# ACADEMIC CATALOG
# AY 2025 – 2026

## COLLEGE OF INFORMATION AND CYBERSPACE


NATIONAL DEFENSE UNIVERSITY
300 5TH Avenue, Building 62, Washington DC, 20319

The College of Information and Cyberspace Academic Catalog is published annually.

The catalog is available online at https://cic.ndu.edu/ under the Academic Catalog

# Table of Contents

## Message from the Deputy Chancellor

It is my immense pleasure to welcome you to Academic Year (AY) 2025-2026 at the National Defense University's College of Information and Cyberspace (CIC). This year, we also welcome a new chapter in CIC leadership as Ms. Elizabeth Phu, former Principal Deputy Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (SOLIC) in OSD for Policy, takes the helm as Chancellor. As a respected national security expert and senior leader, Ms. Phu has over twenty-five years of experience in the Department of Defense. Her leadership and vision will be instrumental in guiding CIC through today's complex information and technology landscape.

I am honored to continue serving the college as Deputy Chancellor, and I remain steadfast in my commitment to supporting CIC's mission: to prepare strategic leaders for the challenges of today and tomorrow. Our college, faculty, and staff are committed to making your educational journey at CIC one of the best academic experiences available. CIC sets the standard for education and remains the premier senior national security institution for cyber and information education within the Department of Defense and the United States Government. In AY25-26, we will continue to meet and exceed that standard.

During AY24-25, the college experienced another year of record enrollment, and we were proud to welcome new faculty from across government, academia, and industry. Our faculty continues to lead cutting edge research in areas such as the cultural dimensions of artificial intelligence, the intersection of international law and emerging technologies, and leadership in complex environments.

CIC also hosted visiting faculty from across the interagency, including the Departments of Energy and State, Defense Information Systems Agency, Department of Homeland Security, and U.S. Cyber Command—further enriching our curriculum with operationally relevant insights.

Experiential learning remained a vital part of our academic programs. Our CIO LDP students traveled throughout Washington, D.C., New York City, and Orlando engaging directly with key institutions. Our JPME II students took part in strategic field studies with allies and partners in Belgium, Estonia, and the United Kingdom. CIC convened the eleventh annual Cyber Beacon symposium and again partnered with U.S. Cyber Command to cohost its annual symposium. Both events fostered critical dialogue on cyber strategy, policy, and operations.

Our Cyber Leadership Development Program (CLDP) continues to grow as a signature initiative. It focuses on the integration of cyberspace and national security, providing a deeper understanding of how effective leadership in the cyber domain is pivotal to the success of U.S. and international security. We also celebrated a significant milestone as the Department of Education approved our official degree name change from Government Information Leadership to Strategic Information and Cyberspace Studies, aligning our academic identity with the evolving mission landscape.

Our faculty, staff, conferences, and engagements all center on supporting our stakeholders and, most importantly, you — our students. At CIC, home of the Ravens, we foster a collaborative learning environment where students build not only expertise, but also lasting relationships and leadership acumen. This is your opportunity to reflect, to challenge assumptions, and to engage deeply with your peers and instructors.

Consider this educational experience an opportunity to gain knowledge, tools, frameworks, and experiences that will prepare you to be the thoughtful, principled leader needed by the United States, its partners, and its allies.

On behalf of the entire CIC Ravens team, welcome! We look forward to all that you will accomplish during your time here.

Sincerely,
Andrew Walsh
Deputy Chancellor
College of Information and Cyberspace

# CIC Academic Catalog 2025-2026

The 2025-2026 Academic Catalog of the College and Information and Cyberspace (CIC) provides current information regarding educational programs, class offerings, academic regulations, and university resources. Students can use this document to familiarize themselves with program and degree requirements relevant to their degree or certificate program.

Statements in this catalog should be treated as solely informational. This document should not be construed as binding between the student and the university. While every effort is made to keep the Academic Catalog updated, CIC reserves the right to amend policies and procedures as it sees fit. Every effort will be made to communicate any alterations.

Information in this catalog is accurate at the date of publication. Please consult the website for recent updates.

## Mission

To Educate 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

To be the leader in education, research, and collaboration in global cyber and information strategy at the nexus of government and academia.

## CIC Overview

The College of Information and Cyberspace (CIC) offers a wide spectrum of educational activities, services, and programs which prepare leaders to play critical roles in national security. Through our Master of Science, certificates, and professional development opportunities—CIC students are molded into lifelong learners, effective communicators, and dynamic thinkers. Students, alumni, faculty, and staff constitute one of the premier global learning communities in the fields of information and cyberspace.

## Strategic Information and Cyberspace Studies - Master of Science Degree

### Overview

The Master of Science in Strategic Information and Cyberspace Studies Degree Program is a selective program that addresses the educational needs of defense and government leaders who seek to lead complex 21st Century organizations. Participants from across defense and other federal, state, and local government organizations create a learning community hallmarked by partnerships, information sharing, and network synergies.

The Master of Science in Strategic Information and Cyberspace Studies focuses on the information instrument of power and cyberspace. It provides graduate-level education to senior military and civilian leaders with an emphasis on the military, government, and private sector dimensions of information and cyberspace as a critical component of national security strategy.

### Modalities

- Fulltime in-residence (10-months, fall and spring semester) – U.S. Military selectees earn Joint Professional Military Education, Phase II (JPME II)
- Part-time online (3 trimesters; fall, spring, and summer)

### Program Learning Outcomes

- Evaluate the national security environment with a focus on the impact of the information instrument of power and cyberspace.
- Create information strategic and policy options that support joint warfighting and achieve national security objectives
- Create cyber strategic and policy options that support joint warfighting and achieve national security objectives
- Evaluate principles of the profession or arms, civil-military relations, and ethics to support strategic-level decision making
- Demonstrate strategic leadership to include effective communication and creative and critical thinking in a joint, interagency, and multinational environment.

## Master of Science Strategic Information and Cyberspace Studies In-residence/JPME
## 33 Credit Hours

| **Core Courses – 27 Credit Hours** |
|---|
| Cyber and Information Effects in Military Operations |
| Cyber Power and Technology Strategy |
| Cyber Strategy and Conflict |
| Diplomacy, Information and Cyber in the Global Environment |
| Governance, Authorities, and Ethics |
| Information Warfare Strategy |
| Practicum, Experiential Learning, and Capstone |
| Strategic Art for the Cyber and Information Environment |
| Strategic Thinking and Communications |
| |
| Three NDU Electives* |

*NDU Electives are 2 credit hours each and offered to resident master's students by CIC and the other NDU colleges.

## Master of Science Strategic Information and Cyberspace Studies Part-time
## 33 Credit Hours

| **Core Courses – 27 Credit Hours** |
|---|
| Cyber Power and Technology Strategy |
| Cyber Strategy and Conflict |
| Diplomacy, Information and Cyber in the Global Environment |
| Governance, Authorities, and Ethics |
| Information Warfare Strategy |
| Multi-Agency Information Enabled Collaboration |
| Strategic Art for the Cyber and Information Environment |
| Strategic Thinking and Communications |
| |
| Three CIC Electives** |

**CIC Electives are 3 credit hours each, students may select any course from the CIC course catalog to mee the MS elective requirements.

## Chief Information Officer Leadership Development Program

### Overview

The Chief Information Officer Leadership Development Program (CIO-LDP) is the CIC's flagship resident program for rising senior-level managers and leaders responsible for promoting and attaining national and international security goals through the strategic use of information and information technology as identified in the CIO competencies. The CIO-LDP is administered in an intensive and highly interactive fourteen-week forum. The student- centered educational experience emphasizes developing leadership skills and abilities while learning CIO content through completion of five courses. Students who complete the program will receive a CIO graduate certificate.

### Modalities

- Full time In-residence (14 weeks)

### Program Learning Outcomes

- Leverage CIO policy and organization competencies to lead within and across federal organizational boundaries by linking critical decisions regarding resources, people, processes, and technologies to mission performance.
- Balance continuity and change in the development implementation, and evaluation of government information resources and management strategies and policies while meeting legislative and executive mandates.
- Demonstrate abilities to construct and implement mission-aligned information and communication technology strategies [including gathering, analyzing, and reporting data; making decisions; implementing decisions; and evaluating organizational performance] in an ethical manner.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

| **Core Courses (15 Credits)** |
|---|
| CIO 2.0 Roles and Responsibilities |
| Cyber Security Fundamentals |
| Emerging and Disruptive Technologies |
| Strategic Performance and Budget Management |
| Strategic Information Technology Acquisition |

# Cyber Leadership Development Program

## Overview

The Cyber Leadership Development Program (Cyber-LDP) prepares students to meet rapidly expanding cyber competencies and effectively integrate elements of cyberspace with national strategy. Courses emphasize current and evolving leadership, management direction, and advocacy to manage cybersecurity risk in this constantly evolving domain. Students will face rigorous case studies and scenarios to develop their skills in partnering, strategic thinking, team building, problem solving, and negotiating on current and emerging technologies. Threats in cyberspace are constantly evolving, and this program provides students with the opportunity to explore solutions in the context of public-private partnerships and challenge the status quo. This program is ideal for students who are currently or projected to be in the National Institute of Standards and Technology (NIST) Workforce Framework for Cybersecurity (NICE) Work Roles in Oversight and Governance or equivalent to enhance and gain competencies. Students who complete the intensive receive a Cyber Leader certificate.

## Modalities

- Full time In-residence (14 weeks)

## Program Learning Outcomes

- Mature an understanding of the cyber threat landscape to include projections for the future to develop a strategic approach to cyberspace activities that incorporate the USG and partnerships with domestic and international partners.
- Apply key strategic concepts, critical thinking, and analytical frameworks to the analysis of national and international security environments in support of formulating, implementing, and evaluating national security, cyber strategy, and statecraft to enable mission success.
- Assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives to develop policy and ensure future mission capabilities.
- Identify, evaluate, and counter major cyber threats and threat actors and ways the U.S. and international community can leverage bilateral and multilateral mechanisms to counter threats as technology rapidly evolves.
- Apply critical, strategic, ethical, and innovative thinking to lead organizations in an increasingly vulnerable technology dependent world.

| **Core Courses (15 Credits)** |
|---|
| Cyber Essentials for Senior Leaders |
| Cyberspace Activities and Authorities |
| Emerging and Disruptive Technologies |
| Engaging Partners and Adversaries through Diplomacy |
| National Security and Cyber Strategy |

# CIC Graduate Certificates

The CIC Graduate Certificates support the educational requirements of the DoD cyber workforce with focused coursework. Students may apply a maximum of three courses (9 CH) from certificates programs to the MS degree whether these courses are electives or core courses. A course can only be used once to meet a certificate requirement; students must take an alternative course to meet program requirements.

## Chief Data Officer (CDO) Graduate Certificate

### Modalities

- Distance (Online)

### Certificate Learning Outcomes

- Apply data analytics tools and methodologies on data sets and communicate results with impactful visualizations.
- Advocate and communicate date sharing practices through organizational culture, policies, and systems development process while fulfilling legal and ethical obligations of data ownership.
- Evaluate enabling technologies and enterprise/data architectures to address requirements for data analytics programs, including real-time Big Data processing and machine learning/predictive analytic capabilities.
- Create a data analytics program through data governance initiatives that support all data life- cycle considerations (e.g., authoritative, source consolidation, updating, purging/avoiding sprawl, and archival).
- Employ emerging technologies (and underlying data) to enhance data-driven decision- making for strategic effect.
- Identify, shape, and formulate data strategies that ensure data availability and transparency, supporting multi-agency and/or multi-national collaboration.

| **Core Courses (15 Credits)** |
|---|
| Data Analytics for Decision Makers |
| Data Management Strategies and Technologies: A Managerial Perspective |
| Data Strategy and Governance |
| Artificial Intelligence Strategies for Data Leaders |
| Strategic Information Technology Acquisition |

## Chief Financial Officer (CFO) Graduate Certificate

### Modalities

- Distance (Online)

### Certificate Learning Outcomes

- Lead within and across organizational boundaries by leveraging knowledge of federal budgeting, financial accounting and reporting, data management and analytics, risk, internal controls, and audit for strategic advantage.
- Synthesize ethics, theory, practices, and technologies to promote effective decision-making and accountability across the enterprise, improve operations, and support financial management excellence.
- Communicate at the strategic level, demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

| **Core Courses (15 Credits)** |
|---|
| Strategic Performance and Budget Management |
| Risk Management, Internal Controls and Auditing for Leaders |
| White House, Congress, and Budget |
| The Future of Federal Financial Information Sharing |
| Data Analytics for Leaders or<br>Data Management Strategies and Technologies: A Managerial Perspective |

## Chief Information Officer (CIO) – Graduate Certificate

### Modalities

- Distance (Online)

### Certificate Learning Outcomes

- Leverage CIO policy and organization competencies to lead within and across federal organizational boundaries by linking critical decisions regarding resources, people, processes, and technologies to mission performance.
- Balance continuity and change in the development, implementation, and evaluation of government information resources and management strategies and policies while meeting legislative and executive mandates.
- Demonstrate abilities to construct and implement mission-aligned information and communication technology strategies, including gathering, analyzing, and reporting data; making decisions; implementing decisions; and evaluating organizational performance in an ethical manner.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

| **Core Courses (15 Credits)** |
|---|
| CIO 2.0 Roles and Responsibilities |
| Strategic Performance and Budget Management |
| Strategic Information Technology Acquisition |
| Emerging and Disruptive Technologies |
| Cybersecurity Fundamentals |

## Chief Information Security Officer (CISO) Graduate Certificate

### Modalities

- Distance (Online)

### Certificate Learning Outcomes

- Exercise strategic leadership and critical thinking in the development and use of cyber security strategies, plans, policies, enabling technologies and procedures in cyberspace.
- Develop and lead programs to provide cyber security, security awareness training, risk analysis, certificate and accreditation, security incident management, continuity of operation and disaster recovery.
- Link people, processes, information, and technology to critical cybermission decisions to share information in a secure environment.
- Develop and lead, in accordance with laws and regulations, an enterprise IA program that promotes and attains national security, agency, and inter-agency goals.
- Communicate at the strategic level demonstrating command of the topic, logical organization, compelling argument, and excellence in English grammar and syntax.

| **Core Courses (15 Credits)** |
|---|
| Cybersecurity Fundamentals |
| Cyber Security for Information Leaders |
| Illicit Use of Cyber |
| Risk Management Framework for Strategic Leaders |
| Critical Information Infrastructure Protection or Continuity of Operations |

## Cyber Leadership Graduate Certificate

### Modalities

- Distance (Online)

### Certificate Learning Outcomes

- Mature an understanding of the cyber threat landscape to include projections for the future to develop a strategic approach to cyberspace activities that incorporates the USG and partnerships with domestic and international partners.
- Apply key strategic concepts, critical thinking, and analytical frameworks to the analysis of national and international security environments in support of formulating, implementing, and evaluating national security, cyber strategy, and statecraft to enable mission success.
- Assess emerging technologies using forecasting methodologies such as monitoring and expert opinion, examining future trends, and assessing international perspectives to develop policy and ensure future mission capabilities.
- Identify, evaluate, and counter major cyber threats and threat actors and ways the U.S. and international community can leverage bilateral and multilateral mechanisms to counter threats as technology rapidly evolves.
- Apply critical, strategic, ethical, and innovative thinking to lead organizations in an increasingly vulnerable technology dependent world.

| **Core Courses (15 Credits)** |
|---|
| Cyber Essentials for Senior Leaders |
| Cyberspace Activities and Authorities |
| Emerging and Disruptive Technologies |
| Emerging Partners and Adversaries through Diplomacy |
| National Security and Cyber Strategy |

# Non-Program Seeking

Non-program seeking status allows students who meet College of Information and Cyberspace (CIC) program eligibility requirements to enroll in courses without declaring an intent to complete a particular CIC program. Students may take up to 9 credits before they must select a program. All courses must be taken for a letter grade and will be recorded on student academic transcripts. Completed courses with grades of B or higher may be applied to the applicable requirements of the selected program.

# Course Descriptions

## CIC – 6422: Artificial Intelligence Strategies for Data Leaders

This course examines leaders' roles in the adoption of artificial intelligence (AI) and other data-enabled technologies. Participants explore the technologies, workforce, infrastructure, and other resources necessary to leverage AI within their organizations.

## CIC-6303: CIO 2.0 Roles and Responsibilities

Students in the CIO 2.0 course examine the essential analytic, relational, technological, and leadership competencies that government CIOs and their staff need to respond to and shape the 21st Century environment. Students assess the high information and IT demands of customers; examine the potential and perils of ubiquitous technology and information saturation; and weigh the tradeoffs of resource constraints, legal and policy mandates, and security in an open environment.

## CIC-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.

## CIC-6166: Cyber and Information Effects in Military Operations

In this course, students will analyze how information and cyberspace operations are integrated into joint warfare and theater campaign strategies. Students will explain what is needed to operationalize information and cyber power for theater strategy and campaigning using joint planning systems and processes. Finally, students will create and propose military actions for campaigns, operations, and activities in the Information Environment and Cyberspace to achieve strategic and operational objectives.

## CIC- 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.

## CIC-6177: Cyber Power and Technology Strategy

This course examines how the economic instrument of power is applied in the global cyber domain and information environment. Students analyze how state and non-state actors build and project cyber power through technology strategy, fiscal and monetary policy, workforce development, research and development, and commercialization. Emphasis is placed on strategic competition over digital infrastructure, the role of Big Tech in cyber and information operations, deterrence through cyber resilience, and the strategic risks and opportunities of disruptive technologies.

## 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-6211: Cybersecurity Fundamentals

This course provides an overview of the fundamentals of cybersecurity from the perspective of a DoD or federal agency senior leader. The course provides a foundation for analyzing the cyber and information security of information systems and critical infrastructure. Law, national strategy, public policy, and risk management methodologies are examined for assuring confidentiality, integrity, and availability information systems and asset.

## CIC-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.

## CIC-6201: Cyber for the Strategic Leaders

This course studies cyber strategies and cyber operations from the lens of strategic leaders. It examines the application of national security strategy in the cyber domain to advance national interests and achieve victory in war, in and through the domain. It explores the relationship among cyber strategy, cyber capabilities, cyber effects, cyber operations, cyber warfighting, deterrence, and national security. It specifically scrutinizes the role that artificial intelligence (AI) plays in cyber operations and security as well as the concepts and practices of AI-enabled offensive and defensive operations in and beyond the cyber domain. The course covers a wide range of topic areas that include but are not limited to threats, vulnerabilities, risk management, intrusion kill chain, as well as offensive and defensive operations in both cyber-only environments and cyber-physical environments.

## CIC -6420: Data Analytics for Leaders

This course provides an overview of data analytics concepts and techniques with a focus on what leaders need to know to leverage data for decision making. Students will learn about the data analytics process from the perspectives of both the decision maker and the data analyst to better understand how to build a sustainable data analytics program within a government organization. Topics include analytics approaches, familiarity with data analytics tools, how to determine data requirements, collecting and preparing data, and data ethics. No prior data analytics experience is necessary.

## CIC-6414: Data Management Strategies and Technologies: A Managerial Perspective

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-6419: Data Strategy and Governance

This course explores data governance as a key component of data strategy for operationalizing data as a strategic asset to enable more effective and efficient decision making. It examines the principles, essential capabilities, and goals set forth in federal agency data strategies and the governance processes necessary to achieve those goals. Case studies allow students to explore the real-world benefits of data governance policies, standards and practices and how they are implemented. The course is designed to provide leaders with knowledge, skills, and attributes to develop and assess data governance programs for their organizations that enable data discovery and sharing and facilitate innovation.

## 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-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 changes. Students will be introduced to an array of emerging technologies at various levels of maturity. Students analyze how emerging technologies use qualitative and quantitative evaluation methods. Students assess emerging technologies using forecasting methodologies such as monitoring and experts' opinion, examining future trends, and assessing.

## CIC-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.

## CIC-6607: 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 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.

## CIC-6171: Governance, Authorities, and Ethics

This course 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.

## CIC-6217: Illicit Use of Cyber

This course explores illicit uses of cyber (e.g. terrorism, crime, human trafficking, etc.) and the impact of these activities on national and global security. The course explores the identity of actors engaged in these activities, their motivation, techniques, and what countermeasures can be adopted to mitigate their impact. The course provides a risk management framework to help information leaders leverage the benefits of cyber technologies while minimizing risks.

## CIC-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.

## CIC-6512: Multi-Agency Information-Enabled Collaboration

The course focuses on multi-agency collaboration in support of national and homeland security and national preparedness planning, decision-making and implementation. It examines current and proposed strategies, means and models for substantially improving the effectiveness of collaboration at the federal, state and local levels, and beyond to include multilateral situations with non-governmental, media, and international organizations and coalition partners. The course assists students to synthesize the underlying principles that define effective collaboration, and critical lessons learned from past challenges and current experiments. Legal, budgetary, structural, cultural and other impediments that inhibit inter-agency mission effectiveness are assessed, as are strategies for addressing them. The course explores evolving network structures, collaborative tool-sets including social media, cross-boundary information-sharing and work processes, emergent governance arrangements, and the behaviors and skills of collaborative leadership as a key component of government strategic leadership.

## 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-6170: Practicum, Experiential Learning, and Capstone

The Practicum, Experiential Learning and Capstone Exercises Course (PEC) provides students with learning opportunities outside the normal classroom experience. Students will be exposed to senior leaders in weekly lecture series, multiple experiential events (on and off campus) multiple practicum experiences (domestic and overseas) throughout the year and a college level Capstone exercise. This course is designed to enhance classroom experience and expose students to real world applications through authentic experiences and peer-to-peer learning.

## CIC-6218: Risk Management for Senior 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-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 risk, describing, and improving internal control techniques and practices, and evaluating and recommending audit management strategies.

## 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 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 take at CIC and NDU, and in their future careers as professional strategic analysts and leaders.

## CIC-6415: Strategic Information Technology Acquisition

This course explores acquisition processes that seek to place information technology systems into the hands of joint warfighters and agency information leaders faster and with more ability to adapt to fluid situations. We examine the role senior military and agency leaders play in the successful acquisition of information technologies and services to achieve strategic organizational goals. Students use the Systems Development Lifecycle (SDLC) as a framework to explore acquisition strategies and charters, requirements management, development, testing, deployment, risk management and sustainment activities, focusing on the acquisition of IT and related services. Acquisition best practices

and techniques cited in the US Digital Services Playbook are explored. IT-related risk management, to include avoidance of counterfeit chips and computer malware, risks of transition to cloud computing and advanced analytics are also discussed. Significant emphasis is placed on the contracting processes and outsourcing of IT networks and services. Ethics issues are explored using Department of Defense acquisition case studies.

## CIC-6328: Strategic Performance and Budget Management

This course is an executive-level view of strategic planning, performance management, and performance budgeting in public-sector organizations Using the Government Performance and Results Act and Kaplan & Norton's Balanced Scorecard as frameworks, students examine the linkage of mission to strategic planning, performance management, measurement, operational strategies, initiatives, and budgets to support senior-level decision making. Emphasis is on transparency, outcomes, and linkage between organizational performance and the organization's budget. With this critical understanding, students develop leadership strategies that shape fiscal budgets to achieve agency strategic outcomes.

## CIC-6164: Strategic Thinking and Communication

This course provides students with an introduction to graduate-level research, writing, and communication, with a particular focus on the critical and creative thinking that drives strategic decision-making. In support of the NDU and CIC missions, the goal is to enrich strategic thinking and provide support throughout the program for both writing and oral communication. This is the course where students can fully synthesize what they have learned across all their courses and articulate ideas that will help them succeed beyond CIC.

## CIC-6606: White House, Congress, and Budget

This course presents a strategic understanding of federal budgeting and appropriations, with particular attention to the role of the White House and Congress. The course focuses on developing leadership strategies to shape the fiscal environment to achieve agency strategic outcomes, examining topics such as the impact of current fiscal issues.

# Admissions

## Minimum Eligibility Requirements

1. U.S. Government Affiliation
    a. Federal Government civilian employees, military, non-federal government employees (state and local government), and private sector employees working in a field relevant to the CIC curriculum and approved by the joint staff.
2. Education
    a. All applicants must possess a bachelor's degree from a regionally accredited U.S. institution or the equivalent from a foreign institution. The minimum grade point average considered for admission is a 3.0 on a 4.0 scale for all previous undergraduate work. In cases where the undergraduate GPS is below 3.0, a cumulative GPA of 3.3 in 6 or more graduate credits (from CIC or other accredited programs) may be used to determine eligibility.
3. Pay Grade/Rank and Experience
    a. A federal civil service pay grade of GS-13 or equivalent/military rank, SNCO: E-7 and above; Chief Warrant Officer: CW2 and above; and Officers: O-4 or above. Non-federal employees, including state and local government, must be of an equivalent grade. Private sector employees must be of an equivalent grade and work in a field relevant to the CIC curriculum.
4. English Language Proficiency (if necessary)
    a. International students whose native language is not English are required to demonstrate their English proficiency by passing an English comprehension test with an ECL of 85 for the CIO Leadership Development Program or a 90 for all other certificate programs. Exceptions can be made for applicants whose university degree is from a regionally accredited U.S. institution, or whose home country is on the DSCA Country Exemption List. Contact the CIC Office of Student Services for further details.

### Military.Reserves.and.National.Guard

Members of the Military Reserves or National Guard who do not meet the above admissions criteria (e.g., Government affiliation) may apply for admission based on their full-time Military Reserve or National Guard status. Education and

grade/rank minimum requirements apply regardless of employer. Contact the CIC Office of Student Services for further details.

### International.Applicants

International students (non-US citizens) must apply through the appropriate Security Assistance Training Field Activity (SATFA) country program manager. For additional information, please visit the CIC international student's webpage at https://cic.ndu.edu/Admissions/International-Students/.

## Application Instructions

A¡ Required.documents.for.Master's.and.Leadership.Development.Programs¿

1. Application for Admission
2. Résumé
3. Employment Verification and Recommendation Form
4. Professional Letter of Recommendation
5. Official Undergraduate and Graduate (if applicable) Transcript(s)
6. Writing Sample

B¡ Required.documents.for.Certificate.and.Non-Program.Seeking¿

1. Application for Admission
2. Résumé
3. Employment Verification and Recommendation Form
4. Official Undergraduate and Graduate (if applicable) Transcript(s)

For further information, please refer to our instructions online at https://cic.ndu.edu/Admissions/Application-Instructions/.

To.Apply

U.S. applicants should submit all the required documents in the same application packet online at https://cic.ndu.edu/Admissions/Apply-Online/. International applicants, please see previous section on international student enrollment for SATFA guidance.

Mail official transcripts to:
NDU CIC Office of Student Services
300 5th Avenue, Marshall Hall, Building 62,
Room 145 Fort McNair, Washington, DC
20319

Email official transcript to: CICOSS@ndu.edu

### Admissions Deadlines

All Certificate, Non-Program Seeking, M.S. degree, and LDP programs are open to new applicants and existing CIC students.

Certificate, Non-Program Seeking, and M.S. degree applications are reviewed for admission to a specific term, please provide a complete application, including all supplemental materials, no later than the dates listed below:

Spring 2026 Semester: September 1, 2025
Summer 2026 Semester: January 1, 2026
Fall 2027 Semester: May 1, 2026

Please.note.that.all.courses.are.taken.for.graduate.credit¡.Thus?all.students.are.required.to.be.admitted.to.a.program.prior.to.registering.for.a.course¡.

# Program Policies

All students are responsible for understanding the academic policies of the university and their academic program, including deadlines, attendance, curriculum requirements, grades, and academic integrity.

## Applying Coursework from Other Institutions

### Graduate Certificate Program Participants

CIC does not accept transfer credits from outside institutions. Courses that cross certificates may only be used to fulfill one certificate requirement; in these cases, an alternate course will be identified for program completion. All coursework applied toward a certificate must be completed within four years of program admission.

## Master of Science Program Participants

Subject to graduate time limit requirements, a student may use up to three NDU CIC classes passed with a grade of B or higher toward attaining the Master of Science degree. Courses from outside institutions are not accepted for transfer. All coursework applied toward the Master of Science degree must be completed within five years of program admission.

## Leave of Absence

Students may apply for a leave of absence due to exceptional circumstances by submitting a written request to NDU CIC Office of Student Services, cicoss@ndu.edu. The letter should provide a detailed explanation of the circumstances leading to the request, and a justification of the time requested. Requests for a leave of absence may be made for up to one academic year. An approved leave of absence will extend the student's program completion timeline. Approval will be provided by e-mail.

## Program Withdrawal

Students seeking to withdraw from NDU CIC programming must submit the program withdrawal form found on our website https://cic.ndu.edu/catalog/policies/to NDU CIC Office of Student Services. Confirmation of withdrawal will be provided via email.

## Continued Enrollment

Students must demonstrate continued progress at NDU CIC to maintain enrollment. This requires a minimum of one course every 12 months, and a cumulative 3.0 overall GPA. Students who fail to meet these standards will be administratively withdrawn from the college. Students are eligible to reapply for admission.

Master of Science (M.S.) Degree Program: All coursework applied toward a M.S. Degree must be completed within five (5) years of program admission. Courses taken after the five-year deadline will be subject to repeat, although the credit itself will not be revoked.

Graduate Certificate Programs: All coursework applied toward a certificate must be completed within four (4) years of program admission. Courses taken after the four-year deadline will be subject to repeat, although the credit itself will not be revoked.

## Academic Probation

Students will be placed on probation upon receiving one (1) course grade of F and/or when their cumulative GPA falls below the required 3.0 for continued enrollment. Students on probation must attend a mandatory counseling session

with their academic advisor and, if applicable, raise the GPA to a 3.0 on a timeline approved by the NDU CIC Office of the Dean. Students who receive a second course grade of F and/or who fail to raise their GPA within the prescribed timeline or credit load will be dismissed from the program.

## Dismissal

CIC may dismiss students from the program for reasons including, but not limited to, unsatisfactory academic progress/performance, and/or upon the decision of the Academic Review Board.

## Reinstatement

Dismissed students who wish to seek reinstatement must reapply for program admission. CIC may grant reinstatement on a case-by-case basis. Once eligibility is reviewed, it will be determined which previous courses, if any, may apply to the reinstated student's body of study.

# Academic Policies

## Student Preparation

Students are expected to prepare for each academic session by reading assigned materials. Readings are often the focus for seminar discussions, or key parts of in-class exercises. Faculty and other seminar participants will assume that reading assignments have been completed by the start of the session.

## Student Assessment

CIC students must demonstrate mastery of intended learning outcomes in each course. Faculty members formally assess student achievement of learning outcomes as detailed in course assessment plans and provide detailed feedback to students on their performance. Faculty members utilize assessment plans highlighting proposed assessment techniques, including but not limited to papers, projects, exercises, and participation. CIC end-of-course assessments require students to apply the material through written papers or presentations. End-of-course assessments submitted for a grade cannot be rewritten or resubmitted.

## Grading

The following letter grades and their achievement equivalents are used by the NDU CIC to evaluate student performance in courses and in the overall program. Grade points corresponding to each letter grade determine a student's academic average and eligibility to graduate. Master of Science and Graduate Certificate students must maintain a GPA of at least 3.0 to graduate. Only one grade of C may be used to fulfill certificate program requirements, while a grade of C cannot be used to fulfill requirements for the Master of Science degree program.

## NDU Grade Scale

The table below shows letter grades, qualitative descriptors, quality points, and percent ranges to be used for grading. While brief, the While brief, the qualitative grade descriptors nonetheless capture the range of graded outcomes, with the grade of B+ generally associated with the expected student performance. Quality points are used to calculate a student's Grade Point Average (GPA), whereas percent ranges are used for final course grades, individual assignments, and other course activities. Course letter grades and overall GPA are displayed on the student's transcript.

| Letter Grade | Qualitative Descriptor | Quality Points | Percentage Range | Point Range for Rounding |
|---|---|---|---|---|
| A | Excellent (or Top tier) Performance | 4.00 | 96-100 | 95.50-100.00 |
| A- | Better than Expected Performance | 3.70 | 90-95 | 89.50-95.49 |
| B+ | Expected Level of Performance | 3.30 | 86-89 | 85.50-89.49 |
| B | Acceptable Performance | 3.00 | 83-85 | 82.50-85.49 |
| B- | Marginal Performance | 2.70 | 80-82 | 79.50-82.49 |
| C | Unacceptable Performance | 2.00 | 70-79 | 69.50-79.49 |
| F (For courses with letter grades) | Failure | 0.00 | 0-69 | 0.00-69.49 |
| P (For Pass-Fail designated course) | Pass | 0.00 | N/A | N/A |
| F (For Pass-Fail designated course) | Fail | 0.00 | N/A | N/A |

Non-GPA Annotations

**Audit:** Students will follow college and university procedures to audit a course. If approved, the Registrar's Office will assign a grade of AU for that course, to be recorded on the student's transcript. The AU grade does not affect a student's GPA or earned credits but serves to reflect attendance in the course.

**Incomplete**: The I grade for a course will be assigned only upon approval of the course instructor and the student's Dean of Faculty and Academic Programs. Incomplete indicates that one or more course requirements have not been completed for reasons that, in the judgment of the course instructor, were unavoidable. A student must initiate the request for an Incomplete grade with the instructor. The student and the instructor will specify in writing the requirements to be completed and the deadline for completion, which may not exceed one calendar year. (College policies may vary; students should refer to their college's student handbook for details.) Upon completion of the outstanding requirements, the student must request that the instructor submit a change of grade to the Registrar's office. Any Incomplete grade not resolved by the documented deadline will convert to an F grade automatically. While the grade is recorded as an Incomplete, the student will not earn credits for the course and the grade will not affect the student's GPA.

**Withdrawal:** A course or program withdrawal request first must be approved by the College's Dean of Faculty and Academic Programs. The request may also require the approval of the student's sponsoring/parent organization. Finally, the request must be approved by the Provost and then submitted to the Registrar's Office for assignment of the W grade in the system of record. The W grade does not affect the student's GPA, and the student will not earn credit for that course. For Distance Learning Students, Deans of Faculty may approve withdrawals

\For.additional.information.on.grades.and.grade.policies.please.refer.to.the.AY.868❷student.handbook¡

# Faculty and Administration

## Leadership

Elizabeth Phu
Chancellor

Andrew Walsh
Deputy Chancellor

Stuart Archer
Dean of Administration

Francis Marlo
Dean of Faculty and Academic Programs

Roman Mills, CAPT
Dean of Students

Matthew Easley
Associate Dean of Joint Warfighting

Marwan Jamal, Ph.D.
Associate Dean of Academic Programs and Planning

Linda Baughman, Ph.D.
Director of Institutional Research

Donna Powers
Director Academic Support

Timothy Hammond
Director of Strategic Engagemnent

Gwyneth Sutherlin, Ph. D.
Director, UC2

Nakia Logan
Director of Student Services

## Cyber Strategy

Nancy Blacker
Department Chair
Associate Professor

Michael Brody
DHS Chair

James Churbuck
Associate Professor of Practice

Deanna Fisher, CDR
Military Faculty

Charles McLaughlin
Professor of Practice

Frank Nuno
Assistant Professor

Joseph Schafer, Ph.D.
Professor

Michael Stamat, Lt Col
Military Faculty

J.D. Work, Ph.D.
Assistant Professor

Chrisopher Martinez, COL
Military Faculty

## Cyber Strategy and Infrastructure

Marwan Jamal, Ph.D.
Department Chair
Professor

Keith Caldwell, LTC
Military Faculty

Linda Jantzen, Ph.D.
Assistant Professor

Jim Chen
Professor

Mike Love, Ph. D.
Associate Professor

Robert Richardson IV
DISA Chair

Nalonie Tyrrell, LTC
Military Faculty

## Information Strategy and Disruptive Technology

Dorothy Potter, Ph.D.
Department Chair
Professor of Practice

Elena Bailey, Ph.D.
Assistant Professor

Abdullah Clark, LTC
Military Faculty

Howard Clark, Ph.D.
Associate Professor

Jill Goldenziel, Ph.D., J.D.
Professor

David Harvey
Professor of Practice

Richard Love, Ph.D.
Professor

Eric Murphy, Col
Military Faculty

John Sullivan
Professor

## Staff

Jairus Akanni
UC2 Contractor

Blair Allan
UC2 Contractor

Samantha Baehr
Event Coordinator

Saya Bobick, Ph.D.
Academic Advisor

Ishid Camp
Academic Specialist

Nicole Cox
Program Manager of Faculty Enhancement

Kristi Galbraith
UC2 Contractor

Nicki Hannum
Academic Specialist

Victor Lima, Capt
Military Staff

Patrick O'Connell
Business Support Contractor

Christine Saba, Ph. D.
Associate IR Director

Marissa Simms
OSS Academic Staff Contractor

Aileen Solomon
Program Manager, UC2

Jeanita Williams
Business Support