Stuxnet: A Significant Cyberwarfare

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Stuxnet: A Significant Cyberwarfare**

1. **Summary of Stuxnet Attack:**

According to Chapple & Seidl (2023), Stuxnet, a computer worm attacked and destroy the uranium enrichment centrifuges located at an Iranian nuclear facility in the Natanz. The virus modifies the activity of the controller to accelerate and decelerate the centrifuge rapidly, causing them to self-destroy. Stuxnet is estimated of destroying one-fifth of the centrifuges in Iran’s nuclear program.

1. **Stuxnet Implications:**

In general, Stuxnet marked the beginning of an era of legitimatization for the cyber domain of warfare. Some main points can be learned from the attacks:

* Damage: the physical damage that the worm cause can compare to any real physical war (the destruction of one-fifth of the centrifuges in Iran’s nuclear program)
* Risk: there are no human risks involved in the attack (To attack a nuclear station in enemy territory aircraft has facing many dangers from the enemy’s air defense)
* Avoid unnecessary human damage: the virus can cause serious damage to computer systems but not to humans (civilians, scientists, and other military personnel that work in the target’s facility). With a physical attack, humans damage can’t be avoided
* Accuracy: target multiple internal system networks and destroy the system silently without any notice.
* Cost: the cost of designing this worm is properly much cheaper than the cost of a physical attack with the same target.

References

Chapple, M., & Seidl, D. (2023). Chapter 6: The Evolving Threat: From Script Kiddies to Advanced Attackers. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)