**สงครามไซเบอร์**

**(Cyber Warfare)**

"สงครามไซเบอร์" (Cyber Warfare) คือ การใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำสงคราม ซึ่งสงครามไซเบอร์ เป็นส่วนหนึ่งของสงครามสารสนเทศ (Information Warfare) สงครามไซเบอร์มีการโจมตีกันหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด อาทิ

-การโจมตีเว็บ หรือบล็อคเว็บ

-การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ต

-การเจาะข้อมูลลับ โดยแฮกเกอร์ที่นอกจากได้ข้อมูลลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้

-การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้ หรือทำงานไม่แม่นยา

-การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก

***สงครามไซเบอร์เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม และต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา***

สงครามไซเบอร์ได้อุบัติขึ้นแล้วในหลายประเทศซึ่งมีทั้งประเภทชัดเจน เปิดเผย และซุ่มเงียบ ซึ่งคำว่า "สงครามเย็น" หรือ Cold War ก็เริ่มกลับนามาใช้กันใหม่อีกครั้ง หลังจากการแพ้สงครามเวียดนามของสหรัฐอเมริกาและการล่มสลายของสหภาพโซเวียตรัสเซีย

ในช่วงสงครามอ่าวที่สหรัฐโจมตีอิรัก และสงครามอิรักครั้งที่สอง สิ่งที่สหรัฐต้องทำก่อนอื่นคือ ทำลายเครือข่ายคอมพิวเตอร์และอิเล็กทรอนิกส์ของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ ไม่เพียงแต่กรณีสงครามอิรักเท่านั้นในการสู้รบปัจจุบัน แต่ละฝ่ายต้องหาทางทำลายระบบคอมพิวเตอร์และอิเล็กทรอนิกส์ที่ควบคุมการยิงของอาวุธก่อน ตัวอย่างเช่น

ในวันที่ 17 เดือนพฤษภาคม ปี 2007 ประเทศเอสโทเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนข้อมูลเสียหายพังยับเยิน

เมื่อต้นเดือนกันยายน ปี 2007 ตึกเพนทากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา

วันที่ 14 ธันวาคม ปี 2007 เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม ปัจจุบันมีอยู่ 8 รูปแบบ คือ

1. การโจรกรรมทางไซเบอร์
2. การทำลายเว็บไซต์
3. การโฆษณาชวนเชื่อทางอินเตอร์เน็ต (เว็บไซต์)
4. การรวบรวมและการล้วงความลับข้อมูล
5. การกระจายเพื่อให้ปฏิเสธบริการ
6. การรบกวนเครื่องมือและอุปกรณ์
7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) พื้นฐานที่สำคัญ
8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้