Cyber War: A Checklist

Brent, Melissa, & Devon

Definition

Arquilla asserts that cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.

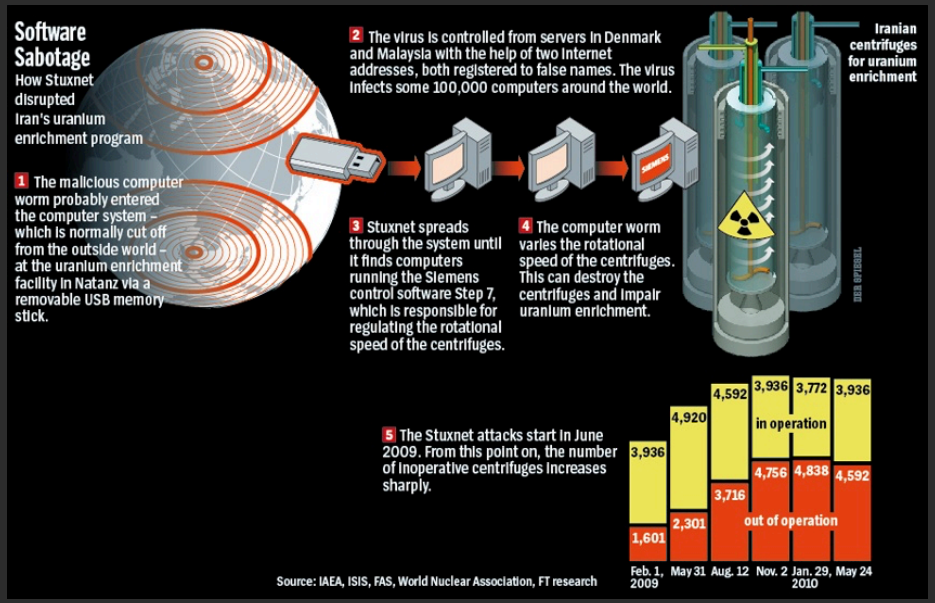
This translates to the usage of computer technology that disrupts or destroys the operations of a state, governing body, or official company -- but directs a particular emphasis regarding attacks on systems that have military or strategic purposes.

Arquilla, John and David Ronfeldt, Cyberwar is Coming!. Santa Monica, CA: RAND Corporation, 1993.

Checklist for a Cyber Attack

- Political Intent
  - Actor has vested interest in attacking target either to send a message or gain intelligence.
- Intent to Harm
  - In real or technical terms, bringing down a system to create problems
- Measurable Effect
- Definite Perpetrator (not an accidental error)
  - Malware, not bad code
  - Response Target

Stuxnet Case



- What: Malicious Computer Virus Targeting Iran's Nuclear Program
- Political Intent: United States had significant interest in preventing progress in Iran's nuclear program
- Intent to Harm: Computer virus directly manipulated systems to create physical harm to nuclear Centrifuges
- Measurable effects: Iran cannot enrich uranium if they do not have functional centrifuges
- Definite Perpetrator: Stuxnet code placed purposefully to harm specific centrifuges

Sony Case

- What: Hacker group named “Guardians of Peace” (GOP) leaks confidential data on Sony Perpetrators.
- Political Intent: North Korean diplomatic official says that movie is an act of war.
- Intent to harm: GOP demands that Sony pull their film, or else. Referenced threats to 9/11.
- Measurable Effect: Movie sales plummeted, digital distribution changed.
- Definitive Perpetrator: Malware is sent by hackers that erases Sony's computer infrastructure.