DOD Releases 2023 Cyber Strategy Summary

DOD 9/12/23

Space Systems Cybersecurity

Daniel Fitzgerald

9/16/23

DOD Releases 2023 Cyber Strategy Summary

-DOD 9/12/23

- The DOD released an unclassified summary of the 2023 cyber strategy [1]
- This 4th iteration builds upon prior work including:
  - 2022 National Security Strategy
  - 2022 National Defense Strategy
  - 2022 National Cybersecurity Strategy
- Sets priorities and associated funding
- Informed by many years of cybersecurity operations, including lessons learned from the Russia-Ukraine war
- Need to work closely with allies, partners, and industry
- Ensure correct cyber capabilities, security, and resilience
- This iteration increases our "collective cyber resilience by building the cyber capability of allies and partners." [1]

The 2023 Cyber Strategy Summary

- An unclassified summary that "establishes how the Department will operate in and through cyberspace to protect the American people and advance the defense priorities of the United States. It implements the priorities of the 2022 National Security Strategy, 2022 National Defense Strategy (NDS), and 2023 National Cybersecurity Strategy. It builds upon and supersedes the 2018 DoD Cyber Strategy." [2]

- The United States depends upon the Internet as a critical infrastructure directly related to national security and well-being of our country.

- "The United States is challenged by malicious cyber actors who seek to exploit our technological vulnerabilities and undermine our military's competitive edge. They target our critical infrastructure and endanger the American people. Defending against and defeating these cyber threats is a Department of Defense (DoD) imperative." [2]

- "The Internet now forms the connective tissue for two thirds of the world's population. It is also under attack by those who seek to undermine a secure and open cyberspace and threaten the security of the United States. The Department will defend the interests of the United States and protect the shared digital environment. We will defend forward, disrupting and degrading malicious cyber actors, and help ensure the resilience of the homeland with all tools at our disposal. We will use cyberspace to fight and win the Nation's wars, supporting and advancing the objectives of the Joint Force. "[2]

2023 Cyber Strategy – 4 Lines of Effort

- “1. **Defend the Nation.** The Department will campaign in and through cyberspace to generate insights about cyber threats. We will defend forward, disrupting and degrading malicious cyber actors' capabilities and supporting ecosystems. The Department will work with its interagency partners to leverage available authorities to enable the defense of U.S. critical infrastructure and counter threats to military readiness.

- 2. **Prepare to Fight and Win the Nation's Wars.** The Department will campaign in and through cyberspace to advance Joint Force objectives. We will ensure the cybersecurity of the Department of Defense Information Network (DODIN) and conduct defensive cyberspace operations in order to protect it. The Department will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace. We will utilize the unique characteristics of cyberspace to meet the Joint Force's requirements and generate asymmetric advantages

- 3. **Protect the Cyber Domain with Allies and Partners**. Our global Allies and partners represent a foundational strategic advantage for the United States. We will build the capacity and capability of U.S. Allies and partners in cyberspace and expand avenues of potential cyber cooperation. We will continue hunt forward operations and other bilateral technical collaboration, working with Allies and partners to illuminate malicious cyber activity on their networks. We will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.

- 4. **Build Enduring Advantages in Cyberspace.** The Department will pursue institutional reforms to build advantages that will persist for decades to come. We will optimize the organizing, training, and equipping of the Cyberspace Operations Forces and Service-retained cyber forces. We will ensure the availability of timely and actionable intelligence in support of cyberspace operations and explore the intersection of emerging technologies and cyber capabilities. We will foster a culture of cybersecurity and cyber awareness, investing in the education, training, and knowledge development of personnel across the defense enterprise.“ [2]

State and Non-state Actors

- People's Republic of China
- Russia
- North Korea, Iran, and Violent Extremist Organizations
- Transnational Criminal Organizations

Key Points

Priority is to defend the nation – identify and mitigate threats before they can harm the American people

Generate insights about cyber threats

Disrupt and degrade malicious cyber actors

Enable defense of US critical infrastructure

Protect the defense industrial base

Advance joint force objectives

Defend the DOD Information Network (DODIN)

Key Points

Build cyber resilience in the Joint Force

Support Joint Force plans and operations

Build cyber capacity and develop capabilities and allies and partners

Expand avenues of cyber cooperation

Continue hunt forward operations and bilateral technical collaboration

Reinforce norms of responsible behavior in cyberspace

Invest in the cyber workforce

Key Points

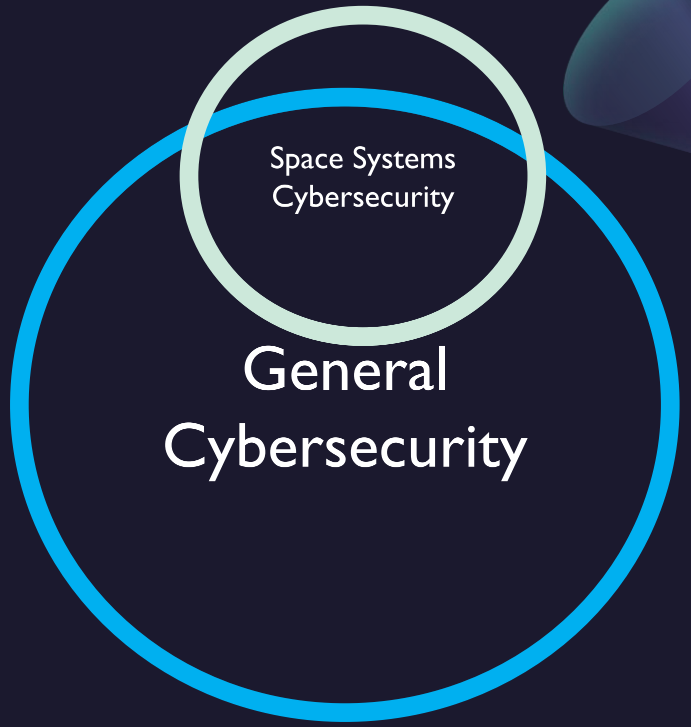
Prioritize intelligence support for cyber operations

Develop and implement new cyber capabilities

Foster cyber awareness

Importance to Space Systems Security

- The DOD recognizes how important cybersecurity is and has been refining its strategy over several years
- Defense of the United States has a dependency upon cyberspace
- The general U.S. cybersecurity is a superset of space cyber
- ~90% of space systems attacks target the ground attack surface so this is directly related
- Some of the direct attacks to the spacecraft (i.e., not through the ground system) may need special consideration



Space Systems Cybersecurity

General Cybersecurity

References

[1] Department of Defense (DOD). (2023). DOD Releases 2023 Cyber Strategy. Retrieved from web 9/16/23 from URL: https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/

[2] United States Department of Defense (2023). DOD Summary 2023 Cyber Strategy of The Department of Defense. Retrieved from web 9/16/23 from URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF