทางไซเบอร์ หรือการบวนการโจมตีทางไซเบอร์
๖. ผนวก ฉ ประเภทของการโจมตีทางไซเบอร์
๗. ผนวก ช กรณีศึกษาการใช้การโจมตีทางไซเบอร์ (Offensive Cyber) ในปฏิบัติการทางทหาร ในสงคราม รัสเซีย - ยูเครน

๑. ปัญหา

ในปัจจุบันภัยคุกคามในรูปแบบใหม่ที่ไม่มีการแจ้งเตือนล่วงหน้า ไม่มีการใช้อาวุธหรือการกระทบกันซึ่งหน้า แต่ได้เกิดขึ้นในโลกที่ไม่สามารถมองไม่เห็นได้ ซึ่งก็คือ ระบบเครือข่ายคอมพิวเตอร์ ทั่วโลกได้รับผลกระทบจากการปฏิบัติการทางไซเบอร์ทั้งทางตรงและทางอ้อม การปฏิบัติการทางไซเบอร์ได้เป็นหัวข้อสำคัญที่มีการถูกพูดถึงทั้งในการดำเนินการจากทางภาครัฐ กองทัพและภาคเอกชน รวมถึงปฏิบัติการทางทหาร ทำให้หลายประเทศทั่วโลกเร่งพัฒนาการปฏิบัติการทางไซเบอร์ให้มีความก้าวหน้า เพื่อเป็นเครื่องมือในการสอดแนม การลาดตะเวนและหาข่าว การป้องกันตนเอง การโจมตีฝ่ายตรงข้าม และการสนับสนุนการปฏิบัติการทางทหาร การโจมตีทางไซเบอร์ถูกพัฒนาขึ้นเป็นส่วนหนึ่งของการปฏิบัติการในสงครามต่าง ๆ เพื่อสร้างความได้เปรียบเหนือฝ่ายตรงข้าม

จากการวิเคราะห์ปัจจัยที่กลุ่มประเทศชั้นนำของโลก เช่น สาธารณรัฐประชาชนจีน สหพันธรัฐรัสเซีย รัฐอิสราเอล สาธารณรัฐสิงคโปร์ และสหรัฐอเมริกา พบว่าการพัฒนาการปฏิบัติการทางไซเบอร์ให้ประสบความสำเร็จได้นั้น ประกอบด้วย ๖ ปัจจัยความสำเร็จ ดังนี้

๑.๑ สนับสนุนให้...

- **เพื่อการศึกษา** –

๑.๑ สนับสนุนให้การปฏิบัติการทางไซเบอร์เป็นหนึ่งในยุทธศาสตร์หลักด้านความมั่นคงของประเทศ ซึ่งทุกประเทศมีการดำเนินการอย่างเป็นขั้นตอน มีการกำหนดนโยบายระดับชาติ ด้านการปฏิบัติการทางไซเบอร์ที่ชัดเจน

๑.๒ จัดตั้งหน่วยงานเฉพาะที่ปฏิบัติงานด้านไซเบอร์ เช่น รัฐอิสราเอลมีการจัดตั้งหน่วย Unit 8200 ซึ่งมีหน้าที่ในการปฏิบัติการทางไซเบอร์และสงครามอิเล็กทรอนิกส์ หรือสหรัฐอเมริกาที่มีการจัดตั้งหน่วย Cyber Command (USCYBERCOM) ให้เป็นศูนย์กลางในการปฏิบัติการทางไซเบอร์ทั้งเชิงรุกและเชิงรับ โดยอยู่ภายใต้กระทรวงกลาโหมของสหรัฐอเมริกา

๑.๓ สนับสนุนการลงทุนในเทคโนโลยีและนวัตกรรมขั้นสูง เช่น การลงทุนด้าน AI เพื่อพัฒนาเป็นเครื่องมือในการค้นหาและเจาะระบบ การพัฒนา Malwares หรือ Zero-Day Exploits เพื่อเป็นอาวุธทางไซเบอร์สำหรับโจมตีฝ่ายตรงข้าม หรือการสร้าง Cyber Range Simulation เพื่อฝึกการโจมตีในสภาพแวดล้อมจำลอง เป็นต้น

๑.๔ ให้ความสำคัญในการพัฒนาบุคลากรด้านไซเบอร์ เช่น การคัดเลือกเยาวชนที่มีศักยภาพสูงให้เข้ารับการฝึกฝนในกองทัพ การให้ทุนการศึกษาเพื่อสร้างบุคลากรทางไซเบอร์ขั้นสูง การคัดเลือกบุคลากรจากมหาวิทยาลัยชั้นนำ และให้การสนับสนุนกลุ่มแฮ็กเกอร์ที่มีความชำนาญ เป็นต้น

๑.๕ สร้างความร่วมมือกับหน่วยงานภายในประเทศและภายนอกประเทศ ในการเสริมสร้างขีดความสามารถและความชำนาญด้านการปฏิบัติการไซเบอร์ เพื่อให้การพัฒนาขีดความสามารถทางไซเบอร์มีความก้าวหน้ายิ่งขึ้น เช่น รัฐอิสราเอลมีการส่งเสริมความร่วมมือระหว่างกองทัพและบริษัทเทคโนโลยีต่าง ๆ ในการพัฒนาเครื่องมือและองค์ความรู้ด้านไซเบอร์ รวมทั้งทำงานร่วมกับสหรัฐอเมริกาและ องค์กร NATO เพื่อแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เป็นต้น

๑.๖ บูรณาการการปฏิบัติการทางไซเบอร์เข้ากับยุทธศาสตร์การป้องกันประเทศ โดยนำการปฏิบัติการทางไซเบอร์ปฏิบัติการร่วมกับการปฏิบัติการทางทหาร เช่น สงคราม รัสเซีย – ยูเครน หรือ กรณี Stuxnet การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานนิวเคลียร์ของอิหร่านในปี ๒๐๑๐ เป็นต้น

จากการวิเคราะห์สถานการณ์ในปัจจุบันจึงไม่สามารถมองข้ามความสำคัญของการโจมตีทางไซเบอร์ในยุคที่สมรภูมิเปลี่ยนแปลงอย่างรวดเร็ว หากต้องการรักษาความได้เปรียบเหนือฝ่ายตรงข้าม การใช้การปฏิบัติการทางไซเบอร์ (Offensive Cyber Operations : OCO) ควบคู่ไปกับการปฏิบัติการทางอากาศ ไม่เพียงเพิ่มโอกาสความสำเร็จในการปฏิบัติภารกิจ แต่ยังสามารถช่วยลดความเสี่ยงให้กับกำลังพลของฝ่ายเราได้อย่างมีนัยสำคัญ การปฏิบัติการทางไซเบอร์ (Offensive Cyber Operations : OCO) ไม่ใช่เป็นเพียงแค่เทคโนโลยี แต่คือ ยุทธศาสตร์ที่จะกำหนดอนาคตของปฏิบัติการทางทหารและความมั่นคงของประเทศ การปฏิบัติการทางไซเบอร์ (Offensive Cyber Operations : OCO) ไม่ใช่เป็นเพียงแค่ส่วนเสริม แต่คือ กุญแจสำคัญในการปฏิบัติการทางอากาศที่มีประสิทธิภาพ ครอบคลุมการปฏิบัติการในทุกมิติอย่างมีประสิทธิภาพ

๒. ปัจจัยเกี่ยวกับปัญหา

๒.๑ ข้อเท็จจริง

- เพื่อการศึกษา –

๒.๑.๑ คณะทำงานฯ ได้ศึกษาการปฏิบัติการทางอากาศของหลากหลายประเทศ เช่น ไทย, สหราชอาณาจักร, สหรัฐอเมริกา, เครือรัฐออสเตรเลีย, สหพันธรัฐรัสเซีย และสาธารณรัฐประชาชนจีน เป็นต้น โดยนำการปฏิบัติการทางอากาศ มาเปรียบเทียบ และสามารถสรุปการปฏิบัติหลักของกำลังทางอากาศ (Core Air Power Roles) ที่เป็นสากล ดังนี้

๒.๑.๑.๑ การตอบโต้ทางอากาศ (Counter Air) เป็นกลยุทธ์ทางการทหารที่มุ่งเน้นการทำลายหรือจำกัดขีดความสามารถของศัตรูในการปฏิบัติการทางอากาศ โดยมีวัตถุประสงค์หลัก เพื่อควบคุมและรักษาความได้เปรียบทางอากาศ (Air Superiority) มี ๒ ประเภทหลัก ดังนี้

๒.๑.๑.๑ (๑) การตอบโต้ทางอากาศเชิงรุก (Offensive Counter Air : OCA)

๒.๑.๑.๑ (๒) การตอบโต้ทางอากาศเชิงรับ (Defensive Counter Air : DCA)

๒.๑.๑.๒ การข่าวกรอง การเฝ้าตรวจ และการลาดตระเวน (Intelligence, Surveillance and Reconnaissance : ISR) เป็นกระบวนการสำคัญในปฏิบัติการทางทหาร โดยมุ่งเน้นการรวบรวม วิเคราะห์ ติดตามข้อมูลเกี่ยวกับศัตรูและสภาพแวดล้อมการปฏิบัติการ เพื่อสนับสนุนการตัดสินใจและการวางแผนของผู้บังคับบัญชา

๒.๑.๑.๓ การเคลื่อนที่ทางอากาศ (Air Mobility) เป็นความสามารถในการเคลื่อนย้ายกำลังพล ยุทโธปกรณ์ และทรัพยากรต่าง ๆ ทางอากาศอย่างรวดเร็วและมีประสิทธิภาพ ซึ่งมีบทบาทสำคัญในการสนับสนุนปฏิบัติการทางทหารและการบรรเทาสาธารณภัย โดยสามารถดำเนินการในพื้นที่ที่การเข้าถึงทางบกหรือทางน้ำเป็นไปได้ยาก ทำให้การลำเลียงทางอากาศเป็นปัจจัยสำคัญในการตอบสนองต่อสถานการณ์ฉุกเฉินและการปฏิบัติการที่ต้องการความรวดเร็ว

๒.๑.๑.๔ การโจมตี (Attack) เป็นการใช้กำลังทางอากาศ เช่น เครื่องบินรบ เฮลิคอปเตอร์ หรืออากาศยานไร้คนขับ (UAV) เพื่อโจมตีเป้าหมายบนพื้นดินหรือในอากาศ โดยมีวัตถุประสงค์เพื่อทำลายหรือทำให้ขีดความสามารถของศัตรูลดลง การโจมตีทางอากาศเป็นส่วนสำคัญของปฏิบัติการทางทหารที่ช่วยสนับสนุนและเพิ่มประสิทธิภาพในการรบ

๒.๑.๑.๕ การบัญชาการและควบคุม (Command and Control : C2) เป็นกระบวนการที่ผู้บังคับบัญชาใช้ในการสั่งการและควบคุมกำลังพล ทรัพยากร เพื่อบรรลุภารกิจที่กำหนด โดยอาศัยการตัดสินใจ การสื่อสารและการประสานงานอย่างมีประสิทธิภาพ

๒.๑.๑.๖ การป้องกันทางอากาศ (Air Defense) เป็นการใช้มาตรการและระบบต่างๆ เพื่อป้องกันและตอบโต้การโจมตีทางอากาศจากศัตรู โดยมีวัตถุประสงค์เพื่อปกป้องพื้นที่สำคัญ กำลังพลและทรัพยากรของประเทศ ซึ่งรวมถึงการใช้เครื่องบินขับไล่ ระบบป้องกันภัยทางอากาศและการเฝ้าระวังทางเรดาร์

๒.๑.๒ หลักการและเครื่องมือของการโจมตีทางไซเบอร์

๒.๑.๒.๑ หลักการการโจมตีทางไซเบอร์ในปัจจุบันที่นิยมใช้กัน คือ Cyber Kill Chain เป็นการระบุกรอบขั้นตอนการโจมตีพื้นฐานทางไซเบอร์ โดยแบ่งขั้นตอนการโจมตีออกเป็น ๓ เฟสใหญ่ และประกอบด้วย ๗ ขั้นตอนย่อย ดังนี้

- เพื่อการศึกษา -

- **เพื่อการศึกษา** –

๒.๑.๒.๑ (๑) เฟสที่ ๑ เตรียมการโจมตี ประกอบด้วย

ขั้นตอนที่ ๑ การลาดตระเวน คือ การเก็บรวบรวมข้อมูลของเป้าหมายก่อนเริ่มการโจมตี

ขั้นตอนที่ ๒ เตรียมอาวุธสำหรับโจมตี โดยผู้โจมตีเตรียมหาวิธีเจาะระบบและเตรียมมัลแวร์เพื่อส่งไปยังเป้าหมาย

๒.๑.๒.๑ (๒) เฟสที่ ๒ บุกรุกโจมตี ประกอบด้วย

ขั้นตอนที่ ๓ ผู้โจมตีส่งมัลแวร์ไปยังเป้าหมายผ่านช่องทางต่าง ๆ เพื่อใช้เจาะเข้าระบบของเหยื่อ

ขั้นตอนที่ ๔ ผู้โจมตีทำการเจาะระบบของเป้าหมายด้วยวิธีต่าง ๆ เช่น ใช้ช่องโหว่ของระบบหรือ Social Engineering เป็นต้น

ขั้นตอนที่ ๕ ผู้โจมตีทำการติดตั้งมัลแวร์บนเครื่องคอมพิวเตอร์ของเป้าหมายเพื่อให้คอยรับคำสั่งและกระทำการตามที่ผู้โจมตีต้องการ

๒.๑.๒.๑ (๓) เฟสที่ ๓ เก็บเกี่ยวผลลัพธ์ประกอบด้วย

ขั้นตอนที่ ๖ ผู้โจมตีสร้างช่องทางในการรับส่งคำสั่งกับมัลแวร์ที่ได้ดำเนินการติดตั้งไว้เพื่อให้สามารถจัดการและควบคุมมัลแวร์ให้ทำตามความต้องการ

ขั้นตอนที่ ๗ เก็บเกี่ยวผลประโยชน์ตามที่ต้องการจากระบบเครือข่ายของเป้าหมาย เช่น ขโมยข้อมูล เปลี่ยนแปลงแก้ไขข้อมูล หรือทำลายระบบ เป็นต้น

๒.๑.๒.๒ รูปแบบการโจมตีทางไซเบอร์มี ๓ รูปแบบ ดังนี้

๒.๑.๒.๒ (๑) การก่อกวน (Disruption) คือ การมุ่งเน้นการขัดขวางหรือรบกวนการทำงานของระบบ หรือบริการ เช่น การโจมตีแบบ DDoS (Distributed Denial of Service) เพื่อทำให้ระบบเครือข่ายหรือเว็บไซต์ไม่สามารถให้บริการได้ชั่วคราว หรือการปล่อยมัลแวร์เพื่อสร้างความวุ่นวาย หรือทำให้ระบบทำงานผิดปกติ เป็นต้น

๒.๑.๒.๒ (๒) การจารกรรม (Espionage) คือ การมุ่งเน้นการล้วงข้อมูลที่เป็นความลับหรือข้อมูลสำคัญ เช่น การเจาะระบบเพื่อขโมยข้อมูลส่วนบุคคล ข้อมูลการเงิน หรือข้อมูลทางธุรกิจ ด้วยการใช้งานฟิชชิง (Phishing) เพื่อหลอกลวงเหยื่อให้เปิดเผยข้อมูลสำคัญ เป็นต้น

๒.๑.๒.๒ (๓) การทำลาย (Degradative) คือ การที่มุ่งเน้นการทำลายระบบ ข้อมูลหรือทรัพย์สินดิจิทัล เช่น การลบหรือแก้ไขข้อมูลในระบบ การปล่อยแรนซัมแวร์ (Ransomware) เพื่อเข้ารหัสข้อมูลและเรียกค่าไถ่ หรือการโจมตีเพื่อทำลายโครงสร้างพื้นฐานที่สำคัญ เป็นต้น

๒.๑.๒.๓ เครื่องมือของการโจมตีทางไซเบอร์ เป็นชุดคำสั่งที่ถูกเขียนขึ้นตามวัตถุประสงค์ที่ต้องการโดยบุคลากรที่มีความเชี่ยวชาญขั้นสูง ซึ่งมีการพัฒนาตามวัตถุประสงค์ของผู้โจมตี เช่น มัลแวร์, ไวรัส, เวิร์ม, โทราจันและสปายแวร์ เป็นต้น

- เพื่อการศึกษา –

๒.๑.๓ สถานการณ์...

๒.๑.๓ สถานการณ์การปฏิบัติการทางไซเบอร์เพื่อสนับสนุนการรบ เช่น การปฏิบัติการทางทหารในสงคราม รัสเซีย - ยูเครน การโจมตีทางไซเบอร์จะมีการดำเนินการก่อนการปฏิบัติการทางทหารเสมอ เพื่อก่อกวน ลดทอนขีดความสามารถ ทำให้ระบบการป้องกัน หรือระบบอำนวยความสะดวกต่างๆ เกิดความขัดข้อง หรือสูญเสียประสิทธิภาพในการรบ

๒.๑.๔ การพัฒนาการปฏิบัติการทางไซเบอร์ของประเทศต่าง ๆ มีปัจจัยความสำเร็จ ๘ ข้อ ได้แก่

๒.๑.๔.๑ การกำหนดนโยบายการพัฒนาการปฏิบัติการทางไซเบอร์

๒.๑.๔.๒ การจัดตั้งหน่วยงานเฉพาะ เพื่อรับผิดชอบด้านการปฏิบัติการทางไซเบอร์

๒.๑.๔.๓ การสร้างความร่วมมือด้านการปฏิบัติการทางไซเบอร์ระหว่างกองทัพและเอกชน

๒.๑.๔.๔ การสร้างความร่วมมือด้านการปฏิบัติการทางไซเบอร์ระหว่างประเทศพันธมิตร

๒.๑.๔.๕ การกำหนดกระบวนการและแนวทางการปฏิบัติการทางไซเบอร์

๒.๑.๔.๖ มีกระบวนการฝึกอบรมและพัฒนาบุคลากรด้านไซเบอร์ให้มีความเชี่ยวชาญ

๒.๑.๔.๗ มีอาวุธไซเบอร์เพื่อใช้ในการปฏิบัติการทางไซเบอร์

๒.๑.๔.๘ มีบุคลากรที่มีความเชี่ยวชาญในการปฏิบัติการทางไซเบอร์

๒.๑.๕ การโจมตีทางไซเบอร์ขัดต่อกฎบัตรสหประชาชาติ ข้อ ๒(๔) ที่ระบุว่า รัฐสมาชิกต้องงดเว้นจากการใช้กำลังหรือการข่มขู่ที่จะใช้กำลังในลักษณะใด ๆ ที่เป็นการละเมิดบูรณภาพแห่งดินแดนหรือเอกราชทางการเมืองของรัฐอื่น ซึ่งการโจมตีทางไซเบอร์ที่มีผลกระทบคล้ายคลึงกับการโจมตีทางกายภาพ เช่น การทำลายโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure : CII) ถูกตีความว่าเป็นการใช้กำลังเช่นกัน

๒.๒ ข้อสมมุติ

๒.๒.๑ สถานการณ์และขีดความสามารถปัจจุบันยังไม่มีการริเริ่มนำแนวคิดการโจมตีทางไซเบอร์ (Offensive Cyber Operations) มาช่วยในการสนับสนุนการปฏิบัติการทางอากาศ

๒.๒.๒ กองทัพอากาศมีหน่วยงาน โครงสร้างพื้นฐานและบุคลากรด้านเทคโนโลยีสารสนเทศ แต่ยังไม่มีความเชี่ยวชาญด้านการโจมตีทางไซเบอร์

๒.๒.๓ การศึกษาและพัฒนาด้านเทคโนโลยีสารสนเทศและไซเบอร์ จำเป็นต้องพึ่งพาสถาบันภาคเอกชนทั้งในและนอกประเทศ

๒.๒.๔ การศึกษาและพัฒนาต้องนำแนวทางจากประเทศที่ประสบผลสำเร็จมาเป็นต้นแบบ

๒.๒.๕ การโจมตีทางไซเบอร์ส่งผลต่อความได้เปรียบต่อการปฏิบัติทางอากาศ

๒.๒.๖ ด้านนโยบายระดับชาติ ได้ดำเนินการตามกระบวนการพัฒนาการปฏิบัติการทางไซเบอร์ทั้ง ๖ ข้อ เรียบร้อยแล้ว ดังนี้

๒.๒.๖.๑ มีการกำหนดนโยบายการพัฒนาการปฏิบัติการทางไซเบอร์

๒.๒.๖.๒ มีการจัดตั้งหน่วยงานเฉพาะ เพื่อรับผิดชอบด้านการปฏิบัติการทางไซเบอร์

๒.๒.๖.๓ มีการสร้างความร่วมมือด้านการปฏิบัติการทางไซเบอร์ระหว่างรัฐบาล กองทัพ และเอกชน

๒.๒.๖.๔ มีการสร้าง...

๒.๒.๖.๔ มีการสร้างความร่วมมือด้านการปฏิบัติการทางไซเบอร์ระหว่างประเทศพันธมิตร

๒.๒.๖.๕ มีการกำหนดกระบวนการและแนวทางการปฏิบัติการทางไซเบอร์

๒.๒.๖.๖ มีกระบวนฝึกอบรมและพัฒนาบุคลากรด้านไซเบอร์ให้มีความเชี่ยวชาญ

๒.๓ เกณฑ์การพิจารณา

๒.๓.๑ เกณฑ์การพิจารณาหลัก

๒.๓.๑.๑ ต้องได้มาซึ่งขีดความสามารถการโจมตีทางไซเบอร์

๒.๓.๑.๒ ต้องสนับสนุนการปฏิบัติการทางอากาศ

๒.๓.๑.๓ ต้องมีอาวุธสำหรับสนับสนุนการโจมตีทางไซเบอร์

๒.๓.๑.๔ ต้องมีบุคลากรที่มีความเชี่ยวชาญสำหรับดำเนินการโจมตีทางไซเบอร์

๒.๓.๒ เกณฑ์การพิจารณารอง

๒.๓.๒.๑ ควรเป็นการดำเนินการที่มีชั้นความลับ

๒.๓.๒.๒ ควรเป็นการส่งเสริมการพัฒนาแบบยั่งยืน

๒.๓.๒.๓ ควรมีความอิสระในการปฏิบัติงาน

๒.๓.๒.๔ ควรมีความเหมาะสมระหว่างระยะเวลาดำเนินการและงบประมาณที่ใช้

๒.๔ คำจำกัดความ

๒.๔.๑ ไซเบอร์ (Cyber) หมายถึง สิ่งที่เกี่ยวข้องหรือสัมพันธ์กับอินเทอร์เน็ต ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบควบคุมกำกับดูแลและเก็บข้อมูล (Supervisory Control and Data Acquisition : SCADA) ระบบควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Embedded Systems) เป็นต้น

๒.๔.๒ มิติไซเบอร์ (Cyberspace) หมายถึง มิติที่มีการประยุกต์ใช้หลักการด้านอิเล็กทรอนิกส์ และหลักการด้านสเปกตรัมแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) ในการจัดเก็บ แก้ไข หรือแลกเปลี่ยนข้อมูลบนโครงสร้างพื้นฐานทางกายภาพ

๒.๔.๓ การปฏิบัติในมิติไซเบอร์ (Cyber space Operations) หมายถึง การดำเนินการโดยใช้ขีดความสามารถทางไซเบอร์ในมิติไซเบอร์ เพื่อให้บรรลุวัตถุประสงค์ที่ตั้งไว้

๒.๔.๔ ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่อง ซึ่งถูกนำมาใช้เพื่อให้ได้ผลตามที่ต้องการ

๒.๔.๕ การแสวงหาประโยชน์จากช่องโหว่ (Exploitation) หมายถึง การนำเทคนิคการปฏิบัติการในมิติไซเบอร์มาดำเนินการกับช่องโหว่ หรือใช้ช่องโหว่เป็นทางผ่านเพื่อให้เกิดผลตามที่ต้องการ

๒.๔.๖ Cyber Attack หมายถึง การโจมตีทางไซเบอร์ต่อฝ่ายตรงข้ามโดยมีวัตถุประสงค์เพื่อขัดขวาง ทำลาย หรือควบคุม การใช้งานมิติไซเบอร์ของฝ่ายตรงข้าม รวมถึงการทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลของฝ่ายตรงข้าม

๒.๔.๗ Offensive Cyber หมายถึง การโจมตีทางไซเบอร์ (Cyber Attack) ที่กระทำโดยหน่วยงานหรือองค์กรที่ได้รับมอบหมายให้รับผิดชอบโดยตรง เพื่อผลประโยชน์ของรัฐในการป้องกันหรือสร้างความได้เปรียบในการปฏิบัติการต่อเป้าหมาย

- **เพื่อการศึกษา** –

๒.๔.๘ สงครามไซ...

๒.๔.๘ สงครามไซเบอร์ (Cyber Warfare) หมายถึง การปฏิบัติในมิติไซเบอร์ซึ่งมีมูลเหตุหรือวัตถุประสงค์ทางการเมืองหรือทางทหาร โดยนำเทคนิคการปฏิบัติในมิติไซเบอร์มาใช้ป้องกัน รวมทั้งโจมตี หรือแสวงหาประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม

๒.๔.๙ ช่องโหว่ Zero Day (Zero-Day Vulnerability) หมายถึง ช่องโหว่ในซอฟต์แวร์ ฮาร์ดแวร์ หรือระบบเครือข่ายที่ยังไม่ได้รับการเปิดเผยหรือแก้ไข โดยที่ผู้พัฒนาและผู้ดูแลระบบยังไม่ทราบถึงการมีอยู่ของช่องโหว่นี้ ทำให้แฮ็กเกอร์หรือผู้ไม่หวังดีสามารถใช้ประโยชน์จากช่องโหว่ดังกล่าวเพื่อโจมตีระบบก่อนที่จะมีการอุดช่องโหว่หรือออกแพตช์แก้ไข

๒.๔.๑๐ อาวุธทางไซเบอร์ (Cyber Weapon) หมายถึง เครื่องมือ ซอฟต์แวร์ หรือเทคนิคที่ถูกออกแบบเพื่อโจมตีระบบคอมพิวเตอร์ เครือข่าย หรือโครงสร้างพื้นฐานด้านสารสนเทศที่เป็นเป้าหมาย

๒.๔.๑๑ มัลแวร์ (Malware) หมายถึง ซอฟต์แวร์ที่เป็นอันตราย ถูกออกแบบมาเพื่อสร้างความเสียหาย, ขโมยข้อมูล, หรือควบคุมระบบโดยไม่ได้รับอนุญาต คำว่า Malware มาจาก Malicious Software ซึ่งรวมถึง ไวรัส, โทรจัน, แรนซัมแวร์ และอื่นๆ

๓. ลำดับข้อไขที่เป็นไปได้

๓.๑ ข้อไขที่ ๑ จัดหาอาวุธและบุคลากรที่มีความเชี่ยวชาญสำหรับการโจมตีทางไซเบอร์ เป็นการจัดหาอาวุธและบุคลากรที่มีความเชี่ยวชาญจากประเทศพันธมิตรหรือหน่วยงานภาคเอกชน

๓.๒ ข้อไขที่ ๒ จัดหาอาวุธและพัฒนาบุคลากรสำหรับการโจมตีทางไซเบอร์ ให้สามารถใช้อาวุธที่จัดหาได้อย่างมีประสิทธิภาพ รวมถึงสามารถดำเนินการพัฒนาอาวุธทางไซเบอร์ได้ในอนาคต เป็นการจัดหาอาวุธจากประเทศพันธมิตรหรือหน่วยงานภาคเอกชน ควบคู่ไปกับการพัฒนาบุคลากรให้มีความเชี่ยวชาญในการใช้อาวุธที่จัดซื้อตลอดจนสามารถดำเนินการโจมตีทางไซเบอร์และการพัฒนาอาวุธทางไซเบอร์

๓.๓ ข้อไขที่ ๓ พัฒนาอาวุธและบุคลากรสำหรับการโจมตีทางไซเบอร์ เป็นการพัฒนาบุคลากรให้มีความเชี่ยวชาญจนสามารถพัฒนาอาวุธที่ใช้เฉพาะการโจมตีทางไซเบอร์ และสามารถดำเนินการพัฒนาอาวุธสำหรับการโจมตีทางไซเบอร์ที่ใช้ในแต่ละภารกิจได้

๔. อภิปราย

๔.๑ จากการพิจารณาข้อไขทั้ง ๓ ข้อไข ปรากฏว่าเป็นแนวทางที่ได้มาซึ่งขีดความสามารถในการโจมตีทางไซเบอร์ สามารถสนับสนุนการปฏิบัติการทางอากาศ มีอาวุธสำหรับสนับสนุนการโจมตีทางไซเบอร์ และมีบุคลากรที่มีความเชี่ยวชาญสำหรับดำเนินการโจมตีทางไซเบอร์

๔.๒ ข้อไขที่ ๒ และข้อไขที่ ๓ เป็นการดำเนินการที่มีชั้นความลับ เนื่องจากใช้บุคลากรภายในหน่วยงานเป็นผู้ปฏิบัติการโจมตีทางไซเบอร์ แต่ข้อไขที่ ๑ เป็นการจัดหาบุคลากรจากภายนอกหน่วยซึ่งมีความเสี่ยงต่อการรักษาความลับในการปฏิบัติภารกิจ

๔.๓ ข้อไขที่ ๒...

- เพื่อการศึกษา –

๔.๓ ข้อไขที่ ๒ และข้อไขที่ ๓ เป็นการดำเนินการส่งเสริมการพัฒนาแบบยั่งยืน เนื่องจากการพัฒนาบุคลากรทางไซเบอร์สามารถต่อยอดพัฒนาอาวุธทางไซเบอร์ได้เองในอนาคต แต่ข้อไขที่ ๑ เป็นการจัดหาบุคลากรจากภายนอกหน่วย ไม่มีการพัฒนาบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์ที่จะสามารถดำเนินการพัฒนาอาวุธทางไซเบอร์ในอนาคต

๔.๔ ข้อไขที่ ๒ และข้อไขที่ ๓ เป็นการดำเนินการที่มีความอิสระในการปฏิบัติงานการโจมตีทางไซเบอร์ เนื่องจากใช้บุคลากรทางไซเบอร์ภายในหน่วยงาน แต่ข้อไขที่ ๑ เป็นการจัดหาบุคลากรจากนอกหน่วย จึงมีข้อจำกัดในความอิสระในการโจมตีทางไซเบอร์

๔.๕ ข้อไขที่ ๒ มีความเหมาะสมระหว่างระยะเวลาดำเนินการและงบประมาณที่ใช้ โดยสามารถลดความเสี่ยงและข้อจำกัดในระยะเริ่มต้น เป็นการใช้ประโยชน์จากเทคโนโลยีที่มีอยู่และเตรียมพร้อมสำหรับการพัฒนาในอนาคต มีความคุ้มค่ากับงบประมาณที่ดำเนินการมากที่สุด เพราะผสมผสานการจัดหาและการพัฒนา สามารถลดค่าใช้จ่ายในระยะยาว แต่ข้อไขที่ ๑ เป็นการจัดหาเทคโนโลยีและบุคลากรในการปฏิบัติการโจมตีทางไซเบอร์ ซึ่งสามารถดำเนินการได้ทันที แต่ต้องใช้ทรัพยากรจำนวนมากซึ่งไม่เหมาะสมในระยะยาว เนื่องด้วยไม่มีการพัฒนาบุคลากรและอาวุธได้ด้วยตัวเอง

๔.๖ ข้อไขที่ ๓ แม้ว่าจะมุ่งเน้นการพัฒนาเทคโนโลยีและบุคลากร แต่ต้องใช้เวลาและทรัพยากรจำนวนมาก ซึ่งไม่เหมาะสมกับสถานะเริ่มต้น อีกทั้งมีค่าใช้จ่ายที่สูงในระยะยาว เพราะต้องลงทุนพัฒนาทั้งบุคลากรและอาวุธ

๔.๗ เมื่อเปรียบเทียบข้อไขทั้ง ๓ ข้อไข พบว่าผ่านเกณฑ์การพิจารณาหลักทั้ง ๓ ข้อไข คือ

๔.๗.๑ เป็นแนวทางที่ได้มาซึ่งขีดความสามารถการโจมตีทางไซเบอร์

๔.๗.๒ สามารถสนับสนุนการปฏิบัติการทางอากาศ

๔.๗.๓ ได้รับอาวุธสำหรับสนับสนุนการโจมตีทางไซเบอร์

๔.๗.๔ มีบุคลากรที่มีความเชี่ยวชาญสำหรับดำเนินการโจมตีทางไซเบอร์

๔.๘ ดำเนินการทดสอบข้อไขในเกณฑ์การพิจารณารองทั้ง ๓ ข้อไข พบว่าข้อไขที่ ๑ ไม่ผ่านเกณฑ์การพิจารณารองทั้ง ๔ ข้อ ข้อไขที่ ๒ ผ่านเกณฑ์การพิจารณารองทั้ง ๔ ข้อ ส่วนข้อไขที่ ๓ ผ่านเกณฑ์การพิจารณารอง ๓ ข้อ

๕. สรุปผล

จากการพิจารณาข้อไขทั้ง ๓ ข้อไข สรุปได้ว่า ข้อไขที่ ๒ จัดหาอาวุธสำหรับการโจมตีทางไซเบอร์และพัฒนาบุคลากรให้สามารถใช้อาวุธที่จัดหาได้อย่างมีประสิทธิภาพ รวมถึงสามารถดำเนินการพัฒนาอาวุธทางไซเบอร์ได้ในอนาคต เป็นแนวทางที่ได้มาซึ่งขีดความสามารถการโจมตีทางไซเบอร์ เพื่อสนับสนุนการปฏิบัติการทางอากาศ ได้รับอาวุธสำหรับสนับสนุนการโจมตีทางไซเบอร์ มีบุคลากรที่มีความเชี่ยวชาญสำหรับดำเนินการโจมตีทางไซเบอร์ สามารถดำเนินการที่มีชั้นความลับ ส่งเสริมการพัฒนาอย่างยั่งยืน มีความอิสระในการปฏิบัติงาน และมีความเหมาะสมระหว่างระยะเวลาดำเนินการและงบประมาณที่ใช้

คณะเจ้าหน้าที่...

- **เพื่อการศึกษา** –

คณะเจ้าหน้าที่ทำงานฯ พิจารณาแล้ว การดำเนินการตามข้อไขที่ ๒ ให้ความสมดุลระหว่างการจัดหาและการพัฒนา ซึ่งช่วยตอบสนองความต้องการในปัจจุบันและวางรากฐานสำหรับอนาคต ช่วยให้การเริ่มต้นใช้งานเทคโนโลยีไซเบอร์ได้ทันที โดยไม่สูญเสียเวลาและทรัพยากรไปกับการพัฒนาทั้งหมด รวมถึงสามารถเพิ่มศักยภาพทั้งในด้านอาวุธและบุคลากร ทำให้ตอบสนองต่อภัยคุกคามและสนับสนุนการปฏิบัติการทางอากาศได้อย่างมีประสิทธิภาพ จึงเป็นแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์เพื่อสนับสนุนการปฏิบัติการทางอากาศที่มีความเหมาะสมที่สุด

น.ท.
หน.คณะเจ้าหน้าที่ทำงาน กลุ่มที่ ๖

- **เพื่อการศึกษา** –

ผนวก ก ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

<u>คำอธิบายเพิ่มเติมลำดับข้อไขที่เป็นไปได้</u>

จากการวิเคราะห์แนวทางการพัฒนาการโจมตีทางไซเบอร์เพื่อสนับสนุนการปฏิบัติทางอากาศ พบว่า มีปัจจัยนำไปสู่ความสำเร็จ ๒ ข้อ คือ มีอาวุธสำหรับการโจมตีทางไซเบอร์ และ มีบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์ โดยอธิบายเพิ่มเติมได้ดังนี้

๑. แนวทางการได้อาวุธสำหรับการโจมตีทางไซเบอร์มานั้น ประกอบด้วย

๑.๑ การพัฒนาเอง

๑.๑.๑ องค์กรหรือรัฐพัฒนาขึ้นเองโดยใช้ทีมนักพัฒนาที่เชี่ยวชาญด้านความปลอดภัยไซเบอร์และการเจาะระบบ

๑.๑.๒ ใช้การวิจัยและพัฒนาเพื่อค้นหาช่องโหว่ (Vulnerability Research)

๑.๒ การซื้อขายในตลาดมืด (Dark Web)

๑.๒.๑ Cyber Weapon หลายชนิดถูกซื้อขายในตลาดมืด เช่น Exploit Kits หรือ Zero-Day Exploit

๑.๒.๒ บางครั้งอาวุธไซเบอร์ถูกขายเป็นบริการ (Cybercrime as a Service : CaaS)

๑.๓ การได้มาจากคู่แข่งหรือศัตรู ขโมยหรือย้อนรอยอาวุธไซเบอร์จากการโจมตีที่เคยเกิดขึ้น

๑.๔ การแลกเปลี่ยนหรือความร่วมมือ บางรัฐหรือองค์กรอาจแลกเปลี่ยนหรือแบ่งปันเทคนิคและเครื่องมือเพื่อใช้ในปฏิบัติการร่วมกัน

๑.๕ การซื้อจากผู้ให้บริการเชิงพาณิชย์ บางบริษัทพัฒนาซอฟต์แวร์ที่สามารถใช้ในลักษณะโจมตีไซเบอร์โดยถูกกฎหมาย

๒. บุคลากรที่มีความเชี่ยวชาญทางไซเบอร์ มีแนวทางให้ได้มาดังนี้

๒.๑ การพัฒนาภายในองค์กร เช่น การฝึกอบรม การส่งเสริมการศึกษาและการให้ประสบการณ์ในงานจริง

๒.๒ การว่าจ้างผู้เชี่ยวชาญ การสรรหา จ้างบุคลากรที่มีทักษะและประสบการณ์ตรงในสายงาน หรือการจ้างที่ปรึกษา ใช้บริการผู้เชี่ยวชาญหรือบริษัทที่ปรึกษาด้านไซเบอร์

๒.๓ การดึงดูดบุคลากรผ่านโครงการเฉพาะ การจัดโครงการการแข่งขัน การสร้างเครือข่ายความร่วมมือกับมหาวิทยาลัยหรือสถาบันการศึกษา

๒.๔ การพัฒนาความสามารถระดับประเทศ การสนับสนุนโดยภาครัฐ สร้างศูนย์พัฒนาทักษะไซเบอร์ การสร้างบุคลากรรุ่นใหม่

- **เพื่อการศึกษา** –

ผนวก ข ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

อธิบายความเสี่ยงที่ควรนำมาพิจารณา

ข้อไขที่ ๑ “จัดหาทั้งอาวุธสำหรับการโจมตีทางไซเบอร์และบุคลากรที่มีความเชี่ยวชาญ” เป็นการจัดหาอาวุธและบุคลากรที่มีความเชี่ยวชาญจากประเทศพันธมิตรหรือหน่วยงานภาคเอกชน

ความเสี่ยงที่ควรนำมาพิจารณา

- อาวุธที่ได้จากการจัดหาไม่ใช่ Zero Day
- อาวุธบางชนิดอาจต้องหาจากตลาดมืด ซึ่งไม่มีความน่าเชื่อถือ
- ต้องมีการจัดซื้อใหม่ทุกครั้งที่ดำเนินการโจมตีทางไซเบอร์
- การจัดหาบุคลากรจากนอกหน่วย เสี่ยงต่อการรักษาความลับ

ข้อไขที่ ๒ “จัดหาอาวุธและพัฒนาบุคลากรสำหรับการโจมตีทางไซเบอร์ ให้สามารถใช้อาวุธที่จัดหาได้อย่างมีประสิทธิภาพรวมถึงสามารถดำเนินการพัฒนาอาวุธทางไซเบอร์ได้ในอนาคต” เป็นการจัดหาอาวุธจากประเทศพันธมิตรหรือหน่วยงานภาคเอกชน ควบคู่ไปกับการพัฒนาบุคลากรให้มีความเชี่ยวชาญในการใช้อาวุธที่จัดซื้อตลอดจนสามารถดำเนินการโจมตีทางไซเบอร์และการพัฒนาอาวุธทางไซเบอร์

ความเสี่ยงที่ควรนำมาพิจารณา

- ปัจจัยด้านการจัดหาอาวุธ มีความเสี่ยงเช่นเดียวกับข้อไขที่ ๑
- ส่วนการพัฒนาบุคลากรให้มีความเชี่ยวชาญ อาจใช้ระยะเวลานาน

ข้อไขที่ ๓ “พัฒนาอาวุธและบุคลากรสำหรับการโจมตีทางไซเบอร์” เป็นการพัฒนาบุคลากรให้มีความเชี่ยวชาญจนสามารถพัฒนาอาวุธที่ใช้เฉพาะการโจมตีทางไซเบอร์และสามารถดำเนินการพัฒนาอาวุธสำหรับการโจมตีทางไซเบอร์ที่ใช้ในแต่ละภารกิจได้

ความเสี่ยงที่ควรนำมาพิจารณา

- การพัฒนาอาจใช้เวลานานเกินกว่าที่คาดการณ์
- เทคโนโลยีการป้องกันทางไซเบอร์พัฒนาขึ้นอย่างรวดเร็ว ทำให้การพัฒนาอาวุธยากมากขึ้น

- **เพื่อการศึกษา** –

ผนวก ค ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

ผลการทดสอบข้อไขกับเกณฑ์การพิจารณา

ผลการทดสอบข้อไขกับเกณฑ์การพิจารณาหลัก

ข้อไข / เกณฑ์การพิจารณาหลัก	ข้อไขที่ ๑	ข้อไขที่ ๒	ข้อไขที่ ๓
๑. ต้องได้มาซึ่งขีดความสามารถการโจมตีทางไซเบอร์	/	/	/
๒. ต้องสนับสนุนการปฏิบัติการทางอากาศ	/	/	/
๓. ต้องมีอาวุธสำหรับสนับสนุนการโจมตีทางไซเบอร์	/	/	/
๔. ต้องมีผู้มีความเชี่ยวชาญสำหรับดำเนินการโจมตีทางไซเบอร์	/	/	/

ผลการทดสอบข้อไขกับเกณฑ์การพิจารณารอง

ข้อไข / เกณฑ์การพิจารณารอง	ข้อไขที่ ๑	ข้อไขที่ ๒	ข้อไขที่ ๓
๑. ควรเป็นการดำเนินการที่มีชั้นความลับ	X	/	/
๒. ควรเป็นการส่งเสริมการพัฒนาแบบยั่งยืน	X	/	/
๓. ควรมีความอิสระในการปฏิบัติงาน	X	/	/
๔. ควรมีความเหมาะสมระหว่างระยะเวลาดำเนินการและงบประมาณที่ใช้	X	/	X

- **เพื่อการศึกษา** –

ผนวก ง ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

<u>คำอธิบายข้อพิจารณาเพิ่มเติมประกอบการเลือกข้อไขที่ ๒</u>

๑. สร้างผลลัพธ์ที่จับต้องได้อย่างรวดเร็ว

โดยข้อไขที่ ๒ ช่วยให้หน่วยงานสามารถรับประโยชน์จากอาวุธไซเบอร์ที่มีอยู่ในตลาดหรือจากแหล่งที่เชื่อถือได้ในระยะสั้น ขณะที่มีการพัฒนาบุคลากรไปพร้อมกัน การเลือกใช้วิธีนี้ทำให้สามารถเริ่มต้นปฏิบัติการได้อย่างรวดเร็วและลดระยะเวลาการพัฒนาเทคโนโลยีตั้งแต่ต้นซึ่งต้องใช้ระยะเวลาหลายปี

๒. ความสมดุลระหว่างการจัดหาและพัฒนาบุคลากร

โดยข้อไขที่ ๒ เน้นการสร้างสมดุลระหว่างการจัดหาเทคโนโลยีที่ทันสมัยจากแหล่งภายนอกและการพัฒนาบุคลากรภายในหน่วย การมีบุคลากรที่ได้รับการฝึกอบรมพร้อมใช้งานอาวุธไซเบอร์ได้อย่างมีประสิทธิภาพ ในด้านการจัดหาอาวุธ ช่วยให้เกิดความพร้อมในเชิงเทคนิคและสามารถตอบสนองต่อภัยคุกคามในระยะสั้น รวมทั้งการพัฒนาบุคลากรเป็นการสร้างฐานความรู้และทักษะในระยะยาว ทำให้สามารถปรับปรุงและพัฒนาอาวุธไซเบอร์ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี

๓. ลดความเสี่ยงและข้อจำกัดในระยะเริ่มต้น

โดยข้อไขที่ ๒ เป็นแนวทางที่ช่วยลดความเสี่ยงที่เกี่ยวข้องกับการจัดหาและพัฒนาบุคลากรไปพร้อมกัน ซึ่งแตกต่างจากข้อไขที่ ๑ ที่พึ่งพาการจัดหาเพียงอย่างเดียวและข้อไขที่ ๓ ที่เน้นการพัฒนาอาวุธไซเบอร์เองทั้งหมด ซึ่งอาจใช้เวลาและงบประมาณมากเกินไป

๔. รองรับการปฏิบัติการทางอากาศในปัจจุบัน

๔.๑ การสนับสนุนการปฏิบัติการทางอากาศต้องการความพร้อมในการตอบโต้ภัยคุกคามทันที เช่น การโจมตีระบบควบคุมการป้องกันของฝ่ายตรงข้ามหรือการแทรกแซงเครือข่ายที่เกี่ยวข้อง

๔.๒ การมีอาวุธไซเบอร์ที่จัดหามาใช้งานร่วมกับบุคลากรที่ได้รับการฝึกอบรมอย่างต่อเนื่อง ช่วยให้สามารถสนับสนุนปฏิบัติการทางอากาศในสถานการณ์จริงได้อย่างมีประสิทธิภาพ

๔.๓ อาวุธไซเบอร์ที่ถูกพัฒนาร่วมกับกลยุทธ์ทางอากาศจะตอบโจทย์ทั้งในแง่ของการโจมตีและการป้องกัน ซึ่งข้อไขที่ ๒ สามารถประสานกันได้

๕. สนับสนุนการปฏิบัติการทางอากาศอย่างมีประสิทธิภาพ

๕.๑ การโจมตีทางไซเบอร์ที่ทันสมัยสามารถแทรกแซงระบบป้องกันภัยทางอากาศของศัตรู เช่น เรดาร์และระบบสื่อสาร ช่วยเพิ่มประสิทธิภาพให้กับปฏิบัติการโจมตีทางอากาศ ลดความเสี่ยงในการปฏิบัติการของเครื่องบินรบและเพิ่มโอกาสความสำเร็จในภารกิจ

๕.๒ การโจมตีทางไซเบอร์มีบทบาทสำคัญในการสนับสนุนปฏิบัติการทางอากาศ เช่น การทำลายหรือรบกวนระบบการควบคุมของศัตรู ซึ่งเป็นการช่วยเพิ่มความได้เปรียบเชิงยุทธศาสตร์

๕.๓ เพิ่มขีดความ...

- เพื่อการศึกษา –

๕.๓ เพิ่มขีดความสามารถในการปฏิบัติการทางอากาศให้มีประสิทธิภาพมากยิ่งขึ้นข้อไขที่ ๒ เป็นตัวช่วยหลักในการสนับสนุนยุทธศาสตร์ทางอากาศได้อย่างมีประสิทธิภาพ

๖. สร้างความร่วมมือระดับนานาชาติ

โดยข้อไขที่ ๒ เน้นการจัดหา พร้อมทั้งหาความร่วมกับพันธมิตรและภาคเอกชน การแลกเปลี่ยนความรู้และเทคโนโลยีกับนานาชาติสามารถช่วยเพิ่มประสิทธิภาพการฝึกอบรมและพัฒนาบุคลากร รวมทั้งการมีความร่วมมือระดับนานาชาติสามารถสร้างเครือข่ายการแลกเปลี่ยนข้อมูลข่าวสารในด้านไซเบอร์ ซึ่งเป็นประโยชน์ต่อการพัฒนาระบบป้องกันและโจมตี

๗. คุ้มค่าและเหมาะสมกับทรัพยากร

โดยข้อไขที่ ๒ จะมีการใช้งบประมาณอย่างมีประสิทธิภาพ โดยลดการใช้จ่ายที่ไม่จำเป็นและมุ่งเน้นไปที่การจัดหาเทคโนโลยีที่จำเป็นและการฝึกอบรมบุคลากร ขณะที่ข้อไขที่ ๓ ต้องใช้ทรัพยากรจำนวนมากสำหรับการพัฒนาอาวุธไซเบอร์ภายในประเทศ รวมทั้งเป็นการผสมผสานระหว่างการจัดหาและการพัฒนาบุคลากร ซึ่งช่วยให้เกิดความคุ้มค่าในระยะสั้นและระยะยาว สามารถใช้งบประมาณที่มีได้อย่างมีประสิทธิภาพ โดยไม่ต้องพึ่งพาการพัฒนาทั้งหมดภายในองค์กร ซึ่งอาจต้องใช้เวลานานและมีความเสี่ยงสูงกว่า

๘. วางรากฐานสำหรับอนาคตและความยั่งยืน

โดยข้อไขที่ ๒ ไม่เพียงแต่มุ่งหวังผลลัพธ์ในระยะเริ่มต้น แต่ยังให้ความสำคัญกับการพัฒนาศักยภาพของบุคลากรเพื่อให้สามารถพัฒนาอาวุธไซเบอร์ได้เองในอนาคต ลดการพึ่งพาจากภายนอก อีกทั้งยังมีการฝึกอบรมและเสริมสร้างความเชี่ยวชาญของบุคลากรภายในองค์กรซึ่งเป็นการวางรากฐานให้กับการพัฒนาความสามารถที่ยั่งยืนในระยะยาว ยังผลให้เกิดความยั่งยืนในขีดความสามารถด้านการปฏิบัติการไซเบอร์

๙. ระยะเวลา

โดยข้อไขที่ ๒ สามารถดำเนินการภายในระยะเวลาที่เหมาะสม โดยสามารถเริ่มใช้งานอาวุธที่จัดหามาในทันที ทั้งยังดำเนินการพัฒนาบุคลากรไปพร้อมกัน ต่างจากข้อไขที่ ๓ ที่ต้องใช้เวลาหลายปีในการจะสามารถพัฒนาเทคโนโลยีทางไซเบอร์ได้ การจัดหาจากภายนอกช่วยให้ได้อาวุธที่พร้อมปฏิบัติงานได้ในระยะเวลาอันสั้น ทั้งยังเกิดการพัฒนาบุคลากรในเวลาเดียวกัน แม้จะต้องใช้เวลาสักระยะ แต่ก็เป็นการเตรียมความพร้อมให้กับองค์กรในระยะกลางถึงระยะยาว ซึ่งสามารถเติมเต็มศักยภาพขีดความสามารถในอนาคต

๑๐. การใช้งบประมาณ

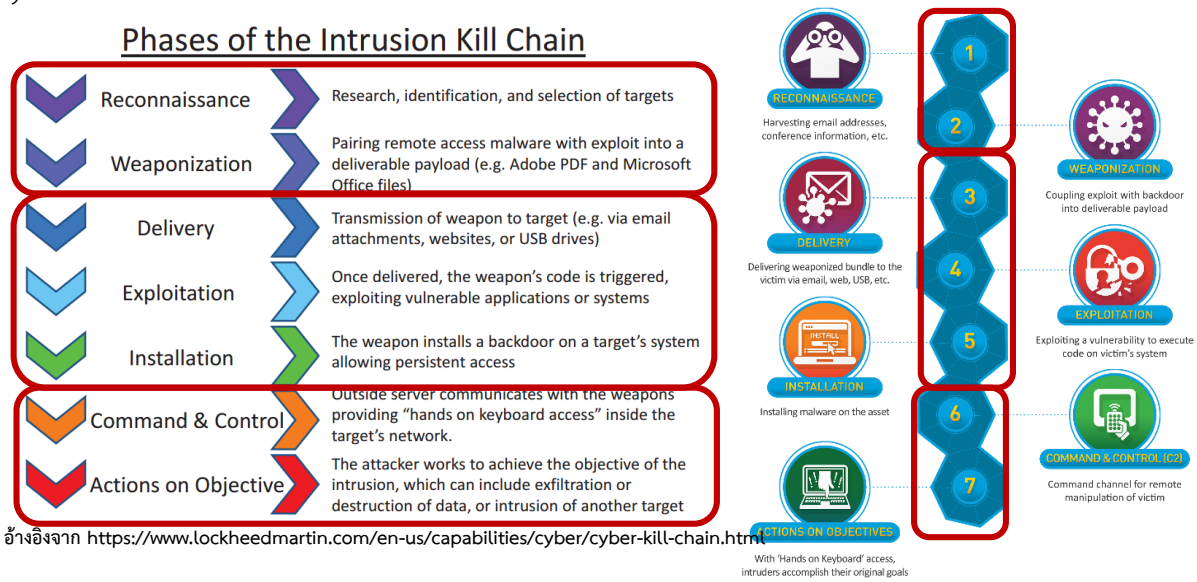
โดยข้อไขที่ ๒ เป็นแนวทางที่ใช้งบประมาณได้อย่างมีประสิทธิภาพ โดยลดค่าใช้จ่ายในการพัฒนาเทคโนโลยีตั้งแต่ต้น ทั้งยังเพิ่มขีดความสามารถทางไซเบอร์ได้อย่างมีนัยสำคัญ การบริหารงบประมาณทำให้สามารถดำเนินการตามแผนโดยไม่ต้องใช้งบประมาณที่มากเกินไป ทำให้มีความเหมาะสม ในการใช้งบประมาณทั้งในส่วนของการจัดหาและการฝึกอบรมให้เกิดความคุ้มค่า ซึ่งช่วยลดค่าใช้จ่ายในระยะยาว เมื่อลงทุนในบุคลากร เนื่องจากสามารถพัฒนาระบบและอาวุธได้เองในอนาคต ในระยะยาวเป็นลดการพึ่งพาการจัดหาในแต่ละครั้ง

- เพื่อการศึกษา –

ผนวก จ ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

<u>ขั้นตอนการโจมตีทางไซเบอร์ หรือการบวนการโจมตีทางไซเบอร์</u>

Cyber Kill Chain



อ้างอิงจาก https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

เฟสที่ ๑ เตรียมการโจมตี

ขั้นตอนที่ ๑ การลาดตระเวน คือ การเก็บรวบรวมข้อมูลของเป้าหมายก่อนเริ่มการโจมตี

ขั้นตอนที่ ๒ เตรียมอาวุธสำหรับโจมตี โดยผู้โจมตีเตรียมหาวิธีเจาะระบบและเตรียม Malicious Payload เพื่อส่งไปยังเหยื่อที่ต้องการ

เฟสที่ ๒ บุกรุกโจมตี

ขั้นตอนที่ ๓ ผู้โจมตีส่ง Malicious Payload ไปยังเป้าหมายผ่านช่องทางต่างๆ เพื่อใช้เจาะเข้าระบบของเหยื่อ

ขั้นตอนที่ ๔ ผู้โจมตีทำการเจาะระบบของเป้าหมายด้วยวิธีต่างๆ ตาม Payload ที่ส่งมา

ขั้นตอนที่ ๕ ผู้โจมตีทำการติดตั้งมัลแวร์บนเครื่องคอมพิวเตอร์ของเป้าหมายเพื่อให้คอยรับคำสั่งและกระทำตามที่ผู้โจมตีต้องการ

เฟสที่ ๓ เก็บเกี่ยวผลลัพธ์

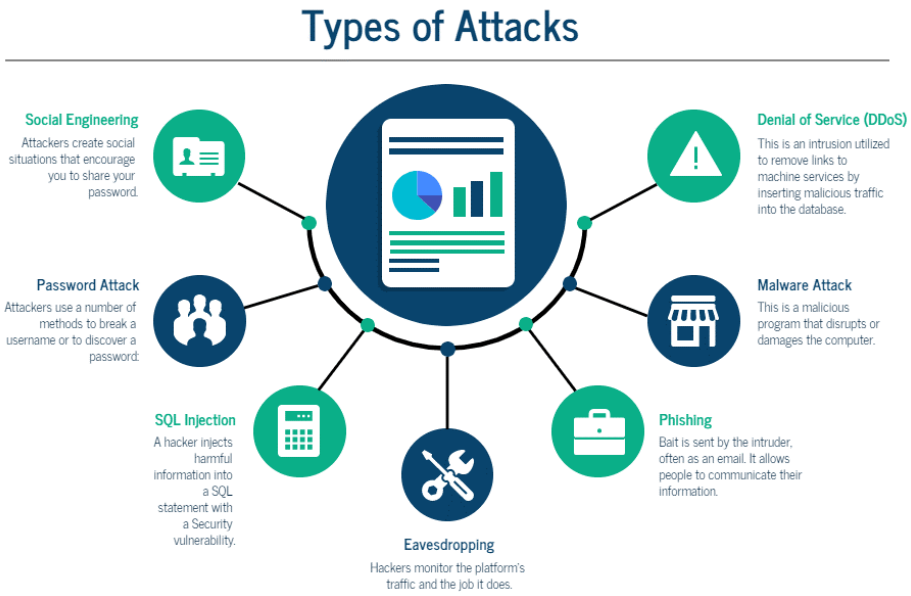
ขั้นตอนที่ ๖ ผู้โจมตีสร้างช่องทางในการรับส่งคำสั่งกับมัลแวร์ที่ติดตั้งไว้นั้น เพื่อให้สามารถจัดการและควบคุมมัลแวร์ให้ทำตามความต้องการ

ขั้นตอนที่ ๗ เก็บเกี่ยวผลประโยชน์ตามที่ตนเองต้องการจากระบบเครือข่ายของเป้าหมาย เช่น ขโมยข้อมูล เปลี่ยนแปลงแก้ไขข้อมูล หรือทำลายระบบ เป็นต้น

- เพื่อการศึกษา –

ผนวก ฉ ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

<u>ประเภทของการโจมตีทางไซเบอร์</u>



ประเภทของการโจมตีทางไซเบอร์

๑. Social Engineering คือ เทคนิคที่ใช้ในการหลอกลวงบุคคลให้เปิดเผยข้อมูลที่เป็นความลับ

๒. Password Attack คือ การโจมตีที่มุ่งเน้นไปที่การขโมยหรือคาดเดารหัสผ่านของผู้ใช้

๓. SQL Injection คือ เทคนิคการโจมตีที่ใช้ในการแทรกคำสั่ง SQL ในฐานข้อมูลของเว็บไซต์หรือแอปพลิเคชัน

๔. Eavesdropping คือ ฟังหรือดักข้อมูลที่กำลังส่งผ่านช่องทางการ การส่งข้อความหรือการสื่อสารทางอินเทอร์เน็ต

๕. Phishing คือ การพยายามหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลส่วนตัวที่สำคัญ ใช้เทคนิคหลอกลวงผ่าน อีเมล, ข้อความ, หรือเว็บไซต์ปลอม

๖. Malware Attack คือ การโจมตีที่ใช้ซอฟต์แวร์เพื่อลงมือทำลาย, ขโมยข้อมูล, หรือทำลายระบบคอมพิวเตอร์ของเป้าหมาย

๗. Denial of Service (DDoS) คือการโจมตีที่มีเป้าหมายเพื่อทำให้ระบบเซิร์ฟเวอร์ หรือเครือข่ายไม่สามารถให้บริการได้ตามปกติ

- เพื่อการศึกษา –

ผนวก ช ประกอบรายงานผลการดำเนินการ เรื่อง รายงานผลการดำเนินการเรื่องแนวทางพัฒนาขีดความสามารถด้านการโจมตีทางไซเบอร์ (Offensive Cyber) เพื่อสนับสนุนการปฏิบัติการทางอากาศต่อคณะกรรมการบริหาร ทอ. (สมมติเพื่อการศึกษา)

<u>กรณีศึกษาการใช้การโจมตีทางไซเบอร์ (Offensive Cyber) ในปฏิบัติการทางทหาร สหพันธรัฐรัสเซีย - ยูเครน</u>

การโจมตีทางไซเบอร์ได้กลายเป็นเครื่องมือสำคัญในกลยุทธ์ทางทหารและการเมือง หนึ่งในตัวอย่างที่โดดเด่น คือ การโจมตีทางไซเบอร์ของรัสเซียต่อยูเครน ซึ่งสะท้อนให้เห็นถึงความซับซ้อนและความรุนแรงของการใช้งานไซเบอร์ในการบ่อนทำลายความมั่นคงของชาติ โดยการโจมตีเหล่านี้ มุ่งเป้าไปยังโครงสร้างพื้นฐานสำคัญ เช่น ระบบพลังงาน การสื่อสารโทรคมนาคม และโครงข่ายโลจิสติกส์ ซึ่งส่งผลกระทบต่อความมั่นคงและความสามารถในการป้องกันประเทศอย่างมีนัยสำคัญ

Source: https://github.com/curated-intel/Ukraine-Cyber-Operations

ก่อนรัสเซียรุกราน รัฐบาลยูเครนระบุว่า หลายกระทรวงและสถาบันการเงินหลายแห่งของยูเครน ไม่สามารถเข้าเว็บไซต์และระบบคอมพิวเตอร์ได้หลังถูกโจมตีทางไซเบอร์ครั้งใหญ่ ด้วยวิธี Distributed Denial of Service (DDoS) เพื่อสกัดกั้นไม่ให้ระบบสามารถทำงานได้ปกติ

นอกจากนี้ รัสเซียโจมตีระบบสื่อสารดาวเทียม Viasat ด้วยมัลแวร์ AcidRain ทำให้ระบบการสื่อสารของยูเครนหยุดชะงักในช่วงต้นของการรุกราน ซึ่งกระทบต่อการติดต่อสื่อสารในพื้นที่การสู้รบในยูเครน หลังจากนั้น รัสเซียจึงใช้การโจมตีทางอากาศต่อยูเครนและเข้ายึดครองพื้นที่ต่างๆ ของยูเครนตั้งแต่ ๒๔ ก.พ.๖๕ และรัสเซียดำเนินการเจาะระบบกล้องวงจรปิดตามสถานที่ต่างๆ ในยูเครน ซึ่งเป็นการหาข้อมูลเป้าหมาย ระบบป้องกันภัยทางอากาศและโครงสร้างพื้นฐานที่สำคัญ เพื่อช่วยในการโจมตีต่อเป้าหมายด้วยขีปนาวุธ

ตัวอย่างการปฏิบัติการร่วมระหว่างการโจมตีทางไซเบอร์และการปฏิบัติการทางทหาร โดยจะเห็นได้ว่าการโจมตีทางไซเบอร์ ถูกใช้ก่อนการโจมตีทางทหารเสมอ เพื่อสร้างความวุ่นวาย ลดทอนขีดความสามารถ ทำให้ระบบป้องกันหรือระบบอำนวยความสะดวกต่างๆ เกิดความขัดข้องหรือสูญเสียประสิทธิภาพโดยสมบูรณ์