Our People – The most powerful weapon in cyber war.

We’re uniquely qualified to train our military in full-spectrum cyber. With unrivaled experience. Proven expertise.

Learn more at ManTech.com
LETTER FROM THE EDITOR

CYBERCON 2020

The key to attack is the element of surprise.

As we find ourselves less than a week from the presidential election, there is no surprise. Nation-state actors and other countries are going to try to attack. It likely won’t happen kinetically, but through cyber means. We know this because intelligence and government officials have said it for four years. And their preferred means is through cyber and disinformation.

Think about that. Think about how unusual of a situation it is in military history that leaders know when and pretty much how the enemy may attack.

But the question now is whether – during a global pandemic and economic uncertainty – the strategy and defenses and billions of dollars of improvements will make a difference. The question is if the new cybersecurity systems and strategies are up to the test. It’s a nearly unprecedented occasion and a fascinating backdrop for this year’s C4ISRNET Cybercon.

I expect today Defense Department leaders will reiterate the importance of the right protections and the right tools and the right cadence of operations for the short term but more importantly, they will discuss how they’re prepared for future conflicts.

Today, we’re going to explore many of the areas the Department of Defense and militaries worldwide need to fortify their systems.

We will look at what industry – and the entire defense supply chain – needs to do to better protect their systems.

We will explore the future tools that cyber operators and IT leaders will need.

We will discuss the new norms in cyberspace and how the international community is figuring out exactly what is acceptable behavior – and what is not.

We will talk about how all of the telework associated with the ongoing pandemic has appeared to create a new threat vector for the service.

And we will hear from military leaders about the role cyber plays in the information warfare space. In all of these discussions, I expect we’ll hear about surprise. (Not so much about the election, but a good amount on surprise.)

Think about telework alone. A year ago, none of us could have expected the situation the Pentagon finds itself in today.

But surprise is just part of the equation. Reacting to surprise may be more important.

Thank you for joining us.

Mike Gruss
Executive Editor,
C4ISRNET and Defense News
The power to do great things.

Transforming IT and cybersecurity

Our team of cyber experts have a proven track record of delivering agile, game-changing cyber solutions. These solutions and services ensure an adaptive defense strategy, offensive threat protection, and a resilient security posture. Let us provide you the power to perform at your best.

leidos.com/on-a-mission/security
8:15AM – 8:19AM  WELCOME REMARKS
Mike Gruss, Executive Editor, C4ISRNET & Defense News

8:19AM – 8:27AM  INDUSTRY FIRESIDE CHAT
Mark Schaad, Director of System Architecture, ManTech

8:27AM – 8:30AM  BREAK

8:30AM – 8:43AM  THE NEXT GENERATION OF CYBER TOOLS, PART 1
The Department of Defense is experimenting with a series of technologies to improve its cybersecurity and to be more effective in cyber operations. For example, the DOD is working closely with the NSA to improve its information assurance program and the services have embarked on a zero-trust mantra for hardware. In this panel, we will discuss the tools, prototypes and strategies the Pentagon is using to keep information safe.

Troy Lange, Chief of Encryption Production and Solutions, NSA
Moderator: Andrew Eversden, Reporter, C4ISRNET

8:30AM – 8:45AM  BREAK

8:45AM – 8:57AM  THE NEXT GENERATION OF CYBER TOOLS, PART 2
The Department of Defense is experimenting with a series of technologies to improve its cybersecurity and to be more effective in cyber operations. Often, cyber operators have a large number of tools they need to use to provide the right capability, but some instruments are not particularly intuitive. During this panel, we will discuss what cyber operators need most to be effective at their job. We focus on what they need before talking anything about the technology.

Col. William Waynick, Director, Air Force Cyberworx
Moderator: Andrew Eversden, Reporter, C4ISRNET

8:57AM – 9:00AM  BREAK

9:00AM – 9:25AM  KEYNOTE FIRESIDE CHAT
John Sherman, Principal Deputy Chief Information Officer, Department of Defense

9:25AM – 9:28AM  BREAK

9:28AM – 9:36AM  INDUSTRY FIRESIDE CHAT
Brett Barraclough, Vice President, Cyber and Information Solutions, Defense Sector, ManTech

9:36AM – 9:39AM  BREAK

9:39 AM – 10:14 AM  MAKING CYBER TRAINING WORK
U.S. Cyber Command’s annual training exercise took place entirely on a new platform this year, a move that will allow most participants to compete remotely. DoD’s cyber warriors have not had a robust environment to train or practice in, creating readiness gaps. But that’s changing. In this panel we will talk about the TRIDENT and Persistent Cyber Training Environment programs as well as other potential avenues the Department of Defense can use to improve its training before going into cyber operations.

Lt. Col. Thomas Monaghan, Program Manager, PCTE
Elizabeth Bledsoe, Deputy Program Manager, PCTE
Moderator: Mark Pomerleau, Reporter, C4ISRNET

10:14AM – 10:20AM  BREAK
Cyber threats surround you.
Is your agency prepared?

Be proactive in your approach to cybersecurity.

With cyber threats all around, government agencies need teamwork, innovation and persistence. KPMG provides these capabilities and offers insight on cybersecurity programs, technologies, and standards. We help agencies manage cybersecurity risks and strengthen their abilities to identify, protect, detect, respond, and recover. Learn more at kpmg.com/us/federalcyber

Anticipate tomorrow. Deliver today.
The coronavirus pandemic means unprecedented numbers of Defense Department employees are working from home. The move has been successful enough that several senior Pentagon leaders have said they expect this to be the new normal and that telework will become a greater part of the work week. But telework also presents cyber challenges and nation state actors are already targeting government employees who may have lax cyber hygiene. On this panel, we will explore the challenges that come from working at home and how the Pentagon can better protect itself.

Maj. Gen. Maria Barrett, Commanding General, NETCOM
Chris Cleary, Chief Information Security Officer, U.S. Navy
Katie Olson, Deputy Director, Defense Digital Service
Moderator: Andrew Eversden, Reporter, C4ISRNET

Each of the services are reorganizing their staff when it comes to information warfare. But how do cyber operations and cybersecurity factor into these decisions and what kind of changes will it mean for the warfighter?

Lt. Gen. Timothy Haugh, Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber
Moderator: Mark Pomerleau, Reporter, C4ISRNET

In February, nearly a dozen nations, including the United States, attributed a 2019 cyberattack on the country of Georgia to Russia’s military, a move that experts said was the most high-profile example yet of an effort to establish acceptable behavior in cyberspace. That event pointed to an unusually high level of cooperation that demonstrated several nation’s long-held desire to establish acceptable levels of behavior in cyberspace. Experts expect the trend to continue across the globe. On this panel, we will discuss why these norms are necessary, why the U.S. and other countries are following this path and what happens even if their “name and shame” technique fails to work.

Mogens Christoffersen, Deputy Head of the Department for Security and Cyber, Danish Ministry of Defense
Heli Tiirmaa Klaar, Estonian Ambassador at Large for Cyber Diplomacy
Moderator: Mark Pomerleau, Reporter, C4ISRNET
Elastic Security

Unified protection for everyone, built on the Elastic (ELK) Stack.

Endpoint Security
One agent, one click. Free and open anti-malware and data collection.

SIEM
Threat detection and response, available free to analysts everywhere.

ela.st/elasticsecurity
12:17PM - 12:25PM
INDUSTRY FIRESIDE CHAT

Arlette Hart, Sr. Technologist for Cybersecurity and Master Solution Architect, Leidos

12:25PM - 12:28PM
BREAK

12:28PM - 12:53PM
THE NEW NORMS IN THE NEW NORMAL, PART 2

The United States and other nations have turned to a “name and shame” technique to curb what they see as inappropriate cyber behavior. On this panel, we will discuss how Congress can help shape these norms, what members want to see in the future and how cyber operations may change in the future.

Congressman Jim Langevin (D-RI), chairman of the House Armed Services Committee’s Subcommittee on Intelligence and Emerging Threats and Capabilities
Moderator: Mark Pomerleau, Reporter, C4ISRNET

12:53PM - 12:55PM
BREAK

12:55PM - 1:03PM
INDUSTRY FIRESIDE CHAT

Bill Brennan, Vice President, Cyber Risk Management, Leidos

1:03AM - 1:06AM
BREAK

1:06PM - 1:30PM
OH SAY CAN YOU CMMC

The Cybersecurity Maturity Model Certification is a Pentagon program that would mitigate several cybersecurity issues that plague the DoD supply chain. Namely, the government would have a mechanism to verify contractors’ cybersecurity claims. The guidance recognizes that security differs from business to business while allowing the government insight into companies’ cyber posture before awarding contracts. What does the Pentagon expect from this program? What kind of obstacles are they running into? How can the DoD ensure this program is a success without bankrupting critical DoD suppliers? And how can the Pentagon ensure its supply chain is safe from backdoors? (Think: Huawei/5G)

Katie Arrington, Chief of Information Security for Acquisition, Department of Defense
Moderator: Andrew Eversden, Reporter, C4ISRNET

1:30AM - 1:33PM
CLOSING REMARKS
Protect the nation from a cyber attack, before lunch.

Do it again, before dinner.
JOHN SHERMAN
Principal Deputy Chief Information Officer, Department of Defense

CHRIS CLEARY
Chief Information Security Officer, U.S. Navy

CONGRESSMAN JIM LANGEVIN (D-RI)

LT. GEN. TIMOTHY HAUGH
Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber

MAJ. GEN. MARIA B. BARRETT
Commanding General, NETCOM

KATIE ARRINGTON
Chief of Information Security for Acquisition, Department of Defense

COL. WILLIAM WAYNICK
Director, Air Force Cyberworx

LT. COL. THOMAS MONAGHAN
Product Manager, Cyber Resiliency and Training, Army PEO STRI

MOGENS CHRISTOFFERSEN
Deputy Head of the Department for Security and Cyber, Danish Ministry of Defense

HELI TIIRMAA KLAAR
Estonian Ambassador at Large for Cyber Diplomacy

TROY LANGE
Chief of Encryption Production and Solutions, NSA

ELIZABETH BLEDSOE
Deputy Product Manager, Cyber Resiliency and Training, Army Program Executive Office Simulation, Training, and Instrumentation
The power to do great things

Reliable, resilient, and secure AI

AI and ML solutions turn data into new opportunities for insight and efficiency. We’re helping our customers gain immediate value across multiple domains. Let us provide you the power to perform at your best.

leidos.com/AI
EXPLORE GREAT CONTENT FROM OUR SPONSORS

START BROWSING
ManTech is the industry leader in offense-informed cyber for national security. As a trusted partner of the Department of Defense and the Intelligence Community, we deliver intelligent cyber solutions that preempt cyberattacks to ensure the safety and high performance of customers’ vital IT infrastructure and networks. Learn more at www.mantech.com

Leidos is a recognized leader in cybersecurity across the federal government, bringing more than a decade of experience defending cyber interests and delivering advanced capabilities honed from protecting some of the world’s most valuable assets. Our solutions ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture. Our diverse portfolio of solutions delivers superior-quality, high-technology products and services to solve the world’s toughest challenges. Learn more at www.leidos.com/onamission

For more than 100 years, KPMG LLP has assisted civilian, defense, and intelligence agencies. Today, we help these organizations adapt to new environments by working with them to transform their business models, leverage data, protect information assets, increase operational efficiencies, and ensure greater transparency while focusing on their mission. Learn more at read.kpmg.us/govcyber

Elastic is a search company that powers enterprise search, observability, and security solutions that arm our nation’s protectors with on-premises and SaaS offerings to evaluate data at scale and speed for mission analytics, performance metrics, monitoring, and log management. We deliver mission-essential support to diverse workloads, from monitoring geographically dispersed tactical systems or traditional IT systems to supporting cyber research analytics, geospatial analysis, and centralized reporting for real time situational awareness. Learn more at elastic.co/federal
Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations most critical data and IP, while driving digital transformation and growth. Rather than offering a static one-size fits all approach that stifles innovation and creates vulnerabilities, Forcepoint is humanly attuned to how people interact with data, providing secure access while enabling employees to create value. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of enterprise and government customers in more than 150 countries.

Your government agency is driven to make life better for citizens and ServiceNow is committed to making work, work better for people. Our cloud-based platform consolidates outdated IT systems, leverages data, and delivers automated, digital workflows that create great experiences for users.

Splunk turns data into doing with the Data-to-Everything Platform. All four branches of the U.S. Military and many agencies in the intelligence community already use Splunk to make confident decisions and take decisive action at mission speeds. Learn more at www.splunk.com/dod