**Name:** Ronit Singh **CDAD-UH 1037** **Date:** 28 November, 2021

# CYBERWARFARE

## Week 13/14 Reading Summary

---

The article by AWS discusses the major responsibility of national governments to safeguard the internet, precisely cyberspace and its resources from threats and hence protect its citizens. In today's increasingly digitized world, everything is interconnected ranging from smart devices to critical infrastructures that people depend on in day-to-day lives. In this scenario, it becomes extremely important to have proper centrally-coordinated security measures and strategies in place to mitigate or prevent threats from occurring. The article mentions the three pillars of cybersecurity – "people, processes and technology" which are considered the key components in building an effective national cybersecurity strategy. The article lists out the various ways through which governments could ensure "cyber-hygiene" namely, "(1) Formulation and Implementation of Public Policies, (2) Development of a Collaborative Response, (3) Creating a Culture of Cybersecurity, (4) Promotion of a Professional and Business Ecosystem" (AWS, 2018). It emphasizes the importance of coordination among nations and information sharing about the vulnerabilities and threats among public and private entities as well as countries. Moreover, a nation's future depends on its youth. Hence, the article explicitly mentions the need for innovation and talented people in this sector which can be achieved by encouraging, educating, and training the youth in cybersecurity focussed fields. The author has included a chart showing the recommended pathways or programs to follow based on each stage of education i.e. high school, university, graduate programs, etc.

The second article *"National Cyber Strategy of the United States of America",* is a "fully articulated cyber strategy" of the United States with an intention to protect American citizens from online threats, improve existing cybersecurity practices, and in turn prosper in cyberspace. The document outlines four pillars of its cyber strategy "to preserve the internet's long-term openness, interoperability, security, and reliability" namely, "(1) Protect the American People, the Homeland, and the American Way of Life, (2) Promote American Prosperity, (3) Preserve Peace through Strength, (4) Advance American Influence". These are the main objectives on which this document is laid out. It mentions that America has been influential and has been leading in the field of technical innovations and will continue to do so in the years to come. In this digitally inter-connected world, protecting cyberspace is one of America's main objectives. Even more so because "the United States is regularly the victim of malicious cyber activity" (page 10). This document's importance is justified by the fact that "the borderless nature of cybercrime, including state-sponsored and terrorist activites, requires strong international law enforcement partnerships" (page 11), which the document mentions in detail. Moreover, it has become increasingly important due to the rising sophistication level of threat actors and cyber espionage cases, with America being the main target. This document also outlines a number of important and well-established cyber priorities and mentions that "the administration will prioritize risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation." (page 8). Hence, moving on to more concrete actions. The document emphasizes evolving with time and securing and upgrading the systems on which public and private companies operate.

***What surprised me?***

I was surprised by the statement that "most cybersecurity risks to critical infrastructure stem from the exploitation of known vulnerabilities" (National Cyber Strategy, page 9). Despite the fact that these are the most important infrastructures on which the country depends and operates on, they are not secure enough. Anyone with a basic knowledge of exploiting systems could gain control of these infrastructures which could turn out to be devastating for the country, if in wrong hands. Hence, governments, as mentioned in the 'national cyber strategy', should prioritize securing "critical infrastructures at greatest risk" (page 8).

---

***Questions?***

1. How do cybersecurity methods or practices for securing IoT devices differ from securing critical infrastructures and Industrial Control Systems?
2. On what basis are the different sectors in the critical infrastructure prioritized with respect to cybersecurity?

---

***Works Cited***

Amazon Web Services, A Call to Action to Protect Citizens, the Private Sector and Governments (2018).

National Cyber Strategy - Archives.
https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.