CYBER LEADERSHIP DEVELOPMENT PROGRAM

The College of Information and Cyberspace Cyber Leadership Development Program is an Executive Leadership Program designed to focus on the integration of cyberspace and national security. The program is designed to provide a broad range of leaders with a deeper understanding of how effective leadership in the cyber domain is pivotal to the success of U.S. and international security.

This intensive 14-week program assembles National Defense University Faculty, senior government policy makers, and technical experts to provide participants with competencies in cyberspace and national security. The educational experience includes extensive seminar instruction, site visits, travel, and practicum. This program emphasizes developing knowledge, skills, and abilities associated with the leadership in the cyber workforce. Successful completion provides graduates with five graduate course equivalents and a graduate certificate in Cyber Leadership.

The program is conducted in person on the National Defense University Campus, in Washington, D.C. Applications accepted online at cic.ndu.edu until the application deadline of 1 June 2025.

The Cyber Leadership Development Program prepares executives to meet rapidly expanding cyber competencies and effectively integrate elements of cyberspace with national strategy.

Classes emphasize current and evolving leadership requirements for the cyber domain, with a focus on the intersection of cyber security, diplomacy and partnerships, technology, laws, and crime.

Students engage on current cyber issues including supply chain, multi-agency deterrence, and emerging and disruptive technologies.

Program:

- Tuition-free for DoD personnel
- Full-time, 14-week in-residence program

Eligibility Requirements:

- Bachelor's degree (3.0 GPA minimum)
- A federal civil service pay grade GS-13 equivalent or above,
- Military
  - Officer: O-4 and above

AY 2025-2026 Cohort Dates:

- 20 August 2025- 21 November 2025

For More Information:

- Website: cic.ndu.edu
- Phone number: 202-685-6300
- Email: cicoss@ndu.edu

Attend our Monthly Virtual Open House for prospective students on the 4th Thursday of every month @ 1– 2pm EST

https://us.bbcollab.com/guest/11be7f3d78e8465eaa4c96a62f143e7b or +1-571-392-7650 PIN: 848 345 3020

Program Requirements		
Course Number	**Course Title**	**Credit Hours**
CIC-6219	Cyber Essentials for Senior Leaders	3
CIC-6220	Engaging Partners and Adversaries through Diplomacy	3
CIC-6221	Cyberspace Activities and Authorities	3
CIC-6330	National Security and Cyber Strategy	3
CIC-6443	Emerging and Disruptive Technologies	3

Course Descriptions:

CEL (6219) – Cyber Essentials for Senior Leaders
This course focuses on educating senior leaders so that they can better execute the responsibilities of a board member within DOD, Federal Agencies, and international partners. Cyber leaders need both technical knowledge and leadership skills to gain the respect of technical team members, understand what technical staff are doing, and appropriately plan and manage security projects and initiatives. This course empowers the senior leader to become an effective security leader and get up to speed quickly on information security issues and terminology. The content of this is essential for a government senior leader to understand how best to work with the private sector to mitigate the risk of cybersecurity breaches. This course provides the essentials for analyzing the cyber and information security of information systems and critical infrastructures, to include the challenges with cyber legislation and governance, risk management analysis of cyber systems, understanding the cyber threat & vulnerability environments, protecting the organizations intellectual property and financial information and budgeting process. Additionally, participants will have the chance to participate in a tabletop breach exercise and to choose from breakout tracks in healthcare, national security, government oversight, and law.

EPA (6220) - Engaging Partners and Adversaries through Diplomacy
With a focus on cyberspace and its attendant challenges and opportunities, this course will examine the role of diplomacy in the national security enterprise. Both a U.S. domestic concern and a function of international engagement, diplomacy presupposes a diverse array of actors and interlocutors who may or may not share U.S. interests and values yet with whom policy practitioners must engage to advance U.S. priorities. The course will explore how diplomacy has been used to reduce risk to the US and U.S. interests, and it will consider the capacity of diplomacy to address as-yet- unseen threats to the homeland and the American people. Students will gain insight into the policy process and how the tools of diplomacy have been used bilaterally and in multilateral forums to advance policy priorities in ways that uphold U.S. principles and values, particularly as they come under threat from strategic competitors and their efforts to undermine U.S. global influence.

ACA (6221) – Cyberspace Activities and Authorities
This course focuses on authorities across US Agencies and international bodies regarding cyber activities to include but not limited to: security, defense, exploitation, and attack. According to the National Cybersecurity Strategy 2023: "Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests." This course explores how the US to include government, law enforcement, and industry, working with allies and partners, use all instruments of power to disrupt and dismantle threat actors to US national security interests.

NCS (6330) - National Security and Cyber Strategy
The Course is primary strategy course of the CIC Cyber Leader Development Program. Students gain understanding of the origins, formulation, and application of national security strategic logic to the cyber domain and information environment. Further, students will examine and learn the implications for subordinate organizations of the latest National Cyber Strategy. In so doing, students comprehend their role and duty in the greater tradition of national security strategy, while gaining appreciation of the value they will bring as practitioners of national security strategy for cyber and information. Participants will assess how strategic logic can be used to define context and desired ends, identify necessary means, design ways, and assess costs, risks and viability – with specific focus on the global cyber domain.

EDT (6443) – Emerging and Disruptive Technologies
This course examines the core concepts of information technology and its rapidly expanding role in solving problems, influencing decision making and implementing organizational change. Students will be introduced to an array of emerging technologies at various levels of maturity. Students analyze how emerging technologies using qualitative and quantitative evaluation methods. Student assess emerging technologies using forecasting methodologies such as monitoring and experts' opinion, examining future trends, and assessing international perspectives.