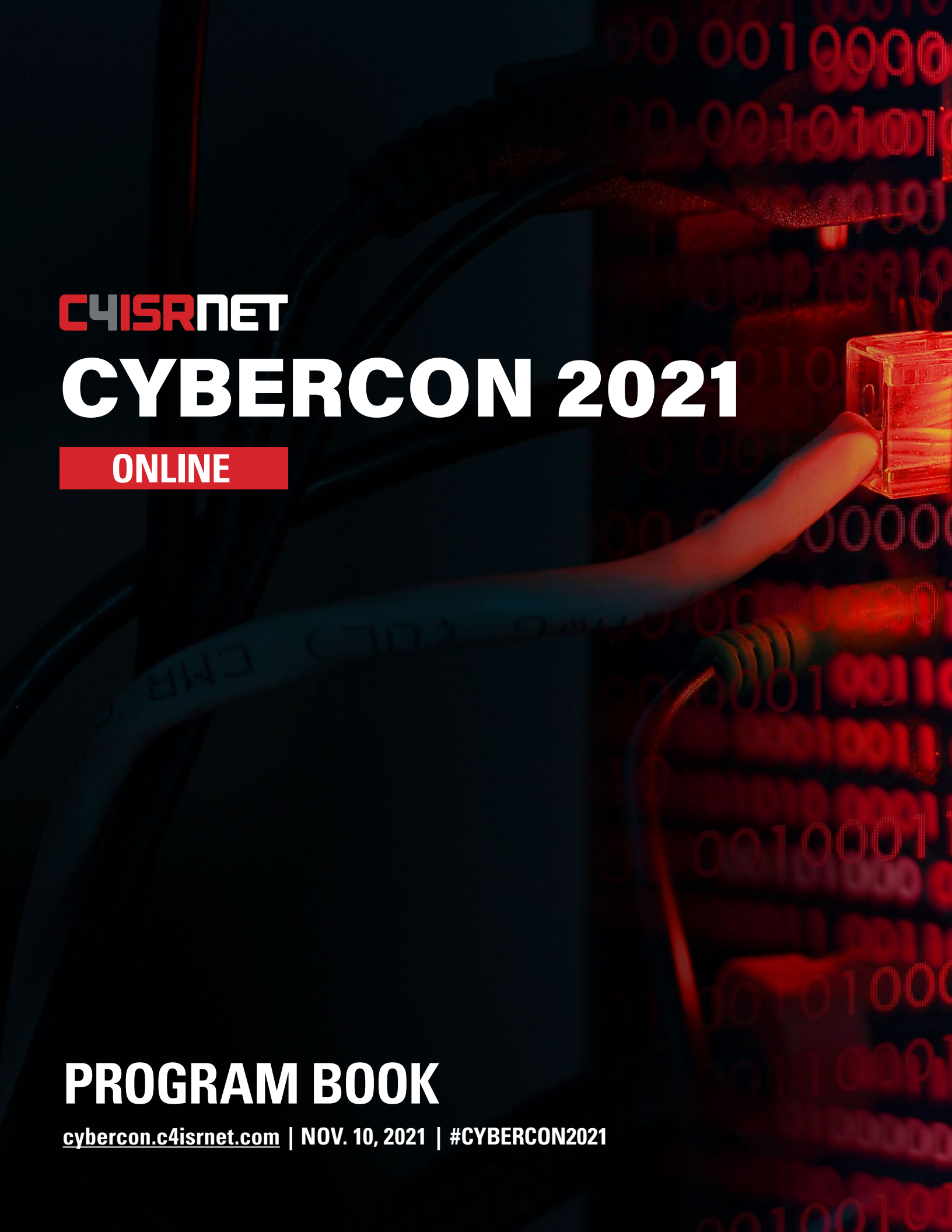


C4ISRNET

CYBERCON 2021

ONLINE

PROGRAM BOOK

cybercon.c4isrnet.com | NOV. 10, 2021 | #CYBERCON2021

Protect the nation from a cyber attack, before lunch.

Do it again, before dinner.

ManTech®

Securing the Future

CYBERCON 2021

Twenty months into this pandemic the rubric by which we measure and discuss cybersecurity has changed.

For example, in April 2020 when we held our first fully virtual event at C4ISRNET, concerns about Zoom loomed. Leaders from some military services were willing to use the video meeting software. Others were worried it wasn't secure enough. As a result, some of our speakers joined from personal computers or on their home Wi-Fi.

But, of course, the risk assessment evolved and now it can feel like we spend all day every day tethered to some kind of video conference meeting. Those concerns seem, not smaller or less sophisticated, but simpler.

This is the fundamental challenge of cybersecurity: the next threat always seems the most dangerous.

In the last 12 months, we've seen the continued acceleration of ransomware. The SolarWinds attack has wrought havoc on government contractors. And we're hearing about data protection from corners of the military that never talked about such topics but are certainly interested in it now.

In other words, the rubric for what's safe has changed.

Today, at CyberCon, we're going to talk about these changes.

We are sure to touch on the ubiquitous-ness of information warfare. We will explore the need for software factories in an era of ever-iterating threats. We will explain the emergence of tactical cyber teams and we will discuss the idea of zero trust, which can feel like a way of living, but has become a fully embraced philosophy for cyber safety.

Too often, when cybersecurity is discussed in national security circles, it is as a nameless, faceless probability, the kind of sickness that may or may not be prevented simply by wearing a mask.
In today's conversations we're going to hear about the details, what works, what doesn't and how to remember that what feels safe today may not feel safe tomorrow.

Thank you for joining us,

Mike Gruss
Editor-in-chief
C4ISRNET, Defense News, Military Times & Federal Times

AGENDA

8:30AM – 8:35AM

WELCOME REMARKS

Mike Gruss, Editor-in-chief, *C4ISRNET, Defense News, Military Times & Federal Times*

8:35AM – 9:10AM

OPENING KEYNOTE

Lt. Gen. Charles "Tuna" Moore, Deputy Commander, *U.S. Cyber Command*

Moderator: Mark Pomerleau, Reporter, *C4ISRNET*

9:10AM - 9:13AM

BREAK

9:13AM - 10:01AM

THE CYBER WARRIOR'S TOOLKIT

Faced with growing, increasingly sophisticated cyberattacks, U.S. Cyber Command is working on a better way to develop, buy and deploy tools to cyber warriors who serve varied needs across the military. The Joint Cyber Warfighting Architecture is Cyber Command's answer to organize disparate tools to foster a highly skilled workforce of cyber operators. We'll explore the technologies the command needs for the cyber toolkit of sensors and data platforms for mission planning. And we'll ask for an update on the command's steps to address concerns about how to best integrate tools purchased throughout the military branches.

Col. Ben Ring, Director, Joint Cyber Warfighting Architecture Capability Management Office, *U.S. Cyber Command*

Randall Sharo, Command Technology Officer (CTO), *U.S. Fleet Cyber Command/U.S. Tenth Fleet*

Moderator: Mark Pomerleau, Reporter, *C4ISRNET*

10:01AM - 10:12AM

BREAK

10:12AM - 10:57AM

THE TACTICAL CYBER AND INFO WARFARE METAMORPHOSIS

Cyber and information ops are decentralizing. With more sophisticated information attacks, the military is bulking up on tactical cyber and info warfare specialists who help commanders. Those tactical leaders need planners who understand the ins and outs of the domain and how to plug into the larger Cyber Command enterprise. What does the emergence of tactical cyber operations mean for a joint all-domain force? Emerging Army, Navy and Air Force teams are prompting new tools, training and strategy as they move their capabilities closer to commands and expand the definition of information operations.

Col. Brian Russell, Commanding Officer, Information Group II MEF, *U.S. Marine Corps*

Moderator: Marjorie Censer, Editor, *Defense News*

10:57AM - 11:00AM

BREAK

11:00AM - 11:08AM

INDUSTRY FIRESIDE CHAT

Aaron Swain, Director of Digital Transformation, *VMware*

Moderator: Mike Gruss, Editor-in-chief, *C4ISRNET, Defense News, Military Times & Federal Times*

11:08 AM - 11:53 AM

A NEED FOR SPEED (IN SOFTWARE DEVELOPMENT)

Defense leaders are all in on fast, simplified software rollouts. The idea is central to the strategy to keep pace with adversaries' advances. Easy software updates for equipment are the new goal — instead of sticking with technology until replacement is unavoidable. And new capabilities reach service members faster through an agile approach that favors lean, rapidly made software with persistent updates, a change from long timelines for comprehensive software packages that can be outdated before implemented. Dedicated software factories, such as Air Force's Kessel Run and Navy's OASIS, use open-source development to quickly deliver improvements over legacy systems, and the Defense Department increasingly embraces this DevSecOps mindset with technology and cloud suppliers that create software for the military or run it for the DoD as a service.

AGENDA

Lt. Col. Vito Errico, Director, *Army Software Factory*
Moderator: Mike Gruss, Editor-in-chief, *C4ISRNET, Defense News, Military Times & Federal Times*

11:53AM - 11:56AM **BREAK**

11:56AM - 12:04AM **INDUSTRY FIRESIDE CHAT**

Brett Barraclough, Vice President, Cyber and Information Solutions, Defense Sector, *ManTech*
Moderator: Marjorie Censer, Editor, *Defense News*

12:04AM - 12:49AM **ADVISER AND ENFORCER: DEVELOPMENTS IN CYBER LEADERSHIP**

The rise of cyber as a domain introduced new responsibilities and positions of trust across defense agencies. In recent years, lawmakers required each service to designate a top cyber adviser to provide insights on recruitment, training and readiness of cyber forces, acquisition of offensive and defensive capabilities, and cybersecurity supply chain risks. At the same time, chief information security officers — rare or nonexistent just 20 years ago — have become essential for operational vigilance and information integrity. With cyber leadership in the spotlight, we'll hear from CISOs and cyber advisers on how they translate cyber policies for the battlefield.

RADM Mike Ryan, Commander, *U.S. Coast Guard Cyber Command*
David Luber, Deputy Director, Cybersecurity Directorate, *National Security Agency*
Moderator: Marjorie Censer, Editor, *Defense News*

12:49PM - 12:52PM **BREAK**

12:52PM - 1:00PM **INDUSTRY FIRESIDE CHAT**

Dan Smith, Vice President, Strategic Initiatives, *ManTech*
Moderator: Daniel Thomas, Senior Editor, Custom Content, *C4ISRNET*

1:00PM - 1:38PM **ZERO TRUST — FROM BUZZWORD TO ESSENTIAL STRATEGY**

With hackers getting better at disguising themselves as legitimate network users, the Pentagon wants to build its defenses on the inside, going beyond perimeter protections to keep adversaries out. The department advocates a zero trust cybersecurity methodology based on the premise that attackers will inevitably find their way in. The idea is that organizations should trust no one and verify everything: users, devices and standing access privileges. As the Pentagon's top IT shop considers creating a portfolio management office to speed up zero trust adoption, let's explore how software and cloud environments must mature to verify identity at each stop along the network: the router, the switch, the computer to the DoD's common access card.

David McKeown, Deputy DoD Chief Information Officer for Cybersecurity, *Department of Defense*
Moderator: Mike Gruss, Editor-in-chief, *C4ISRNET, Defense News, Military Times & Federal Times*

1:38PM - 1:41PM **BREAK**

1:41PM-2:11PM **KEYNOTE**

Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy, *Department of Defense*
Moderator: Mark Pomerleau, Reporter, *C4ISRNET*

2:11PM - 2:14PM **CLOSING REMARKS**

vmware®

DELL Technologies

Accelerate Transformation

To meet the variety of missions you encounter every day, you need responsive IT. Dell Technologies and vmware offers federal agencies the technology expertise, end-to-end solutions and world-class service you need to be prepared for what comes next.

SPEAKERS

CLICK ON SPEAKER PHOTO TO VIEW BIO

LT. GEN. CHARLES "TUNA" MOORE
Deputy Commander,
U.S. Cyber Command

MIEKE EOYANG
Deputy Assistant Secretary of Defense for Cyber Policy,
Department of Defense

DAVID MCKEOWN
Senior Information Security Officer, and Deputy CIO for Cybersecurity,
Department of Defense

RADM MIKE RYAN
Commander,
U.S. Coast Guard Cyber Command

DAVID LUBER
Deputy Director, Cybersecurity Directorate,
National Security Agency

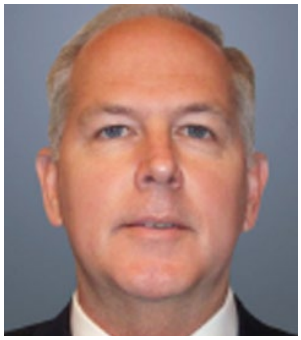
COL. BEN RING
Director, Joint Cyber Warfighting Architecture Capability Management Office,
U.S. Cyber Command

RANDALL SHARO,
Command Technology Officer (CTO), *U.S. Fleet Cyber Command /U.S. Tenth Fleet*

COL. BRIAN RUSSELL
Commanding Officer, Information Group, II MEF,
U.S. Marine Corps

LT. COL. VITO ERRICO
Director,
Army Software Factory

AARON SWAIN
Director of Digital Transformation,
VMware



BRETT A. BARRACLOUGH
Vice President, Cyber and Information Solutions, Defense Sector,
ManTech

DAN SMITH
Vice President, Strategic Initiatives,
ManTech International Corporation

MODERATORS

MIKE GRUSS
Editor-in-chief,
C4ISRNET, Defense News, Military Times & Federal Times

MARJORIE CENSER
Editor,
Defense News

MARK POMERLEAU
Reporter,
C4ISRNET

DANIEL THOMAS
Senior Editor,
Custom Content,
C4ISRNET & Defense News

Offense-Informed Defense is How We Tackle the Toughest Cyber Threats.

Our unique and evolving defensive capabilities produce sophisticated cyber solutions and services that work holistically to defend the network and data from both known and new threats.

ManTech®

Securing the Future

EXPLORE GREAT CONTENT FROM OUR SPONSORS

START BROWSING

THANK YOU TO OUR SPONSORS

DIAMOND

ManTech
Securing the Future

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

PLATINUM

DELL Technologies | vmware

The Dell Technologies federal team is 100% committed to your mission. Whether you're providing critical citizen services, innovating for the next generation, or securing the nation, we bring the right technology, a secure supply chain, targeted expertise, and far-reaching vision to help guide your journey.

VMware Government Solutions provide the digital foundation for the evolution and transformation of government IT, enabling agencies to improve mission outcomes and meet constituent expectations for modern, efficient and cost effective services.

SILVER

servicenow

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. Learn More