



CYBER OPERATIONS FOR NATIONAL DEFENSE

ACHIEVING AND MAINTAINING US SUPERIORITY IN CYBERSPACE

September 19-20, 2019
Mary M. Gates Learning Center, Alexandria, VA

September 19, 2019

7:00—7:45	Registration and Light Breakfast Reception Open
7:45—8:00	Chairperson Opening Remarks Max Harris Principal, Netizen
8:00—8:15	Moderator Opening Remarks Maj. Gen. (ret.) Sarah E. Zabel, USAF Owner, Sarah Zabel Enterprises, LLC
8:15—9:00	Exploiting the Convergence of Cyber and Electronic Warfare to Fight and Win in the Air Domain <ul style="list-style-type: none">• Convergence of 24th and 25th Air Forces and the alignment and optimization of the Air Combat Command to maximize efficiency and mission success• Increased funding for Distributed Cyber Warfare Operations portfolio—overview of current initiatives to develop electronic warfare systems in conjunction with traditional cyber tools• Leveraging partnerships with academia, industry, and other service components to improve readiness Gen. James “Mike” Holmes, USAF, Commander, Air Combat Command (Confirmed)
9:00—9:45	Building a Robust and Agile Cyber Fighting Force <ul style="list-style-type: none">• Overview of planned cyber reforms— how these reforms will create a more effective and resilient cyber policy across the DoD• Improving DoD-industry collaboration for cyber R&D• Challenges of hiring and retaining top cyber talent—ways to mitigate these challenges MajGen Dennis Crall, USMC, Deputy Principal Cyber Advisor, Office of the Secretary of Defense (Confirmed)
9:45—10:30	Preparing the Cyber Force for the Changing Global Operational Environment <ul style="list-style-type: none">• Preparing the US Army’s cyber forces to function within an increasingly competitive, congested, and contested cyberspace• Overview of current training methods—how do events like Cyber Quest help test new technology and train cyber warriors? Robert Kazimer, Deputy Commander, US Army Cyber Center of Excellence (Confirmed)
10:30—11:00	Networking Break & Exhibits
11:00—11:45	Designing Innovative Cyber Capabilities for the Air Force <ul style="list-style-type: none">• Overview of the Cyber Science and Technology division at AFRL—current priorities and challenges• Importance of agility in the R&D and acquisition processes to effectively compete with great power competitors• Thoughts on the future of Air Force cyber capabilities Chad Heitzenrater, Sr. Computer Scientist, Information Directorate, AFRL (Confirmed)
11:45—12:30	Developing and Delivering Electronic and Cyber Capabilities to the Warfighter <ul style="list-style-type: none">• Overview of the processes of R&D and acquisition at PM EW&C• Impact of the integration of cyber and electronic warfare units• Status update on current programs of record including the Terrestrial Layer System COL Kevin Finch, USA, Program Manager, Electronic Warfare and Cyber, PM EW&C, PEO IEW&S (Confirmed)
12:30—1:30	Networking Lunch

1:30—2:30	<p>Optimizing Cyberspace to Support National Security Efforts</p> <ul style="list-style-type: none"> • Implementing a “competitive mindset” across JFHQ-DoDIN to effectively compete with near-peer competitors • Defending and operating the DoD’s information systems—what are the greatest challenges and what can be done to mitigate them? • Cultivating trusted partnerships with industry to improve national cybersecurity and mitigate supply chain risks—what role do OTAs play in encouraging innovation? <p>Ignatius Liberto, Chief of Staff, Joint Force Headquarters-DODIN (Confirmed)</p>
2:30—3:15	<p>Ensuring the Agility and Security of the Air Force’s Software Development & Acquisition Process</p> <ul style="list-style-type: none"> • Overview of the newly-established PEO Digital—how will this office operate as a catalyst for best practices and new contracting strategies across the Air Force? • The importance of agile software development <p>Steven D. Wert, Program Executive Officer, Digital, Air Force Life Cycle Management Center (Confirmed)</p>
3:15—3:45	<p>Networking Break & Exhibits</p>
3:45—4:30	<p>Operationalizing the Army’s Expeditionary Cyber Capabilities</p> <ul style="list-style-type: none"> • Overview of the newly-created 915th Cyber Warfare Support Battalion (CWSB) • Supporting commanders in the field with cyber effects and intelligence—current challenges and how to mitigate them • Integrating tactical operations with strategic cyber capabilities and supporting electronic warfare and cyber planning and integration <p>LTC Matt Davis, USA, Battalion Commander, 915th Cyber Warfare Support Battalion (Confirmed)</p>
4:30—5:15	<p>Understanding NATO’s Role in Cyberspace</p> <ul style="list-style-type: none"> • Overview of NATO’s role in cyberspace and how it has evolved since the recognition of cyberspace as a domain of operations in 2016 • Status update on the Cyberspace Operations Center (CyOC)—role as a centralized planning space and coordinator for operations and missions • Thoughts on the future of NATO’s involvement as non-NATO adversarial powers increase their reach into the cyber domain <p>Laura Brent, Cyber Defense Officer, NATO (Confirmed)</p>
5:15	<p>End of Day One</p>

September 20, 2019

7:30—8:30	Registration and Light Breakfast Reception Open
8:30—8:45	Chairperson Opening Remarks Max Harris Principal, Netizen
8:45—9:00	Moderator Opening Remarks Maj. Gen. (ret.) Sarah E. Zabel, USAF Owner, Sarah Zabel Enterprises, LLC
9:00—9:45	Leveraging Updated Cyberspace Policy and Strategy to Ensure National Security <ul style="list-style-type: none">• Assessing the implications of NSPM 13 and the subsequent new strategy of “defending forward”—how will this enable USCYBERCOM to achieve national security and cyberspace superiority?• Meeting evolving cyber threats—how can US policy keep up with fast-paced and sophisticated cyber threats?• Adapting the US response to various threat levels—how does USCYBERCOM respond differently to threats posed by great power competitors, smaller governments, and criminal organizations? Burke “Ed” Wilson, Deputy Assistant Secretary of Defense for Cyber Policy (Confirmed)
9:45—10:30	Modernizing Cyber Across the Department of Defense <ul style="list-style-type: none">• Overview of current efforts to modernize the DoD’s cyber capabilities—top priorities and biggest challenges• Establishing policies for DoD cyber modernization• Resourcing the DoD’s cyber capabilities—challenges of balancing current needs with budget restrictions, technological obsolescence, and competitor capabilities Dr. Daniel “Rags” Ragsdale, Assistant Director for Cyber, Office of the Director of Defense Research and Engineering (Research and Technology) (Invited)
10:30—11:00	Networking Break & Exhibits
11:00—12:30	Panel Discussion: Leveraging DoD—Industry Partnerships to Ensure Election Security Moderator: Lauren Zabierek, Cyber Project Director, Belfer Center for Science and International Affairs (Confirmed) Panelists: David Becker, Executive Director & Founder, Center for Election Innovation & Research (Confirmed) MG James A. Hoyer, Adjutant General, West Virginia National Guard (Confirmed) Jessica Bowman, Assistant Commissioner, Virginia Department of Elections (Confirmed) Maria Barsallo Lynch, Defending Digital Democracy Project Director, Belfer Center for Science and International Affairs (Confirmed)
12:30—1:30	Networking Lunch

1:30—2:15	<p>The Future of Cybersecurity</p> <ul style="list-style-type: none"> Automation and cybersecurity—how automation and artificial intelligence can help solve problems of speed and scale Expanding the uses of machine learning—potential uses and anticipated challenges Looking towards the future: where is cybersecurity headed, and how will it evolve alongside changing technology? <p>Bobbie Stempfley, Director, CERT Division, Software Engineering Institute, Carnegie Mellon University (Confirmed)</p>
2:15—3:00	<p>Leveraging Enhanced Attribution Capabilities to Deter Malicious Cyber Activity</p> <ul style="list-style-type: none"> Overview of the ongoing Enhanced Attribution project at DARPA—goal of the program, top priorities, and current challenges Evaluating weaknesses in our current system that allow malicious actors in cyberspace to operate with little fear of being caught Thoughts on the future of attribution in cyberspace and how this will impact national security <p>Ian Crone, Project Manager, DARPA (Confirmed)</p>
3:00—3:30	<p>Networking Break & Exhibits</p>
3:30—4:15	<p>Developing Cyberspace Operational Policy to Operate and Defend Coast Guard Systems</p> <ul style="list-style-type: none"> Overview of CG-791—role in manning, organizing, training, and equipping the cyberspace workforce for operations in the cyber domain Developing policies to enable operations using cyberspace and protect Coast Guard systems and networks from cyber threats Thoughts on the future of Coast Guard cyber operations and policy as technology evolves and the global threat landscape changes <p>CDR Boris Montatsky, Chief of Cyberspace Operations Policy Division, CG-791, US Coast Guard (Confirmed)</p>
4:15—5:00	<p>Building the Next Generation of Cyber Warriors</p> <ul style="list-style-type: none"> Overview of current threat landscape and thoughts on how it will evolve in the near and far term futures Combatting the global shortage of nearly 2 million cybersecurity professionals in 2019 Aligning curriculum at NDU and beyond with National Cybersecurity guidelines <p>Dr. John Hurley, Professor, College of Information and Cyberspace, National Defense University (Confirmed)</p>
5:00	<p>End of Symposium</p>