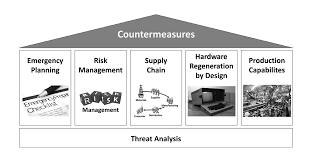
Jon William Taylor

IS 450 Cybersecurity Management

July 31, 2022



In the modern day and age of the world in which we live, technology is always evolving and it exists everywhere. Technology has changed so much over the years that as new technology comes out, the more vulnerable the security of older systems get. With new hacking techniques appearing as the technology progresses, the more vulnerable systems become of being hacked sophisticated weapons systems since the cybersecurity and the policies for guidance are not up to par with an ever changing and constant landscape. When it comes to the defense of the nation, military operations, and classified information about modern technology in the military, it is important that the cybersecurity and the policy guidance of the military weaponry be updated to protect against threats.

A report released from the Government Accountability Office (GAO) showed that vulnerabilities existed in all weapons systems from 2012 to 2017 (*BBC.com*). One finding from the report is that a GAO team was able to easily gain access to the weapons systems and watch the operators respond to the incident and a two person team was able to gain access to a system in one hour and in one day gain full control (*BBC.com*). Another finding was that one team was able to copy, change or delete data with another team able to download 100 gigabytes of information. From the GAO report it shows how vulnerable US military systems are and how easily it is get access and cause real damage if a malicious hacker was able to gain access to one.

One aspect to consider when the topic of the setup and the condition of systems that are state of the art, elderly, and the factors that go into the topic. The average time that an elderly weapons system stays in service is around 30 to 40 years before being retired, with the average lifespan of a USAF aircraft to be 27 years (Koch & Golling). This is usually caused by delays due to change in specifications, production of new parts that are incompatible with the elderly system, or the original business that made the system goes out of business (Koch & Golling). The same can also be said for new state of the art systems as well, especially as elderly systems are given upgrades to stay in service.

Another issue to consider for old and state of the art systems is supply chain issues. The big supply chain issue is with chips with how complex the system has gotten. The process of making a chip has been spread to many companies to build them based off business practices, cost reduction in manufacturing, outsourcing, and the globalization of the supply chain (Koch & Golling). To further this, the market for counterfeits has increased with a report from 2012 saying that a certain amount of tech products in the US military and agencies were fake which brings up the issue of cyberespionage and other national security risks (Koch & Golling).

For the U.S air force, it is important that they cybersecurity of jets and the weapons be top notch in regards to information being stolen through hacking or if a jet’s system is capable of being acquired by a rival nation. One issue is that the cybersecurity of a system is not continuously vigilant throughout the life cycle of a military system and triggered by certain events that result in incomplete coverage of issues through policy (Snyder, et al. *RAND.org*). A similar issue is that control and accountability area spread across many organizations and are as a result poorly integrated which means less unity of command and control for cybersecurity (Snyder, et al. *RAND.org*). The other root causes from the 2015 RAND report highlight that the security of air force weapons and systems are not well integrated but rather put on top of existing applications within the code of the system. Recommendations provided by the report include defining the cybersecurity goals for military systems, fostering innovation and adaptation through decentralization in new Air Force policy, and realigning functional roles and responsibilities for cybersecurity risk assessment around a balance of system vulnerability, threat, and operational mission impact.

A very important issue that should be considered is how secure the cybersecurity of nuclear weapons are in the modern day and age. During times of high or skyrocketing tensions between two nuclear states, it can result in an escalation based off false information from radar or from faulty systems (*WEForum.org*). One recommendation is to have close coordination between the DoD and the private sector to ensure better sync for innovation (*WEForum.org*). A good recommendation is the increase in the number of people involved for the decision and more measures of intelligence sharing (*WEForum.org*). A secondary recommendation would be to establish national cyber emergency response teams to address this issue (*WEForum.org*). A couple such examples include incidents during the Cuban Missile Crisis and the 1995 Norwegian Rocket Incident in which nuclear weapons by Russia were almost launched based off incorrect information from radar.

In the aftermath of the COVID-19 pandemic it is noted important, as the CSIS recommends, to prioritize the cybersecurity of weapons systems. The first step of this process is that the DoD should institute a process that periodically checks for vulnerabilities in weapons systems to mitigate future attacks (Dwyer, *CSIS.org*). The second step of this process is the need to avoid creating a separate process for vulnerability checkups through integration into established acquisition processes (Dwyer, *CSIS.org*). The third step of the process is the elevation of responsibility for cybersecurity oversight for the acquisition department (Dwyer, *CSIS.org*). The fourth step of the process is to encourage acquisition leadership to prioritize cybersecurity and specification of relationships between organizations and principal advisors (Dwyer, *CSIS.org*). The fifth and final step is that the DoD should consider opportunities to apply more cyber expertise towards weapon system cybersecurity (Dwyer, *CSIS.org*). With these steps in mind, it should be imperative for a concise process to help in the implementation of better practices of the cybersecurity of weapons systems.

In the modern day and age of constantly evolving technology, it is important to take the necessary steps to ensure that weapons systems are up to date with current technology to safeguard against malicious attacks. Any system, regardless of age and sophistication, has to be able to defend against cyberattacks that could steal info or compromise the system. The cybersecurity operations surrounding a nuclear weapon must be top notch to prevent a cyberattack launch that could spark a nuclear war. United States Air Force Systems have to stay up to date to prevent a cyberattack aimed to steal data about the jet or to disable it in military operations. The steps outlined by CSIS provide a starting point for the prioritization of cybersecurity in weapons systems security for a post COVID-19 era in the DoD and the U.S. military weapons systems cybersecurity. The most important thing when it comes to the national security of the nation and military operations, is the correct policy guidance and cyber implementation for weaponry against malicious and active threats.

Sources:

“Countermeasures and Threat Analysis picture chart”. 13 May 2013, *CSIS.org*, <https://ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf>.

Dwyer, Morgan. “Prioritizing Weapon System Cybersecurity in a Post Pandemic Defense Department.”, 13 May 2020, *CSIS.org*, <https://www.csis.org/analysis/prioritizing-weapon-system-cybersecurity-post-pandemic-defense-department>.

Koch, Robert and Mario Golling. “Weapons Systems and Cyber Security – A Challenging Union”, *NATO CCD COE Publications,* 2016, <https://ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf>.

Snyder, Don, et al. “Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles.”, 2015, *RAND.org*, <https://www.rand.org/pubs/research_reports/RR1007.html>.

“Threats to the cybersecurity of nuclear weapons.” *WEFourm.org*, 11 Feb 2018, <https://www.weforum.org/agenda/2018/02/nuclear-weapons-and-cybersecurity-threats-vulnerabilities-and-consequences/>.

“US Weapons Systems can be ‘easily hacked’”. *BBC.com*, 11 October 2018, <https://www.bbc.com/news/technology-45823180>.