How cyber warfare is a threat in the united states

Science, Computer Science

A review of the Cyber threat video by Joe Weiss

According to Joe Weiss, the United States and the world at large are facing a major threat in the form of a cyber- instigated warfare. Ever since the Stuxnet program was used to override the Iranian nuclear stations, tensions have risen among nations about the immense power of cyber terrorism and how badly prepared their governments are (Security Week, 2015). Weiss states that the rate at which malicious hackers adopt increasingly sophisticated methods of accessing critical systems is frightening since current law enforcement lacks the capacity to keep at par with the malicious individuals.

Weiss asserts that the most disturbing aspect of the situation is that the most dangerous of attacks are stealthy till the moment they wreak havoc. He posits that the United States faces the threat of cyber-attack mainly due to the fact that most of the nation’s economic processes are automated. The clockwork nature of the economic and technological systems makes it easier for persons with the right resources to find a weakness (Security Week, 2015). Critical infrastructures under the greatest threat include power grids, aircraft guiding systems, military equipment, major factories and pipelines. According to the speaker, the greatest impediment to avoidance of these types of attacks is the lack of the right forensic tools to trace to root of these obscure computers and hackers. He additionally claims that about 750 of these attacks have already happened without the knowledge of the public and asserts that the public should be wary since attacks of massive

proportions could be catastrophic to critical infrastructures that support systems such as healthcare and military.

NIPP's Cyber Security Mandate

The mandate of Homeland security's NIPP is to protect infrastructure critical to the country's most important systems. The plan has a strategy that aims to protect the infrastructure from cyber-attacks such as the Stuxnet attack on Iran. The strategy aims at collaboration of the government agencies with major infrastructure owners in a bid to share information and develop approaches that can enhance the nation's cyber security (DHS, 2013). The strategy is based on a directive from the president regarding the strengthening of cyber security. In the directive, the issue of information sharing in terms of volume and timeliness among stakeholders in the community of critical infrastructure was stressed. The issued directive also sought the creation of a defense approach that was independent of technology so as to separate the increasing threat of overriding critical systems from a computer (Singer, 2012). Moreover, the proposed cyber security strategy afforded civil rights to the people in terms of allowing network privacy to the public (US Strategic Command, 2017). The complex nature of the environment of America's critical infrastructure is also cited to be helpful in securing the critical systems. This is in the form of monitoring the network bridges that interconnects several infrastructures so as to detect foul play in its advent.

The cyber component moreover aims to follow seven tenets in its bid to protect theses infrastructure. The first tenet is the management of risk

through implementation of effective firewalls and other systems to detect and inhibit intrusion from hackers (IT-ISAC). The second tenet is the increment in understanding of the interconnections and dependencies of all critical system so as to strengthen weak links (DHS, 2013). The third tenet is free, effective and timely sharing of quality information among stakeholders in the community of critical infrastructure. The fourth tenet is the provision of unique outlooks and perspectives so as to brainstorm on how best to implement cyber security measures. The fifth tenet of the component seeks to increase the collaboration between players in different regions within the country. The sixth tenet is the involvement of the international community since threats from outside the country are also feasible due to the distal capability of technology. The last tenet is the consideration of security during the design of critical infrastructure assets so as to create a national tamper-proof framework.

Organizations Impacting Cyber Security

There are organizations specific to the cyber security program in collaboration with NIPP. The National Cyber Security and Communications Integration Center (NCCIC) is an organization within Homeland security whose main mandate is to provide a framework for information sharing with regard to cyber security. Agencies specific to the center include:

NCCIC Operations and integration- this organization plans and coordinates the synchronization of information sharing and analyses among cyber security stakeholders

The US Computer Emergency Readiness Team. This organization focuses on the identification of threats to the country’s network (DHS, 2017).

The Industrial Critical Systems Emergency Readiness Team. This organization focuses on the identification of threats to the country’s critical systems.

The National Coordinating Center for Communications. This organization coordinates the restoration and protection of the country’s telecommunication systems.

In addition to sector specific agencies, the government has also accorded several federal agencies with cyber security obligations.

These agencies include:

The Federal Bureau of Investigations (FBI). This agency has been granted the lead role of investigating cyber-attacks in the country.

The US Secret Service. This agency runs a computer forensics institute that equips law enforcement agencies with cyber security knowledge.

The Federal Trade Commission. This organization enforces cyber security with reference to financial crimes.