CyberEdBoard Talks

Public/Private Partnership: How to Engage With the NSA's Cybersecurity Collaboration Center

A Conversation With the Center's Chief, Morgan Adamski

CyberEdBoard Talks Excerpt
Access the full interview by becoming a member.
Visit CyberEdBoard.io to submit your application.

CyberEdBoard

Morgan Adamski
Chief, NSA Cybersecurity Collaboration Center

The CyberEdBoard Talks series is designed to address the most critical challenges executive members are discussing in the private global ecosystem and is presented by respected industry experts and chief cybersecurity practitioners.

One of the unique benefits of CyberEdBoard is that you must be a member to access this session and all other content and engagement opportunities. "The global community continues to grow at a pace that reconfirms the critical importance of cybersecurity collaboration and executive information sharing, and we are thrilled to support each member's unique needs within the private ecosystem," said CyberEdBoard Executive Director Chris Ancharski.

This edition of the CyberEdBoard Talks series was held on Sept. 22, 2021, exclusively for CyberEdBoard members.

At a time when nation-state cybersecurity threats to the U.S. are more sophisticated and relentless than ever, the concept of partnership between the public and private sectors is paramount. The NSA Cybersecurity Collaboration Center was built to focus on co-creating cybersecurity tradecraft through collaborations with industry to change the way we secure the nation.

In this exclusive CyberEdBoard Talks session, Tom Field, senior vice president of editorial at ISMG, and Morgan Adamski, chief of the Cybersecurity Collaboration Center, discuss:

- Detection: How the center is fostering better and more proactive information sharing about adversaries and threats;
- Innovation: New ways to discover and track adversaries;
- Mitigation: The joint development of mitigation guidance to protect against threats.

As the chief of the NSA Cybersecurity Collaboration Center, Adamski leads complex and groundbreaking initiatives for NSA Cybersecurity. Most recently, as the deputy strategic mission manager, she led efforts to build bidirectional analytical relationships with private sector partners that provide cybersecurity services to the Defense Industrial Base. She has been at the forefront of the NSA Computer Network Defense, Computer Network Exploitation, and Cyber Analysis missions for over a decade. She holds an M.S. degree in Strategic Intelligence from Mercyhurst University and a B.A. degree in Peace, War, and Defense with a specialization in National Security from the University of North Carolina-Chapel Hill.

Visit cybercenter.nsa.gov to learn more, and contact us if you are interested in partnering with the center.

The ‘Four Big Threats’

TOM FIELD: What are the threats that concern you the most today?

MORGAN ADAMSKI: There are four big threats: Russia, China, Iran and North Korea. Russia focuses a majority of its efforts on the information, misinformation, disinformation warfare campaign. They see the value in that, because of the crowdsourcing of our use of social media, and we closely track that. China has always had a huge thumb on intellectual property theft. That concerns us because if U.S. taxpayers spend a significant amount of money funding and supporting the development of U.S. military technology, so that we have a competitive advantage, they don’t want the Chinese to steal the plan and not have to invest money into those development opportunities. So we need to better protect our intellectual property.

Iran is a volatile threat. It has destructive capabilities and a willingness to leverage them. We can’t always predict what the collateral damage and third-order effects of those operations will be, so we have to better understand the capabilities of our adversaries in Iran. Then we can better protect against them. North Korea is looking at cryptocurrency and how to fund its weapons development efforts. So taking advantage of cryptocurrency, using ransomware and stealing money come into play when we look at North Korea.

Supporting Our Allies

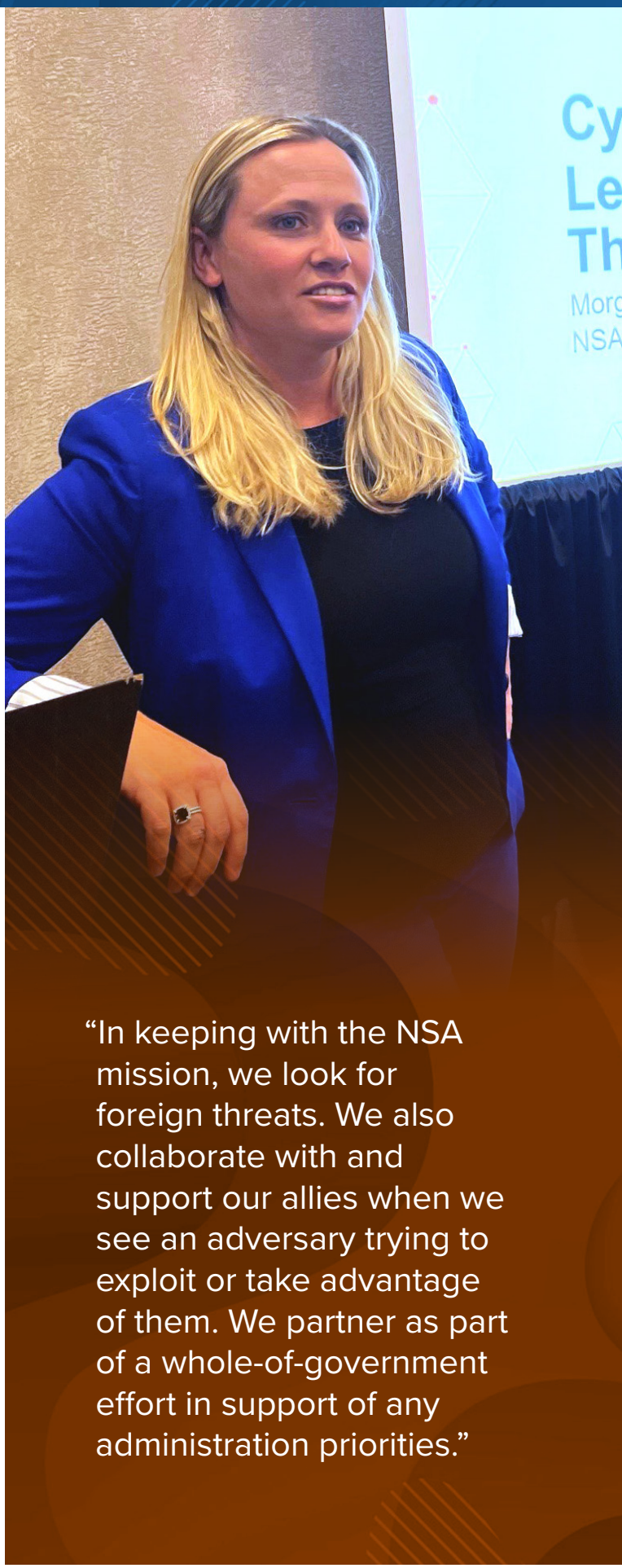
AGNIDIPTA SARKAR (*Group CISO at Biocon Limited*): Do current political international events, such as the situation in Afghanistan and the recent elections in Canada, get on your radar?

ADAMSKI: In keeping with the NSA mission, we look for foreign threats. We also collaborate with and support our allies when we see an adversary trying to exploit or take advantage of them. We partner as part of a whole-of-government effort in support of any administration priorities. As a combat support agency, the NSA secures and protects the communications with the war fighters. One of the key things that keeps me at NSA is wanting to ensure that we bring those war fighters home. To be able to do that, we have to secure the networks and the communications that they leverage to maneuver through those regions.

Defensive Vulnerabilities

FIELD: A lot of defensive vulnerabilities have had a high profile this year, particularly in terms of critical infrastructure. Which ones concern you the most?

ADAMSKI: When we talk about defensive vulnerabilities here at the Collaboration Center, we’re very much concerned about our adversary taking advantage of vulnerabilities in the Defense Industrial Base, which is critical to the Department of Defense. The DIB is massive; it ranges from small to medium to large-sized companies. The large companies have a significant amount of sustenance, capability, insight and knowledge about how to protect



“In keeping with the NSA mission, we look for foreign threats. We also collaborate with and support our allies when we see an adversary trying to exploit or take advantage of them. We partner as part of a whole-of-government effort in support of any administration priorities.”

"We want to interact with internet service providers and cloud providers who have significant market share and are providing capabilities to the Defense Industrial Base national security systems. We want to block threat activity at the layer above the customer layer and stop the attackers before they get to the customers."

themselves against the threats that target them every day, but we worry about the small and medium-sized DIB companies, which don't necessarily have those capabilities and insights. They're still figuring out the right type of cybersecurity services to have in place to better protect them.

At the Collaboration Center, we figure out how to protect against the very sophisticated threats that are targeting the big data companies and also protect the small and medium-sized companies that we know our adversaries are actively exploiting because they see it as a way to get into the supply chain. As we integrate more technology, collaboration platforms, and ways to move data quickly, we have to figure out the key vulnerabilities and how to set up all those networks.

The Center for Cybersecurity Standards

PATRICK ANGEL (*VP/CISO at Cleveland Clinic Foundation*): I've been working with a group to build a secure voting technology. We're developing the system now, and my question is: What government organization should I work with to roll this out properly and make sure that it gets the government review that's needed?

ADAMSKI: NIST puts out a significant amount of standards and information related to network configuration and guidance that should likely be followed. The Collaboration Center does not give stamps of approval. We provide guidance and insight based on our technical expertise.

But the Collaboration Center is also home to the Center for Cybersecurity Standards, which focuses on technology applications and capabilities that will be used in significant government networks in the future. It can help point you in the right direction, but start with NIST.

The Collaboration Center and the FBI

FIELD: One of the attendees says, "Many of us are already relying on and collaborating with the FBI's InfraGard portal," and asks, "How do you overlap or interact with InfraGard?"

ADAMSKI: We work significantly with our FBI counterparts to ensure that we are sharing both timely information that can be applicable to their field offices to share with their partners as well as creating products that contain mitigation guidance. A lot of our indicators of compromise feed into those FBI portals, and that information may be helpful to determine if something malicious is happening in your network. That's a great first step. If you have something malicious, you need to ask: What do I need to better secure my network? Do I have any insights on the malicious activity that may help the Intelligence Community or the Department of Defense better understand what the adversary is trying to accomplish?

Tracking Adversaries

FIELD: How you creating new ways to discover and track adversaries?

ADAMSKI: We have a very robust signature development effort that enables us to share tradecraft information was internet service providers and cloud providers. That tradecraft is directly applicable to our industry counterparts, because they need to be able to leverage those signatures on their own apertures and networks to better understand the pattern of activity they're seeing across their networks. We want to interact with internet service providers and cloud providers who have significant market share and are providing capabilities to the Defense Industrial Base national security systems. We want to block threat activity at the layer above the customer layer and stop the attackers before they get to the customers.

Mitigation Guidance

FIELD: What is some of the joint development and mitigation guidance that you're involved with?

ADAMSKI: We have released 40 products over the last year and a half. We recently released our cybersecurity advisories on the password spraying that we're seeing from our Russian adversaries. A lot of industry partners see this password spraying on a daily basis. We released cybersecurity information sheets that focus on the top vulnerabilities and also our advisory on the top 25 CVEs that we know the Chinese actively exploit.

Insider Threat

FIELD: We've had some high-profile insider cases in the U.S. government over the past decade. What lessons have we learned from those incidents, and what recommendations do you have going forward to prevent occurrences, not just within government, but within the private sector as well?

> "Cyber happens at lightning speed. Very rarely do we have a comprehensive picture. It's going to take a persistent effort to continually evolve how these private and public sector relationships should exist and progress going forward."

ADAMSKI: Learn, adapt, move forward and constantly assess. Our adversaries will continue to target the things we care the most about. It does not matter how many times we kick them out or how many things we put in front of them – if they really care about the information, they will find a way to get it. We have to constantly assess what's happening, what lessons we've learned, what we did and what we need to do differently. We have to assess our mitigations every once in a while to ensure they are working and don't reduce the functionality that we need to be able to operate on missions.

Public and Private Sector Partnerships

FIELD: Where do you see potential speed bumps on the road to a successful partnership between private and public sector entities?

ADAMSKI: There are speed bumps when we don't give each other a little bit of grace in this space. The NSA has been trying to be very forward-leaning in the last nine months or so, but we're still constrained by authorities, policy, and how and where we share information. We're trying to do the best we can, as quickly as possible, and we are very open to feedback on what is working and what is not. Cyber happens at lightning speed. Very rarely do we have a comprehensive picture. It's going to take a persistent effort to continually evolve how these private and public sector relationships should exist and progress going forward.

Breakdowns in Collaboration

ADAMSKI: I'd like to ask the group about the fundamental breakdowns that you see in a collaboration between the public and private sectors.

REBECCA WYNN (*Global CISO and Chief Privacy Officer, [24]7.ai*): A lot of times when we do share things with the NSA or the FBI, it goes into a black hole and we don't get closure on it. Getting even an email saying, "That was beneficial to other people," or "You made a positive impact on the world" would help.

ADAMSKI: I completely agree. Feedback is critical to the conversation, and it also helps NSA analysts learn what is helpful for industry and what is not.

Discussion Takeaways

FIELD: What can our attendees take away from this discussion and act upon to move the ball forward?

ADAMSKI: First and foremost, I would encourage all of the attendees to think about partnering with the U.S. government in any capacity on the cyberthreats they're seeing. Building a comprehensive picture together of what's happening is the only way we're going to be able to counter these threats at scale and stay to the left of them. Secondly, I encourage you to read up on what we're trying to accomplish here at the Cybersecurity Collaboration Center and if you're willing to partner with us, contact us. Lastly, look at the cybersecurity advisories that the government is pushing out. They contain a lot of good information that we're trying to get out to the larger community. ■

The full transcript and recording are available for members within the CyberEdBoard engagement platform. Visit CyberEdBoard.io to submit your application.

About ISMG

Information Security Media Group (ISMG) is an intelligence and education firm focused exclusively on cybersecurity. Our 30 global media properties provide security professionals and senior decision-makers with industry- and geo-specific news, research and educational events.

CyberEdBoard Talks Excerpt

Access the full interview by becoming a member.
Visit CyberEdBoard.io to submit your application.

CyberEdBoard

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io