Air Force Institute of Technology

CSCE 525: Introduction to Cyber Warfare and Security

Nathan Flack

12 October 2018

CTC 3

**Question: Produce a warfighting analogy that might be used to explain cyber to a non-cyber military member. What parts of the analogy are the most useful for describing cyber conflict? Where does the analogy break down?**

Cyber education and training research and innovation is receiving a lot of attention. One of the big reasons for this is that users, especially untrained users, continue to be the weakest link in cybersecurity systems. Additionally, there is a huge shortage of trained cybersecurity professionals in today’s workforce as shown here (need link).

Serious Games related to cyber may be a potential catalyst to turn both of these trends around providing realistic and engaging training games to users across all professions as well as illicit greater interest in the cyber profession.

Below I will provide an overview of three serious games related to cyber and cybersecurity developed by the Naval Postgraduate School (NPS) that you might want to check out. Bring some friends too and you might just have a little fun (and learn something too!). If you want to know more about serious games, check out this link: <http://www.growthengineering.co.uk/what-are-serious-games/>

CyberWar 2025: The paper linked above describes a new game called CyberWar 2025 developed by David Long and Christopher Mulch at NPS. It is a cyber themed boar game designed for 2, 3, or 6 players. It allows players to develop a cyber strategy and engage other players through scanning the domain, attacking opponents, and defending their own territory while seeking to gain research and action points to use during future turns. The game is in its final stages of development, and according to communication directly with the creator, will be posted to NPS’ site globalECCO.org very soon. This game can be played with other gloabalECCO users through a web browser. Anyone with a DoD email address can request an account on the site to play 11+ serious games and CyberWar 2025 in the near future.

CyberStrike: This is the game on which the creators of CyberWar 2025 based their game. “[It] is a six-player game that simulates the complex strategic environment of cyber conflict” (from GlobalECCO.org). Each player selects 1 of 6 roles (criminals, terrorists, hackers, or states) that each have the distinct capabilities and goals. This game is designed to engage players to think about the big picture of cyber conflict and how different cyber actors might behave in order to reach their goals.

Play Here: <https://globalecco.org/game-lobby;jsessionid=1EDF5403A8D30EF228761A1BB7B29558>

CyberCIEGE: This is a game that feels more like SimCity, where users invest virtual money to operate and defend computer networks against cyber adversaries. It is self-described as “An innovative video game and tool to teach computer and network security” (from my.nps.edu). This game feels more like a real-world simulation than a board game, but still provides a more-or-less realistic environment for simulation and training, which can be utilized to teach topics that would be hard to exercise in the real world. You can try a demo version today by clicking the link for an evaluation version of the game, under the “Development and Availability” section in the link below.

Explore more about CyberCIEGE here: <https://my.nps.edu/web/c3o/cyberciege>

I chose to examine cyber from the perspective of the nuclear community. Many nuclear control systems were developed before cyber threats were even on the radar. They were created to be stand-alone systems not connected to the Internet. Additionally, strong controls have been put in place to ensure a human is in the decision-making process when dealing with nuclear capabilities. I believe someone in the nuclear field would see cyber as strictly a means of communication connecting decision makers to operators enabling Command and Control or ways to connect sensors together to regulate nuclear plants. Many of the communication challenges revolve around communication in and through a nuclear event, which is a battle against the physical environment and not with actors in cyberspace. However, it seems as if a new era is emerging in nuclear cybersecurity.

First, nuclear systems are becoming more accessible to cyber actors as they become more connected. Patrick Tucker, a reporter for Defense One, identified calls from within the U.S. Government to create “more digital links between various parts of the nuclear enterprise.”[[1]](#footnote-1) While these new connections provide many important operational capabilities, the report makes clear that these actions could increase the attack vectors for our countries most expensive, powerful, and dangerous weapons.

Second, the worldwide nuclear community may be awakening to the potential issues that exist today and could be introduced in the future. In January 2018, Chatham House, an independent policy institute in London, England released a report titled “Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences,” which outlines the array of cyber risks, vulnerabilities, and considerations that nuclear states should consider while operating current nuclear capabilities and developing future systems. The report included a clear call to nuclear capable countries to reduce the cyber risk carried by their nuclear command, control, and communication systems. While many in the nuclear community might think that no other country or entity would dare to attack a nuclear capability because of the escalation it would cause, they should be very cautious. The report states, “It might seem likely that no country would be willing to face the consequences of starting a cyber offensive campaign in the nuclear weapons domain. However, an escalation is possible if cyber operations continue against key strategic assets of a country.”[[2]](#footnote-2) Outside control or influence on our cyber-enabled nuclear systems could spell disaster for the U.S. and other nuclear capable countries around the world.

1. Patrick Tucker, "As America's Nukes and Sensors Get More Connected, the Risk of Cyber Attack Is Growing," Defense One, January 17, 2018, 1, accessed October 03, 2018, https://www.defenseone.com/technology/2018/01/americas-nukes-and-sensors-get-more-connected-risk-cyber-attack-growing/145229/. [↑](#footnote-ref-1)
2. . Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences,* International Security Department, Chatham House, January 2018, 15, accessed October 2, 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf. [↑](#footnote-ref-2)