College of Information and Cyberspace
Schedule of Courses
Academic Year 2025-2026
Summer Trimester

CONTACT DIRECTORY

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

TELEPHONE:
202-685-6300
DSN 325-6300

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 one of the 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.

ENROLLMENT PROCEDURES

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

Registration Periods

Semester	Registration Opens	Registration Closes
FALL 8 September 2025 – 30 November 2025	15 June 2025	1 September 2025
SPRING 12 January 2026 – 5 April 2026	15 October 2025	5 January 2026
SUMMER 27 April 2026 – 19 July 2026	16 February 2026	20 April 2026

COURSE AVAILABILITY IN BLACKBOARD

Each course offering has a site on 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 Friday before the course start date.

DROP POLICY

Students may dis-enroll at any time prior to the Course Start Date (CSD) without a grade recorded on the transcript. In accordance with academic policy, any drop on or after the Course Start Date will result in a grade being assigned in the course. Students who seek to withdraw from a course after the course start date but before the withdrawal period ends will receive a grade of W for the course. Students who seek to withdraw after the withdrawal period end will receive a failing grade for the course. To request to drop a course, students should log into NDU Connect, navigate to Registrar Request, Drop Course Request and select request drop next to the appropriate course.

Course Models

NDU CIC Summer 2026 *Courses* will be offered in the following format:
Distance Learning.

Distance Learning (DL)

The Distance 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 students who can't attend. During the 12 weeks students 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
27 April – 19 July 2026	18 May 2026

CIC-6175: Cyber, Strategy and Conflict

In the contemporary security environment, cyberspace has emerged as a critical domain conflict. State and non-state actors increasingly exploit digital technologies to disrupt critical infrastructure, gather intelligence, influence populations, and contest political, military, and economic power. Events such as Stuxnet, and the persistent activities of groups like Volt Typhoon and Salt Typhoon illustrate how cyber capabilities are used to

achieve strategic effects below the threshold of armed conflict. This course examines the evolving character of cyber conflict and its implications for strategy, statecraft, and national security. Through historical cases, theoretical frameworks, and analysis of contemporary operations, students will explore how cyber capabilities are integrated into broader strategies of competition, coercion, and warfare

CIC-6414 – Data Management Strategies and Technologies

This course explores the concepts of data management and the data lifecycle as key components for improving mission effectiveness through the development of enterprise-wide and local data management programs and analytic solutions. It examines management issues such as data governance and organizational information behaviors and values. The course uses the data lifecycle framework to explore big data, data analytics, and enabling information technologies and methodologies from a senior leader perspective. Case studies allow students to explore data management issues and implementation. While geared to managers, the course provides sufficient insight into the underlying technologies to ensure that students can evaluate the capabilities and limitations of data management options and strategies.

CIC-6178: Diplomacy, Information and Cyber in the Global Environment

A detailed examination of how state and non-state actors engage in diplomacy and statecraft in and through cyberspace, to advance their national interests. Statecraft practices and the institutions, resources, and capabilities of the diplomatic instrument of power have a dramatic role in the interplay between international relations and cyber/information activities. Students will comprehend how strategic interests in the cyber domain and information environment can be advanced or constrained by digital international relations and cyber diplomacy.

CIC-6330: National Security and Cyber Strategy

Students gain an 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 Cybers 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 assed costs, risks and viability – with specific focus on the global cyber domain.

CIC-6218 – Risk Management Framework for Strategic Leaders

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.

CIC-6159 – Strategic Art for the Cyber and Information Environment

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

CIC-6607- The Future of Federal Financial Information Sharing

This course focuses on 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 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 between 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.

Class Schedule by Date

Course Offering ID	Course Title	Course Number	Course Abbreviation	Course Start Date	Course End Date
CIC-6175_SUM25-26_05	Cyber Strategy and Conflict	6175	CSC	4/27/2026	7/19/2026
CIC-6414_SUM25-26_21	Data Management Strategies and Technologies	6414	DMS	4/27/2026	7/19/2026
CIC-6178_SUM25-26_05	Diplomacy, Information and Cyber in the Global Environment	6178	DCE	4/27/2026	7/19/2026
CIC-6330_SPR25-26_03	National Security and Cyber Strategies	6443	NSC	4/27/2026	7/19/2026
CIC-6218_SUM25-26_02	Risk Management Framework for Strategic Leaders	6218	RMF	4/27/2026	7/19/2026
CIC-6159_SUM25-26_08	Strategic Art for the Cyber and Information Environment	6159	ART	4/27/2026	7/19/2026
CIC-6607_SUM25-26_04	The Future of Federal Financial Information Sharing	6607	FFR	4/27/2026	7/19/2026