

10 Year Anniversary

# CYBER BEACON

THE FUTURE IS NOW

October 19 & 20, 2023



## WELCOME TO THE 10<sup>th</sup> ANNUAL CYBER BEACON CONFERENCE !

To capitalize on efficiency of artificial intelligence (AI) and generate discussion, the planners for National Defense University College of Information and Cyberspace used eight generative AI tools to develop the conference agenda. This agenda demonstrates both the strengths and weaknesses of generative AI and recognizes the amazing advances in such a short amount of time. Join us October 19th and 20th for the 10<sup>th</sup> Annual Cyber Beacon!

The quickly evolving technology in the digital age is having a major impact on modern warfare. Cyberattacks are becoming increasingly common and sophisticated, and could have a devastating impact on critical infrastructure and military operations.

Here are some of the ways that quickly evolving technology is impacting modern warfare:

- **Cyberwarfare:** Cyberwarfare is the use of computer networks to attack an enemy's critical infrastructure or military systems. Cyberwarfare can be used to disrupt communications, disable power grids, or even launch attacks on military targets.
- **The use of artificial intelligence (AI):** AI is being used to develop new weapons and systems that are more powerful, more accurate, and more autonomous than ever before. AI is also being used to automate tasks, such as target identification and decision-making.
- **The use of big data:** Big data is being used to collect and analyze information about the enemy, the battlefield, and the weather. This information can be used to make better decisions and to develop more effective strategies.

These are just a few of the ways that quickly evolving technology is impacting modern warfare. The digital age is changing the way wars are fought, and it is important for militaries to adapt to these changes to stay ahead of the curve.



# THE AGENDA

10 Year Anniversary

# CYBER BEACON

October  
19 Thursday

*Technology Security – AI, Workforce, Zero Trust, Data, Critical Infrastructure*

9:30 – 9:45	Opening Remarks
9:45 – 10:15	Fireside Chat
10:15 – 11:15	AI & National Security Strategy
11:15 – 12:15	Future of the Cyber Workforce
12:15 – 1:00	Lunch
1:00 – 2:00	Zero Trust, AI & Machine Learning
2:00 – 3:00	Future of Critical Infrastructure Protection
3:00 – 3:15	Break
3:15 – 4:15	Big Data & National Defense
4:15-4:45	Virtual Fireside Chat
4:45-5:00	Closing Remarks
5:00-7:30	Reception for All Attendees, in Honor of CIC Alumni

20 Friday

*Technology Security – Emerging Technologies, Joint Warfighter*

9:00 – 9:30	Opening Remarks
9:30 – 10:15	Keynote
10:15 – 11:15	Emerging Technology & National Security Interests
11:15 – 12:15	Joint Warfighter & Cyberspace Operations: U.S. Military Responsibilities, Authorities & Capabilities in Cyber Warfare
12:15 – 12:30	Closing Remarks & AI Poster Awards



Day 1

OCTOBER 19<sup>th</sup>

# 10 Year Anniversary CYBER BEACON

## OPENING REMARKS

by

Dr. Cassandra C. Lewis, Chancellor, College of Information and Cyberspace,  
National Defense University



Dr. Cassandra C. Lewis is the Chancellor, and former Dean of Faculty and Academic Programs, at the College of Information and Cyberspace (CIC), National Defense University (NDU). She serves as the principal advisor to the NDU President and Provost on curriculum and academic programs related to cyberspace and information. As a member of NDU's senior leadership executive council, Dr. Lewis is instrumental in strategic planning and coordination of University initiatives. Dr. Lewis is the chief administrator of CIC's academic programs, with responsibility for financial, facilities, and personnel management. She maintains relationships with partner NDU components, U.S. government agencies, the private sector, international allies and Department of Defense and civilian educational institutions and universities and has engaged in international capacity building on the behalf of the University.

Under her leadership CIC's academic programs and curricula continue to be rigorous, relevant, and of high quality, to effectively fulfill its mission; and the College continues to be recognized as an institution of choice for education, scholarship, and thought leadership in cyber and information. Her track record and involvement in government, academia, industry, and the non-profit sector reflect her commitment to leader development, educational innovation, and building an inclusive and resilient workforce. Her research and teaching portfolios span a range of fields including: the politics of education; online teaching practices; access and equity in higher education; national security and cyber workforce policy and strategy; cyber leader development; and storytelling for organizational and personal change.

Dr. Lewis is a community-minded educator dedicated to advancing opportunities for underserved women and K-16 students both locally and abroad. She has a particular passion for fostering transformational leadership and advancing careers in STEM.

Dr. Lewis holds a Bachelor's degree in the Interdisciplinary Social Sciences/International Studies from the State University of New York at Buffalo; Master's degree in Higher Education from Boston College; a Ph.D. in Education Policy from the University of Maryland, College Park; and a Certificate in Executive Leadership Coaching from Georgetown University.

10 Year Anniversary

# CYBER BEACON

## FIRESIDE CHAT

with

**Admiral (Ret) Mike Rogers, Brunswick Group**



**Michael S. Rogers** is a retired four-star admiral of the United States Navy. Rogers served as the second commander of the United States Cyber Command (USCYBERCOM) from April 2014 to May 2018 while concurrently serving as the 17th director of the National Security Agency (NSA) and as chief of the Central Security Service (CSS). During his tenure, he helped transform and elevate U.S. Cyber Command into a unified combatant command. Rogers relinquished command to General Paul M. Nakasone on May 4, 2018 and retired from the Navy a few weeks later on June 1, 2018. Prior to 2014, Rogers served as the Commander of the Tenth Fleet and Commander of the United States Fleet Cyber Command, with responsibility for all of the Navy's cyberwarfare efforts. In 2009, he was the director of intelligence for the Joint Chiefs of Staff after having been the director of intelligence for Pacific Command from 2007 onwards.

## MODERATED

by

**Major Titus Lowell, (USMC), Student, Cyber Leader Professional Development Program, College of Information and Cyberspace, National Defense University**



Major Titus Lowell was born and raised in the rural farming town of Mattawa, Washington. He graduated from Whitworth University with a Bachelor of Science in Computer Science and Mathematics in 2001. He received his commission in 2007 with the United States Marine Corps under a Naval Flight Officer contract. After flight school, he was designated an EA-6b Prowler Electronic Countermeasures Officer and logged over 1100 hours in the EA-6b flying missions in Operations UNIFIED PROTECTOR, ENDURING FREEDOM, and INHERENT RESOLVE. After the retirement of the EA-6b, Major Lowell was redesignated as a Cyberspace Operations Officer.

# FIRST PANEL

## AI & National Security Strategy

(10:15 - 11:15)

**Abstract 1:** Emerging technologies, including AI, quantum computing, and critical infrastructure, have a profound impact on society, U.S. national security, and the international environment among nations/societies. These technologies shape national security strategies, fuel global competition, and have implications for military capabilities and the balance of power. It is crucial for nations to stay ahead in these areas to ensure their security and economic prosperity.

**Abstract 2:** The 2023 National Cybersecurity Strategy aims for a reinvigoration of federal research and development for cybersecurity to maintain resilience in the way of artificial intelligence among other areas across departments and agencies. The establishment of national laboratories and federally funded research centers will assist, but it is unclear how each federal organization will collaborate, and implement plans for the development of artificial intelligence.

QR Code to Access the Poll



# 10 Year Anniversary CYBER BEACON

## Moderator

### **Caroline Boyd, Principal, Government Programs, Meritalk**



Caroline Boyd is the former Assistant Secretary of Technology for the Commonwealth of Virginia, serving under Governor James S. Gilmore, III. She currently is the Principal of Government Programs for MeriTalk and 300Brand companies. Having served as a senior technology leader in government, Boyd understands what makes government executives tick. She manages government participation across MeriTalk programs and guides client-focused events. Previously, Boyd served as the General Manager of the GovMark Council, a not-for-profit organization that facilitates education and networking for senior-level marketing executives serving the government IT market – both inside government and out. In addition, she has held positions with CES Government, webMethods, and the Commonwealth of Virginia. During her appointment as Assistant Secretary of Technology, Boyd worked closely with the Secretary of Technology and the Virginia General Assembly in the statutory creation of the Office of the Secretary of Technology. Boyd produced four Governor's Commission on Information Technology conferences, and was integral in the organization of two national meetings of the Congressional Advisory Commission on E-Commerce.

Boyd served on the Board of Directors of the Virginia Center for Innovative Technology until 2002. She was appointed the Executive Director of the Virginia eCommunities Task Force from 2000-2002. Before serving the Commonwealth of Virginia, Boyd worked in the Government Relations Division of Sprint Corporation in Washington, DC.

## Panelists

### **Dr. Melissa Thomas, Professor, College of Information and Cyberspace, National Defense University**



Melissa Thomas is a professor at the College of Information and Cyberspace at the National Defense University. She holds a BA in computer and information science from UC Santa Cruz, a JD from UC Berkely, and a PhD in political economy and government from Harvard University. Previously, as a subject matter expert in governance, she worked with donors and partner low-income country governments, primarily in sub-Saharan Africa, participating in negotiations, providing support, and conducting mixed methods and computational research. She has held academic positions at The Paul H. Nitze School of Advanced International Studies, Johns Hopkins University; the US Army School of Advanced Military Studies; and the Air Force Cyber College. Her work has appeared in leading academic and policy outlets, including *Foreign Affairs*, *International Affairs*, *Defense Studies*, Columbia University Press, and Oxford University Press. Her current research interests are cyber strategy, hacking, and artificial intelligence.

### **John Bansemer, Director, Cyber AI Project, Center for Security and Emerging Technology (CSET), Georgetown University**



John Bansemer is the Director of the CyberAI Project and Senior Fellow at Georgetown's Center for Security and Emerging Technology (CSET). In addition to his work at CSET, he is an adjunct professor at Georgetown University's School of Foreign Service. Prior to joining CSET, John served in a variety of cyber, space and intelligence positions within the U.S. Air Force before retiring as a Lieutenant General. His last role was serving as the Assistant Director for National Intelligence, Partner Engagement, within the Office of the Director of National Intelligence. Prior to that assignment, he served as the Deputy Chief, Central Security Service, at the National Security Agency. He also held a variety of staff positions including on the Air Staff and the National Security Council staff. His joint experience includes serving as the director of intelligence at European Command. John holds a master's degree in computer science from James Madison University and was a national defense fellow at Harvard University.

# 10 Year Anniversary

# CYBER BEACON

## **Chuck Brooks, President and Consultant of Brooks Consulting; Adjunct Professor at Georgetown University**



Chuck Brooks is President and Consultant of Brooks Consulting International with over 25 years of experience in cybersecurity, emerging technologies, marketing, business development, and government relations. Chuck also serves as an Adjunct Professor at Georgetown University, teaching graduate courses on risk management, homeland security, and cybersecurity.

Chuck has received presidential appointments for executive service by two U.S. Presidents, and served as the first Director of Legislative Affairs at the DHS Science & Technology Directorate. He has also served in executive roles for companies such as General Dynamics, Rapiscan, and Xerox. He has been named "Cybersecurity Person of the Year" by Cyber Express, Cybersecurity Marketer of the Year, a Top Cybersecurity SME to Follow, and a "Top 5 Tech Person to Follow" by LinkedIn.

As a thought leader, blogger, and event speaker, he has briefed the G20 on energy cybersecurity, The US Embassy to the Holy See and Vatican on global cybersecurity cooperation. He has served on two National Academy of Science Advisory groups, including one on digitalizing the USAF, and another on securing BioTech. He has also addressed USTRANSCOM on cybersecurity and serves on an industry/government Working group for CISA focused on security space systems.

Chuck's clients have included leading companies such as AT&T, IBM, Intel, Rockwell Automation, Ivanti, Blackberry/Cylance, Serco, Xerox, Juniper Networks, Netscout, and General Dynamics. He is also a contributor to Forbes, The Washington Post, Dark Reading, Homeland Security Today, Skytop Media, GovCon, Barrons, The Hill, and Federal Times on cybersecurity and emerging technology topics. He has 108,000 followers on LinkedIn and 61,000 subscribers to his newsletter "Security and Tech Insights."

Chuck has an MA from the University of Chicago, a BA from DePauw University, and a certificate in International Law from The Hague Academy of International Law.

## **Lt Col Joseph Chapa, (USAF), Chief Responsible AI Ethics Officer, Department of the Air Force**



Joseph Chapa is an officer in the U.S. Air Force and holds a doctorate in philosophy from the University of Oxford. His areas of expertise include just war theory, military ethics, and especially the ethics of remote weapons and the ethics of artificial intelligence. He is a senior pilot with more than 1,400 pilot and instructor pilot hours. He currently serves as the Department of the Air Force's first Chief Responsible AI Ethics Officer and the DoD's liaison to the Special Competitive Studies Project. His book, *Is Remote Warfare Moral?* was published in July, 2022.

# SECOND PANEL

## Future of Cyber Workforce

(11:15 - 12:15)

**Abstract 1:** The future of the digital workforce is incredibly exciting, especially for CIOs and professionals in the cyber field. As technology continues to advance at an unprecedented pace, the role of the workforce is also evolving. Traditional jobs are being replaced by digital counterparts, and this shift is creating new opportunities and challenges for businesses and individuals alike. In the US, the digital workforce is set to become the driving force behind the economy. With the increasing reliance on technology and automation, businesses are recognizing the need to invest in skilled professionals who can navigate the digital landscape. CIOs are at the forefront of this transformation, leading their organizations in adopting new technologies and harnessing the power of data. The future of work will be heavily influenced by digital technologies. From artificial intelligence and machine learning to robotics and blockchain, these innovations will reshape industries across the board. The digital workforce will play a crucial role in leveraging these technologies to drive innovation, efficiency, and growth. Moreover, the digital workforce is not limited to a specific sector or industry. It spans across various fields, from healthcare and finance to manufacturing and education. This means that professionals with digital skills will have endless opportunities to contribute to different sectors and make a significant impact.

**Abstract 2:** The ability to maintain optimal, modern organizations depends on securing cyberspace as described in the 2022 National Security Strategy. The U.S. should determine ways to strengthen norms to mitigate cyber threats, which may involve new and different types of partnerships between government agencies, private industry and partner nations to deny criminal sanctuary. The 2023 National Cybersecurity Strategy describes the U.S. as having an opportunity to restructure incentives for establishing a resilient foundation for building a better future digital ecosystem. President Biden's elevation of leadership on Cybersecurity through the creation of the National Cyber Director is evidence of the urgency and level of commitment required to counter events such as SolarWinds Orion and other malicious cyber activities. Given the actions of the U.S. Government and the state of play vis-a-vis Russia and China relations, the future development of the cyber workforce is critical.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

### John Curran, Executive Editor, Meritalk



John Curran is Executive Editor at MeriTalk, where he leads the news reporting staff in providing daily coverage of the technologies, policies and programs that matter most to Federal CIOs and the agencies they serve. He was managing editor at Telecommunications Reports, and before that ran news operations at Dow Jones and reported for Reuters.

## Panelists

### David Harvey, Professor of Practice, College of Information and Cyberspace, National Defense University



Mr. Harvey has nearly 30 years of audit and financial management experience in the federal sector. Prior to joining the faculty of the College of Information and Cyberspace in October 2018, Mr. Harvey served as the Chief Audit Executive leading the internal audit function at the Federal Retirement Thrift Investment Board, where he reported to the agency's Board and its Executive Director as part of Thrift Savings Plan oversight. In that role, he oversaw the annual audit of information security controls under the Federal Information Security Management Act (FISMA), cyber-penetration testing and follow-up, and other reviews. Mr. Harvey also served as the Deputy Director of the Corporate Controls and Reviews Department at the Pension Benefit Guaranty Corporation, where he oversaw documenting and testing of financial reporting, NIST 800-53, and entity-wide governance controls; performing entity-wide, business process, and improper payment risk assessments; and remediating Office of Inspector General and Government Accountability Office recommendations. Mr. Harvey started his career as an auditor with the Defense Contract Audit Agency. His teaching experience includes serving on the adjunct faculty of American University and Northern Virginia Community College as well as developing and presenting continuing professional education seminars.

### Steven Hernandez, Chief Information Security Officer (CISO), Department of Education



Steven Hernandez is an information assurance expert serving the past twenty years in a variety of contexts and missions. He has worked on the front lines in operations centers and led research teams attempting to balance security, privacy, and mission delivery considerations. Transforming risk management in international manufacturing, healthcare, non-profits, and governments at the federal, state, and local levels is extensive through his professional portfolio. Leading tactical, day-to-day security operations as well as guiding and influencing broad security initiatives such as the US government's FedRAMP program across large organizations with international presence are areas he's frequently called upon to support. Presently he is the Chief Information Security Officer and Director of Information Assurance Services at the U.S. Department of Education. Steven also serves as the co-chair of the US Government Federal CISO Council and government chair of the ACT-IAC Cybersecurity Community of Interest. Prior to his position at Education, he held a variety of roles at the Office of Inspector General, US Department of Education including CTO, CIO, CISO, Senior Official for Privacy and Chief Services Engineering Officer. He is an inaugural member of the United States Scholarship of Service Hall of Fame. He served on the Board of Directors for the International Information Systems Security Consortium (ISC)<sup>2</sup>, served on the U.S. (ISC)<sup>2</sup> Government Advisory Board for Cybersecurity (GAB), judged for the Government Information Security Leadership Awards (GISLA) and contributed to its Executive Writers Bureau. Mr. Hernandez is the lead author and editor of the third edition of the (ISC)<sup>2</sup> Official Guide to the CISSP CBK, the (ISC)<sup>2</sup> Official Guide to the HCISPP CBK, and several published works regarding international information assurance.

10 Year Anniversary

# CYBER BEACON

## **Dr. Tiina K.O. Rodrigue, Chief Information Security Officer (CISO), Bureau of Consumer Financial Protection (CFPB)**



Tiina K.O. Rodrigue is the Chief Information Security Officer (CISO) at the Bureau of Consumer Financial Protection (CFPB). Tiina uses her more than 25 years of experience to guide teams to design, develop, and implement secure business applications in the cloud. Her technical solution, full-lifecycle experience begins during the development process, includes secure technology selection, security architecture, and implementation methodology through continuously improved production in the cloud. As CISO, she leads the Bureau to solutions, optimizations, and well-managed operations to federal standards, leveraging best in class capabilities and practices for scalability and flexibility.

Previously, Tiina was the Director, Technology and Cybersecurity Services at MAXIMUS Federal Information Technology (MFIT). Federally, she also served as the Senior Advisor-Cybersecurity, Office of the Chief Information Security Officer (CISO), in the Technology Office (TO) of Federal Student Aid (FSA), U.S. Department of Education (ED) in Washington, DC. In her role as Senior Advisor at FSA, she championed FSA and ED's interdepartmental cybersecurity efforts with government entities such as the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and Department of State. She led departmental security activities with institutions of higher education (IHEs), financial lenders, guaranty agencies, and private collection agencies to establish an industry-wide professionalized cyber workforce, gather meaningful metrics, and create ground-truth security. Additionally, Ms. Rodrigue was the Program Director, Professional Services at CipherCloud (San Jose, CA), a Silicon-Valley-based Cloud Access Security Broker (CASB) start-up where she supervised concurrent teams globally deploying a policy-based, on the fly encryption product in federal, financial and health-care environments for data protection in clouds such as Salesforce, O365, Box, Adobe, Amazon Web Service (AWS), Google, and Dropbox. Tiina served as the CISO for U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS). During her tenure at DHS she was promoted to Chief Technology Officer (CTO) at USCIS, bridging the technology concerns of security, infrastructure, change, architecture and capability management.

## **Seeyew Mo, Assistant National Cyber Director for Cyber Workforce, Training and Education at the Office of National Cyber Director (ONCD)**



Mr. Seeyew Mo serves as the Assistant National Cyber Director for Cyber Workforce, Training and Education at the Office of National Cyber Director (ONCD). In his role, Seeyew leads and supports the creation and implementation of the National Cyber Workforce and Education Strategy. He believes in taking a holistic view – doctrine, people, and technology – to making advancements in cyber workforce and digital safety awareness. He is an expert in the intersection of cybersecurity, technology, and national security with 18 years of experience that spans tech development, policymaking, and political campaigning.

10 Year Anniversary

# CYBER BEACON

## Brian Epley, Principal Deputy Chief Information Officer (PDCIO), Department of Energy



Brian Epley currently serves as Principal Deputy Chief Information Officer (CIO) at the U.S. Department of Energy, where he leads day-to-day operations within the Office of the CIO and assists the CIO in the formation of the office's strategic direction for the protection and modernization of IT, cybersecurity, and data usage across the DOE enterprise to achieve the Department's business goals. Brian joins the Department from the Environmental Protection Agency, where he served for nearly 7 years in leadership roles including Principal Deputy Assistant Administrator for Administration and Resources Management; Deputy CIO and Director of the Office of Information Technology Operations, and Chief Technology Officer for the Office of Environmental Information.

Brian is a seasoned professional with more than 25 years' experience across public and private sectors. Throughout his career he has distinguished himself as an innovative change leader with the unique ability to deliver strategically aligned and value-add services. Prior government roles include Homeland Security Presidential Directive-12 Technical Director of the Department of Veterans Affairs Office of Information and Technology and IT Services Director and Chief Information Security Officer for the Virginia Information Technologies Agency. Brian also held various leadership roles in the private sector at the Computer Science Company, Northrop Grumman, and as the founding President of Inter Solve-IT focused on enterprise transformation, research and development, IT, and enterprise operations.

Brian served on the Virginia Commonwealth University School of Business Society Board of Directors and Virginia State University IT Advisory Council Board of Directors. Brian received the Department of Veterans Affairs honor award for, "Getting to Green" on the President's Management Agenda of Human Capital and the "Top 40 Under 40 Award" for service in the Commonwealth of Virginia. Brian holds a Master of Business Administration degree, International Business and a Bachelor of Science degree, Management Information Systems; both from the Virginia Commonwealth University. Brian was also selected and worked as a Ph.D. candidate, Information Security Assurance at George Mason University's Volgenau School of Engineering and Computing.

## THIRD PANEL

# Zero Trust, AI & Machine Learning

(1:00 – 2:00)

**Abstract 1:** Artificial Intelligence (AI), Zero Trust and automation are three important concepts in the field of cybersecurity. Zero Trust is a security model that requires strict identity verification for every person and device trying to access resources on a network. AI and automation can be used to strengthen Zero Trust by ensuring speedy investigations and remediation routines are established and working. This can then provide organizations with 24/7 protection at speed and scale.

**Abstract 2:** The move to Zero Trust has been a significant shift from the historic perimeter-based approach to cybersecurity. The transition to Zero Trust was initiated under EO 14028 on Strengthening Cybersecurity and OMB later released the Federal Zero Trust Strategy. Automation and visibility are essential elements of zero trust. AI is quickly developing and adding capacity to ZT.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

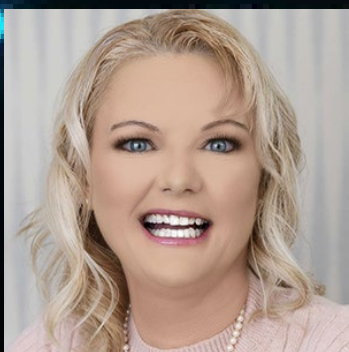
### Jason Miller, Executive Editor, Federal News Network



Jason Miller has been executive editor of Federal News Network since 2008. Jason directs the news coverage on all federal issues. He has also produced several news series – among them on whistleblower retaliation at the SBA, the impact of the Technology Modernization Fund and the ever changing role of agency CIOs.

## Panelists

### Dr. Amy Hamilton, Visiting Faculty Chair, Department of Energy, College of Information and Cyberspace, National Defense University



Amy S. Hamilton, Ph.D. is the Visiting Faculty Chair from the Department of Energy to the Department of Defense (DOD) National Defense University (NDU) College of Information and Cyberspace (CIC). She has served for the past three years as the Senior Advisor for National Cybersecurity Policy and Programs at the Department of Energy. She spent two years as a senior cyber security policy analyst at the Office of Management and Budget, Executive Office of the President. She served in the Michigan Army National Guard as a communications specialist and was commissioned into the U.S. Army Officer Signal Corp, serving on Active Duty and later the U.S. Army Reserves. She has worked at both the U.S. European Command and the U.S. Northern Command & North American Aerospace Defense Command (NORAD) on multiple communications and IT projects.

She became a certified Project Management Professional through the Project Management Institute in 2007 and earned her Certified Information Security Manager certification in 2011. She presented on the “The Secret to Life from a PMP” at TEDxStuttgart in September 2016. She taught Project Management Tools at Colorado Technical University and was a facilitator for the Master’s Degree Program in Project Management for Boston University. She is an award-winning public speaker and has presented in over twenty countries on overcoming adversity, reaching your dreams, cyber security, and project management.

### Randy Resnick, Director, Zero Trust Portfolio Management Office, Department of Defense



Mr. Randy Resnick serves as the Director of the newly established Zero Trust Portfolio Management Office within DoD CIO/CS. Mr. Resnick joins us from the National Security Agency (NSA) with over 34 years of experience in offense and defense cybersecurity. In his most recent assignment, Mr. Resnick served as NSA’s Zero Trust Strategic Lead. In that role, Mr. Resnick successfully led and executed numerous ZT activities at the tactical, operational, and strategic levels and also provided NSA leadership during the successful ZT POM 23-27 Issue Paper process. His leadership and technical direction led to the development of the first DoD Zero Trust Reference Architecture, the first NSS Zero Trust Reference Architecture, DoD’s ZT maturity model, DoD’s initial strategy for Zero Trust and the construction of two Zero Trust Innovation testbed labs in collaboration with DISA and USCC. Prior to serving as NSA’s Zero Trust Strategic Lead, Mr. Resnick held positions as their Cybersecurity Innovations Director for the NSA Cybersecurity Directorate, served as Chief of NSA’s Red Team, and served as the Deputy Mission Manager for NC2/NC3/NLCC missions.

As the Zero Trust Portfolio Management Office Director, Mr. Resnick’s focus will be to provide strategic guidance, direct alignment of DoD ZT efforts, and prioritize resources to accelerate Zero Trust adoption across the DoD Enterprise while strengthening coordination and collaboration with key partners and stakeholders across the Department, the IC, Interagency, and Industry.

A native New Yorker, Mr. Resnick holds a Bachelor of Science degree in Electrical Engineering from Fairleigh Dickinson University and a Master’s Degree in Engineering Management from George Washington University.

# 10 Year Anniversary

# CYBER BEACON

## Linus Barloon II, Global Head of Threat Detection and Response, CDW



Major Linus J. Barloon II is a Cyberspace Officer assigned to the White House Communications Agency (WHCA) as the Chief of Cyber Operations Division in the J3 Directorate, Joint Base Anacostia-Bolling, Washington, D.C. Captain Barloon has been active duty for the last 22 years, being trained as a FB-111A Avionics Technician and as a Ground Radio Maintenance technician. After 12 years being enlisted, Capt Barloon was selected for Officer Training School and earned his commission on 28 Jun 2002. Since his commissioning, he has served in many leadership roles, to include: Network Operations Security Center Crew Commander, Flight Commander of both the Air Force Network Red/Blue Team and his current position. As a Flight Commander for the Air Force Blue Team, he was responsible for building the ability to “hunt” for the cyber adversary on Air Force networks. In his current capacity, he is responsible for training, organizing and equipping joint forces to proactively protect, detect, react and recover from the cyber threat on networks directly associated with supporting the President, Vice President, First Lady and other Senior White House Staff. He is an experienced speaker in the cyber community having been requested to speak at national Security Agency’s Red Blue Symposium, the Defense Information System Agency’s Cyber Technical Exchange, AFCEA Luncheons and Breakout Panels and other venues. He is also the Vice Chair of the Advanced Threat Response Panel for the National Board of Information Security Examiners to influence the development of cyber curriculums at all levels of education at the National level.

## Renata Spinks, Chief Executive Officer (CEO), CyberSec International



Ms Renata C. Spinks is the CEO of tech-start-up (CyberSec International); whose mission is to provide Cybersecurity Software and Services to the public sector. She previously served as the Assistant Director/Deputy CIO of the Command, Control, Communications, and Computers (C4) Department in the Headquarters Marine Corps Senior Executive Service (2021-2023) and the Nation's first Cyber Technology Officer at Marine Forces Cyberspace Command (MARFORCYBER); (2018-2021). Her drive to revolutionize cyber, information technology and business transformation is evident in the initiatives she's led to date. As the Asst IT Director/Deputy CIO of IC4, she also served as the Senior Information Security Officer for the US Marine Corps. Her accomplishments span from authorizations, governance, policy, engineering, network modernization, digital transformation, emergent technology adoption and deployment, budget as well as workforce management. Prior to her USMC Senior Executive Service appointment, Ms. Spinks' accomplishments include working with DHS ICE, DOJ, CIA and the ODNI while serving as a criminal research specialist; utilizing forensics and human intelligence to investigate human trafficking and child exploitation as well as innovating in the US Treasury Big Data Analytics Office of Financial Research space. Ms. Spinks holds a BS in Information Systems, a MS in Technology Management, multiple information technology certifications, and is pursuing her Doctorate in Cybersecurity. Her tenure in the Senior Ranks evolved her as the go-to executive for innovation and earned her the reputation of getting things done with excellence. She leads with a People First mindset. Ms. Spinks' love for cyber and pattern of excellence progressively elevates her and is evident in her ascension to Senior Executive now turned CEO; at an unprecedented pace.

## Imran Umar, Vice President, Booz Allen Hamilton



Imran Umar is a cyber leader spearheading Booz Allen’s zero trust practice. With an extensive background supporting commercial, Department of Defense, and federal civilian clients, Imran provides technical solutions that enable organizations to move towards a resilient zero trust architecture. Along with zero trust, Imran advances the adoption and fusion of machine learning and artificial intelligence to improve cyber resiliency at an enterprise scale. Using concepts such as zero trust network access (ZTNA) and zero trust application access (ZTAA), he and his team of cybersecurity analysts determine an organization’s current zero trust maturity status, identify key gaps in architecture, and develop tailored solutions to transition them towards a data-centric security model that enforces least privileged access. Imran has a master’s in information and telecommunication systems, with a focus on cybersecurity, from Johns Hopkins University, and a bachelor’s from George Mason University.

# FOURTH PANEL

## Future of Critical Infrastructure Protection

(2:00 – 3:00)

**Abstract 1:** Critical infrastructure has become digitized in most of the U.S., which makes the disruption or destruction of key systems a target for state and non-state actors looking to disrupt the wellbeing of American citizens. The national security strategy describes the aim of deterring cyber-attacks and responding decisively with all appropriate tools as part of an allied effort with other nations to deny sanctuary. The National Cybersecurity Strategy (NCS) outlines critical infrastructure protection as the first of five pillars for approaching resilience in cyberspace and notes the current administration's efforts to engage industry to construct consistent, predictable and regulatory frameworks. However, the challenge is balancing security and innovation across the private sector in the context of a dynamic geopolitical environment. To that end, the "Shields Up" campaign prior to Russian invasion of Ukraine aided with combating malicious activity. There is much more work to do to protect critical infrastructure in the absence of systems to permanently link public and private stakeholders to operate at the speed and scale needed according to the NCS.

**Abstract 2:** Critical Infrastructure Protection (CIP) systems are becoming increasingly interconnected and digitized, which enhances efficiency, but also increases vulnerability to cyber threats. In the future, CIP will need to focus on protecting these interconnected networks from cyberattacks, ensuring robust cybersecurity measures are in place. The emergence of advanced technologies like the Internet of Things (IoT), artificial intelligence (AI), and automation will introduce new challenges and opportunities for CIP. While these technologies can enhance efficiency, they also introduce new vulnerabilities that could be exploited. Future CIP strategies will need to address these emerging risks and develop proactive measures to protect critical infrastructure. Collaboration between government agencies, private sector entities, and international partners will continue to be crucial for effective CIP. Encouraging public-private partnerships will help facilitate information sharing, resource allocation, and coordinated responses to potential threats.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

### **Martin Matishak, Senior Cybersecurity Reporter, The Record**



Martin Matishak is a senior cybersecurity reporter for The Record. He spent the last five years at Politico, where he covered Congress, the Pentagon and the U.S. intelligence community and was a driving force behind the publication's cybersecurity newsletter.

## Panelists

### **Harry Wingo, JD, Assistant Professor, College of Information and Cyberspace, National Defense University**



Professor Wingo leads the Chief Information Officer (CIO) Leadership Development Program (LDP) at the National Defense University (NDU) College of Information and Cyberspace (CIC). He has over 25 years of government and corporate leadership experience, including 15 years focused on information and communications technology law and policy. He has served as President and CEO of the D.C. Chamber of Commerce, Senior Policy Counsel at Google, Counsel to the Senate Committee on Science, Commerce & Transportation, Special Counsel to the General Counsel of the Federal Communications Commission and an Associate with the law firm of Skadden, Arps, Slate, Meagher & Flom. Before his career in law and technology, Professor Wingo served for more than six years as a Navy SEAL officer. He is a graduate of Yale Law School and the United States Naval Academy.

### **Rodney MacAlister, Founder and Principle of the MacAlister Group & Associates; Senior Advisor (CSIS)**



Rodney MacAlister is Founder and Principle of The MacAlister Group & Associates, a virtual consultancy, that he formed in 2014 among a global network of colleagues. He is also a Senior Advisor at the Center for Strategic and International Studies in Washington, DC.

MacAlister was CEO and Founder of Monetizing Gas Africa Inc. (2015-2022) a company which developed natural gas and power generation infrastructure in Sub-Saharan Africa, emphasizing LNG and hybrid options for the Energy Transition to solve renewable energy's intermittency while aiding decarbonization.

He previously served as General Manager of VAALCO Energy in Gabon (oil production, 2011-2014); MD of the Africa Middle Market Fund (Private Equity, 2008-2011); CEO of the US African Development Foundation in the G.W. Bush Administration (USG development agency, 2006-2007); Independent consultant in operating in conflict zones (2003-2006); and various positions at ConocoPhillips, 1978-2003, much of it in Africa, including 13 years in Business Development, and GM in the Congo (Brazzaville). He also headed Conoco's Washington office for 8 years. In Cape Town, South Africa, he headed the State Dept. Overseas Security Advisory Council.

MacAlister holds BA and MA degrees in International Relations from the University of Redlands, California, and spent a year of post-graduate work at The Sorbonne, Paris. He resides in Northern Virginia after living (again) in Africa 2011-2022.

# 10 Year Anniversary

# CYBER BEACON

## **Zach Tudor, Associate Laboratory Director, Idaho National Laboratory**



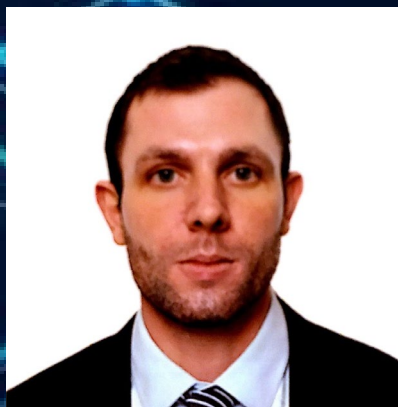
Mr. Zachary (Zach) Tudor is the associate laboratory director of Idaho National Laboratory's (INL) National and Homeland Security (N&HS) directorate.

Under Tudor's leadership, INL has developed into a major center for national security technology development and demonstration, employing 800 scientists and engineers across nearly \$500 million in programs. Tudor is responsible for leading divisions including INL's Nuclear Nonproliferation, Cyber Research and Development, Critical Infrastructure Protection, and Defense Systems missions. These missions include safeguarding and securing vulnerable nuclear material, enhancing the overall security and resilience of the nation's infrastructure, and providing protective material science solutions and heavy manufacturing of armor for national defense. The laboratory's national security missions support major programs for the Department of Energy, Department of Defense (DOD), Department of Homeland Security (DHS) and the Intelligence Community.

Previously, Tudor was a program director in the Computer Science Laboratory at SRI International, where he served as a management and technical resource for operational and research and development cybersecurity programs for government, intelligence and commercial projects. He supported DHS' Cyber Security Division on projects including the Linking the Oil and Gas Industry to Improve Cybersecurity consortium, and the Industrial Control Systems Joint Working Group. He has served on the NRC's Nuclear Cyber Security Working Group, was vice chair of the Institute for Information Infrastructure Protection at George Washington University and served as board chair for the International Information System Security Certification Consortium, or (ISC)<sup>2</sup>, a non-profit organization which specializes in training and certifications for cybersecurity professionals, often described as the "world's largest IT security organization".

A retired U.S. Navy Submarine Limited Duty Electronics Officer and chief data systems technician, Tudor holds an M.S. in information systems concentrating in cybersecurity from George Mason University, where he also was an adjunct professor teaching graduate courses in information security. His professional credentials include the Certified Information Systems Security Professional, Certified Information Security Manager, and Certified Computer Professional.

## **Peter Colombo, Senior Advisor, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency (CISA)**



Peter is the Deputy Section Chief of CISA's Cyber Performance Goals (CPGs) Section, within the Cybersecurity Division (CSD). He has previously served as a Senior Advisor with CSD working on Industrial Control Systems (ICS) and critical infrastructure-focused cybersecurity initiatives, to include supporting the original drafting of the CPGs and management of the Controls Systems Working Group (CSWG). Prior to joining CISA, he was a program manager for Federally Funded Research and Development (FFRDC) initiatives at the US Department of Veterans Affairs and intelligence projects at the US Department of the Treasury. Prior to his work in civilian government service, he served as an artillery officer in the United States Army. He holds a bachelors from the University of Virginia, and a Masters from Georgetown University.

## **Dr. Michael Powell, National Cybersecurity Center of Excellence, National Institute of Standards and Technology**



Michael Powell is a Cybersecurity Engineer at the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) in Rockville, Maryland. His research focuses on cybersecurity for the manufacturing sector, particularly how it impacts industrial control systems.

Dr. Powell joined the NCCoE in 2017. In his previous positions, he was responsible for the management/oversight of building and commissioning of US Navy DDG-51 class ships. He also served in the United States Navy for over 20 years, retiring as a Chief Petty Officer. He holds a Bachelor's degree in Information Technology, A Master's degree in Public Administration, and a Master's degree in Information Technology. Dr. Powell completed his Doctorate degree in Applied Computing at Pace University in West Chester, New York.

## FIFTH PANEL

# Big Data and National Defense

(3:15 – 4:15)

**Abstract 1:** Big data has become a crucial player in the modern battlefield of cybersecurity. With the exponential growth of information being generated and collected, organizations must navigate the complexities of managing and protecting this valuable resource. In the realm of cybersecurity, big data is both a weapon and a shield.

**Abstract 2:** “Big data” continues grow even bigger with demand for data-intensive applications from machine learning and artificial intelligence to large language models. Whatever the scale of the data, to be useful it must be made visible, accessible, understandable, linked, trustworthy, and secure. Fulfilling these goals creates new requirements not just for more data, more storage, and faster processors, but for new skills, new organizational structures, and new ways of thinking. In this panel we address progress and challenges in implementing a sound data strategy in the context of national security organizations.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

**Suzanne Smalley, Covering Privacy, Disinformation, and Cybersecurity Policy, The Record**



Suzanne Smalley is a reporter covering privacy, disinformation and cybersecurity policy for The Record. She was previously a cybersecurity reporter at CyberScoop and Reuters. Earlier in her career Suzanne covered the Boston Police Department for the Boston Globe and two presidential campaign cycles for Newsweek. She lives in Washington with her husband and three children.

## Panelists

**Michael Brody, JD, Visiting Faculty Chair, Department of Homeland Security, College of Information and Cyberspace, National Defense University**



Michael Brody has been working in homeland security policy development since 2004. He began his career in the Office of the Governor of Illinois where he was responsible for developing new policy directives for the State in homeland security. His work there led to his role as Director of the Illinois Homeland Security Market Development Bureau which provided grants and management consulting to innovative, high-tech homeland security companies based in Illinois. In 2008, Brody joined the Federal Emergency Management Agency serving as Reporting Section Chief for the National Preparedness Assessments Division, where he managed a team of analysts that produced reports for Congress on national, all-hazards preparedness including the National Preparedness Report. From 2012 to early 2014, Brody served as the Policy, Outreach and Communications Manager for the Homeland Security Information Network (HSIN), where he was responsible for stakeholder management and strategic messaging. Starting in the Spring of 2014, Brody worked as the Director for Policy, Architecture and Governance in the Information Sharing and Services Office of the OCIO – managing enterprise strategy development, new business engagements, communications and policy for a portfolio of programs that deliver vital IT mission support services across the homeland security enterprise. Most recently, since May, 2019, Mr. Brody serves as a Professor, representing DHS at the National Defense University and its College of Information and Cyberspace. He holds a Bachelor's Degree from the University of Pennsylvania, 2000, magna cum laude, a Juris Doctorate from the University Of Illinois College of Law, 20003, cum laude, a Masters Degree in Security Studies from the Naval Post-Graduate School's Center for Homeland Defense and Security, 2010, a Masters of Science Degree in National Security Strategy from the National War College, 2018, Distinguished Graduate (Top 10% of Class), and is DHS Senior Fellow.

**Linda Jantzen, Assistant Professor, College of Information and Cyberspace, National Defense University**



COL (USA Ret.) Linda Jantzen served for over twenty years as a network service provider in the U.S. Army in command and staff assignments at every level including deployments to Korea, the first Gulf War, Somalia, Bosnia, Germany, Kuwait, Iraq and Afghanistan. Pentagon tours include Chief of Operations for the Chief of Army Legislative Liaison and acting Chief Data Officer and Director of the Army Architecture Integration Center. Prior to coming to CIC she was Assistant Professor and Associate Dean of Faculty at National War College. COL Jantzen has authored several papers and articles on topics including adoption of innovation, digital transformation, and network operations in Iraq and Afghanistan. She is currently researching data culture and the use of data within the context of military operations. She is an avid student of military history focusing on the First World War. She has several degrees, including: B.A., Mass Communications, University of Illinois at Chicago; M.S., Telecommunications, Michigan State University; M.S., National Security Strategy, National War College, NDU; M.S., Science & Technology Studies, Virginia Tech.

# 10 Year Anniversary

# CYBER BEACON

## **Cameron F. Kerry, Ann R. & Andrew H. Tisch Distinguished Visiting Fellow, The Brookings Institute**



Cameron Kerry is a global thought leader on privacy, artificial intelligence, and cross-border challenges in information technology. He joined Governance Studies and the Center for Technology Innovation at Brookings in December 2013 as the first Ann R. and Andrew H. Tisch Distinguished Visiting Fellow. He leads two projects: The Privacy Debate, which engages policymakers and stakeholders on the national legislative debate on privacy, and the Forum for Cooperation on AI, a series of roundtables bringing together officials and experts from several countries to identify avenues of cooperation on AI regulation, standards, and research and development.

Previously, Kerry served as general counsel and acting secretary of the U.S. Department of Commerce, where he was a leader on a wide range of issues including technology, trade, and economic growth and security. He continues to speak and write on these issues, focusing primarily on privacy, artificial intelligence, and international data flows, along with other digital economy issues. During his time as acting secretary, Kerry served as chief executive of this Cabinet agency and its 43,000 employees around the world as well as an adviser to then President Barack Obama. His tenure marked the first time in U.S. history two siblings have served in the president's Cabinet at the same time.

As general counsel, he was the principal legal adviser to the several Secretaries of Commerce and Commerce agency heads. Kerry spearheaded development of the White House blueprint on consumer privacy, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. He then led the administration's implementation of the blueprint, drafting privacy legislation and engaging with international partners, including the European Union. He also was a leader in the Obama administration's successful effort to pass the America Invents Act, the most significant overhaul of the patent system in more than 150 years. He helped establish and lead the Commerce Department's Internet Policy Task Force, and was the department's voice on cybersecurity issues and similar issues in the White House "Deputies Committee." Kerry also played a significant role on intellectual property policy and litigation, cybersecurity, international bribery, trade relations and rule of law development in China, the Gulf Oil spill litigation, and other challenges facing a large, diverse federal agency. He traveled to the People's Republic of China on numerous occasions to co-lead the Transparency Dialogue with China as well as the U.S.-China Legal Exchange and exchanges on anti-corruption.

In addition to his Brookings affiliation, Kerry is a visiting scholar at the MIT Media Lab. He also served as senior counsel at Sidley Austin LLP in Boston, Massachusetts and Washington, D.C., where his practice involved privacy, security, and international trade issues.

## **Deborah Karagosian, Chief Executive Officer (CEO), Villuminati**



Deborah Karagosian is a graduate of the U.S. Military Academy and the School of Advanced Military Studies (SAMS) and attained master's degrees in computer systems, strategic management, and military theater operations. She's led multi-functional teams to solve the most complex problems in the cyberspace domain and served as the lead author of several CONOPs. As the founder of DKI Solutions, she brought together a mission-focused team supporting multiple government and industry organizations and served as a government-recognized expert on Russian and Chinese cyber and influence operations. At Booz Allen Hamilton, she continues to serve, guiding highly technical teams to identify and solve wicked problems arising from this new era of Great Power Competition.

10 Year Anniversary

# CYBER BEACON

## FIRESIDE CHAT

with

**General (Retired) Keith B. Alexander**



**Keith Brian Alexander** is a retired four-star general of the United States Army, who served as director of the National Security Agency, chief of the Central Security Service, and commander of the United States Cyber Command. He previously served as Deputy Chief of Staff, G-2 (Intelligence), United States Army from 2003 to 2005. He assumed the positions of Director of the National Security Agency and Chief of the Central Security Service on August 1, 2005, and the additional duties as Commander United States Cyber Command on May 21, 2010. Alexander retired on March 28, 2014. In May 2014, Alexander founded IronNet Cybersecurity, a private-sector cybersecurity firm based in Fulton, Maryland.

## MODERATED

by

**Gina Thomas**

**Distance Learning Student, College of Information and Cyberspace,  
Master of Science – MS Government Information Leadership, National  
Security and Cyberspace Studies, Distance Learning Program**



As a senior systems engineer for Acuity Innovations LLC, a Small Woman Owned Business, Gina leads a team of test engineer professionals to ensure MILSATCOM systems are fully evaluated and meet operational requirements. Retired from the United States Army in 2018 with 22 years of service, she served her local county government as the Senior IT Project Manager in Colorado. In 2019 she went on to serve as the Deputy Branch Chief for Defensive Cyberspace Operations/DODIN Operations for the Joint Force Headquarters – Cyber (Army), Cyberspace Operations-Integrated Planning Element (CO-IPE) in support of U.S Northern Command at Peterson Space Force Base, CO. Ms. Thomas holds Bachelor of Arts degree in Biochemistry from Benedictine College, A Master of Science Degree from Embry Riddle Aeronautical University in Organizational Leadership and is currently pursuing a Master of Science from the National Defense University in Government Information Leadership from the College for Information and Cyberspace.

10 Year Anniversary

# CYBER BEACON

## CLOSING REMARKS

by

**Erfana Dar, Student, Joint Professional Military Education II Resident Program, College of Information and Cyberspace, National Defense University**



A career Foreign Service officer, she served as Senior Post Management Officer in the Executive Office of the Bureau for Near Eastern Affairs from 2022-2023 and Counselor for Management Affairs at the U.S. Embassy in Kuala Lumpur from 2019-2022. She began her diplomatic career in 2003 and served in reporting and management positions in U.S. Missions in Greece, Moldova, Iraq, Brussels and Cote d'Ivoire.

In Washington she has served as Senior Advisor in the Bureau for European and Eurasian Affairs, in the Office of the Undersecretary for Management as a Special Assistant, and as a Watch Officer in the Office of the Secretary, Executive Secretariat. She has received numerous State Department performance awards. A graduate of Gonzaga University, Erfana speaks French, Russian and Kashmiri. She is married to U.S. diplomat Andrew Johnson.

Day 2

OCTOBER 20<sup>th</sup>

10 Year Anniversary

# CYBER BEACON

## OPENING REMARKS

by

**Dr. Amy Hamilton, Visiting Faculty Chair, Department of Energy,  
College of Information and Cyberspace, National Defense University**



Amy S. Hamilton, Ph.D. is the Visiting Faculty Chair from the Department of Energy to the Department of Defense (DOD) National Defense University (NDU) College of Information and Cyberspace (CIC). She has served for the past three years as the Senior Advisor for National Cybersecurity Policy and Programs at the Department of Energy. She spent two years as a senior cyber security policy analyst at the Office of Management and Budget, Executive Office of the President. She served in the Michigan Army National Guard as a communications specialist and was commissioned into the U.S. Army Officer Signal Corp, serving on Active Duty and later the U.S. Army Reserves. She has worked at both the U.S. European Command and the U.S. Northern Command & North

American Aerospace Defense Command (NORAD) on multiple communications and IT projects. She became a certified Project Management Professional through the Project Management Institute in 2007 and earned her Certified Information Security Manager certification in 2011. She presented on the “The Secret to Life from a PMP” at TEDxStuttgart in September 2016. She taught Project Management Tools at Colorado Technical University and was a facilitator for the Master’s Degree Program in Project Management for Boston University. She is an award-winning public speaker and has presented in over twenty countries on overcoming adversity, reaching your dreams, cyber security, and project management.

10 Year Anniversary

# CYBER BEACON

## MORNING KEYNOTE

by

**Laura Galante, Cyber Threat Intelligence Integration Center (CTIIC),  
Office of the Director of National Intelligence (ODNI)**



Laura Galante has served as the Intelligence Community's Cyber Executive and Director of the Cyber Threat Intelligence Integration Center (CTIIC) for the Office of the Director for National Intelligence since May 2022. In this role, Ms. Galante is responsible for driving a coordinated approach to cyber intelligence collection and analysis, aligning strategic investments with national security priorities, and leading intelligence efforts to respond to major cybersecurity incidents.

Ms. Galante brings extensive security industry experience to her current role. From 2017 to 2021, she assisted multiple Ukrainian government agencies to improve their cyber defense operations, directed an international task force to monitor cyber and information threats to

Ukraine's 2019 presidential election and served as an expert witness in multiple cyber warfare trials. She spoke frequently on states' use of cyberspace at international and industry conferences including a 2017 TED Talk.

Ms. Galante was previously the Director of Global Intelligence at Mandiant (formerly FireEye Inc.), the cybersecurity firm. Her team discovered and attributed multiple state and criminal cyber operations, to include the Russian military's "APT28." She developed intelligence products to improve the security posture of Fortune 500 companies, critical infrastructure providers, non-profits, government agencies, and international partners. Prior to her role at Mandiant, Ms. Galante served at the Defense Intelligence Agency where she led a team responsible for analyzing Russian cyber capabilities. She began her career at the Department of State.

Ms. Galante holds a B.A. in Foreign Affairs and Italian from the University of Virginia and a J.D. from the Catholic University of America. She is a Term Member of the Council on Foreign Relations and a former Senior Fellow at the Atlantic Council. Ms. Galante is a proud 4-H alumna, a livestock club leader, and lives on a farm in rural Virginia with her husband and son.

## FIRST PANEL

# Emerging Technology & National Security Interests

(10:15 – 11:15)

**Abstract 1:** Here are some key lessons on the use of emerging technologies in modern warfare from the Russia-Ukraine conflict: Drones are a game-changer, Resilient communications are critical, AI and big data analytics enable intelligence advantages, Cyber threats are persistent, and Satellite intelligence is now indispensable. Overall, the war shows existing and emerging technologies alike now play a pivotal role in modern military operations. Agility in adoption and employment of new tools and tactics is increasingly vital for battlefield advantage.

**Abstract 2:** The 2022 National Security Strategy highlights the challenge emerging technology presents in the context of maintaining credibility for deterrence. The Russo-Ukrainian War provides a critical example of failing this challenge. The US-backed successful counter of the Russian military followed perceptions of lackluster innovation and development of defense solutions for the contemporary battlefield on the part of Ukraine. The U.S. Government, and the governments of Partners and Allies, should continue to invest in all aspects of understanding emerging technology. The goal should be to create a shared military-technological collaborative approach. However, rapid proliferation of defense technology, strained relational capacity across partnerships, and status quo systems of multilateralism complicate goal achievement.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

### Frank Konkell, Vice President, Editorial, NextGov/FCW



Frank Konkell is vice president of editorial and an editor at large for Nextgov/FCW. He writes about the intersection of government and technology. Frank began covering tech in 2013 upon moving to the Washington, D.C., area after getting his start in journalism covering local and state issues at daily newspapers in his home state of Michigan. Frank was born and raised on a dairy farm and graduated from Michigan State University.

## Panelists

### Dr. Jill Goldenziel, Professor, College of Information and Cyberspace, National Defense University



Dr. Jill Goldenziel is a Professor at the National Defense University's College of Information and Cyberspace. She is also an Affiliated Scholar at the University of Pennsylvania's Fox Leadership International Program and Penn's Partnership for Effective Public Administration and Leadership Ethics.

Dr. Goldenziel's award-winning scholarship focuses on international law, lawfare, information warfare, U.S. and comparative constitutional law, the law of war, refugees and migration, and leadership. Her award-winning work has appeared in the *Cornell Law Review*, the *American Journal of International Law*, the *American Journal of Comparative Law*, the *Virginia Journal of International Law*, the *University of Pennsylvania Journal of Constitutional Law*, and the *Arizona State Law Journal*, among other scholarly journals. Dr. Goldenziel is also a *Forbes.com* contributor on Defense and National Security and is frequently quoted and cited in the press.

Dr. Goldenziel is a sought-after speaker and consultant. She regularly advises elite Marine units, the Joint Force, Combatant Commands, and civilian agencies on lawfare and legal issues, and has briefed senior military and civilian leadership on her research. She received the 2022 Serge Lazareff Prize from NATO's Allied Command Operations Office of Legal Affairs at Supreme Headquarters Allied Powers Europe for her work on legal operations (known elsewhere as lawfare or counter-lawfare). Since 2016, Dr. Goldenziel has had High-Level involvement in the processes to negotiate, create, and implement the UN Global Compact for Migration (GCM), as a representative of the Academic Council on the UN System. She spoke as the primary representative from academia at the 2022 UN International Migration Review Forum Stakeholder's Meeting, spoke alongside world leaders before 164 UN Member-States at the Intergovernmental Conference to Adopt the GCM, and submitted draft language for both documents and the New York Declaration for Refugees and Migrants.

Dr. Goldenziel was previously a Professor at U.S. Marine Corps University-Command and Staff College, a Climenko Fellow and Lecturer on Law at Harvard Law School, a Research Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs, a Lecturer on Government and Social Studies at Harvard College, and a Visiting Assistant Professor at the Boston University School of Law. She clerked for Judge Thomas Buergenthal (Ret., International Court of Justice) and Prof. William W. Park on ICSID investor-state international arbitration tribunals. She has been a Visiting Scholar at iCourts at the University of Copenhagen and a Scholar-in-Residence at the International Arbitration practice of WilmerHale in London.

Dr. Goldenziel holds a Ph.D. and an A.M. in Government from Harvard University, a J.D. from the New York University School of Law, and an A.B. from Princeton University.

# 10 Year Anniversary

# CYBER BEACON

## Shawn Powers, Executive Director of the United States Advisory Commission on Public Diplomacy, Department of State



Shawn Powers serves as the Executive Director of the United States Advisory Commission on Public Diplomacy, a body authorized by Congress to oversee and promote U.S. Government activities that intend to understand, inform, and influence foreign publics. He has a Ph.D. from the Annenberg School for Communication and Journalism at the University of Southern California (USC) and more than a decade of experience working at the nexus of public diplomacy, development, and national security.

Shawn's career began in 2003 at the Center for Strategic and International Studies (CSIS), where he was a research assistant in the International Security Program. In 2004, he started his graduate work at USC and led a number of research projects on international broadcasting and global media at the Center on Public Diplomacy (CPD). Since 2010, Shawn has taught at Georgia State University, where he launched and directed its Center for Global Information Studies and remains an Associate Professor on leave.

As an academic, Shawn researched the geopolitics of information and technology and recently published (with Michael Jablonski) *The Real Cyber War: A Political Economy of Internet Freedom* (The University of Illinois Press, 2015). He has over 40 publications in academic and mainstream outlets, including *The Washington Post*, *Guardian*, and *Huffington Post*. Shawn previously worked with the Advisory Commission on its 2014 report, *Data Driven Public Diplomacy*, when he led a team of investigators in assessing the Broadcasting Board of Governors' research and evaluation efforts. His research has been supported by grants from the British Council, Department of Defense, Department of State, European Commission, Knight Foundation, Open Society Foundation, and U.S. Institute for Peace, and he's received fellowships from the London School of Economics, University of Pennsylvania, Oxford, and Central European University.

Shawn received B.A.'s in International Affairs and Communication from University of Georgia before earning his M.A. and Ph.D. from USC. He serves on the executive committee of the International Studies Association International Communication division, and has been invited to speak at the Al Jazeera Forum, Austrian Diplomatic Academy, British Broadcasting Corporation, Council on Foreign Relations, United Nations, World Summit of Nobel Peace Laureates, and over 30 universities.

## Justin Fanelli, Chief Technology Officer, Department of the Navy



Mr. Justin Fanelli is the Acting CTO for the Dept of Navy and the Technical Director of PEO Digital. As CTO, he is chartered to measurably improve technology-driven mission outcomes within the Dept of Navy. As TD, the PEO is chartered to expedite the performant, secure transformation of enterprise IT infrastructure within the Dept of Navy's acquisition apparatus. He currently serves as an Advisor for Advanced Research Project Agency – Health (ARPA-H). Recent roles for Mr. Fanelli have included, Chief Data Architect for Defense Health, Technical Director for Navy Manpower, Personnel, Training and Education (MPTE), Executive Lead for Navy's Digital Transformation in 5G and DevSecOps. With Dept of Navy roles, Mr Fanelli's team has recently been recognized for transforming modern service delivery including multi-billion dollars in cost avoidance and leapahead impacts with the Etter Award. Within Defense Healthcare, Mr. Fanelli's teams delivered the first one-stop data enterprise for revolutionized healthcare and research outcomes. Previously within DOD, Mr. Fanelli has served as a Service Chiefs Fellow at the Defense Advanced Research Project Agency (DARPA), Principal Engineer for Navy Enterprise Business Systems and Chief Systems Engineer for Command and Control (C2).

Outside of the office, Mr. Fanelli teaches technology courses at Georgetown University and advises on innovation. He holds a Bachelors degree in Electrical Engineering from the Pennsylvania State University, a Masters degree in Electrical and Systems Engineering from the University of Pennsylvania and is a Senior Executive Fellow at the Harvard Kennedy School. He is certified in Lean Six Sigma, Agile Development, GIAC Security Leadership, Defense Acquisition University Engineering and Program Management, has served as Philadelphia Mayor's Commission on Technology (MCOT) Board Member, North Catholic High School Alumni Association President, currently serves as an advisor to National Science Foundation startups, a partner at NextGen Ventures, a Cornerstone Schools Executive Board Member, volunteer and speaker at TechImpact and AFCEA and is a member of the Cosmos Club. His awards include National Intelligence Meritorious Unit Citation, Civilian Exemplary Achievement Award, Secretary of the Navy's Innovation Award, Project Management Institute's Project of the Year, Federal Health IT Innovation Award and he is a two time FedHealth 100 honoree. He lives in Arlington, VA and loves book recommendations.

10 Year Anniversary

# CYBER BEACON

**Sam Bendett, Adjunct Senior Fellow, Technology and National Security Program,  
Center for Naval Analysis (CNA)**



Samuel Bendett is an Adviser with CNA Strategy, Policy, Plans and Programs Center (SP3), where he is a member of the Russia Studies Program. His work involves research on the Russian defense and technology developments, unmanned and autonomous military systems and Artificial Intelligence, as well as Russian military capabilities and decision-making during crises. He is an honorary “Mad Scientist” with the USARMY TRADOC’s Mad Scientist Initiative. He is also a Russian military autonomy and AI SME for the DOD’s Defense Systems Information Analysis Center.

Prior to joining CNA, Mr. Bendett worked at the National Defense University on emerging and disruptive technologies for government response in crisis situation, where he conducted research on behalf of the Office of the Secretary of Defense for Policy (OSD-P) and Acquisition, Technology and Logistics (OSD-AT&L). His previous experience includes working for US Congress, private sector and non-profit organizations on foreign policy, international conflict resolution, defense and security issues.

Mr. Bendett’s analyses, views and commentary on Russian military robotics, unmanned systems and Artificial Intelligence capabilities appear in the C4ISRnet, DefenseOne, War on the Rocks, Breaking Defense, The National Interest, War Is Boring, and The Strategy Bridge. He frequently presents on the Russian unmanned systems and AI to the US government, private industry and academia, as well as think tanks and policy centers. Between 2008 and 2016, he was a foreign policy and international affairs contributor to the RealClearWorld.com blog. Samuel Bendett received his M.A. in Law and Diplomacy from the Fletcher School, Tufts University and B.A. in Politics and English from Brandeis University. He has native fluency in Russian.



## SECOND PANEL

# Joint Warfighting & Cyberspace Operations: U.S. Military Responsibilities, Authorities, & Capabilities in Cyber Warfare

(11:15 – 12:15)

**Abstract 1:** The military responsibility of conducting Cyberspace operations assumes the requisite authorities and capabilities to gain warfighting advantages to safeguard vital national interests, as outlined in the 2022 National Security Strategy. Cyberspace operations complement the Joint Force global campaigns, linking Allies and partners such as the Quad to rapidly respond to attacks according to the 2022 National Defense Strategy. However, the proliferation of technology has increased the capabilities of adversarial state and non-state actors to operate in cyberspace, which places a premium on determining the placement of cyberspace capabilities to protect DOD networks. Moreover, the Department of Defense, and the Joint Force, maintains multi-service modernization efforts to ensure U.S. Cyber Mission Forces can effectively support global campaign operations while also defending the nation from cyber-attacks. The ability to conduct strategically focused cyberspace operations in a globally contested domain will continue to challenge cyberspace professionals, especially members of the Joint Force. Senior military officials should consider establishing a permanent single-source service provider for recruiting, training, educating and equipping cyberspace professionals for cyberspace operations and Joint Warfighting.

**Abstract 2:** Joint warfighting and cyberspace operations refer to the coordinated efforts of multiple military branches or services to conduct operations in the cyberspace domain. This involves leveraging cyberspace capabilities to support broader military objectives and enhance overall warfighting effectiveness. Cyberspace operations can encompass offensive, defensive, and intelligence activities in the cyberspace domain. The integration of cyberspace operations into joint warfighting allows for the synchronization of cyber capabilities with other military domains such as land, sea, air, and space. This integration enables the military to leverage cyberspace as a domain for gaining and maintaining a competitive advantage over adversaries.

QR Code to Access the Poll



# 10 Year Anniversary

# CYBER BEACON

## Moderator

### Christina Ayiotis, Cyber Strategist and Consultant, CRM, CIPP/E



An internationally recognized business executive and attorney, Christina Ayiotis brings a unique strategic perspective, honed from years of building substantive (geopolitically contextualized) cyber expertise. A true "Cyber Connector," she brings together cross-functional/international constituencies to foster productive collaborative solutions. She founded and Co-Chaired the Georgetown Cybersecurity Law Institute and served on AFCEA International's Cyber Committee and The Cybersecurity Canon Committee. Ranked #18 on *Thomson Reuters' 2018 List of Top 50 Social Influencers in Risk, Compliance and RegTech*, she is featured in *Women Know Cyber: 100 Fascinating Females Fighting Cybercrime* (May 2019) and is recognized as one of *The Top 15 Women in Cybersecurity and InfoSec Today* (March 2019); *Top 50 Women in Internet Security* (January 2017); *Top 20 Women in #InfoSec to follow on Twitter* (July 2016) and *Top #InfoSec People to Follow on Twitter*. She taught a Masters Level *Information Policy* class at GW, served as Deputy General Counsel—Information Governance at CSC, and led global programs at Booz Allen Hamilton, Ernst & Young International, and Deloitte Touche Tohmatsu. She served on the Boards of Directors of ARCS MWC, Fairfax Law Foundation, ARMA NOVA, Hellenic American Women's Council and Women's Bar Association of DC. She earned a *Zertifikat Deutsch als Fremdsprache* from the Goethe Institute and studied French at the Alliance Française, Paris. In 2008, she earned the Certified Records Manager certification. A *magna cum laude* graduate of Virginia Commonwealth University (BS-Biology/ BA-Philosophy; Minors- Mathematics/French; University Honors), she earned a Juris Doctorate from William & Mary Law School. She has been an active Member in Good Standing of the Virginia State Bar since 1991 and the District of Columbia Bar since 1993.

## Panelists

### Dr. J.D. Work, Professor, College of Information and Cyberspace, National Defense University



J.D. Work is a Professor at the National Defense University (NDU) College of Information and Cyberspace (CIC). His research focuses on cyber intelligence, operational art, and strategy in conflict and competition. Mr. Work has over 25 years' experience working in cyber, intelligence, and operations roles for the private sector and U.S. Government. He holds additional affiliations with the Saltzman Institute of War and Peace Studies at the School of International and Public Affairs at Columbia University, the Krulak Center for Innovation and Future Warfare at the Marine Corps University, and the Cyber Statecraft Initiative at the Atlantic Council.

### Dr. Aaron Brantly, Associate Professor, Virginia Tech



Aaron Brantly, an associate professor of political science and director of the Tech4Humanity lab at Virginia Tech, has worked on issues related to cybersecurity from multiple angles, including human rights and development, intelligence and national security, and military cybersecurity. His interests span the political science and computer science divide. He is currently working on a yearlong project on cyber deterrence funded by OSD Minerva R-Def.

10 Year Anniversary

# CYBER BEACON

## Dr. Melissa Griffith, Lecturer, Johns Hopkins University School of Advanced International Studies (SAIS)



**Dr. Melissa K. Griffith** is a Lecturer in Technology and National Security at Johns Hopkins University School of Advanced International Studies' (SAIS) Alperovitch Institute for Cybersecurity Studies as well as a Non-Resident Research Fellow at the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC). She works at the intersection between technology and national security with a specialization in cybersecurity, semiconductors, and 5G networks focused on national risk and resilience models.

Griffith's book project investigates how relatively small countries, with limited resources, have become significant providers of national cyber-defense for their populations. Her work sheds important light on the components and dynamics of cyber power and cyber conflict, as well as the vital role that public-private cooperation and both security and economic policy play in cyber-defense. Concurrent research projects examine (1) the security implications of 5G; (2) collective defense and resilience in cyberspace; (3) emerging technologies and great power competition; and (4) power and smaller states in international politics.

Previously, Griffith was the Director of Emerging Technology and National Security and a Senior Program Associate at the Woodrow Wilson International Center for Scholars' Science and Technology Innovation Program (STIP); a Pre-Doctoral Fellow at Stanford University's Center for International Security and Cooperation (CISAC); an Affiliated Researcher at UC Berkeley's Center for Long-Term Cybersecurity (CLTC); a Visiting Scholar at George Washington University's Institute for International Science & Technology Policy (IISTP); a Visiting Research Fellow at the Research Institute on the Finnish Economy (ETLA) in Helsinki, Finland; and a Visiting Researcher at the Université Libre de Bruxelles (ULB) in Brussels, Belgium.

Griffith holds a Ph.D. in Political Science from the University of California, Berkeley (2020); an M.A. in Political Science from the University of California, Berkeley (2014); and a B.A. in International Relations from Agnes Scott College (2011). She was an English Teaching Assistant with the Fulbright Program from 2012-2013.

10 Year Anniversary

# CYBER BEACON

## CLOSING REMARKS

by

**James Schmeling, Chief Executive Officer, National Defense University  
Foundation (NDUF)**



NDUF's President and CEO James Schmeling, J.D., has over 25 years of unparalleled experience in building and leading organizations focused on higher education, military veteran nonprofits, and public private partnerships. Schmeling is a U.S. Air Force veteran. Post-service he earned a B.A. in political science with a minor in international studies (Latin America) from Iowa State University and a Juris Doctorate (JD) with distinction from the University of Iowa College of Law.

# POSTER CONTEST

QR Code to Vote on Posters



# MASH UP

## Poster #1



**THE FUTURE IS NOW**



**CYBER BEACON**

Exploring Cyberspace Through Engaging Thought

# 2023

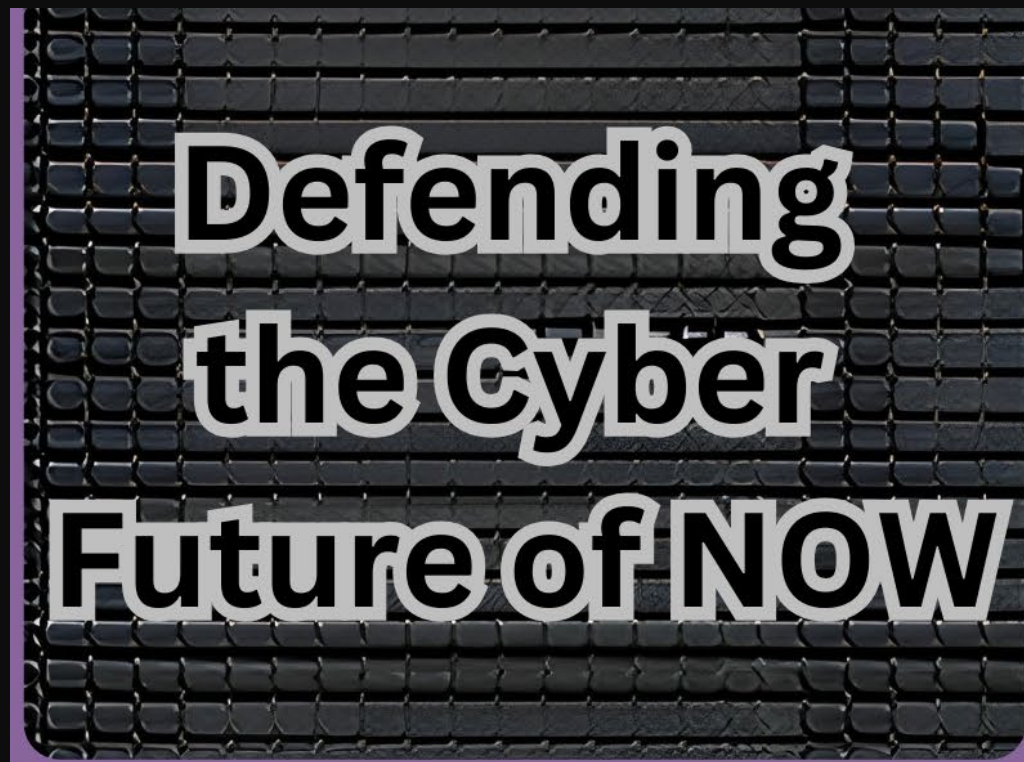
# DISTANCE LEARNING (DL)

## Poster #1



# DISTANCE LEARNING (DL)

## Poster #2

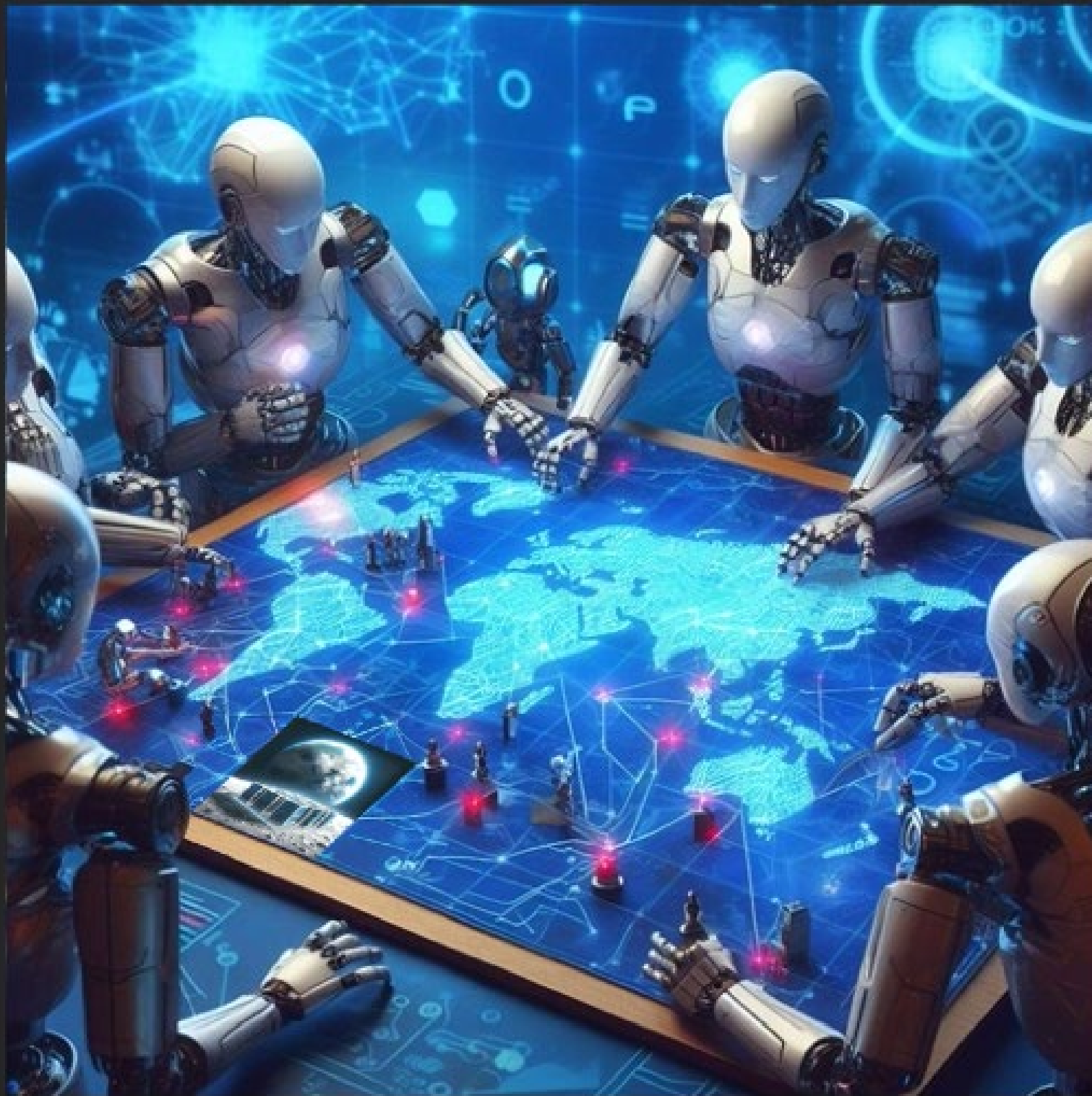


# JPME

## Poster #1

### The Future of Cyber

*"Who controls the tech, controls the cyber"*



**A strategy game of computational & data resourcing for  
cyber hegemony**

# JPME

## Poster #2



# JPME

## Poster #3

### Cyber Beacon 2023 The Future is NOW!!



# JPME

## Poster #4



**CYBER BEACON 2023 THE  
FUTURE IS NOW!!**

JPME

Poster #5



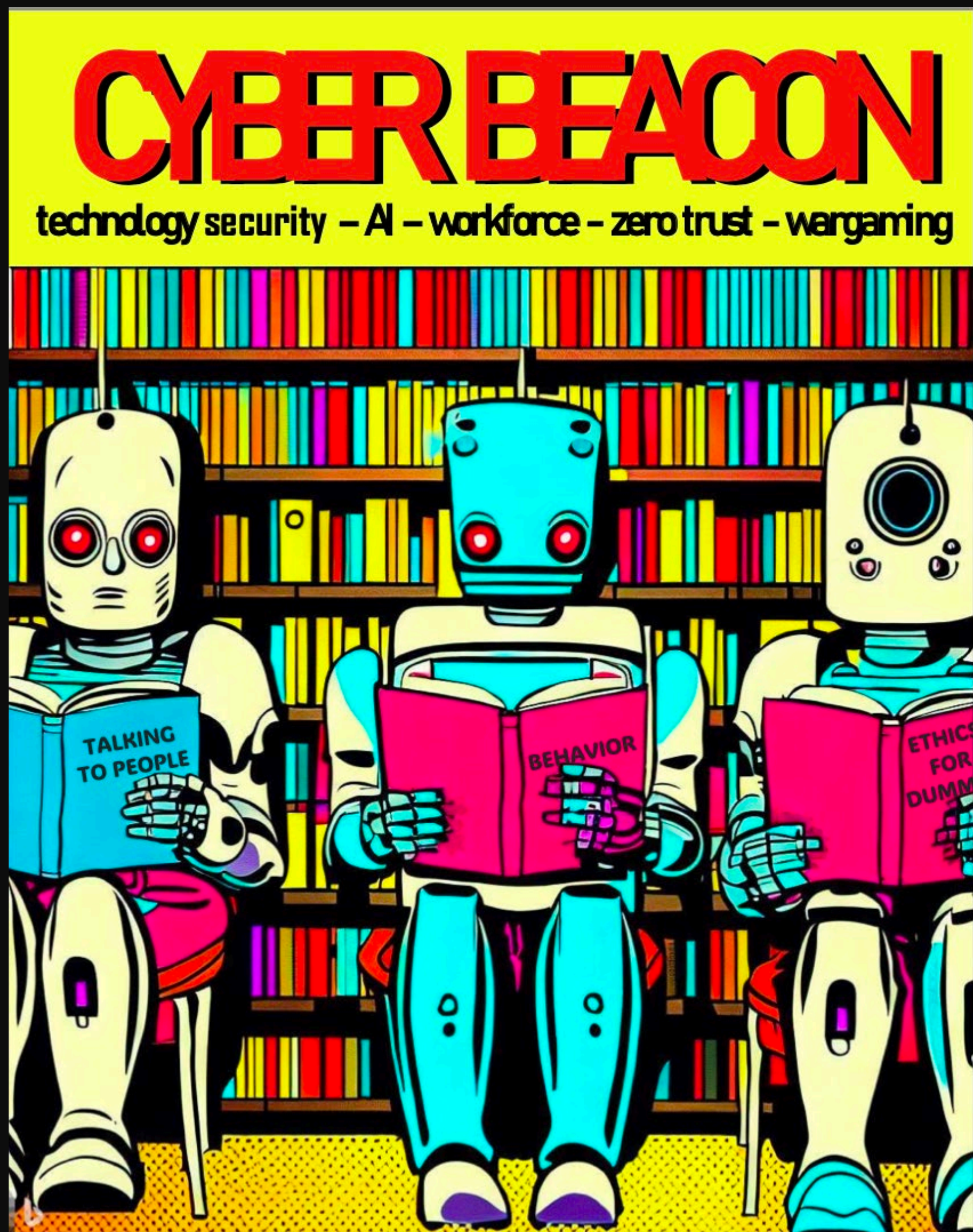
# JPME

## Poster #6



# LDP

## Poster #1



# LDP

## Poster #2

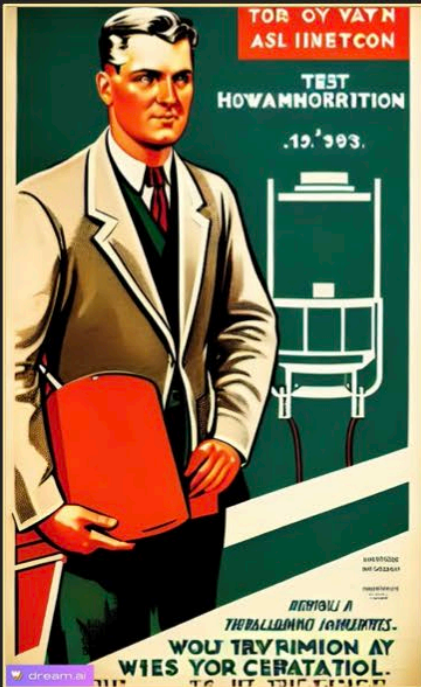


### *Cyber Beacon 2023: A Conference Poster Centennial Retrospective*

1923



1933



1943



1953



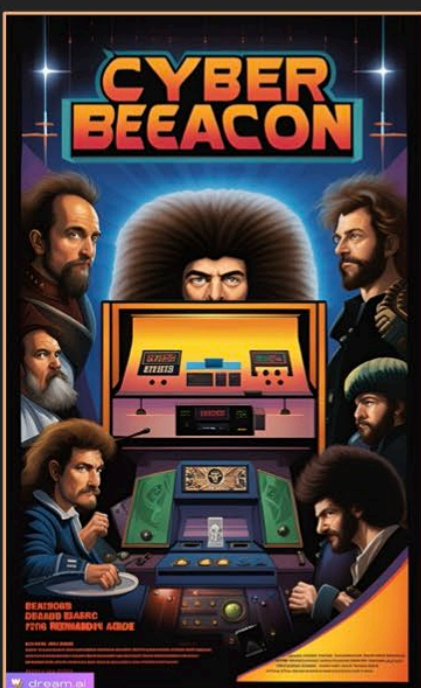
1963



1973



1983



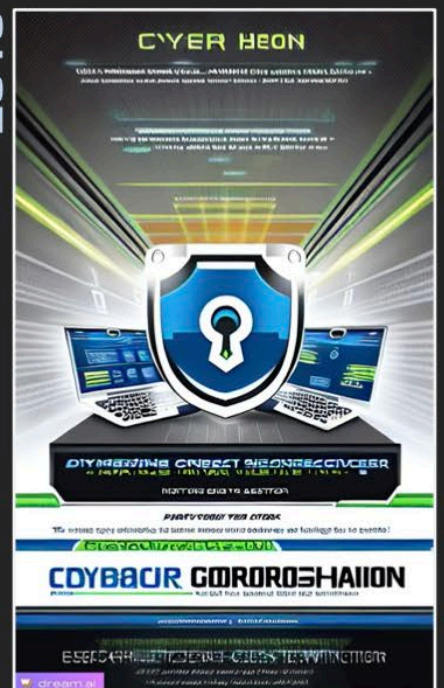
1993



2003



2013



Ten images generated using dream.ai; no human post-processing.

# LDP

## Poster #3

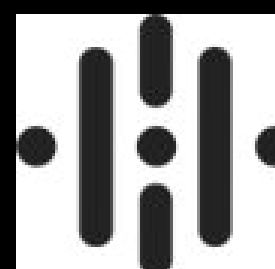


THANK YOU TO OUR  
SPONSORS !



**Booz  
Allen®**

**CIRCADENCE** 

 **Recorded Future®**

# INFORMATION HALL



JOIN US AGAIN  
AT OUR  
UPCOMING EVENTS!

# Department of Defense

## UNIVERSITY CONSORTIUM FOR CYBERSECURITY WORKSHOP

Hosted by  
National Defense University  
College of Information and Cyberspace

December 6, 2023

0900 - 1600 EST

<https://cic.ndu.edu/UC2>





# UC2

## University Cybersecurity Consortium

Connect with us



### Mission



Serve as a hub for cybersecurity research in the DoD where the SECDEF and academic institutions can connect

### Communicate



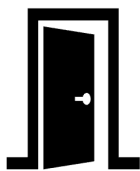
Build a shared vocabulary to improve two-way communication about hard problems.

### Collaborate



Create partnerships to learn where research can go next when DoD and academia work together.

### Access



Provide opportunities to understand the priorities, hurdles, and horizons across the community.



**SAVE THE DATE**



# CYBER BEACON 2024

**JOIN US AGAIN**

**October  
17 & 18, 2024**