# วิเคราะห์ข้อมูลสงครามไซเบอร์ (CW)

เรียบเรียงโดย พันจ่าอากาศเอกหญิง อภิญญา โพยประโคน
เจ้าหน้าที่สงครามไซเบอร์ กองพัฒนายุทธวิธีและหลักนิยม ศูนย์การสงครามทางอากาศ


ภัยคุกคามในโดเมนที่ "มองไม่เห็นแต่ทำลายล้างได้จริง" นั่นคือ มิติไซเบอร์ (Cyber Domain)

## 1. สภาวะแวดล้อมภัยคุกคามทางไซเบอร์ (Cyber Threat Landscape)

ปัจจุบันภัยคุกคามไซเบอร์ต่อกองกำลังทางอากาศไม่ได้จำกัดอยู่แค่การเจาะระบบสำนักงาน แต่พุ่งเป้าไปที่ **ระบบอาวุธ (Weapon Systems)** และ **ระบบควบคุมบังคับบัญชา (C2)** โดยตรง:

**การโจมตีห่วงโซ่อุปทานดิจิทัล (Digital Supply Chain Attack)**

- **ภัยคุกคาม:** การฝังมัลแวร์หรือ "ประตูลับ" (Backdoor) ไว้ในซอฟต์แวร์ระบบการบิน หรือชิปประมวลผลตั้งแต่ขั้นตอนการผลิต (คล้ายกรณีเครื่องยนต์หรือระบบอิเล็กทรอนิกส์การบินที่ต้องพึ่งพาซัพพลายเออร์ภายนอก)
- **ผลกระทบ:** ข้าศึกสามารถสั่ง "Shut down" เครื่องบินหรือระบบป้องกันภัยทางอากาศได้จากระยะไกลในวินาทีที่เริ่มสงคราม

**การทำลายความน่าเชื่อถือของข้อมูล (Data Integrity Attack)**

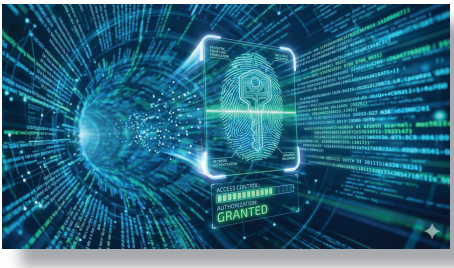
• **ภัยคุกคาม:** การเจาะเข้าสู่ระบบ Data Link เพื่อเปลี่ยนแปลงพิกัดเป้าหมาย หรือปลอมแปลงสัญลักษณ์ฝ่ายเดียวกัน/ฝ่ายศัตรู (Blue/Red Force Spoofing)

• **ผลกระทบ:** เกิดการยิงกันเอง (Fratricide) หรือทำให้นักบินตัดสินใจผิดพลาดเนื่องจากภาพสถานการณ์ในการรบ (Air Picture) ถูกบิดเบือน

**การโจมตีโครงสร้างพื้นฐานที่สนับสนุนกองทัพ (Critical Infrastructure Attack)**

• **ภัยคุกคาม:** การโจมตีระบบไฟฟ้า ประปา หรือเครือข่ายน้ำมันที่ส่งให้กับฐานทัพอากาศ ผ่านระบบควบคุมอุตสาหกรรม (ICS/SCADA)

• **ผลกระทบ:** แม้เครื่องบินจะพร้อมรบ แต่อาจไม่สามารถเติมน้ำมันหรือระบายความร้อนให้ระบบเซ็นเซอร์ในอาคาร TSC ได้ ทำให้ปฏิบัติการหยุดชะงัก




## 2. แนวคิดยุทธวิธีการใช้กำลังทางอากาศเพื่อต่อต้านสงครามไซเบอร์ (RTAF Cyber-Air Tactics)

เพื่อให้กองทัพอากาศสามารถปฏิบัติภารกิจได้แม้ภายใต้การโจมตีทางไซเบอร์ ดิฉันขอเสนอแนวคิดยุทธวิธี ดังนี้:

**ยุทธวิธีที่ 1: การตั้งรับแบบ "Zero Trust" ในระบบเครือข่ายการรบ**

• **แนวคิด:** เลิกใช้หลักการ "กำแพงกั้น" แต่ใช้การตรวจสอบสิทธิ์ทุกขั้นตอน ไม่ว่าจะเป็นข้อมูลที่ส่งมาจากเครื่องบิน F-35, UAV หรือสถานีเรดาร์

• **การปฏิบัติ:** ระบบต้องตรวจสอบ Digital Signature ของทุกแพ็กเกจข้อมูลใน Link T เพื่อยืนยันว่าข้อมูลพิกัดเป้าหมายมาจากเซ็นเซอร์จริง ไม่ใช่การปลอมแปลง

**ยุทธวิธีที่ 2: ยุทธวิธีการรบแบบ "Isolated Mode" (Cyber Resilience)**

• **แนวคิด:** ฝึกให้นักบินและเจ้าหน้าที่ควบคุมอากาศยานสามารถทำการรบได้ในสภาวะที่เครือข่ายล่ม (Disconnected Operations)

• **การปฏิบัติ:** หากระบบคลาวด์หรือระบบบัญชาการส่วนกลางถูกโจมตี เครื่องบินแต่ละหมู่บินต้องมีขีดความสามารถในการประมวลผลและตัดสินใจเอง (Autonomous Edge Computing) โดยใช้ฐานข้อมูลสำรองภายในเครื่อง

**ยุทธวิธีที่ 3: การตอบโต้ไซเบอร์เชิงรุกเพื่อการป้องกัน (Active Cyber Defense - ACD)**

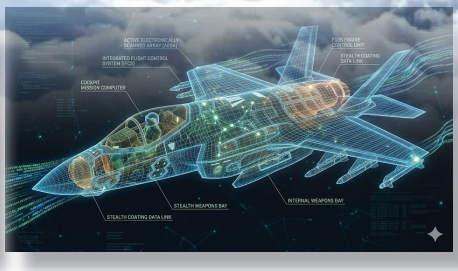
• **แนวคิด:** เมื่อตรวจพบความพยายามในการเจาะระบบควบคุมบังคับบัญชา ต้องมีหน่วยปฏิบัติการไซเบอร์ที่สามารถ "สวนกลับ" เพื่อทำลายแหล่งที่มาของมัลแวร์นั้นทันที

• **การปฏิบัติ:** บูรณาการยุทธการไซเบอร์เข้ากับแผนการบิน (Air Tasking Order) หากข้าศึกใช้การโจมตีไซเบอร์รบกวนเรดาร์เรา เราอาจตอบโต้ด้วยการส่ง UAV เข้าไปปล่อยมัลแวร์รบกวนระบบเครือข่ายเซ็นเซอร์ของข้าศึกเช่นกัน

**ยุทธวิธีที่ 4: การกู้คืนระบบแบบฉับพลัน (Rapid System Recovery)**

• **แนวคิด:** เตรียมซอฟต์แวร์ระบบการบินและข้อมูลทางยุทธวิธีฉบับ Clean Version ไว้ในสื่อบันทึกข้อมูลที่ตัดขาดจากอินเทอร์เน็ต (Air-gapped)

• **การปฏิบัติ:** หากระบบอาวุธถูกมัลแวร์โจมตีจนใช้งานไม่ได้ เจ้าหน้าที่เทคนิคต้องสามารถ "Re-image" ระบบทั้งหมดให้กลับมาเป็นปกติได้ภายในเวลาไม่กี่นาทีที่หน้าลานจอด (Flight Line)

## 3. การบูรณาการร่วมกับโครงการ TSC (Cyber-Simulation Training)

เพื่อให้ยุทธวิธีข้างต้นใช้งานได้จริง เราควรบรรจุสถานการณ์โจมตีทางไซเบอร์ลงใน **Tactical Simulation Center (TSC)** ดังนี้:

**1. Cyber Injection:** จำลองสถานการณ์ให้ภาพเรดาร์ในห้องนักบินหายไป หรือเป้าหมายปลอมปรากฏขึ้นจากการโจมตีไซเบอร์ เพื่อฝึกไหวพริบนักบิน

**2. Red Team Operations:** ให้หน่วยไซเบอร์ของกองทัพสวมบทบาทเป็นข้าศึก พยายามเจาะระบบจำลองการฝึกเพื่อหาจุดอ่อนของสถาปัตยกรรมเครือข่ายเรา

*****บทสรุปสำหรับผู้บังคับบัญชา*****

"ในสงครามสมัยใหม่ กระสุนนัดแรกอาจไม่ได้ยิงจากปากลำกล้อง แต่เป็นโค้ดคำสั่งที่ถูกส่งผ่านโครงข่ายไซเบอร์ การป้องกันประเทศที่สมบูรณ์จึงต้องหลอมรวมเอา **โล่ไซเบอร์** เข้าเป็นเนื้อเดียวกับ **ดาบทางอากาศ** "

**********