



ACQUISITION

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

CLEARED
For Open Publication
Feb 24, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

February 26, 2025

**Maryland General Assembly
House Environment and Transportation Committee
251 Taylor House Office Building
Annapolis, Maryland 21401
Delegate Marc Korman, Chair**

**House Health and Government Operations Committee
241 Taylor House Office Building
Annapolis, Maryland 21401
Delegate Joseline A. Peña-Melnyk, Chair**

**Remarks of
Mr. John Garstka
Director, Cyber Warfare
United States Department of Defense**

Support of: House Bill 1062 – Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments

Testimony

Chairman Korman, Chairperson Peña-Melnyk, and honorable committee members, the Department of Defense is grateful for the opportunity to support the policies reflected in House Bill 1062.

The Office of the Director of National Intelligence (ODNI), in their 2024 Annual Threat Assessment, highlighted the cyber threat to commercial critical infrastructure posed by China and Russia.¹ (See Figure 1). This document states:

“China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks.”

“If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets.

Furthermore, this threat assessment states:

“Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war.”

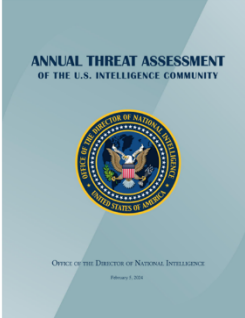
¹ [2024 Annual Threat Assessment of the U.S. Intelligence Community](#)

“Russia maintains its ability to target critical infrastructure, including under water cables and industrial control systems, in the United States as well as in allied and partner nations.

(U) People's Republic of China

- (U) "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."
- (U) "Beijing's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States..."
- (U) "If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets."

GRAPHIC IS UNCLASSIFIED



Reference: ODNI Annual Threat Assessment of the USIC 2024

GRAPHIC IS UNCLASSIFIED

(U) Russia

- (U) "Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war."
- (U) "Moscow views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets."
- (U) "Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries."

Figure 1. The Cyber Threat is a Clear and Present Danger, 1 of 2

Furthermore, the ODNI released in June of 2024 specific information on cyber attacks on commercial critical infrastructure that took place over a five month period.² A third of these attacks by malicious cyber actors were on water and wastewater management, as portrayed in Figure 2. The key take away is that there are a range of malicious cyber actors with the capability and intent to degrade commercial critical infrastructure in the United States. Consequently, the new reality is that commercial critical infrastructure providers need to be capable of operating in a contested cyberspace environment.

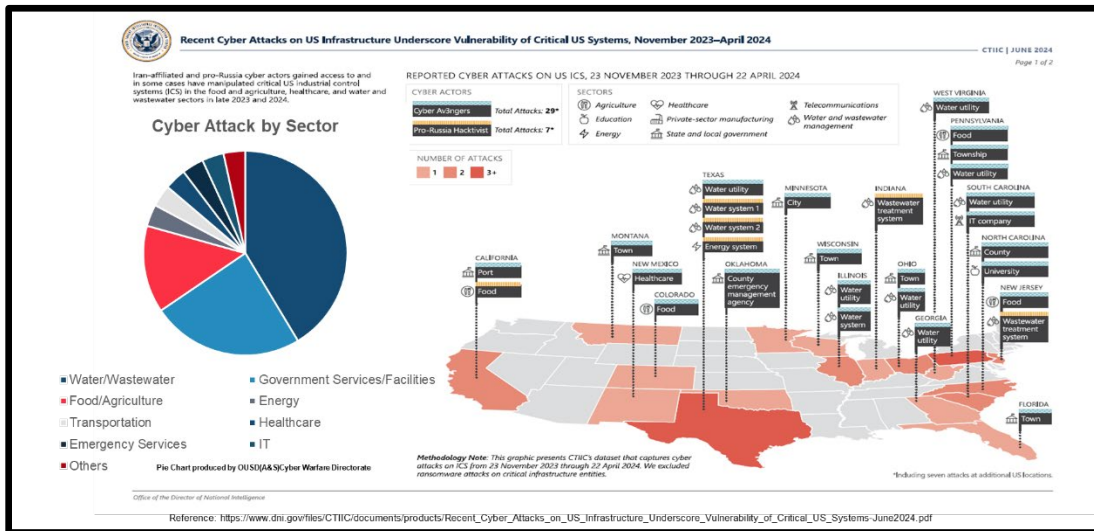


Figure 2. The Cyber Threat is a Clear and Present Danger, 2 of 2

²https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

The Department of Defense is dependent upon commercial critical infrastructure to develop capabilities for the Joint Force and to conduct military operations. This relationship is portrayed in the mission stack, as portrayed in Figure 3.

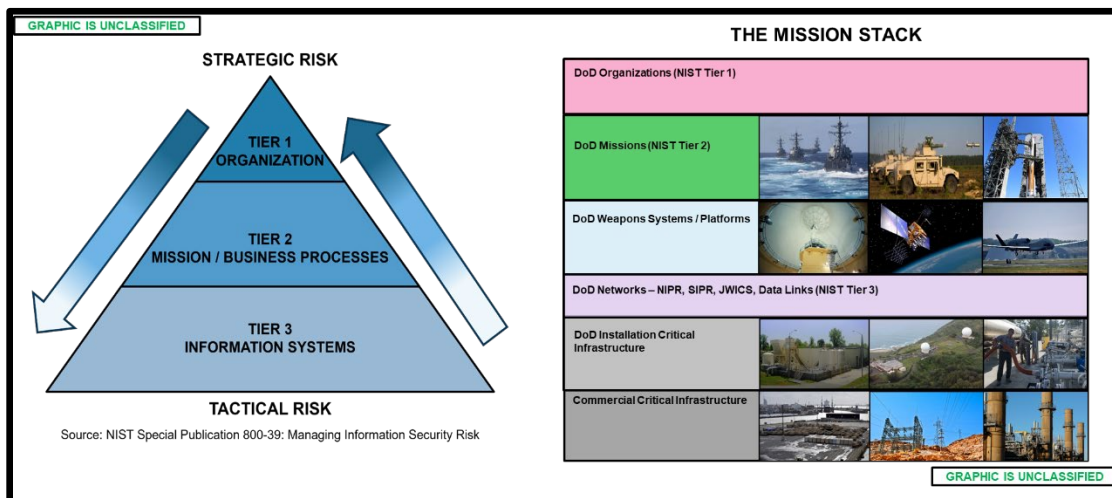


Figure 3. The Mission Stack

National Security Memorandum 22 and DoD policy guidance have highlighted the importance of securing commercial critical infrastructure upon which the Department of Defense and other Federal Agencies depend on to conduct their missions³.

Specifically, DoD’s guidance has highlighted the importance of working with State and Local governments to help bolster the cybersecurity of commercial critical infrastructure supporting DoD’s ability to conduct its mission.

The newly appointed Secretary of Defense highlighted as one his three priorities “Restoring Deterrence.” In the current threat environment, **Cybersecurity is a key element of Deterrence.**

The Department in its Fiscal Year 2024 budget allocated over \$250M to cyber harden installation critical infrastructure (e.g, water, fuel, power) on DoD installations that support priority DoD missions. Additionally, the Department has recently developed an increased understanding of the challenges that small and medium sized businesses face in improving their cybersecurity posture. We are applying this insight to explore options for bending the cybersecurity cost curve to help companies that the Department is dependent upon improve their cybersecurity posture.

³ National Security Memorandum 22: National Security Memorandum on Critical Infrastructure Security and Resilience, April 2024.

There is an emerging understanding that the Department must play a role in cyber hardening priority commercial critical infrastructure that the DoD depends on to conduct its missions. To accomplish this objective, DoD needs to work closely with State and Local governments. The state of Maryland hosts, at least, 9 major military installations that support a range of important DoD missions. All of these DoD installations are dependent upon water provided by the commercial providers in the State of Maryland (See Figure 4).

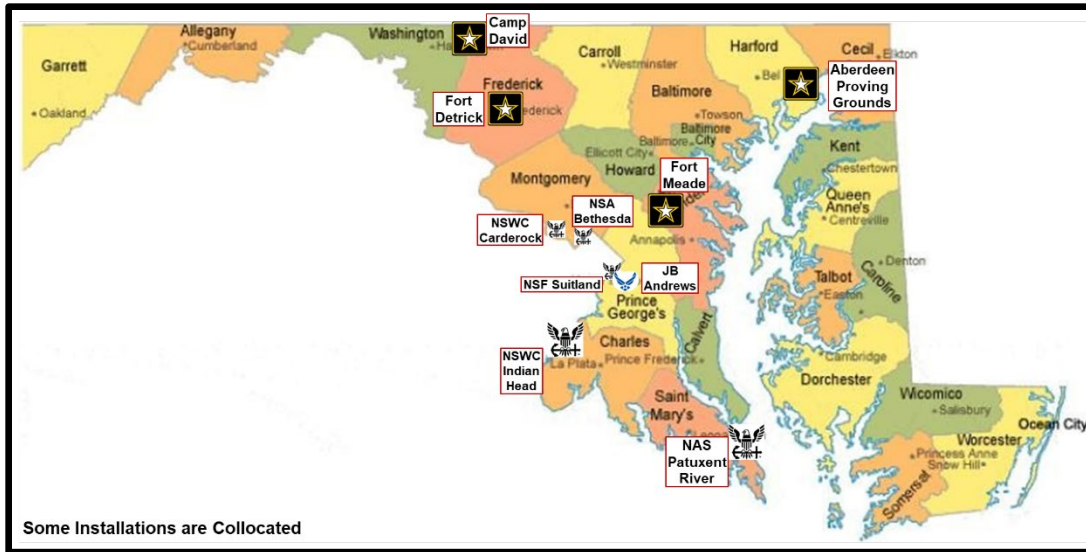


Figure 4. Major Military Installations in Maryland (not all inclusive)

The legislation being proposed by Senator Hester in House Bill 1062 will enhance the cybersecurity posture of water providers and enhance the ability of state of Maryland to operate in a contested cyberspace environment. This legislation will improve the safety and availability of the water supply for residents of the State of Maryland and help secure the water supply that DoD installations depend on. This legislation will improve the overall cybersecurity posture of the State of Maryland and in doing so will contribute in a meaningful way to National Security.

Yours etc.,

John J. Garstka
Director, Cyber Warfare