College of Information and Cyberspace
Schedule of Courses
Academic Year 2024-2025
Spring Semester

CONTACT DIRECTORY

INTERNET HOME PAGE:
http://cic.ndu.edu/

TELEPHONE:
202-685-6300
DSN 325-6300

FAX:
202-685-4058
DSN 325-4058

E-MAIL:
CICOSS@ndu.edu

MAILING ADDRESS:
College Of Information and Cyberspace
Office of Student Services
300 5th Avenue, Bldg 62, Rm 145
Ft. Lesley J. McNair, DC 20319-5066

Welcome

Located at Fort Lesley J. McNair on the Washington, DC waterfront, the College of Information and Cyberspace (NDU CIC) is the largest of five graduate-level colleges that comprise the National Defense University. The CIC educates future thought leaders and change agents who will make the difference in government and strives to meet your workforce education needs for information leadership and management.

The CIC Office of Student Services processes admissions and registration, maintains students' academic records, and publishes the CIC ***Schedule of Courses***. The Office of Student Services also manages the admission and enrollment systems used by students, faculty, and advisors.

Information about our programs and courses is available on our website at https://cic.ndu.edu/. Please let us know if you need additional information by contacting the Office of Student Services at 202-685-6300 or by email at CICOSS@ndu.edu.

ENROLLMENTPROCEDURES

Course Registration
Students who are admitted to the CIC at NDU will be sent detailed instructions regarding course registration, account information for online systems, and advisor information. Instructions on how to register for courses through NDU Connect can be found on our website at Course Registration

Members of special program cohorts will receive registration instructions from the program director.

Registration Periods
Registration opens on the dates below and will close on the Thursday prior to the Course Start Date (CSD).

Semester	Registration Opens	Registration Closes
FALL 9 September 2024 – 1 December 2024	1 July 2024	3 September 2024
SPRING 13 January 2025 – 6 April 2025	15 October 2024	6 January 2025
SUMMER 28 April 2025 – 20 July 2025	17 February 2025	21 April 2025

COURSE AVAILABILITY IN BLACKBOARD

Each course section has a site on the CIC's online learning platform, Blackboard. This site will be available to students on the Friday before the Course Start Date. Students must access Blackboard and sign in immediately following the Course Start Date to begin course work. Please note that students will NOT see their course registration in Blackboard until noon on the Friday before the course start date.

DROP POLICY

Students may dis-enroll at any time prior to the Course Start Date (CSD) via email notification to the Office of Student Services. Students who seek to withdraw from a course after the course start date must complete a Course Withdrawal Form. The form is available on the CIC website at https://cic.ndu.edu/Current-Students/Student-Registration/.

In accordance with academic policy, any drop on or after the Course Start Date will result in a grade being assigned in the course. See the online CIC Catalog for the complete grading policy.

Course Models

NOTE

Each course section has a site on the CIC's online learning platform, Blackboard. This site will be available to students at **12:00pm (noon) on the Friday before the Course Start Date.** Students must access Blackboard and sign in immediately following the Course Start Date.

NDU CIC Fall 2025 *Intensive Courses* will be offered in the following format:
Distributed Learning.

Distributed Learning (DL)

The Distributed Learning (DL) format engages students and faculty virtually over 12 weeks via Blackboard. Most DLs are asynchronous with a few optional live synchronous sessions weaved in for guest speakers etc., most synchronous sessions will be recorded for student who can't attend. During the 12 weeks student engage in weekly lessons, assignments and discussion boards. Each course will end with a final assessment which is typically a substantive paper or project that allows students to demonstrate their mastery of the intended learning outcomes. To receive credit for a course, students must be actively engaged virtually in every DL lesson as assigned by faculty.

Class Schedule by Course

Please recall that the last day to withdraw from a course with a grade of 'W' is:
Distributed Learning - The Monday of the 4th week of class:

DL	Last Day to Withdraw
13 January 2025 – 6 April 2025	3 February 2025

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.

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.

CIP (6230) – Critical Information Infrastructure Protection

This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy production, transportation systems, communications, water supply, and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis and synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Students learn the importance of interconnection reliability and methods for observing, measuring, and testing negative impacts. Special consideration is paid to the key role of Supervisory Control and Data Acquisition (SCADA) systems in the flow of resources such as electricity, water, and fuel. Students will learn how to develop an improved security posture for a segment of the nation's critical information infrastructure.

CYI (6232)– Cyber Intelligence

This course examines the cyber leader's role in cyber intelligence. As decision makers, cyber leaders both enable and consume cyber intelligence: as enablers, they formulate and implement intelligence policy and strategy, acquire and deliver enterprise level information technology ("strategic IT") systems, and plan, program, budget for, and execute intelligence programs in cyberspace; as consumers, they plan and execute intelligence activities in cyberspace or make decisions based on threats emanating in or through cyberspace. This course includes perspectives and issues applicable to the U.S. Intelligence Community (IC) in general and elements unique to cyberspace. It is not intended to impart intelligence-specific skills and tradecraft to professional intelligence officers, and no prior experience in or knowledge of intelligence is required.

DAL (6402) – Data Analytics for Leaders

This course examines how organizations can improve mission execution by employing data analytics capabilities. Establishing and maturing these capabilities requires leadership as well as an ability to both conduct analytics and interpret analytic results. Students will apply qualitative and quantitative measures on data sets to better enable organizations to meet mission needs and organization priorities. The quality of data and the sources from which data are collected are explored. Compliance, security, and the 'ethical' use of data will also be topics of discussion within the course.

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.

FFR (6607) - The Future of Federal Financial Information Sharing

This course focuses on the changing directions of financial and management reporting for Chief Financial Officers in a dynamic environment. In response to evolving citizen and shareholder expectations, financial statement reporting, budgetary reporting, and cash reporting must be accurate, transparent, and accountable, and result in "clean" audit opinions. New reporting expectations and changing accounting standards require new relationships among federal, state, and local governments, and government contractors, as well as enhanced reporting to internal constituents of the CFO, including program managers and the organizational head. Successful reporting can be facilitated by enterprise architecture, financial systems, and data management techniques.

FIE (6167) – Foundations of the Information Environment

This course introduces and explores the foundational concepts of cyberspace as a
component of the information environment. We first examine the information environment – the physical, virtual, and human aspects — in order to understand how and why our actions have strategic value. Then we consider the actions themselves from the technical and human perspective, with particular focus on information-related capabilities and activities in and through cyberspace, in order to understand how to deploy them. Finally, we learn about how to generate, acquire, and manage the resources for cyber and information operations.

GOV (6171) – Governance of the Global Information Environment and Cyber Domain

The Governance of the Information Environment and Cyber Domain Course (Governance) provides students of national cyber and information strategy with the opportunity to comprehend how information and cyber drive and define nations, their governments, and in turn, their relations in the global context. It is essential that future national security strategists have the capacity to evaluate strategic choices in terms of global and national governance, rights, duties and obligations. Thus, Governance has been developed by crossing leading cyber and information threats, with levels of national and international governance, to identify and examine the key authorities and case studies essential for a future cyber and information strategist. By taking Governance, students will analyze how: law is both a driver and definer of national security strategy; states form and interact through the law; states and private actors use and influence law to pursue vital interests, security, rights, and order; and how future national security strategists and leaders have essential responsibilities to define, engage, and use law when developing national security strategy for cyber and information.

IWS (6151) – Information Warfare Strategy

This course provides theories, frameworks, and tools for strategic planning and strategy execution. It weds direct and indirect methods of influence. Upon successful completion, students will be able to plan and implement strategies with emphasis on the information instrument of state power in a way that is practical, actionable, and intrepid. These strategies support every warfighting function and all the instruments of state power.

MAC (6512) – Multi-Agency Information Enabled Collaboration

This course focuses on inter-agency collaboration in national, homeland security, and national preparedness planning, decision making, and implementation. It examines current and proposed strategies, means and models for improving inter-agency collaboration at Federal, State, and local levels, and beyond to include multilateral non-governmental and internation organizations and coalition partners.

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.

NSS (6159) – National Security Strategy

In this course, students gain understanding of the origins, formulation, and application of national security strategic logic to the cyber domain and information environment. 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. Through the use of readings, case studies, exercises and writing assignments, 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 and information environment. Upon completion of NSS, students will be strongly positioned to apply discerning and incisive strategic analysis to their thesis projects, the balance of the courses they will take at CIC and NDU, and in their future careers as professional strategic analysts and leaders.

PAD (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.

RIA (6608) – Risk Management, Internal Controls and Auditing for Leaders

This course presents a strategic understanding of risk management, internal controls, and auditing as they relate to the functions and responsibilities within the CFO and audit communities. This course examines how

effective leadership can enhance efficiency, effectiveness, accountability, and transparency of an organization to include federal, state, and local governments. The primary focus is on the importance of identifying and assessing risks, describing, and improving internal controls techniques and practices, and evaluating and recommending audit management strategies. The course includes practical discussions to illustrate how these processes can be integrated and leveraged to solve problems, make informed decisions, and minimize compliance costs.

RMF (6218) – Risk Management Framework

This course prepares future Chief Information Security Officers (CISO), Senior Information Security Officers (SISO) and senior staff involved in the cyberspace component of national military and economic power for their role as an overall cyber risk assessment and acceptance leader. Students explore how cyber security relates to information security, security governance, security program management, system risk assessment and authorization as well as day-to-day cyber security monitoring management. Students will explore enterprise security strategies, policies, standards, controls, programs, cyber operations, security assessment and measures/metrics, incident response, resource allocation, workforce issues, ethics, roles, and organizational structure.

Class Schedule by Date

Course Offering Number	Abbreviation	Section	Course Start Date	On-Site Course Start Date	On-Site Course End Date	Course End Date
CIC-6221_SPR24-25_02	ACA	02	1/13/2025	DL	DL	4/6/2025
CIC-6219_SPR24-25_02	CEL	02	1/13/2025	DL	DL	4/6/2025
CIC-6230_SPR24-25_01	CIP	01	1/13/2025	DL	DL	4/6/2025
CIC-6232_SPR24-25_02	CYI	02	1/13/2025	DL	DL	4/6/2025
CIC-6420_SPR24-25_01	DAL	01	1/13/2025	DL	DL	4/6/2025
CIC-6443_SPR24-25_04	EDT	04	1/13/2025	DL	DL	4/6/2025
CIC-6607_SPR24-25_01	FFR	01	1/13/2025	DL	DL	4/6/2025
CIC-6167_SPR24-25_06	FIE	06	1/13/2025	DL	DL	4/6/2025
CIC-6171_SPR24-25_05	GOV	05	1/13/2025	DL	DL	4/6/2025
CIC-6151_SPR24-25_06	IWS	06	1/13/2025	DL	DL	4/6/2025
CIC-6512_SPR24-25_01	MAC	01	1/13/2025	DL	DL	4/6/2025
CIC-6330_SPR24-25_02	NCS	02	1/13/2025	DL	DL	4/6/2025
CIC-6159_SPR24-25_06	NSS	06	1/13/2025	DL	DL	4/6/2025
CIC-6220_SPR24-25_02	PAD	02	1/13/2025	DL	DL	4/6/2025
CIC-6608_SPR24-25_01	RIA	01	1/13/2025	DL	DL	4/6/2025
CIC-6218_SPR24-25_01	RMF	01	1/13/2025	DL	DL	4/6/2025