Q&A Executive Viewpoint A conversation with MORGAN ADAMSKI

MORGAN ADAMSKI
Chief of the Cybersecurity Collaboration Center, National Security Agency

This conversation is adapted from a presentation at an FCW event.

Proactive partnerships to protect critical systems

The Cybersecurity Collaboration Center came together with a clear vision: to develop robust, open and collaborative relationships with industry, government and academia to prevent and eradicate threats to national security systems (NSS), the Defense Department and the defense industrial base (DIB).

The center was created for the express purpose of enabling NSA to work with those sectors in an unclassified environment. Think about that: I just said "NSA" and "an unclassified environment" in the same sentence. This is huge for us. This is evolving our mission, and we know it's something we must do in order to be at the forefront of enabling the critical cybersecurity change that needs to happen in the U.S.

In particular, we partner with cybersecurity companies to better understand vulnerabilities to critical systems and jointly develop mitigation guidance to protect against the most sophisticated threats.

Constant analytical exchange with our industry partners helps us build a more complete picture of the ever-evolving cyberthreats in real time. These conversations need to be happening every day, not just in times of crisis.

The direct connection of experts on both sides yields incredible results. It is not transactional information sharing. It is a conversation about what we are seeing, what we don't understand and who else has the pieces of the puzzle to help us build that comprehensive picture.

There is no silver bullet in cybersecurity. Rather, it takes a layered defense and proactive collaboration to prevent threats against critical systems.

Providing actionable mitigation guidance

No one entity has complete visibility into malicious activity across all systems, software development, cloud environments and network traffic. Each person from industry, government and academia brings a unique perspective to the table, and today's evolving threat landscape requires a whole-of-community effort to defend against those cyberthreats.

Having a more comprehensive threat picture helps us create advisories and mitigations that we share with DOD, the DIB, cybersecurity analysts and network defenders in real time.

DOD recently delegated to NSA the authority to expand its information-sharing capabilities to directly engage with the DIB and its service providers. This delegation encompasses DIB members themselves as well as the technology and cybersecurity providers that support them.

The DIB consists of hundreds of thousands of technology, manufacturing and service companies around the world that work with DOD to design, develop and produce critical systems, platforms and technologies required to defend the nation. Data companies often store critical national security information on their privately owned networks and have a wide range of cyber defense postures and capabilities, from excellent to non-existent. Those systems are constantly targeted by foreign adversaries to steal information and valuable intellectual property, giving a strategic advantage to our adversaries and competitors.

NSA's engagement with these authorized cybersecurity partners is focused on the exchange of information that is critical to discover foreign adversaries who pose a threat to these networks and to provide

> **There is no silver bullet in cybersecurity.** Rather, it takes a layered defense and proactive collaboration to prevent threats against critical systems.

actionable mitigation guidance about that activity and critical vulnerabilities by sharing advisory standards and indicators of compromise. Importantly, threat information between NSA and cybersecurity partners is focused on partner-generated threat assessments and indicators of compromise.

In addition, we often collaborate with the Cybersecurity and Infrastructure Security Agency (CISA), which secures all the classified .gov sites and is responsible for big portions of domestic critical infrastructure. As federal partners, we work together to form solutions because we have found that foreign adversaries use the same tactics, techniques and procedures to target all those sectors.

By sharing this information across federal agencies and industry partners, we're jointly developing mitigation and tradecraft, and we're building a stronger defense. Staying ahead of adversaries requires innovation, though. Our adversaries constantly adapt to gain access to our networks and evade detection. This calls for continuous collaboration on our part.

The threats to our nation's security are pervasive. China has used a staggering degree of intellectual property to build its economy and military with global ambitions. Russia has waged an information war often by using U.S. infrastructure and technologies to sow and amplify divisions in society with an ultimate goal of eroding trust in democratic institutions. Iran is a volatile threat and has attacked the U.S. and our allies either directly or via proxies. Meanwhile, North Korea uses cyber operations most notably to steal money to fund its weapons development programs.

Our adversaries exploit gaps and seams between government organizations and authorities. They're able to gain and maintain access in a manner that mitigates detection or response. We have to improve our collective understanding of how actors manipulate trust and leverage other techniques to achieve their objectives.

Cybersecurity standards for commercial technology

The Cybersecurity Collaboration Center is actively working on appropriate mechanisms to share more threat information that others can use to defend their networks. In addition to tracking adversaries, we're working on initiatives that will improve the digital ecosystem and ensure our collective security. And we're working with the private sector to detect and counter malicious activity directed at the private sector.

We've released more than 40 cybersecurity products and guidance to support our NSS, DOD and DIB customers. We have also released several joint advisories with the U.K.'s National Cyber Security Centre, CISA and the FBI to publicly call out our adversaries so they know that we know what they're doing. We're also partnering with CISA and the FBI to release an advisory on Chinese state-sponsored actions with mitigation guidance to defend against more than 50 tactics, techniques and procedures used by those cyber actors when targeting critical infrastructure in the U.S. and among our allies.

As a community, sharing information, actively patching and making sure your systems are updated regularly continue to be the most effective ways to remediate current and potential threats. When we do those simple things, we make it harder for the adversaries. There is also a long game to be played, and we can't lose sight of it.

As technology advances, NSA has an interest in the security of commercial products used to protect NSS, critical infrastructure, weapons systems and the DIB.

Within the Cybersecurity Collaboration Center, the Center for Cybersecurity Standards amplifies NSA's ability to prevent threats by partnering with vendors to ensure cybersecurity standards are baked into the development of the commercial products on which we all rely.

Currently, we are focusing on preventing adversaries from exploiting 5G networks, automating security in U.S. government and DIB cloud interfaces and underlying network architectures, and developing cryptographic standards that will satisfy current requirements, support future environments and protect against emerging threats.

Standards cannot be developed in a vacuum, though. The Center for Cybersecurity Standards relies on partnerships with the National Institute of Standards and Technology and with industry to build security into those products and standards.

It's through this kind of public/private collaboration that we continue to make it increasingly difficult for our adversaries to traverse across systems, software, cloud environments or network traffic, and keep our nation safer.

Cybersecurity is multidimensional. We can't afford to just share information. We are all targeted at different angles, and we must defend from all angles. ■