CYBER SYMPOSIUM 2023

FOCUS ON THE FUTURE

United States Cyber Command and The College of Information and Cyberspace National Defense University Marshall Hall

Dec 5th, 2023

CYBER SYMPOSIUM 2023

FOCUS ON THE FUTURE

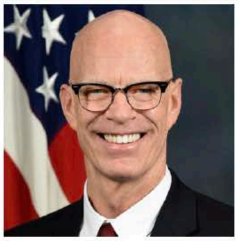
0730 - 0800	Check-in and Breakfast
0800 - 0805	Opening Remarks
0805 - 0810	Welcoming Remarks
0810 - 0840	Keynote Address
0840 - 0900	Break and Network
0900 - 1015	Panel 1: Technology & Capabilities
1015 - 1030	Break and Network
1030 - 1145	Panel 2: People & Partnerships
1145 - 1245	Lunch and Network
1245- 1315	Afternoon Keynote Address
1315 - 1430	Panel 3: Strategy & Policy
1430 - 1445	Break and Network
1445 - 1600	Panel 4: Synthesis & Insights
1600 - 1630	Leader Fireside Chat
1630 - 1700	Closing Remarks
1700 - 1900	Social

CYBER SYMPOSIUM 2023

FOCUS ON THE FUTURE

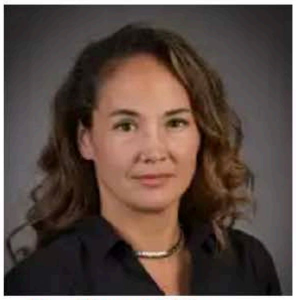
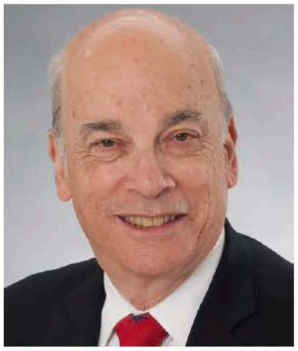
Focus on the Future:
Technology, People, and Policy

0730-0800	Check-in and Breakfast
0800-0805	Opening Remarks: Chancellor Lewis (College of Information and Cyberspace, NDU)
0805-0810	Welcoming Remarks RDML Velez (J5 USCYBERCOM)
0810-0840	Keynote Address: GEN Nakasone (CDR, USCYBERCOM)
0840-0900	Break & Network
0900-1015	Panel 1 Technology & Capabilities • Moderator: Ms. Katie Sutton (Chief Technology Advisor to the CDR, USCYBERCOM) • Panelist 1: Mr. Dennis Dias (U.S. Naval Academy) • Panelist 2: Dr. Melissa Thomas (Professor, College of Information and Cyberspace) • Panelist 3: Mr. Sri Iyer (Senior Manager Emerging Technology at Amazon)
1015-1030	Break & Network
1030-1145	Panel 2 People & Partnerships • Moderator: COL Pedro Rosario (USCYBERCOM J1) • Panelist 1: Dr. Nina Kollars (Professor of Cyber and Innovation Policy Institute, U.S. Naval War College) • Panelist 2: Dr. Joe Billingsley (Senior Policy Advisor, Cyber Work Force and Education, WH ONCD) • Panelist 3: Mr. Frank Kramer (Atlantic Council)
1145-1245	Lunch & Network
1245-1315	Afternoon Keynote Address: Dr. Dan Ragsdale (Deputy Asst National Cyber Director (ONCD), White House)
1315-1430	Panel 3 Strategy & Policy • Moderator: Markus Rauschecker, J.D. (Cybersecurity Program Manager, CHHS, UMB) • Panelist 1: Dr. Jim Miller (Asst. Dir. Policy and Analysis, Johns Hopkins APL) • Panelist 2: Dr. Doyle Hodges (Johns Hopkins) • Panelist 3: Ms. Michele Markoff (Distinguished Scholar, College of Information and Cyberspace)
1430-1445	Break & Network
1445-1600	Panel 4 Synthesis & Insights • Moderator: Brig Gen Novotny (Dep J5 USCYBERCOM) • Panelist 1: Dr. Richard Love (Professor, College of Information and Cyberspace) • Panelist 2: Dr. Joe Chapa (Chief Air Force AI Cross-Functional Team) • Panelist 3: Dr. Michael Sulmeyer (Principal Cyber Advisor to the Secretary of the Army) • Panelist 4: BRIG Robert "Doc" Watson (USCYBERCOM Deputy J3)
1600-1630	Leader Fireside Chat: Lt Gen Haugh w/ Dr. Cassandra Lewis (Chancellor, College of Information and Cyberspace)
1630-1700	Closing Remarks: Lt Gen Haugh
1700-1900	Social: Hosted by the Military Cyber Professionals Association (MCPA)

Leaders (in order of appearance)	
 Dr. Cassandra Lewis	Dr. Cassandra C. Lewis is the Chancellor, and former Dean of Faculty and Academic Programs, at the National Defense University (NDU) College of Information and Cyberspace (CIC). She serves as the principal advisor to the National Defense University President and Provost on curriculum and academic programs related to cyberspace and information. She maintains relationships with partner NDU components, U.S. government agencies, the private sector, international allies, Department of Defense and civilian educational institutions and universities, and has engaged in international capacity building on the behalf of the University. 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.
 RDML Velez	Rear Admiral Dennis Velez is the Director of Plans and Policy, U.S. Cyber Command. At sea, Velez completed tours aboard USS Stout (DDG 55), USS Carr (FFG 52), USS Gettysburg (CG 64), and USS Donald Cook (DDG 75). He served on afloat staffs with Commander, U.S. Second Fleet/Striking Fleet Atlantic aboard USS Mount Whitney (LCC 20) and as the deputy commander for Destroyer Squadron Fifteen in Japan. He was the commanding officer of USS Fitzgerald (DDG 62) and USS San Jacinto (CG 56). Ashore, Velez served as officer in charge of Western Hemisphere Group Caribbean Area Coordinator; Surface Placement branch head, Head Junior Surface Warfare Distribution, Assistant Captain detailer and deputy director for Surface Warfare Distribution at Naval Personnel Command; Joint Staff Strategic Plans and Policy Directorate as chief, North East Asia Division and assistant director for Political-Military Affairs, Asia. He is a 1992 graduate of the United States Naval Academy with a Bachelor of Science in Aerospace Engineering. He also earned a Master's degree in Information Technology Management from Touro University in 2004.
 GEN Paul Nakasone	General Paul M. Nakasone assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in May 2018. He previously commanded U.S. Army Cyber Command from October 2016 -April 2018. GEN Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. GEN Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. He has also commanded a company, battalion, and brigade, and served as the senior intelligence officer at the battalion, division and corps levels. GEN Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.
 Dr. Dan Ragsdale	Dr. Daniel "Rags" Ragsdale is the Deputy Assistant National Cyber Director at the Office of the National Cyber Director (ONCD) in the White House. He previously served in DoD for over 40 years including a wide range of operational and academic roles as an Army Officer and then Civilian, culminating with service as Principal Director for Cyber and then Acting Director of Defense Research and Engineering (R&E) for Modernization in OUSD R&E. He was also a Program Manager at DARPA, Vice Dean for Education at the US Military Academy (USMA), Founding Director of the Texas A&M Cybersecurity Center, and Vice President of DoD Strategy at Two Six Technologies. He is a 1981 graduate from West Point. He has a Master of Science degree in Computer Science from the Naval Postgraduate School and a Ph.D. in Computer Science from Texas A&M University.
 Lt Gen Haugh	Lt. Gen. Timothy D. Haugh is the Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Maryland. Prior to this assignment, Lt. Gen. Haugh served as Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, Joint Base San Antonio-Lackland, Texas. The general has commanded at the squadron, group, wing, numbered air force, and joint levels and served on staffs at major command, agency and combatant command headquarters. Lt. Gen. Haugh's previous joint general officer assignments include serving as the Commander, Cyber National Mission Force, and the Director of Intelligence, U.S. Cyber Command. He holds a Bachelor of Arts, Russian Studies, Lehigh University, Bethlehem, Pa., a Master of Science, Telecommunications, Southern Methodist University, Dallas, a Master of Science, Joint Information Operations, Naval Postgraduate School, Monterey, and a Master of Science, National Resource Strategy with a concentration in Information Operations, Industrial College of the Armed Forces, Fort McNair.

Panel 1 Technology and Capabilities	
 Ms. Katie Sutton	Ms. Katie Sutton joined United States Cyber Command in June 2023 as the Chief Technology Advisor to the Commander and Director of Pentagon Operations to advise the Commander on the development of engineering strategies and policies necessary to execute the Command's authorities for service-like functions, workforce management, acquisition, and enhanced budget control. Additionally, she is responsible for engaging with academia, media, and industry to represent USCYBERCOM cybersecurity, policy, and strategic communications initiatives. She graduated with highest honors from the University of Illinois at Urbana-Champaign with a BS in Electrical Engineering and has an MS from Stanford University in Electrical Engineering.
 Mr. Dennis Dias	Mr. Dennis Dias currently serves as the Office of Naval Research Chair of Cyber Science at the US Naval Academy where he teaches the Capstone course for senior cyber operations majors. These courses cover offensive and defensive hacking operations using open-source tools. He was selected for elevation to the Senior Executive Service (SES) in 2015. He led the NSA Office of Analytics and Tradecraft (A&T). Prior to his assignment as Chief of A&T, Mr. Dias was the Deputy Office Chief of the Tailored Access Operations (TAO)/Telecommunications and Networking Technologies Office and a Director of Cybersecurity Operations (DCO) in the National Threat Operations Center. Mr. Dias has a BS degree in Engineering from the US Naval Academy and a MS in Computer Systems Management from the University of Maryland University College. He is a 2009 graduate of the Defense Leadership and Management Program and a 2008 graduate of the Army War College.
 Dr. Melissa Thomas	Dr. 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.
 Mr. Sri Iyer	Mr. Sri Iyer is a Senior Technology Leader at Amazon for the Worldwide Public Sector | AI/ML, Quantum, and Specialty Solutions. He is an experienced Emerging Technology leader with a demonstrated history of helping organizations solve complex business problems using disruptive technology as an enabler. He has led development of numerous Data Analytics, Artificial Intelligence, Quantum, and Automation projects for clients across public and private sectors. He is skilled in Agile Methodologies, Cloud Computing, Data Analytics, Machine Learning, and Software Development. He is a strong sales professional with over a dozen industry certifications and a Master's degree focused in Information Technology Management and Data Science.

Panel 2 People and Partnerships

COL Pedro Rosario	COL Pedro J. Rosario assumed his present duties as Director, Manpower and Personnel, U.S. Cyber Command in July 2023. He was previously the G1 for 1st Special Forces Command (Airborne) at Ft. Liberty, North Carolina. COL Rosario has held command and staff positions in the United States, Iraq, and Afghanistan. COL Rosario has served in Joint assignments in HQs, U.S. Special Operations Command and has served on a Special Operations Joint Task Force in both Iraq and Afghanistan. COL Rosario is a Senior Service College graduate of the Dwight D. Eisenhower School, where he received a graduate degree in National Security and Resource Strategy. COL Rosario is also a Command and Staff College graduate of the Naval Postgraduate School (NPS), where he received a graduate degree in Irregular Warfare from the Defense Analysis Program (Special Operations Low Intensity Conflict). At NPS, COL Rosario was the recipient of the Hans Jones Award for excellence in thesis research in Special Operations and Irregular Warfare.
 Dr. Nina Kollars	Dr. Nina Kollars is a former adjunct senior fellow for the Defense Program and Associate Professor in the Cyber & Innovation Policy Institute (CIPI) within the Naval War College. Dr. Kollars is a scholar of future warfighting, military technological change, innovation, cybersecurity, and cyber warfare/information operations. She holds a PhD in Political Science from The Ohio State University, an MA in International Affairs from the Elliott School at George Washington University. She has served as a fellow at a number of military institutes to include: Brute Krulak Center at Marine Corps University, the Special Operations Journal, and the Modern War Institute at USMA. She is a senior analyst for the Congressional Cyber Solarium Commission and manages the CIPI Gravely Directed Research Program at the Naval War College. Dr. Kollars is a published security studies scholar, a public speaker, and writer.
Dr. Joe Billingsley	Dr. Joe Billingsley is a Senior Policy Advisor for Cyber Workforce and Education in the Office of the National Cyber Director (ONCD) at the White House. He is also Founder of the non-profit Military Cyber Professionals Association (MCPA) and Adjunct Professor at the Institute of World Politics. Previously, he served as Director of Strategic Engagement at the National Defense University (NDU) College of Information and Cyberspace (CIC), on the Advisory Board of the Cyber Security Forum Initiative (CSFI), Adjunct Faculty at George Washington University, and as an Army Officer where he was a Strategist (FA59) and among the first cohort transferred into the Cyber Branch (17A). He established numerous programs including the *Military Cyber Affairs* peer-reviewed journal, *CYBER* magazine, DEF CON *National Service Panel*, and *Cyber Embassy Night* series. He edited papers from CYBERCOM's 2022 *Cyber Symposium* and published it as a book with NDU Press titled *Integrated Deterrence and Cyberspace*. He is a graduate of programs at the University of Connecticut, Naval Postgraduate School (NPS), Capitol Technology University, Army War College, Naval War College, Army Signal School, and Military Intelligence School.
 Mr. Frank Kramer	Mr. Franklin D. Kramer is a distinguished fellow and board director at the Atlantic Council. He has served as a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs. At the US Department of Defense, Frank Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa, and Latin America. He has been chairman of the board of the World Affairs Council of Washington, DC; a distinguished research fellow at National Defense University; and an adjunct professor at the Elliott School of International Affairs at George Washington University. He has written extensively, with recent publications including *China and the new globalization*; *Free but secure trade*; *NATO deterrence and defense: Military priorities for the Vilnius summit*; *NATO priorities: Initial lessons from the Russia-Ukraine war*; *Here's the 'concrete' path for Ukraine to join NATO*; and *Providing long-term security for Ukraine: NATO membership and other security options.*

Panel 3 Strategy and Policy	
 Prof. M. Rauschecker	Markus Rauschecker, JD, CIPP-US, is the Cybersecurity Program Director at the University of Maryland Center for Health and Homeland Security (CHHS) and Lecturer in Law at the University of Maryland Carey School of Law. In his role, Markus focuses on legal and policy issues in cybersecurity. He works with government agencies and the private sector to increase their understanding of the many legal and policy issues they face in cybersecurity. Through CHHS, Markus supports clients with planning, training, and exercises to enable them to better prepare for and respond to cyber incidents. Markus also serves by appointment of the Maryland Attorney General on the Maryland Cybersecurity Council. Markus is part of the Council's Critical Infrastructure Subcommittee, which addresses critical infrastructure cybersecurity in Maryland and the Council's Legislative Subcommittee which makes recommendations on state legislation related to cybersecurity and data privacy.
 Dr. Jim Miller	Dr. Jim Miller is assistant director for policy and analysis at the Johns Hopkins Applied Physics Laboratory. He also serves on the Defense Science Board; the National Security Agency Advisory Board Panel on Cybersecurity; and the National Academies of Science, Engineering, and Medicine's Panel for Cybersecurity Resilience. For his contributions as principal deputy undersecretary of defense for policy from 2009 to 2012 and undersecretary of defense for policy from 2012 to 2014, he was awarded the Department of Defense's highest civilian award, the Medal for Distinguished Public Service, four times. Dr. Miller received a B.A. in economics (with honors) from Stanford University. He earned Master's and Ph.D. degrees in Public Policy from the John F. Kennedy School of Government at Harvard University. He is a member of the International Institute for Strategic Studies and the Council on Foreign Relations.
 Dr. Doyle Hodges	Dr. Doyle Hodges is a national security scholar, strategist, analyst, and leader. He is a retired naval officer and has expertise in civil-military relations, maritime and defense strategy, maritime operations including air defense and anti-submarine warfare, naval salvage, law of the sea, technology and national security, and ethics and military technology. He has been a non-resident senior fellow at the Center for Strategic and Budgetary Assessments (CSBA), a lecturer at the Princeton School of Public and International Affairs, an adjunct professor in the Schar School of Policy and Government at George Mason University, and an Associate Professor at the U.S. Naval War College. He has also been an Executive Editor at the *Texas National Security Review*. He has a Master of Arts, M.A., in Public and International Affairs at Princeton University as well as a Ph.D. in Public and International Affairs, Security Studies, also from Princeton University.
 Ms. Michele Markoff	Ms. Michele Markoff is the inaugural Distinguished Scholar of the College of Information and Cyberspace at National Defense University, as well as recipient of the 2023 Rear Admiral Grace Hopper Award. For decades, Ms. Markoff had served as the senior State Department subject matter expert overseeing the development and implementation of foreign policy initiatives on cyberspace issues. She previously served as Deputy Coordinator for Cyber Issues in the Office of the Coordinator for Cyber Affairs, and most recently as the Acting Deputy Assistant Secretary of State for International Cyberspace Security in the new Bureau of Cyberspace and Digital Policy. Ms. Markoff has a B.A. in International Relations from Reed College, an M.A. in International Relations and an M.Phil. in Political Science from Yale University, and a M.Sc. in National Security Strategy from the National War College of the United States. She also attended high school in the former Soviet Union and attended the Chinese University of Hong Kong.

Panel 4 Synthesis and Insights	
 Brig Gen Reid Novotny	Brigadier General Reid J. Novotny is the Deputy Director, Plans and Policy, J5, U.S. Cyber Command. Before this assignment, he served as the Group Commander for the 175th Cyberspace Operations Group comprised of two National Mission Teams, a Cyber Protection Team, a Cyber Operational Support Squadron, and a Cyber Intelligence Surveillance and Reconnaissance Squadron. Brigadier General Novotny represented the largest force of cyber professionals in the state of Maryland who operate in support of State, County, and Local governments through partnerships. Brigadier General Novotny also served as the National Guard J6 on the State's Joint Staff, responsible for coordinating the employment of Maryland National Guard service component forces and equipment providing communications, cyber, and information management capabilities in support of joint domestic operations and exercises. He earned a bachelor's degree in computer science at The George Washington University, a master's degree in computer security at The George Washington University in Washington, DC, and a Master's degree in Strategic Communications at George Mason University in Fairfax, Va.,
 Dr. Richard Love	Dr. Richard Love is currently a professor at NDU's College of Information and Cyberspace and recently served as a professor of strategic studies at U.S. Army War College's (USAWC) School of Strategic Landpower and as assistant director of the Peacekeeping and Stability Operations Institute from 2016-2021. From 2002 to 2016, Dr. Love served as a professor and senior research fellow at NDU's Institute for National Strategic Studies / WMD Center. He holds a Ph.D. in International Relations and Security Studies from the University of New South Wales in Australia, an LLM from American University School of Law , and a Juris Doctor in Corporate and Security Law from George Mason University School of Law. His master's studies in East-West relations were at the Jagellonian University in Krakow, Poland, and the University of Munich, in Germany, and his B.S. degree is from the University of Virginia.
 Dr. Joe Chapa	Dr. Joseph Chapa, lead for Air Staff's artificial intelligence cross-functional team since July 2021, took on a new role as chief responsible AI ethics officer at the Department of the Air Force. His appointment comes more than two months after the Defense Innovation Unit released Responsible AI Guidelines in a move to help the Department of Defense apply ethical principles of the technology to prototyping and acquisition programs with industry partners. The USAF lieutenant colonel previously served as staff officer at AF Warfighting Integration Capability, an organization responsible for identifying investment opportunities to expand the service's warfighting capability portfolio. Chapa logged more than 1,400 pilot hours, supported several military combat and humanitarian missions. Joe earned a PhD in philosophy from the University of Oxford. His book, *Is Remote Warfare Moral? Weighing Issues of Life + Death From 7,000 Miles*, is highly acclaimed in both academic and military circles, coherently and importantly bridging the gap between theory and practice.
 Dr. Michael Sulmeyer	Dr. Michael Sulmeyer assumed the position as the Principal Cyber Advisor to the Secretary of the Army and the Army Chief of Staff on March 14, 2022. He is responsible for advising both the SA and CSA on all cyber matters, including issues of readiness, capabilities, and strategy. Prior to his appointment as the Principal Cyber Advisor, Dr. Sulmeyer was the Director of the Rapid Vulnerability Review in the Office of the Deputy Secretary of Defense. Previously, he served as the Special Assistant to the President and Senior Director of Cyber Policy at the National Security Council. Prior to that, he was Senior Advisor to the Commander, U.S. Cyber Command. His educational background includes Oxford University, Marshall Scholar PhD (DPhil) in Politics; Stanford Law School, Doctor of Jurisprudence (JD); King's College in London, an MA in War Studies; and Stanford University, BA in Political Science.
 BRIG R. "Doc" Watson	Brigadier Robert "Doc" Watson is currently the Deputy J5 at U.S. Cyber Command. Most recently before this position, following unit command and upon promotion to Colonel, he served as the Director of Joint Cyber within Joint Capabilities Group. In 2021, he was promoted to Brigadier and appointed as the Director General Joint Information Warfare, Joint Capabilities Group. Brigadier Watson has deployed on multiple occasions to East Timor and Afghanistan, the last as the J3 of International Security Assistance Force, Special Operations Forces. His most recent command appointment was as the Commanding Officer of the 7th Signal Regiment (Electronic Warfare) in 2016/17. He enlisted in the Australian Army in 1992. He served in the Royal Australian Corps of Signals as an Operator Electronic Warfare before being accepted to the Royal Military College, Duntroon. On graduation in 1997, he returned to the Signals Corps. He holds Master's Degrees in Information Technology (USQ) and Military Studies (ANU) and is a Graduate of the Australian Institute of Company Directors.

About United States Cyber Command (USCYBERCOM)

Mission: USCYBERCOM conducts and synchronizes activities to secure, operate, and defend the Department of Defense (DOD) information network (DODIN); attain freedom of action in cyberspace while denying the same to adversaries; and, when directed, conduct cyberspace operations (CO) in order to deter or defeat threats to US interests and infrastructure, ensure DOD mission assurance, and achieve joint force commander objectives.

Vision: Achieve and maintain superiority in the cyberspace domain to influence adversary behavior, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests.

History: USCYBERCOM brought together the components previously created by the DOD to ensure and develop the US military's ability to operate effectively in cyberspace. Cyber Command's creation marked the culmination of years of concern related to the global spread of digital networks and the consequent transformation of international communication and commerce.

The Command became a unified combatant command on 4 May 2018 (from 2010 to 2018 it was a sub-unified command under United States Strategic Command). It represents the culmination of a series of organizational steps in the DOD's efforts to coordinate the activities of the various Services and Defense agencies that have built and continue to operate the Department's seven million networked devices and the roughly 15,000 networks that link them.

USCYBERCOM's evolution--like that of its predecessor organizations--has reflected a series of decisions strongly influenced by the emerging possibilities and risks entailed in the spread of information technology as well as the political, operational, and organizational constraints on the US government and the DOD.

About: USCYBERCOM's task is to plan and execute global CO and activities to defend and advance national interests in collaboration with domestic and international partners across the competition continuum. Its responsibilities include providing mission assurance for the DOD by directing the security, operation, and defense of the Department's information networks (i.e., the DODIN); contributing to deterring of or defeating strategic threats to national interests and infrastructure; and helping the combatant commanders achieve their missions in and through cyberspace.

USCYBERCOM comprises a headquarters organization that directs operations through its components. These include the Cyber National Mission Force Headquarters (CNMF-HQ); the Joint Force Headquarters DODIN (JFHQ-DODIN); and Joint Task Force ARES; plus its Joint Force Headquarters-Cyberspace (JFHQ-C) elements, each of which is paired with one of the Services' Cyber Components. Those Service components are Army Cyber Command, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/16th Air Force, and U.S. Coast Guard Cyber.

About the College of Information and Cyberspace (CIC) at National Defense University (NDU)

Mission: The College of Information and Cyberspace (CIC) at National Defense University (NDU) educates joint warfighters, national security leaders, and the cyber workforce on the cyber domain and information environment to lead, advise, and advance national and global security.

Vision: CIC is the premier senior national security educational institution focused on the information environment. CIC is the desired educator of leaders who perform national and military actions within the cyberspace domain using the information instrument of national power.

History: CIC has a rich history that began at the dawn of the computer age, having been originally established in 1964 as the Department of Defense Computer Institute (DODCI) and boasting former faculty like the legendary computing pioneer, Grace Hopper. In 1982, DODCI moved to the newly established NDU alongside sister colleges like the National War College. Around 1990, DODCI was renamed the Information Resources Management College (IRMC) and moved within the capital from the Navy Yard to Fort McNair. The iCollege, as it had been branded, was officially renamed to its current title in the 2017 National Defense Authorization Act to reflect the prioritization of information and cyberspace national security challenges. Since its founding, CIC continues to evolve to address the nation's most pressing security challenges.

About: CIC is known for its thought leadership, prestigious educational experience, close cooperation with senior public and private sector partners, and hosting events of national strategic importance. It is our nation's only strategically oriented and thoroughly joint graduate institution focused on information and cyberspace. Our faculty is comprised of world-class experts with terminal degrees, as well as practitioners such as senior military officers, industry professionals, and visiting chairs from government agencies. The CIC curriculum is designed to prioritize the needs of the DoD Cyberspace Workforce in coordination with the DoD Chief Information Officer, and other key stakeholders including US Cyber Command and Congress, in accordance with DoD Directive 8140.01.

Graduate Education: NDU is a regionally accredited school, with initial accreditation granted in 1997. CIC is within the scope of the NDU accreditation and includes both unclassified as well as classified Top Secret-Sensitive Compartmented Information (TS-SCI) courses. Courses are offered in-person, online, and hybrid. CIC offers a 36-credit hour Master of Science (MS), as well as multiple graduate certificates (in Cyber Leadership, Chief Information Security Officer, Chief Information Officer, Chief Financial Officer, and Chief Data Officer). A full-time 10-month in-residence centrally selected version of our MS program confers Joint Professional Military Education (JPME) Phase II (War College / Senior Service College) credit for eligible US military officers. A prestigious 14-week Leadership Development Program (LDP) is offered on-site twice a year. Other programs are part-time and self-nominated. Tuition is waived in all CIC programs for DoD personnel (military and civilian).

Students: CIC currently has hundreds of students enrolled and the student body is interservice, interagency, and international. The CIC has a global network of alumni that are senior leaders in the national security, diplomatic, intelligence, and technology communities. Those interested may attend the monthly virtual open house and apply. More information can be found at cic.ndu.edu.

CYBER SYMPOSIUM 2023

FOCUS ON THE FUTURE

United States Cyber Command and
The College of Information and
Cyberspace National Defense University
Marshall Hall

Dec 5th, 2023