Cyber Warfare Distilled

น.ท.กรกช วิไลลักษณ์ ร.น.

สารบัญ

1 ภัยคุกคามไซเบอร์ 5

1.1 กำลังอำนาจแห่งชาติ 5

1.2 ภัยคุกคามทางไซเบอร์ 6

1.3 ผลกระทบของภัยคุกคามทางไซเบอร์ 6

1.4 ประเภทของภัยคุกคาม 8

2 ลักษณะพื้นที่การรบและแนวทางการใช้กำลัง 11

2.1 สงครามทางบก 11

2.2 สงครามทางเรือ 13

2.3 สงครามทางอากาศ 13

2.4 สงครามไซเบอร์ 14

3 หลักนิยมสงครามไซเบอร์ 15

3.1 ปฏิบัติการไซเบอร์ 15

3.2 หลักการรักษาความมั่นคงปลอดภัย 17

3.2.1 เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย 17

3.2.2 สถานะของทรัพยากรสารสนเทศ 18

3.2.3 แนวทางการป้องกัน 18

4 เครื่องมือและเทคนิคที่เกี่ยวข้องกับปฏิบัติการไซเบอร์ 19

4.1 เครื่องมือเชิงรุก (Offensive Tools) 19

4.1.1 มัลแวร์ประเภทต่างๆ (Malware) 19

4.1.2 การเจาะระบบ (Exploitation) 20

4.1.3 EMP Weapons 21

4.2 เครื่องมือเชิงรับ (Defensive Tools) 21

4.2.1 การควบคุมการเข้าถึงทรัพยากร 21
4.2.2 การกำหนดสภาวะของทรัพยากร 23
4.2.3 กระบวนการเฝ้าตรวจความมั่นคงปลอดภัย 24

5 ขีดความสามารถด้านไซเบอร์ของ ทร. 27
5.1 การเตรียมทรัพยากรมนุษย์ 27
5.2 การกำหนดนโยบายและการปฏิบัติ 27
5.3 การประยุกต์ใช้เทคโนโลยี 28

บรรณานุกรม 28

บทที่ 1

ภัยคุกคามไซเบอร์

ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารส่งผลโดยตรงต่อแนวคิดเกี่ยวข้องกับการปฏิบัติการทางทหาร โดยเห็นได้จากการประยุกต์ใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและระบบเครือข่ายในการปฏิบัติภารกิจเพื่อความมั่นคงในหลากหลายมิติ เช่น ระบบควบคุมบังคับบัญชา ระบบค้นหา วิเคราะห์ และประเมินค่าเป้าหมาย ด้วยเหตุที่ว่าเทคโนโลยีสารสนเทศและการสื่อสารช่วยให้วงรอบการตัดสินใจของผู้บังคับบัญชารวดเร็วและตอบสนองต่อสถานการณ์ที่เปลี่ยนแปลงไปได้อย่างแม่นยำ จนกล่าวได้ว่าการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารได้อย่างเหมาะสมจะเพิ่มโอกาสที่หน่วยจะบรรลุภารกิจ

เครือข่ายอินเทอร์เน็ตซึ่งในระยะเริ่มแรกถูกพัฒนาขึ้นเพื่อตอบโจทย์เกี่ยวกับสงครามนิวเคลียร์ โดยถูกออกแบบให้มีความพร้อมใช้ มีความเข้ากันได้กับอุปกรณ์แตกต่างชนิด และสามารถทำงานได้แม้ว่าเครือข่ายส่วนหนึ่งจะถูกทำลายไปจากอาวุธนิวเคลียร์ โดยในระหว่างยุคแรกๆของการพัฒนาไม่ได้มีการพิจารณาปัจจัยเกี่ยวกับความมั่นคงปลอดภัย จนเมื่อเกิดการแพร่ระบาดของหนอนอินเทอร์เน็ต (worm) ใน ค.ศ.1980 จึงมีความตระหนักรู้ถึงความเสี่ยงด้านความมั่นคงปลอดภัยของเครือข่ายอินเทอร์เน็ตเป็นครั้งแรก และมีรายงานความมั่นคงปลอดภัยของเครือข่ายอินเทอร์เน็ตอย่างต่อเนื่องจนถึงปัจจุบัน

1.1 กำลังอำนาจแห่งชาติ

การประเมินกำลังอำนาจแห่งชาติสามารถกระทำได้หลากหลายไม่ว่าจะเป็น DIME – Diplomatic, Information, Military, Economy หรือ MIDLIFE – Military, Intelligence, Diplomatic, Law Enforcement, Information, Finance, Economic หรือ PMESII – Political, Military, Economic, Social, Informational, Infrastructure โดยเมื่อพิจารณาอย่างถี่ถ้วนจะพบว่าองค์ประกอบของกำลังอำนาจแห่งชาติที่ได้ยกตัวอย่างมีความเหลื่อมทับระหว่างกันโดยเฉพาะอย่างยิ่งข้อมูลข่าวสารซึ่งปรากฏอยู่ในทุกๆแนวคิด เนื่องจากข้อมูลข่าวสารเป็นปัจจัยอันดับต้นๆที่ต้องคำนึงถึงในการทำสงครามทุกๆสมรภูมิ ประกอบกับความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารที่มีความก้าวหน้าแบบก้าวกระโดดในช่วง 2-3 ทศวรรษที่ผ่านมาจึงทำให้การสร้าง ประมวลผล และแพร่กระจายข้อมูล

ข่าวสารกระทำได้อย่างรวดเร็ว ในที่นี้ผู้เขียนจะใช้ DIME ในการเปรียบเทียบและวิเคราะห์เนื่องจาก DIME ยังคงถูกใช้งานอย่างแพร่หลายในหลักนิยมของกองทัพสหรัฐซึ่งเป็นหลักนิยมหลักที่กองทัพไทยนำมาประยุกต์ใช้

1.2 ภัยคุกคามทางไซเบอร์

การโจมตีต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารถูกรายงานเป็นครั้งแรกในช่วงทศวรรษที่ 1990 โดยมีเหตุการณ์สำคัญๆ เช่น ในปี 1999 กระทรวงกลาโหมสหรัฐอเมริการายงานการถูกโจมตีจากระบบเครือข่ายที่มีต้นทางจากสหภาพโซเวียตและส่งผลให้ข้อมูลสำคัญเกี่ยวกับเทคโนโลยีทางทหารถูกโจรกรรม และเชื่อกันว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยทางเครือข่ายที่มีรัฐเป็นตัวแสดงครั้งแรก อย่างไรก็ตามสหภาพโซเวียตปฏิเสธความรับผิดชอบโดยสิ้นเชิงต่อเหตุการณ์ดังกล่าว โดยเหตุการณ์ในครั้งนั้นได้รับชื่อว่า “Moonlight Maze” ต่อมาในปี 2007 กลุ่มแฮกเกอร์ที่เชื่อกันว่าได้รับการสนับสนุนจากรัฐบาลรัสเซียทำการโจมตีต่อเว็บไซต์ของหน่วยงานราชการเอสโตเนียจน รัฐบาลเอสโตเนียต้องขอรับการสนับสนุนทรัพยากรจากประเทศในกลุ่ม NATO เข้ามาช่วยแก้ปัญหาและฟื้นคืนระบบและปรากฏรายงานเหตุการณ์ความมั่นคงปลอดภัยเกิดขึ้นอย่างต่อเนื่องจนถึงปัจจุบัน

ในปัจจุบันหน่วยงานในรัฐบาลสหรัฐอเมริกานิยมเรียกเหตุการณ์ด้านความมั่นคงปลอดภัยที่มี “รัฐ” เป็นตัวแสดงว่า “Advance Persistent Threat: APT” โดยผลกระทบที่เกิดขึ้นจะส่งผลต่อความมั่นคงปลอดภัยของโครงสร้างพื้นฐานข้อมูลข่าวสารของรัฐที่ถูกโจมตีโดยขอบเขตความมั่นคงปลอดภัยจะครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ ของทรัพยากรสารสนเทศและการสื่อสารซึ่งเป็นองค์ประกอบหนึ่งของกำลังอำนาจแห่งชาติ (DIME)

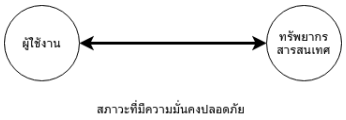
ภัยคุกคาม (Threats) หมายถึง บุคคล เหตุการณ์ ใดๆก็ตามที่เป็นสาเหตุของการลดทอดความมั่นคงปลอดภัยของทรัพยากรสารสนเทศซึ่งประกอบด้วยโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร ตลอดจนข้อมูลข่าวสารที่รับ-ส่งผ่านช่องทางการสื่อสาร โดยภัยคุกคามดังกล่าวรวมไปถึงเหตุการณ์ที่เกิดขึ้นโดยภัยธรรมชาติและอุบัติเหตุ โดยบุคคลที่ทำการโจมตีนิยมเรียกกว่า “ผู้ไม่ประสงค์ดี” “ผู้บุกรุก” หรือ “แฮกเกอร์” เมื่อพิจารณาถึงแหล่งที่มาของการโจมตีจะสามารถจำแนกแหล่งที่มาได้ 2 ลักษณะ ได้แก่

- **ผู้บุกรุกจากภายนอก** หมายถึง ผู้บุกรุกที่ทำการโจมตีต่อทรัพยากรสารสนเทศจากภายนอกองค์กร
- **ผู้บุกรุกจากภายใน** หมายถึง ผู้บุกรุกที่ทำการโจมตีต่อทรัพยากรสารสนเทศจากภายในองค์กร

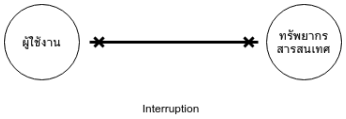
ทั้งนี้ผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารที่แตกต่างกันออกไปเช่น ความเชื่อพื้นฐานทางศาสนา ลัทธิการเมือง แรงจูงใจทางการเงิน ชื่อเสียง ความอยากรู้อยากเห็น ฯลฯ

1.3 ผลกระทบของภัยคุกคามทางไซเบอร์

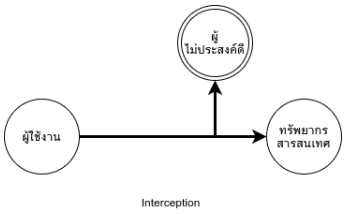
ผลกระทบของการโจมตี การเข้าถึงและใช้ประโยชน์จากทรัพยาการสารสนเทศและการสื่อสารของผู้ใช้งานหากเป็นไปอย่างมั่นคงปลอดภัยสามารถแสดงได้ดังภาพที่ 1.1 โดยจะเห็นว่าผู้ใช้งานจะสามารถเข้าใช้งานทรัพยากรสารสนเทศ



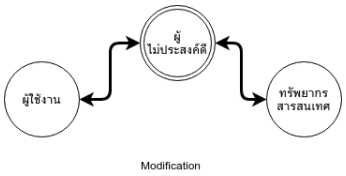
ภาพที่ 1.1: สภาวะที่มีความมั่นคงปลอดภัย



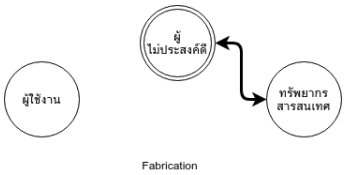
ภาพที่ 1.2: การสกัดขัดขวาง



ภาพที่ 1.3: การดักรับดักฟัง



ภาพที่ 1.4: การเปลี่ยนแปลงแก้ไข



ภาพที่ 1.5: การปลอมแปลง

ได้โดยไม่มีบุคคลอื่นเข้าถึงทรัพยากรที่ผู้ใช้งานเข้าถึงอยู่โดยไม่มีสิทธิ์ ทั้งนี้เมื่อจำแนกผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศไม่ว่าจะมีแหล่งกำเนิดจากภายในหรือภายนอกองค์กรจะสามารถจำแนกได้ 4 ประเภท ได้แก่

1. **การสกัดขัดขวาง (Interruption)** คือ การทำให้ทรัพยากรสารสนเทศไม่สามารถให้บริการได้ เช่น การเข้ารหัสไฟล์หรือฮาร์ดดิสก์โดยซอฟต์แวร์เรียกค่าไถ่ การโจมตีแบบกระจาย (Distributed Denial of Service: DDoS) การขโมยอุปกรณ์ ดังแสดงในภาพที่ 1.2 ยกตัวอย่างการขโมยอุปกรณ์ย่อมส่งผลให้ผู้ใช้งานไม่สามารถเข้าถึงทรัพยากรนั้นๆได้

2. **การดักรับดักฟัง (Interception)** คือ การเข้าถึงทรัพยากรสารสนเทศระหว่างที่กำลังถูกส่งผ่านระบบการสื่อสารหรือระบบเครือข่าย เช่น การใช้โปรแกรม sniffer ดักรับดักฟังเครือข่าย หรือการดักรับสัญญาณที่แพร่กระจาย การคุ้ยขยะเพื่อค้นหาข้อมูลสำหรับเข้าใช้งานระบบ ดังแสดงในภาพที่ 1.3 จะเห็นว่าทรัพยากรสารสนเทศเหล่านั้นจะถูกเข้าถึงได้จากผู้ไม่ประสงค์ดีซึ่งถ้าหากปราศจากมาตรการป้องกันที่เหมาะสมผู้ไม่ประสงค์ดีย่อมทำความเข้าใจและล่วงรู้ถึงข้อมูลที่รับ-ส่งนั้นๆได้

3. **การเปลี่ยนแปลงแก้ไข (Modification)** คือ การทำให้ทรัพยากรสารสนเทศและการสื่อสารถูกเปลี่ยนสภาพไปโดยไม่มีสิทธิ์ หรือไม่ได้รับอนุญาต ดังแสดงในภาพที่ 1.4 ในที่นี้จะยกตัวอย่าง การเปลี่ยนแปลงแก้ไขข้อมูลเงินเดือนในระบบงานเงินเดือน การแก้ไขหน้าเว็บโดยไม่ได้รับอนุญาต

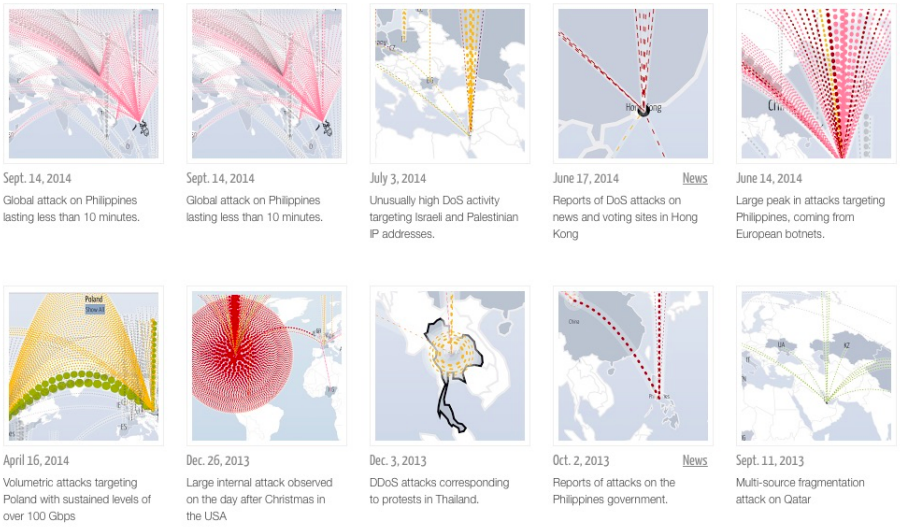
4. **การปลอมแปลง (Fabrication)** คือ การสร้างทรัพยากรสารสนเทศและการสื่อสารเข้าสู่โครงสร้างพื้นฐานหรือระบบ เช่นการปลอมข้อมูล หรือการปลอมแปลงตัวตน ดังแสดงในภาพที่ 1.5

เมื่อพิจารณาผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารดังที่ได้กล่าวมาจะมีความเชื่อมโยงกับหลักการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารซึ่งประกอบด้วย การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการรักษาความพร้อมใช้ (Availability) ของทรัพยากรสารสนเทศและการสื่อสารทั้งปวง โดยจะได้กล่าวถึงหลักการรักษาความมั่นคงปลอดภัยโดยละเอียดต่อไปในบทที่ 3

1.4 ประเภทของภัยคุกคาม

การจำแนกประเภทภัยคุกคาม เมื่อพิจารณาผลกระทบของภัยคุกคามที่ได้กล่าวมาแล้วจะพบว่าแนวทางการโจมตีต่อทรัพยากรสารสนเทศและการสื่อสารจะถูกแบ่งเป็น 2 ลักษณะคือ ภัยคุกคามแบบแอคทีฟ (active threats) และภัยคุกคามแบบพาสซีฟ (passive threats)

- **ภัยคุกคามแบบแอคทีฟ** หมายถึง การโจมตีที่ผู้ไม่ประสงค์ดีอาจถูกตรวจพบได้จากกระบวนการเฝ้าตรวจความมั่นคงปลอดภัย เช่นการทำให้ระบบปฏิเสธการให้บริการด้วยมัลแวร์จำพวกบอทเน็ต (DDoS via botnet) SQL Injection การโจมตีแบบคนกลาง (Man-In-The-Middle) เป็นต้น



ภาพที่ 1.6: ภัยคุกคามทางไซเบอร์ขนาดใหญ่

- **ภัยคุกคามแบบพาสซีฟ** หมายถึง การโจมตีที่ผู้ไม่ประสงค์ดีจะไม่ถูกตรวจพบจากกระบวนการการเฝ้าตรวจความมั่นคงปลอดภัย เช่นการดักรับดักฟัง (eavesdropping and sniffing) การสืบค้นข้อมูลจาก search engine การโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม (social engineering) เป็นต้น

ภัยคุกคามจำแนกจากแรงจูงใจ แรงจูงใจที่ทำให้ผู้ไม่ประสงค์ดีตัดสินใจโจมตีต่อโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารแตกต่างกันในแต่ละบุคคลและกลุ่มบุคคล และด้วยแรงจูงใจที่แตกต่างกันย่อมส่งผลต่อผลกระทบต่อพลังอำนาจแห่งชาติในระดับที่แตกต่างกันออกไปดังแสดงในภาพที่ 1.6 แสดงเหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารของประเทศต่างๆหลายประเทศ เมื่อรวบรวมหลักฐานจากเหตุการณ์ที่ผ่านๆมาจะสามารถจำแนกแรงจูงใจเหล่านั้นได้หลายประการดังนี้

- **Script Kiddy** หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ที่ชอบศึกษาทดลองซอฟต์แวร์สำหรับเจาะระบบแต่ไม่มีความสามารถในการพัฒนาซอฟต์แวร์จึงต้องใช้ซอฟต์แวร์ที่ถูกพัฒนาขึ้นมาจากแฮกเกอร์ที่มีความสามารถสูงโดยซอฟต์แวร์เหล่านั้นสามารถดาว์นโหลดได้จากแหล่งซอฟต์แวร์เปิดบนเครือข่ายอินเทอร์เน็ต โดยพบว่าเหตุการณ์ด้านความมั่นคงปลอดภัยส่วนใหญ่เป็นผลจากการโจมตีกลุ่มคนในกลุ่มนี้และพบว่าผลเสียหายที่เกิดขึ้นไม่มีนัยสำคัญอย่างไรต่อพลังอำนาจแห่งชาติ

- **Criminal** หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากแรงขับเคลื่อนขององค์กรอาชญากรรมที่มุ่งหาประโยชน์จากการโจมตีโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร จากสถิติพบกว่าปริมาณการโจมตีที่เกิดขึ้นจากกลุ่มนี้มีจำนวนมากรองลงมาจากการโจมตีของกลุ่มสคริปคิดดี้

- **Hacker Groups** หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินกิจกรรมของกลุ่มแฮกเกอร์ที่มี

ฝีมือโดยมักเป็นผู้พัฒนาเครื่องมือสำหรับใช้โจมตีต่อโครงสร้างพื้นฐานระบบสารสนเทศโดยพบว่าผลกระทบของภัยคุกคามจากกลุ่มนี้มีมากถึงร้อยละ 80 ของผลเสียหายทั้งหมด ลักษณะเฉพาะของภัยคุกคามจากกลุ่มนี้คือการกระทำเพื่อหวังผลประโยชน์ในรูปของตัวเงิน และเศรษฐกิจ

- **Insider** หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลการดำเนินการของกลุ่มคนภายในองค์กร ซึ่งเป็นจุดที่มักจะได้รับการปกป้องต่ำกว่าโครงสร้างพื้นฐานที่เชื่อมต่อกับเครือข่ายภายนอก โดยมีแรงจูงใจในการกระทำส่วนใหญ่เพื่อแก้แค้นองค์กร หรือได้รับการสนับสนุนทางการเงินจากองค์กรคู่แข่ง

- **Political/Religious** หมายถึง ภัยคุกคามทางไซเบอร์ที่เป็นผลของการดำเนินการจากบุคคลที่มีความเชื่อทางการเมืองตรงข้ามกระทำต่อกันเพื่อล้มล้างหรือสร้างสภาวะที่ฝ่ายตนต้องการ โดยมักไม่หวังผลความเสียหายต่อพลังอำนาจแห่งชาติ อย่างไรก็ดีเมื่อพิจารณาขอบเขตการใช้ความเชื่อทางศาสนาเป็นเครื่องมือจะพบว่าแนวโน้มการใช้โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารในการปลูกฝังและขยายจำนวนผู้ร่วมอุดมการณ์ของกลุ่มก่อการร้ายเพิ่มขึ้นอย่างมีนัยสำคัญ

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

สงครามไซเบอร์เป็นพื้นที่ยุทธภูมิใหม่ซึ่งเกิดขึ้นตามสภาพการเปลี่ยนแปลงทางยุทธศาสตร์ที่เป็นผลจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร อย่างไรก็ดีสิ่งที่ไม่เคยเปลี่ยนแปลงไปเลยคือการใช้กำลังอำนาจแห่งชาติเพื่อควบคุมพื้นที่สนามรบ (Battle Space) อันได้แก่ พื้นที่ทางบก พื้นที่ทางทะเล ห้วงอากาศ อวกาศ และไซเบอร์ ในบทต่อไปจะได้กล่าวถึงลักษณะเฉพาะและหลักนิยมของการปฏิบัติทางทหารในพื้นที่สนามรบแต่ละแบบ

บทที่ 2

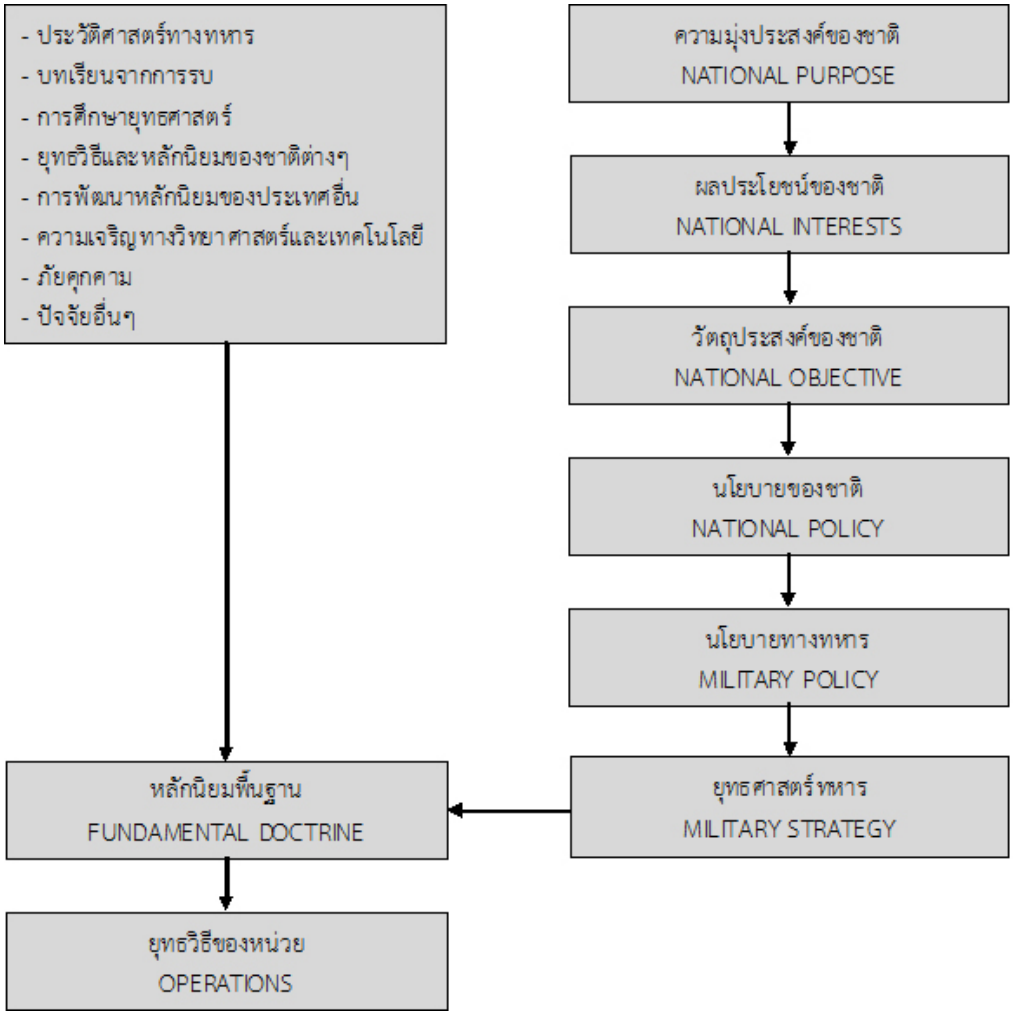
ลักษณะพื้นที่การรบและแนวทางการใช้กำลัง

หลักนิยมการใช้กำลังเป็นแนวคิดที่ใช้กำหนดทิศทางการใช้กำลังรบเพื่อสนับสนุนวัตถุประสงค์ของชาติ การพัฒนาหลักนิยมจึงต้องคำนึงถึงปัจจัยสำคัญหลายประการดังแสดงในภาพที่ 2.1 จะเห็นว่าปัจจัยสำคัญในการกำหนดหลักนิยมพื้นฐานของกำลังรบใดๆจะต้องสอดคล้องกับมุ่งประสงค์ของชาติ ผลประโยชน์ของชาติ ตลอดจนประวัติศาสตร์ทางทหาร บทเรียนจากการรบ หลักนิยมชาติอื่นๆ ฯลฯ

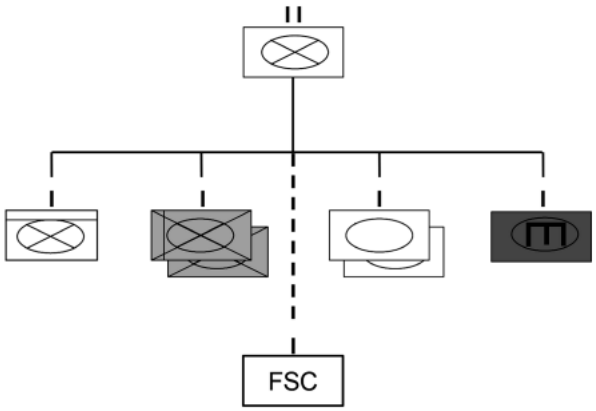
แม้ว่าจุดมุ่งหมายของการรบทางบก ทางทะเล และทางอากาศมีความคล้ายคลึงกันโดยมีความต้องการหลักๆ เพื่อ ยึดพื้นที่ (Command) การควบคุมพื้นที่ (Control) หรือการปฏิเสธการใช้ประโยชน์ของพื้นที่ๆนั้นๆจากฝ่ายตรงข้าม (Denial) โดยการก้าวเข้าสู่สภาวะสงครามในการรบทางบก ทางทะเล และทางอากาศมีความตรงไปตรงมาโดยมักเริ่มขึ้นเมื่อกำลังของแต่ละฝ่ายเคลื่อนเข้าหากัน เพื่อยึดครอง ควบคุม หรือปฏิเสธการใช้ประโยชน์เหนือพื้นที่นั้นๆจากฝ่ายตรงข้ามด้วยกองกำลังของตน บนหรือในยุทธบริเวณนั้นๆ แต่สงครามไซเบอร์คุณลักษณะแตกต่างจากพื้นที่การรบอื่นๆอย่างมีนัยสำคัญ

2.1 สงครามทางบก

สงครามทางบก การดำเนินกลยุทธบนพื้นที่ทางบกมีมาควบคู่กับการวิวัฒนาการของมนุษย์ โดยอาวุธ ยุทธวิธีและการดำเนินกลยุทธของการทำการรบทางบกได้รับการพัฒนามาอย่างต่อเนื่อง นับตั้งแต่การขว้างปาหิน พัฒนาเป็นหอก ธนู เครื่องยิง ระเบิด ปืน ปืนใหญ่ ปืนกล รถถัง และกล่าวได้ว่าการพัฒนาของอาวุธชนิดต่างๆส่งผลโดยตรงต่อหลักนิยม ยุทธวิธีและการจัดกำลังซึ่งจะต้องถูกพัฒนาให้เหมาะสมกับอาวุธในแต่ละแบบ โดยมีแนวคิดพื้นฐานในการแบ่งมอบการบังคับบัญชาให้หน่วยรองและควบคุมการปฏิบัติ (Chain of Command and Span of Control) สำหรับการรบในยุคปัจจุบันจะพบว่าการใช้กำลังเพื่อทำการรบทางบกจะมีลักษณะเป็นการจัดกำลังผสมเหล่าที่ผนึกกำลังรบที่มีอำนาจการยิง และสามารถดำเนินกลยุทธด้วยการจู่โจม รวดเร็ว รุนแรง สามารถเอาชนะกำลังรถถังและ



ภาพที่ 2.1: ปัจจัยกำหนดหลักนิยม



ภาพที่ 2.2: การจัดหน่วยระดับกองพันผสม

ยานเกราะ และมีส่วนยิงสนับสนุนจากอาวุธยิงสนับสนุน เช่นการจัดกองพันรบผสมเหล่าดังภาพที่ 2.2 แสดงการจัดกองพันผสมซึ่งประกอบด้วยกองร้อยรถถัง กองร้อยรถสายพาน กองร้อยรถสายพานลาดตระเวณ และทหารราบ เพื่อปฏิบัติการรบด้ยวิธีรุก รับ และร่นถอยได้อย่างอ่อนตัวและมีประสิทธิภาพ และเมื่อพิจารณาประวัติศาสตร์สงครามที่ผ่านๆมาจะเห็นว่าการยุทธในปัจจุบันต่างก็มีการใช้กองกำลังผสมเหล่าในการทำการรบ

2.2 สงครามทางเรือ

สงครามทางเรือ เมื่อพิจารณาพื้นที่ปฏิบัติการของการยุทธทางเรือจะพบว่าพื้นที่การยุทธมีอาณาเขตกว้างขวางซึ่งเกื้อกูลต่อการเคลื่อนกำลังโดยมีอุปสรรคเกี่ยวกับภูมิประเทศน้อยกว่าการยุทธทางบก มีความเร็วในการเคลื่อนกำลังมากกว่าการรบทางบกโดยในหนึ่งวันอาจเคลื่อนที่ได้หลายสิบไมล์ในขณะที่การรบทางบกอาจใช้ระยะเวลานานกว่าในการรุกคืบเข้าไปในภูมิประเทศ หลักนิยมการยุทธทางเรือก็ได้รับอิทธิพลจากความก้าวหน้าของเทคโนโลยีเช่นเดียวกัน โดยเห็นได้จากการเปลี่ยนหลักนิยม ยุทธวิธีของกำลังทางเรือเมื่อมีการพัฒนาเรือบรรทุกเครื่องบิน และกล่าวได้ว่าการยุทธทางเรือในปัจจุบันขึ้นอยู่กับ ยุทธศาสตร์ในการใช้กำลังรบทางเรือ ระบบอำนวยการรบ การควบคุมบังคับบัญชาอันเป็นผลจากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารของอุปกรณ์ตรวจจับและระบบอาวุธ โดยมักมีแนวคิดการจัดกำลังเข้าทำการรบแบบ Capability-Based

2.3 สงครามทางอากาศ

สงครามทางอากาศ การยุทธทางอากาศมีแนวคิดในการควบคุมเป็นสำคัญโดยจะต้องมีการจัดกำลังและการบังคับบัญชาตามคุณลักษณะของอาวุธ และมอบความรับผิดชอบทางยุทธการให้กับผู้บังคับบัญชาเพียงคนเดียวเพื่อสนธิกำลังทางอากาศทั้งปวงไว้ด้วยกันในลักษณะของ Centralized Control and Decentralized Execution เนื่องจากมูลค่าของกำลังรบสูงมากและมีจำนวนจำกัด การควบคุมบังคับบัญชาจึงต้องกระทำอย่างรัดกุม มีการจัดลำดับความ

สำคัญอย่างเหมาะสม เพื่อตอบสนองยุทธศาสตร์การใช้อากาศยานเพื่อ การครองอากาศ การควบคุมห้วงอากาศ ซึ่งมีความคล้ายคลึงกับแนวคิดการใช้กำลังทางเรือเนื่องจากมีสภาพทางกายภาพคล้ายคลึงกันคือการไม่สามารถระบุดขอบเขตพื้นที่ได้อย่างชัดเจนนั่นเอง

2.4 สงครามไซเบอร์

สงครามไซเบอร์ สงครามไซเบอร์มีความคล้ายคลึงกับสงครามทางเรือและสงครามทางอากาศเนื่องจากการไม่สามารถระบุขอบเขตทางกายภายได้อย่างแน่นอนและการเชื่อมต่อกันเสมือนไร้พรมแดนซึ่งในสงครามทางเรือและทางอากาศคู่ขัดแย้งสามารถเคลื่อนย้ายกำลังเข้าปะทะกันได้เมื่อเกิดความขัดแย้ง อย่างไรก็ดีขอบเขตของสงครามไซเบอร์ไม่ได้ถูกจำกัดที่ทรัพยากรทางทหารหรือทรัพยากรของรัฐคู่กรณีแต่เพียงอย่างเดียวเนื่องจากเป้าหมายที่อาจถูกโจมตีอาจเป็นโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสารอื่นๆที่อยู่นอกการควบคุมของหน่วยงานรัฐหรือกองทัพ นอกจากนี้ การระบุคู่ขัดแย้งอย่างชัดเจนในสงครามไซเบอร์ก็กระทำได้ยากลำบาก ยกตัวอย่างเช่นหน่วยงานของรัฐ ก. อาจถูกโจมตีและยึดครองจาก รัฐ ข. เพื่อใช้โจมตีต่อรัฐ ค. โดยที่รัฐ ก. ไม่มีเจตนาเข้าร่วมในความขัดแย้งของรัฐ ข. และ ค. อละในการทำสงครามไซเบอร์จะไม่พบเห็นการปะทะกันทางกายภาพระหว่างกองกำลังแต่ละฝ่าย

บทที่ 3

หลักนิยมสงครามไซเบอร์

3.1 ปฏิบัติการไซเบอร์

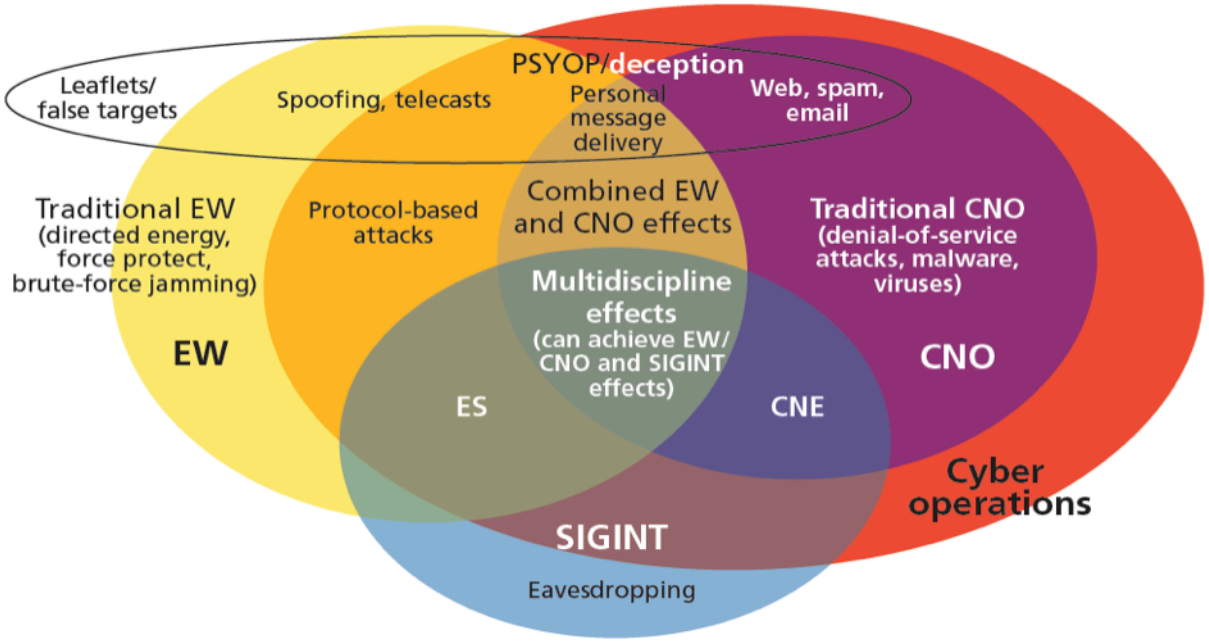
ในปัจจุบันสหรัฐอเมริกายังไม่มีการกำหนดหลักนิยมสงครามไซเบอร์อย่างเป็นทางการแต่มีการประยุกต์ใช้แนวทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารจนกล่าวได้ว่าแนวทางดังกล่าวเป็นปฏิบัติการเชิงรับ โดยหากกระทำสำเร็จจะมั่นใจได้ว่าทรัพยากรที่เกี่ยวข้องกับข้อมูลข่าวสารทั้งปวงถูกสร้าง รับ-ส่ง ผ่านโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสารอย่างมั่นคงปลอดภัย และสามารถบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ สำหรับการปฏิบัติเชิงรุก สหรัฐอเมริกากำหนดแนวทางการปฏิบัติเกี่ยวกับสงครามไซเบอร์เป็นส่วนหนึ่งของปฏิบัติการข้อมูลข่าวสาร (IO) ดังแสดงในภาพที่ 3.1 และเรียกปฏิบัติการที่เกี่ยวข้องกับสาขานี้ว่า “ปฏิบัติการด้านเครือข่ายคอมพิวเตอร์ (Computer Network Operation)” ครอบคลุมถึงปฏิบัติการสาขาย่อยๆ 3 สาขาได้แก่

- **การเจาะระบบเครือข่าย (Computer Network Exploitation)** หมายถึงกิจกรรมทั้งปวงที่หวังผลให้สามารถเข้าถึง และควบคุมทรัพยากรสารสนเทศของฝ่ายตรงข้ามได้ เช่นการเจาะระบบเครือข่าย การฝังโทรจัน การล่อลวงด้วยเทคนิคที่เกี่ยวข้องกับวิศวกรรมเชิงสังคม (Social Engineer)

- **การโจมตีระบบเครือข่าย (Computer Network Attack)** หมายถึงกิจกรรมทั้งปวงที่กระทำขึ้นเพื่อทำลายทรัพยากรสารสนเทศของฝ่ายตรงข้ามให้ไม่สามารถใช้งานได้

- **การป้องกันระบบเครือข่าย (Computer Network Defense)** หมายถึงกิจกรรมทั้งปวงที่กระทำขึ้นเพื่อไม่ให้ฝ่ายตรงข้ามเข้าใช้ประโยชน์ทรัพยาการสารสนเทศของฝ่ายเรา

เมื่อพิจารณาภาพที่ 3.1 จะเห็นว่าปฏิบัติการไซเบอร์ยังครอบคลุมถึงการดักรับดักฟังสัญญาณและคลื่นแม่เหล็กไฟฟ้า การปฏิบัติการจิตวิทยาและการลวง การปลอมแปลงสัญญาณ ตลอดจนการโจมตีต่อโพรโทคอลทางการสื่อสาร ดังนั้นหากต้องการป้องกันการโจมตีทางไซเบอร์จึงมีความจำเป็นอย่างยิ่งที่จะต้องจัดเสริมสร้างปัจจัยที่เกี่ยวข้องกับทรัพยากรสารสนเทศ 3 ปัจจัยหลัก ได้แก่

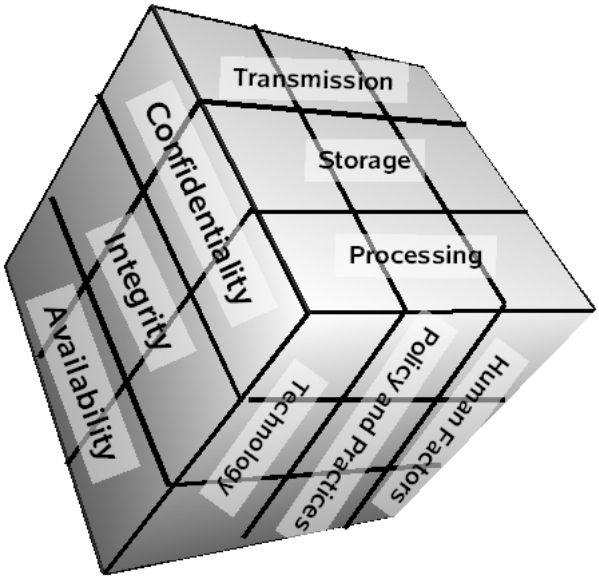


ภาพที่ 3.1: ภาพรวมการปฏิบัติการข้อมูลข่าวสาร

- **ทรัพยากรมนุษย์ (People)** ได้แก่ บุคลากรต่างๆที่เกี่ยวข้องกับการวางแผนและการปฏิบัติการทางทหาร โดยบุคลากรเหล่านี้จะต้องมี “ความตระหนักรู้” เกี่ยวกับความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานทรัพยากรสารสนเทศทั้งปวงนับตั้งแต่กระบวนการสร้างข้อมูลข่าวสาร การปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย การพัฒนาให้บุคลากรมีทักษะและความรู้ที่เกี่ยวข้องกับปฏิบัติการ ฯลฯ

- **กระบวนการบริหารจัดการข้อมูลข่าวสาร (Process)** ได้แก่การกำหนดระเบียบวิธีปฏิบัติ ระเบียบปฏิบัติประจำที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศและการสื่อสารอย่างมั่นคงปลอดภัย การเฝ้าตรวจความมั่นคงปลอดภัยของโครงสร้างพื้นฐานระบบสารสนเทศและการสื่อสาร การคัดเลือกและกำหนดสิทธิ์ในการเข้าถึงทรัพยากร ข้อกำหนดการเชื่อมต่อเครือข่าย ข้อกำหนดการพิสูจน์ตัวจริง ฯลฯ

- **เทคโนโลยีสารสนเทศและการสื่อสาร (Technology)** ได้แก่การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างมั่นคงปลอดภัย เช่นการประยุกต์ใช้งานวิทยาการรหัสลับที่มีความมั่นคงปลอดภัยสูงในการเข้ารหัสข้อมูลที่มีความลับก่อนการรับ-ส่งผ่านเครือข่าย การเข้ารหัสฮาร์ดดิสก์เพื่อป้องกันข้อมูลรั่วไหลหากเกิดการโจรกรรม เทคโนโลยีการประมวลผลข้อมูลขนาดมหึมาในการสร้าง Common Operational Picture ฯลฯ



ภาพที่ 3.2: แบบจำลองการรักษาความมั่นคงปลอดภัยของ J. McCumber

3.2 หลักการรักษาความมั่นคงปลอดภัย

ภาพที่ 3.2 แสดงแบบจำลองการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศของ J. McCumber ซึ่งแสดงองค์ประกอบที่จำเป็นในการรักษาความมั่นคงปลอดภัยใน 3 มิติคือ เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย (desired goals) สถานะของสารสนเทศ (information state) และ แนวทางป้องกัน (safe guards)

3.2.1 เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย

- **การรักษาความลับ (Confidentiality)** หมายถึง การจัดการให้ทรัพยากรนั้นถูกล่วงรู้และแปลความหมายได้จากผู้ที่มีสิทธิ์ เช่นพาสเวิร์ดสำหรับการเข้าระบบควรเป็นสิ่งที่รู้เฉพาะบุคคล ข้อมูลระดับชั้นลับมากจะต้องไม่ถูกล่วงรู้จากผู้ที่ได้รับสิทธิ์เข้าถึงข้อมูลระดับชั้น “ลับ” เป็นต้น

- **การรักษาความครบถ้วนสมบูรณ์ (Integrity)** หมายถึง การจัดการให้ทรัพยากรนั้นมีความครบถ้วนสมบูรณ์ มีกลไกตรวจสอบการถูกเปลี่ยนแปลงแก้ไข เช่นรายชื่อการแต่งตั้งดำรงตำแหน่งจะต้องไม่ถูกเปลี่ยนในขั้นตอนการนำเสนอผู้บังคับบัญชาจากผู้ไม่มีสิทธิ์โดยตรวจสอบไม่ได้ เป็นต้น

- **การรักษาความพร้อมใช้ (Availability)** หมายถึง การจัดการให้ทรัพยากรนั้นถูกเข้าถึงและใช้งานได้จากผู้มีสิทธิ์อยู่เสมอ เช่นระบบไฟฟ้าจะต้องพร้อมใช้งานไม่มีเหตุการณ์ไฟดับ ระบบบริการเว็บจะต้องพร้อมใช้งานในเวลาปฏิบัติราชการ เป็นต้น

3.2.2 สถานะของทรัพยากรสารสนเทศ

- **การจัดเก็บ (Storage)** หมายถึง ทรัพยากรสารสนเทศใดๆที่ถูกจัดเก็บในแหล่งจัดเก็บข้อมูลเช่นสภาวะที่สารสนเทศนั้นถูกจัดเก็บในหน่วยความจำ ฮาร์ดดิสก์ การจัดเก็บเอกสารที่มีชั้นความลับที่มีการตรวจสอบการเข้าถึงห้องและมีการตรวจสอบสิทธิ์ เป็นต้น

- **การประมวลผล (Processing)** หมายถึง ทรัพยากรสารสนเทศใดๆที่ถูกกำลังถูกประมวลผล ทั้งในกระบวนการนอกระบบสารสนเทศและการสื่อสาร เช่นการพิมพ์ผลการทำ IPB แล้วทิ้งถังขยะโดยไม่มีการทำลายข้อความ ฯลฯ

- **การรับส่ง (Transmission)** หมายถึง ทรัพยากรสารสนเทศใดๆที่กำลังถูกรับ-ส่งผ่านตัวกลางการสื่อสาร เช่น การส่งข้อมูลพิสูจน์ตัวจริงผ่านเครือข่าย เป็นต้น

3.2.3 แนวทางการป้องกัน

- **กระบวนการ (Process)** หมายถึง การกำหนดระเบียบ วิธีปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศต่างๆ

- **ทรัพยากรมนุษย์ (People)** หมายถึง บุคคลที่มีส่วนเกี่ยวข้องกับทรัพยากรสารสนเทศ นั้นๆ

- **เทคโนโลยี (Technology)** หมายถึง เทคโนโลยีที่เกี่ยวข้องและสามารถนำมาประยุกต์ใช้ในการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศ เช่นเทคโนโลยีการเข้ารหัสลับ เทคโนโลยีที่เกี่ยวข้องกับการพิสูจน์ตัวจริง เป็นต้น

จากแบบจำลองนี้เมื่อต้องการรักษาความมั่นคงปลอดภัยให้กับทรัพยากรใดๆผู้มีส่วนเกี่ยวข้องจะต้องพิจารณาเป้าหมายหลักของการรักษาความมั่นคงปลอดภัยร่วมกับมุมมองอื่นๆคือสถานะของสารสนเทศ และแนวทางป้องกัน ยกตัวอย่างเช่นพื้นผิวที่เป็นจุดตัดกันระหว่าง การรับส่งข้อมูล การรักษาความลับ และเทคโนโลยี แสดงให้เห็นถึงความจำเป็นที่จะต้องมีการเลือกใช้เทคโนโลยีที่เหมาะสมสำหรับการรักษาความลับของข้อมูลข่าวสารที่ถูกรับส่งระหว่างกันซึ่งเทคโนโลยีที่เกี่ยวข้องในกรณีนี้อาจเกี่ยวข้องกับการเข้ารหัสข้อมูลข่าวสารนั้นๆ กระบวนการพิสูจน์ตัวจริงของอุปกรณ์สื่อสารเพื่อให้มั่นใจได้ว่าการรับส่งข้อมูลนั้นจะไม่ถูกส่งต่อไปยังอุปกรณ์ที่ไม่ได้รับสิทธิ์ ทั้งนี้แบบจำลองนี้จะถูกใช้ในการพิจารณากำหนดนโยบายและข้อกำหนดที่เกี่ยวข้องกับการควบคุม การประยุกต์ใช้งานเทคโนโลยีต่างๆ เช่น วิทยาการรหัสลับ เทคโนโลยีโทรคมนาคม อย่างเหมาะสม

บทที่ 4

เครื่องมือและเทคนิคที่เกี่ยวข้องกับปฏิบัติการไซเบอร์

4.1 เครื่องมือเชิงรุก (Offensive Tools)

4.1.1 มัลแวร์ประเภทต่างๆ (Malware)

หมายถึงซอฟต์แวร์ที่มีชุดคำสั่งที่สามารถสำเนาตัวเองเข้าไปในระบบคอมพิวเตอร์แล้วสามารถแพร่กระจายไปสู่ระบบคอมพิวเตอร์อื่นๆผ่าน เครือข่ายคอมพิวเตอร์ ระบบจดหมายอิเล็กทรอนิกส์ หรืออุปกรณ์ต่อพ่วงต่างๆเช่น USB Drive โดยซอฟต์แวร์เหล่านั้นถูกพัฒนาขึ้นเพื่อละเมิดความมั่นคงปลอดภัยของทรัพยากรสารสนเทศและการสื่อสารจึงส่งผลต่อ การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรที่มัลแวร์นั้นทำงานอยู่ สามารถจำแนกประเภทตามคุณลักษณะจำเพาะของมัลแร์ได้หลายประเภทเช่น

- ไวรัสคอมพิวเตอร์ (Computer Virus) หมายถึงมัลแวร์ที่มีความสามารถในการติดเข้าระบบคอมพิวเตอร์แต่ไม่สามารถแพร่กระจายตัวเองผ่านระบบเครือข่ายได้ และจะต้องใช้สื่ออื่นในการแพร่กระจายเช่นดิสก์หรือ USB Drive เป็นต้น

- หนอนอินเทอร์เน็ต (Internet Worm) หมายถึงมัลแวร์ที่เผยแพร่ตัวเองผ่านระบบเครือข่ายคอมพิวเตอร์โดยอาจมีความสามารถที่หลากหลายตั้งแต่การส่งจดหมายอิเล็กทรอนิกส์ไปให้ผู้อื่น

- คีย์ล๊อกเกอร์ (Key Logger) หมายถึงมัลแวร์ที่เมื่อถูกติดตั้งบนเครื่องคอมพิวเตอร์แล้วจะทำการดักรับข้อมูลการกดคีย์บอร์ดของผู้ใช้งานแล้วส่งต่อข้อมูลดังกล่าวไปให้ผู้ไม่ประสงค์ดี เป็นต้น

- โทรจัน (Trojan) หมายถึงมัลแวร์ที่เมื่อถูกติดตั้งแล้วจะทำการสร้างการเชื่อมต่อไปยังผู้ไม่ประสงค์ดี โดยอาจรอรับคำสั่งโดยยังไม่สร้างความเสียหายให้กับความมั่นคงปลอดภัยของระบบ แต่เมื่อได้รับคำสั่งอาจทำการ

อย่างอื่นๆเช่น คัดลอกข้อมูล ดักฟังข้อมูล หรือเป็นฐานสำหรับใช้โจมตีเครื่องอื่นๆที่เชื่อมต่อในเครือข่ายเดียวกัน เป็นต้น

ในปัจจุบันมัลแวร์ได้รับการพัฒนาให้มีความสามารถและประสิทธิภาพสูงขึ้นโดยสามารถสร้างความเสียหายและทำลายความมั่นคงปลอดภัยได้หลายหลายและยากต่อการตรวจจับมากยิ่งขึ้นเนื่องจากกาเผยแพร่ซอฟต์แวร์ต้นแบบสามารถกระทำได้ง่ายผ่านเครือข่ายอินเทอร์เน็ต

4.1.2 การเจาะระบบ (Exploitation)

การเจาะระบบสามารถกระทำได้หลากหลายวิธีขึ้นอยู่กับทักษะและช่องโหว่ที่เกี่ยวข้องดังนั้นรูปแบบการโจมตีที่เกิดขึ้นจึงขึ้นอยู่กับกระทบที่ผู้โจมตีต้องการอันได้แก่ การสกัดขัดขวาง การดักรับดักฟัง การเปลี่ยนแปลงแก้ไข และการปลอมแปลง ทรัพยากรสารสนเทศที่ตกเป็นเป้าหมายของการโจมตี ทั้งนี้เป้าหมายหลักจึงเป็นระบบและบริการต่างๆที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตและเครือข่ายภายใน โดยผู้โจมตีจะเลือกพิจารณาโจมตีต่อช่อวโหว่หรือข้อบกพร่องด้านการรักษาความมั่นคงปลอดภัย โดยหากโจมตีต่อทรัพยากรหนึ่งสำเร็จก็มักจะใช้ทรัพยากรนั้นเป็นฐานสำหรับการโจมตีในลำดับถัดๆไป รูปแบบการโจมตีที่สำคัญมีดังต่อไปนี้

วิศวกรรมสังคม (Social Engineering) หมายถึง การโจมตีต่อทรัพยากรสารสนเทศผ่านความอ่อนแอในการตัดสินใจของมนุษย์ มีลักษระคล้ายคลึงกับการปฏิบัติการจิตวิทยา วิธีการโจมตีด้วยเทคนิคนี้จะไม่มีความเกี่ยวข้องกับความรู้ความชำนาญเกี่ยวกับระบบสารสนเทศและการสื่อสารสูงแต่มุ่งเน้นในการสร้างสภาวะการณ์ที่เหมาะสมทำให้เหยื่อหลงเชื่อแล้วทำอย่างใดอย่างหนึ่งที่อาจทำให้การโจมตีด้วยเทคนิคอื่นๆประสบความสำเร็จ เช่น การหลอกให้บางคนหลงกลเพื่อเข้าถึงระบบด้วยการหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ จะเห็นว่าการโจมตีด้วยเทคนิควิศวกรรมสังคมเป็นจุดอ่อนที่ป้องกันยากเพราะเกี่ยวกับคน แต่สามารถลดผลสำเร็จของการโจมตีได้ด้วยการกำหนดีขั้นตอนการปฏิบัติที่เป็นมาตรฐาน และการสร้างความตระหนักรู้ให้กับบุคคลากรที่เกี่ยวข้องกับระบบในทุกๆระดับตั้งแต่ผู้บริหาร ผู้ใช้งาน และผู้ดูแลระบบ

การเดารหัสผ่าน (Password Guessing, Bruteforce) หมายถึงการโจมตีด้วยการส่งข้อมูลการพิสูจน์ตัวจริงเข้าสู่ระบบด้วยข้อมูลกลุ่มตัวอักษรและเลขที่ใช้สำหรับการพิสูจน์ทราบตัวจริงของผู้ใช้ โดยปกติรหัสผ่านจะใช้คู่กับชื่อผู้ใช้หรือยูสเซอร์เนม (Username) สำหรับล็อคอินเข้าสู่ระบบซึ่งเป็นกลไกสำคัญในการพิสูจน์และกำหนดสิทธิ์ที่ผู้ใช้งานพึงมีต่อระบบ ดังนั้นการป้องกันการโจมตีด้วยเทคนิคนี้จึงต้องกำหนดและบังคับนโยบายที่เกี่ยวข้องกับวิธีการพิสูจน์ตัวจริงโดยห้ามใช้งาน

- รหัสผ่านที่สั้น เช่น 123456, asdfgjkl เป็นต้น
- คำที่รู้จักและคุ้นเคย เช่น password, blue, admin เป็นต้น
- ใช้ข้อมูลส่วนตัวในรหัสผ่าน เช่น ชื่อ หมายเลขโทรศัพท์ วันเกิด เป็นต้น
- ใช้รหัสผ่านเดียวกันกับทุกๆ ระบบที่ใช้

- เขียนรหัสผ่านไว้บนแผ่นกระดาษแล้วเก็บไว้ในที่ ๆ หาได้ง่าย
- ใช้พาสเวิร์ดเดิมๆเป็นระยะเวลานาน

การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service) หมายถึงการโจมตีที่ผู้โจมตีหวังผลให้ระบบที่ตกเป็นเป้าหมายไม่สามารถให้บริการได้ โดยผู้โจมตีอาจโจมตีต่อช่องโหว่หรือบั๊กของทรัพยากรสารสนเทศนั้นแล้วส่งผลให้ระบบปฏิเสธการให้บริการ หรือการโจมตีด้วยการร้องขอทรัพยากรพร้อมๆกันจำนวนมากจากเครือข่ายของซอฟต์แวร์อัตโนมัติที่เรียกว่า บอท (botnet) ซึ่งผลการโจมตีจากเทคนิคดังกล่าวจะทำให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึงและใช้งานทรัพยากรนั้นๆได้ และในบางกรณีอาจเปิดโอกาสให้ผู้ไม่ประสงค์ดีสามารถฝังซอฟต์แวร์มุ่งประสงค์ร้ายเช่น โทรจัน หรือคีย์ล็อกเกอร์ ลงบนเป้าหมายเพื่อแฝงตัวเข้าโจมตีด้วยเทคนิคอื่นๆต่อไป

การโจมีแบบคนกลาง (Man-in-Middle Attacks) อีกรูปแบบหนึ่งของการโจมตีคือ การพยายามที่จะใช้บัญชีผู้ใช้ที่ถูกต้องในการล็อคอินเข้าไปในระบบ ซึ่งการให้ได้มาซึ่งข้อมูลเหล่านี้ก็โดยการใช้การโจมตีแบบคนกลาง การโจมตีแบบคนกลางของการสื่อสารผ่านระบบคอมพิวเตอร์ เป็นรูปแบบที่พบเห็นได้ทั่วไป การโจมตีประเภทนี้จะทำให้คอมพิวเตอร์สองเครื่องดูเหมือนว่าจะสื่อสารกันอยู่ โดยที่ไม่รู้ว่ามีคนกลางคอยเปลี่ยงแปลงข้อมูลอยู่การป้องกันการโจมตีแบบคนกลางก็อาจใช้วิธีการเข้ารหัสข้อมูลควบคู่กับการ พิสูจน์ทราบตัวจริงของคู่รับคู่ส่ง การโจมตีแบบคนกลางแบ่งออกเป็น 2 ประเภท คือ แบบแอ็คทีฟ (Active) และแบบพาสซีฟ (Passive) สำหรับแบบแอ็คทีฟนั้นข้อความที่ส่งถึงคนกลางจะถูกเปลี่ยนแปลงแล้วค่อยส่งต่อ ถึงผู้รับ ส่วนแบบพาสซีฟนั้นจะส่งต่อข้อความเดิมที่ได้รับ

4.1.3 EMP Weapons

EMP Weapons หมายถึงอาวุธที่ถูกออกแบบขึ้นเพื่อแพร่คลื่นอิเล็กโทรแมคเนติก โดยการส่งคลื่นแม่เหล็กไฟฟ้ากำลังสูงซึ่งส่งผลให้อุปกรณ์อิเล็กทรอนิกส์ได้รับความเสียหาย อย่างไรก็ดียังไม่มีรายงานผลสำเร็จของการใช้งานอาวุธลักษณะนี้ในการทำการรบ แต่ปัจจุบันมีการวิจัยเพื่อพัฒนาประสิทธิภาพและผลสำเร็จของการใช้อาวุธลักษณะนี้อย่างต่อเนื่อง

4.2 เครื่องมือเชิงรับ (Defensive Tools)

4.2.1 การควบคุมการเข้าถึงทรัพยากร

การควบคุมการเข้าถึงทรัพยากร การควบคุมการเข้าถึงทรัพยากรสารสนเทศจะถูกดำเนินการโดยการกำหนดและใช้งานมาตรการควบคุม (access control) ซึ่งหมายถึง กระบวนการ วิธีการ หรือระบบซึ่งจะทำการตรวจสอบผู้ใช้งานก่อนอนุญาตให้ผู้ใช้งานที่ผ่านการตรวจสอบนั้นเข้าถึงทรัพยากรสารสนเทศใดๆได้ ยกตัวอย่าง มาตรการควบคุมสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทั่วไปที่นิยมใช้คือ การป้อนรหัสผู้ใช้งานและรหัสผ่าน มาตรการควบคุมสำหรับการผ่านเข้าออกห้องอาจมีการติดตั้งระบบคีย์การ์ดให้เฉพาะผู้ที่มีการ์ดเท่านั้นจึงจะสามารถเข้าออกได้ หรือแม้กระทั่งการแจกจ่ายกุญแจเฉพาะเจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องในการเข้าถึงห้องใดห้องหนึ่ง ก็จัดเป็นมาตรการการควบคุม ทั้งนี้มาตรการควบคุมสามารถจำแนกเป็น 3 ประเภทคือ

- การควบคุมการเข้าถึงภาพบังคับ (mandatory access control) หมายถึงหลักการควบคุมการเข้าถึงแบบที่ผู้ใช้งานไม่สามารถเปลี่ยนแปลงสิทธิการเข้าถึงทรัพยากรได้ด้วยตนเอง เหมาะสำหรับการควบคุมทรัพยากรที่มีข้อมูลและสิทธิ์ของผู้ใช้งานมีความชัดเจน เนื่องจากผู้ใช้งานแต่ละคนจะถูกแบ่งมอบสิทธิในการเข้าถึงทรัพยากรเป็นกลุ่มๆ (classes or categories) ในแต่ละกลุ่มจะมีการจัดลำดับความมั่นคงปลอดภัยเช่น การแบ่งข้อมูลออกแบบ ลับที่สุด ลับมาก ลับ และ ไม่จัดลำดับชั้นความลับเป็นต้น

- การควบคุมการเข้าถึงโดยผู้ใช้ (discretionary access control) มีหลักการการควบคุมการเข้าถึงทรัพยากรในลักษณะของการให้สิทธิแก่เจ้าของหรือผู้ได้รับสิทธินั้น เมื่อมีการร้องขอการพิสูจน์สิทธิ์จากผู้ใช้งาน กลไกการตรวจสอบสิทธิที่ได้รับอนุญาตของผู้ใช้งานจะถูกตรวจสอบ และกลไกนี้จะเป็นผู้ส่งต่อสิทธิที่ผู้ใช้งานได้รับให้สามารถเข้าถึงทรัพยากรได้อีกต่อหนึ่ง ซึ่งกลไกนี้เป็นกลไกมาตรฐานที่ระบบฐานข้อมูลนิยมใช้ในการควบคุมการเข้าถึง โดยทั่วไปเป็นที่เข้าใจได้ว่าผู้ใดสร้างหรือเป็นเจ้าของทรัพยากร ผู้นั้นจะสามารถเข้าถึงและมอบสิทธิการเข้าถึงให้แก่ผู้อื่นได้

- การควบคุมการเข้าถึงตามบทบาท (role-based access control) เป็นการควบคุมการเข้าถึงทรัพยากรตาม “หน้าที่” ที่ผู้ใช้งานมีต่อทรัพยากรสารสนเทศ กลไกควบคุมการเข้าถึงแบบนี้มีความเหมาะสมต่อการควบคุมการเข้าถึงทรัพยากรในระบบสารสนเทศ หรือโครงสร้างพื้นฐานระบบสารสนเทศที่มีความซับซ้อน เนื่องจากในระบบที่มีความซับซ้อนมากๆมักมีความต้องการควบคุมทรัพยากรที่หลากหลาย หน้าที่ของผู้ใช้งานจึงถูกนำมาพิจารณาในการกำหนดสิทธิ ทำให้มั่นใจได้ว่าจะไม่มีผู้ใช้งานคนใดที่สามารถเข้าถึงหรือบริหารระบบได้ทั้งหมด การที่มีผู้สามารถเข้าถึงหรือบริหารระบบได้แต่เพียงผู้เดียวย่อมมีความเสี่ยงในการที่ข้อมูลหรือสารสนเทศในระบบนั้นจะถูกเปลี่ยนแปลงแก้ไขอย่างไม่ถูกต้อง ตัวอย่างหนึ่งของการควบคุมการเข้าถึงตามบทบาทคือการควบคุมการเข้าถึงซอฟต์แวร์ที่ใช้ในการปรับแต่งคุณสมบัติของระบบปฏิบัติการซึ่งกำหนดให้ผู้ใช้งานต้องได้รับสิทธิ์เป็นผู้ดูแลระบบ (administrator) เป็นต้น

มาตรการการควบคุมที่ได้กล่าวมา มักถูกใช้ร่วมกับกลไกสำคัญต่อไปนี้ การแสดงตน การพิสูจน์ตัวจริง การกำหนดสิทธ์ และการกำหนดความรับผิดชอบ ในกรณีนี้จะยกตัวอย่างมาตรการควบคุมการเข้าถึงและใช้บริการธุรกรรมผ่านอินเทอร์เน็ตของสถาบันการเงินแห่งหนึ่ง ซึ่งลูกค้าสามารถเข้าใช้งานได้ผ่านเว็บบราวเซอร์ และซอฟต์แวร์ที่ทำงานบนโทรศัพท์เคลื่อนที่

- การแสดงตน (identification) เป็นกลไกที่ใช้ในการควบคุมผู้ใช้งานที่ต้องการเข้าถึงทรัพยากรตามช่องทางที่ทรัพยากรนั้นๆกำหนดขึ้น ในกรณีนี้ผู้ใช้งานจะต้องใช้งานอาจถูกร้องขอให้ใช้งานผ่านเว็บบราวเซอร์ที่ได้รับความนิยมใช้งาน (เช่น ไฟร์ฟอกซ์ กูเกิ้ลโครม) และซอฟต์แวร์ที่ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้นเท่านั้น หากการร้องขอใช้งานจากซอฟต์แวร์อื่นๆเช่น โอเปราบราวเซอร์ หรือซอฟต์แวร์ที่ไม่ได้ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้น จะไม่เข้าถึงและพิสูจน์ตัวจริงได้

- การพิสูจน์ตัวจริง (authentication) เป็นกลไกที่ใช้ในการตรวจสอบความถูกต้องของผู้ที่มาแสดงตนขอเข้าถึงทรัพยากรสารสนเทศ การพิสูจน์ตัวจริงนิยมกระทำด้วยการตรวจสอบ “ความถูกต้อง” ของข้อมูลสำหรับการพิสูจน์ตัวจริง โดยแบ่งลักษณะของข้อมูลนั้นได้ 3 ลักษณะคือ

- ข้อมูลที่ผู้แสดงตนทราบ (something you know) เช่นชื่อผู้ใช้งาน รหัสผ่าน หมายเลขพินสำหรับใช้งานเอทีเอ็ม
- ข้อมูลที่ผู้แสดงตนมี (something you has) เช่นบัตรเอทีเอ็ม หมายเลขบัตร
- ข้อมูลที่ผู้แสดงตนเป็น (something you are) เช่นข้อมูลลายนิ้วมือ ข้อมูลม่านตา

สำหรับกรณีการเข้าถึงบริการธนาคารอิเล็กทรอนิกส์ในปัจจุบันนิยมใช้กลไกในการพิสูจน์ตัวจริงโดยใช้แหล่งที่มาของข้อมูลร่วมกันเพื่อให้มั่นใจได้ว่าผู้ที่แสดงตนนั้นเป็นผู้ที่มีสิทธิเข้าถึงทรัพยากรนั้นจริงๆ โดยการใช้ข้อมูลชื่อผู้ใช้งาน รหัสผ่าน ร่วมพาสเวิร์ดแบบใช้ครั้งเดียว (one-time password: OTP) ที่ระบบจะเป็นผู้ส่งรายละเอียดไปยังโทรศัพท์มือถือเป็นครั้งๆไป เป็นต้น

- การกำหนดสิทธิ์ (authorization) คือกลไกในการตรวจสอบและส่งมอบสิทธิ์สำหรับการเข้าถึงทรัพยากรสารสนเทศให้กับผู้ใช้งานที่ผ่านการพิสูจน์สิทธิตามที่ได้กำหนดไว้ในมาตรการการควบคุมการเข้าถึงสารสนเทศสำหรับผู้ใช้งานรายนั้นๆ ซึ่งการกำหนดสิทธิ์ก็จะสอดคล้องกับประเภทของการควบคุมการเข้าถึงดังที่ได้กล่าวมาแล้วในตอนต้น

- การกำหนดความรับผิดชอบ (accountability) เป็นกลไกที่ทำให้มั่นใจได้ว่าผู้ใช้งานที่เข้าใช้งาน ตลอดจนผู้ไม่ประสงค์ดีที่พยายามเข้าใช้งานจะสามารถถูกตรวจสอบและเป็นผู้รับผิดชอบผลของการกระทำที่มีต่อทรัพยากรสารสนเทศนั้นๆได้ วิธีการและเทคโนโลยีสำคัญที่ใช้ในการตรวจสอบและกำหนดความรับผิดชอบคือการจัดเก็บข้อมูลการจราจร การจัดเก็บประวัติการใช้งานหรือที่นิยมเรียกว่าล็อก (logs) ของทรัพยากรต่างๆที่มี

4.2.2 การกำหนดสภาวะของทรัพยากร

การเฝ้าตรวจความมั่นคงปลอดภัยทรัพยากรสารสนเทศ และการตอบสนองต่อการโจมตีที่เกิดขึ้นจากภัยคุกคามรูปแบบต่างๆต่อทรัพยากรสารสนเทศอย่างเหมาะสม จะทำให้มั่นใจได้ว่าการโจมตีที่เกิดขึ้นจะถูกบริหารจัดการได้อย่างมีประสิทธิภาพและใช้ทรัพยากรที่เกี่ยวข้องได้แก่ งบประมาณ บุคลากร กระบวนการบริการจัดการและการประยุกต์ใช้เทคโนโลยีที่เหมาะสม เหตุการณ์ต่างๆที่เกิดขึ้นในทรัพยากรสารสนเทศจะถูกตรวจสอบและกำหนดสถานะให้กับทรัพยากรเหล่านั้นตามสภาวการณ์ที่แท้จริงโดยเป็นผลจากการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ทราบว่าทรัพยากรใดมีความต้องการการเฝ้าตรวจอย่างไร ทั้งนี้สถานะของทรัพยากรๆนั้นจะถูกกำหนดเป็น 3 สถานะหลักๆได้แก่

ภาวะปกติ (normal) คือเหตุการณ์ปกติของทรัพยากรที่ถูกเฝ้าตรวจ จึงไม่มีความจำเป็นต้องถูกบริหารจัดการเนื่องจากผลการเฝ้าตรวจแสดงให้เห็นถึงสภาพปกติของทรัพยากรนั้นๆ

ภาวะเฝ้าระวัง (escalation) คือเหตุการณ์ที่เกิดขึ้นเมื่อผลการเฝ้าตรวจตรวจพบสิ่งสภาพผิดปกติของทรัพยากรสารสนเทศนั้นๆ โดยเหตุการณ์ดังกล่าวอาจส่งผลต่อความสามารถในการดำเนินการของทรัพยากร หรือการละเมิดมาตรการควบคุมบางอย่างที่ถูกกำหนดขึ้นไว้ในนโยบายการรักษาความมั่นคงปลอดภัย เมื่อเกิดเหตุการณ์ลักษณะนี้จึงมีความจำเป็นต้องได้รับการบริหารจัดการอย่างเหมาะสมจากผู้มีส่วนเกี่ยวข้อง

ภาวะวิกฤต (emergency) คือเหตุการณ์ที่เกิดขึ้นกับทรัพยากรสารสนเทศแล้วส่งผลกระทบต่อชีวิตและทรัพย์สินของมนุษย์ ผลกระทบจากภัยคุกคามต่อโครงสร้างพื้นฐานสำคัญของการดำเนินธุรกิจ ผลกระทบต่อเนื่องจากภัยคุกคามที่ทำให้เกิดสภาวะเฝ้าระวังบนทรัพยากรสารสนเทศแล้วส่งผลอื่นๆต่อทรัพยากรที่เกี่ยวข้องกัน หรือเหตุการณ์ที่เกิดขึ้นแล้วละเมิดนโยบายการรักษาความมั่นคงปลอดภัยอย่างร้ายแรง

4.2.3 กระบวนการเฝ้าตรวจความมั่นคงปลอดภัย

เมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ผู้รับผิดชอบความมั่นคงปลอดภัยของหน่วยจะเป็นผู้รับผิดชอบหลักในการแก้ไขสถานการณ์ให้กลับสู่สภาวะปกติโดยเร็ว ตามแผนเผชิญเหตุที่ถูกกำหนดไว้ล่วงหน้าเพื่อรองรับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นร่วมกับคณะทำงานรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team: CIRT) ซึ่งถูกกำหนดหน้าที่ให้ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย และให้บริการสิ่งจำเป็นสำหรับรับมือกับเหตุการณ์นั้นๆ เช่น การแจ้งเตือน การให้คำแนะนำ การอบรม และการบริหารจัดการเหตุการณ์ เป็นต้น โดยปกติกระบวนการบริหารความมั่นคงปลอดภัย การบริหารความมั่นคงปลอดภัยประกอบการปฏิบัติหลักๆ ดังต่อไปนี้

การเตรียมความพร้อม (preparation) ในขั้นตอนนี้หน่วยจะทำการเตรียมความพร้อมสำหรับการเผชิญสถานการณ์ไม่พึงประสงค์ด้วยการฝึกฝนบุคลากร กำหนดนโยบาย ออกแบบกระบวนการ และเตรียมการทรัพยากรให้สอดคล้องกับเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น โดยอาจมีการเตรียมความรู้ ซอฟต์แวร์ และอุปกรณ์ที่จำเป็น เช่น ซอฟต์แวร์สำหรับการเฝ้าฟังเครือข่าย (sniffer) สายเคเบิลแบบครอส (crossover cable) แผ่นสำหรับการติดตั้งระบบปฏิบัติการ เป็นต้น ทั้งนี้การเตรียมความพร้อมอาจทำในรูปแบบของรายการที่หน่วย

การเฝ้าระวังและการเฝ้าตรวจ (detection and identification) เป็นขั้นตอนที่สำคัญอย่างยิ่งยวดเนื่องจากเป็นขั้นตอนเดียวที่จะสามารถบ่งชี้ได้ว่าเหตุการณ์ไม่พึงประสงค์นั้นเกิดขึ้นจริงๆ ในขั้นตอนนี้การวิเคราะห์อย่างรอบด้านจะทำให้ผู้มีหน้าที่รับผิดชอบและองค์กรสามารถดำเนินการตอบสนองต่อเหตุการณ์ไม่พึงประสงค์ได้อย่างเหมาะสม โดยหากการวิเคราะห์ผิดพลาดย่อมส่งผลเสียต่อการแก้ไขสถานการณ์เนื่องจากไม่สามารถแก้ไขปัญหาได้ตรงจุดหรือต้องใช้ระยะเวลาแก้ไขปัญหานานกว่าที่ควร

การแก้ไขสถานการณ์วิกฤติ (incident response) เป็นขั้นตอนที่คณะทำงานแก้ไขสถานการณ์เข้าแก้ไขเหตุการณ์ไม่พึงประสงค์เพื่อป้องกันการลุกลามของเหตุการณ์ไม่พึงประสงค์นั้นๆ การแก้ไขสถานการณ์อาจทำได้หลากหลายวิธีขึ้นอยู่กับสาเหตุของปัญหาที่แท้จริง ยกตัวอย่างเช่น หากเกิดเหตุการณ์โจมตีต่อระบบบริการสมาชิกเนื่องจากการโจมตีโดยการเปลี่ยนแปลงหน้าโฮมเพจ คณะทำงานแก้ไขสถานการณ์อาจตัดสินใจตัดการเชื่อมต่อของระบบบริการเว็บ แล้วสร้างช่องทางไปยังระบบสำรอง จากนั้นจึงทำการแก้ไขทรัพยากรของระบบเว็บเพื่อตรวจสอบผลกระทบของการโจมตีครั้งนั้นๆ

การบรรเทาสถานการณ์ (mitigation) เป็นขั้นตอนที่เกี่ยวข้องกับการค้นหาผลกระทบที่เกิดขึ้นจากเหตุการณ์ไม่พึงประสงค์ เพื่อทำให้มั่นใจได้ว่าทรัพยากรที่ตกเป็นเป้าหมายนั้นถูกแก้ไข และสามารถฟื้นคืนสภาพกลับไปสู่การให้บริการได้ ดังนั้นการค้นหาสาเหตุที่จริงของเหตุการณ์ไม่พึงประสงค์จึงเป็นสิ่งสำคัญอย่างยิ่ง โดยทั่วไปคณะทำงานแก้ไขสถานการณ์จะทำการขจัดสาเหตุของเหตุการณ์ไม่พึงประสงค์ เช่นหากเหตุการณ์ไม่พึงประสงค์เกิดจากการฝังตัวของมัลแวร์ที่ทำการลักลอบดักรับข้อมูลการป้อนรหัสผ่าน คณะทำงานก็จะทำการตรวจสอบและกำจัดมัลแวร์นั้นๆ

และทำการป้องกันที่จำเป็นเพื่อป้องกันการเกิดเหตุการณ์ไม่พึงประสงค์นั้นๆซ้ำ

การรายงานสถานการณ์ (reporting) เป็นขั้นตอนที่กระทำควบคู่ไปกับการเฝ้าตรวจโดยการรายงานสถานการณ์จะต้องกระทำในโอกาสแรกตั้งแต่ผู้มีหน้าที่รับผิดชอบตรวจพบสิ่งผิดปกติขึ้น ทั้งนี้การรายงานจะต้องครอบคลุมทั้งข้อมูลเชิงเทคนิค และข้อมูลทั่วไปของทรัพยากรสารสนเทศที่ได้รับการเฝ้าตรวจ ข้อมูลทั่วไปของทรัพยากรสารสนเทศจะถูกใช้ในการประมาณสถานการณ์ของทรัพยากรในการดำเนินธุรกิจและธุรกรรมขององค์กร นอกจากนี้เมื่อเกิดเหตุการณ์ไม่พึงประสงค์ขึ้นผู้มีหน้าที่รับผิดชอบจะสามารถใช้ข้อมูลดังกล่าวในการประเมินผลกระทบต่อการดำเนินธุรกิจในภาพรวมและประมาณการณ์ผลเสียหายตลอดจนแนวทางการแก้ไขได้อย่างทันท่วงที

การฟื้นคืนสภาพ (recovery) เป็นส่วนหนึ่งของกระบวนการบรรเทาสถานการณ์และขั้นตอนที่ผู้มีหน้าที่รับผิดชอบทำการฟื้นคืนสภาพให้กับทรัพยากรที่ได้รับผลกระทบจากการโจมตี โดยปกติแล้วจะพิจารณาจากลำดับความเร่งด่วนของทรัพยากรนั้นๆต่อการดำเนินธุรกิจ โดยต้องคำนึงถึงความเป็นไปได้ที่ผู้มีหน้าที่รับผิดชอบอาจไม่สามารถกำจัดสาเหตุของเหตุการณ์ไม่พึงประสงค์ได้ ดังนั้นผู้มีหน้าที่รับผิดชอบจะต้องทำการเฝ้าตรวจและวิเคราะห์ทรัพยากรสารสนเทศนั้นๆอย่างใกล้ชิดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ไม่พึงประสงค์ซ้ำขึ้น ด้วยการกำหนดตัวชี้วัดที่เป็นสิ่งบอกเหตุขึ้นแล้วทำการตรวจสอบตัวชี้วัดนั้นๆจนมั่นใจได้ว่าสาเหตุของเหตุการณ์ไม่พึงประสงค์นั้นๆถูกขจัดหมดสิ้นไปอย่างสมบูรณ์

การฟื้นฟูสภาพ (remediation) เป็นขั้นตอนหนึ่งที่กระทำอย่างต่อเนื่องโดยเป็นส่วนหนึ่งของกระบวนการบรรเทาสถานการณ์ โดยทำการวิเคราะห์และเฝ้าตรวจทรัพยากรในวงที่กว้างขึ้นกว่าจุดเกิดเหตุนั้นๆ ยกตัวอย่างเช่น องค์กรหนึ่งตรวจพบการแอบดักรับดักฟังข้อมูลบนเครือข่ายและคาดว่าผู้ไม่ประสงค์ดีสามารถดักรับดักฟังข้อมูลที่ใช้ในการพิสูจน์ตัวจริงต่อระบบบริหารทรัพยากรขององค์กร และค้นพบว่าปัญหานั้นเกิดจากผู้ไม่ประสงค์ดีติดตั้งมัลแวร์ลงบนคอมพิวเตอร์เครื่องหนึ่งของบริษัท คณะทำงานแก้ไขสถานการณ์จึงพิจารณาค้นหาและทำลายมัลแวร์ที่อาจถูกติดตั้งบนเครื่องคอมพิวเตอร์เครื่องอื่นๆที่เชื่อมต่อในเครือข่ายที่ถูกตรวจพบตั้งแต่เริ่มต้นพร้อมๆกับตัดการเชื่อมต่อเครือข่ายนั้นไปยังเครือข่ายอื่นๆในองค์กร และทำการบังคับนโยบายให้ผู้ใช้งานที่เกี่ยวข้องทำการเปลี่ยนพาสเวิร์ด เป็นต้น

การถอดบทเรียน (lessons learned) เป็นขั้นตอนที่สรุปรวมสิ่งที่เกิดขึ้นนับตั้งแต่เหตุการณ์ไม่พึงประสงค์อุบัติขึ้น โดยรวบรวมข้อมูลที่เกี่ยวข้องนับตั้งแต่การวิเคราะห์สาเหตุ การดำเนินการต่างๆที่เกี่ยวข้องโดยละเอียด โดยหวังผลให้ลดระยะเวลาตลอดจนการใช้งานทรัพยากรที่อาจถูกนำมาใช้เมื่อมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นครั้งๆถัดๆไป รวมถึงทำให้กระบวนการวิเคราะห์หาสาเหตุที่แท้จริงสามารถทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้นเนื่องจากมีการสรุปรวมองค์ความรู้ต่างๆที่เกี่ยวข้องกับการแก้ไขสถานการณ์ไม่ถึงประสงค์

บทที่ 5

ขีดความสามารถด้านไซเบอร์ของ ทร.

5.1 การเตรียมทรัพยากรมนุษย์

- การจัดตั้งหน่วย
- การจัดอบรม
- การเผยแพร่เอกสาร
- การสร้างความตระหนักรู้
- การจัดแข่ง CTF

5.2 การกำหนดนโยบายและการปฏิบัติ

- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔
- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒
- พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.๒๕๕๐ และฉบับแก้ไข
- ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘
- แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘

5.3 การประยุกต์ใช้เทคโนโลยี

- การประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย
- การเฝ้าตรวจทรัพยากรสารสนเทศ

XeTeX

บรรณานุกรม

[1] M. C. Libicki, *Cyberdeterrence and Cyberwar*. Arlington, VA: RAND PROJECT AIR FORCE, 2009.

[2] J. Carr, *Inside Cyber Warfare*. O'Reilly Media, Inc., 2nd ed., 2013.

[3] A. Singer, P.w, Friedman, *Cybersecurity and Cyberwar - What everyone needs to know*. No. 1, 2014.

[4] J. Andress and S. Winterfeld, *Cyber Warfare - Techniques, Tactics, and Tools for Security Practitioners 2nd edition*. Elsevier, 2014.

[5] V. Subrahmanian, M. Ovelgonne, T. Dumitras, and A. Prakash, *The Global Cyber-Vulnerability Report*. Terrorism, Security, and Computation, Cham: Springer International Publishing, 2015.