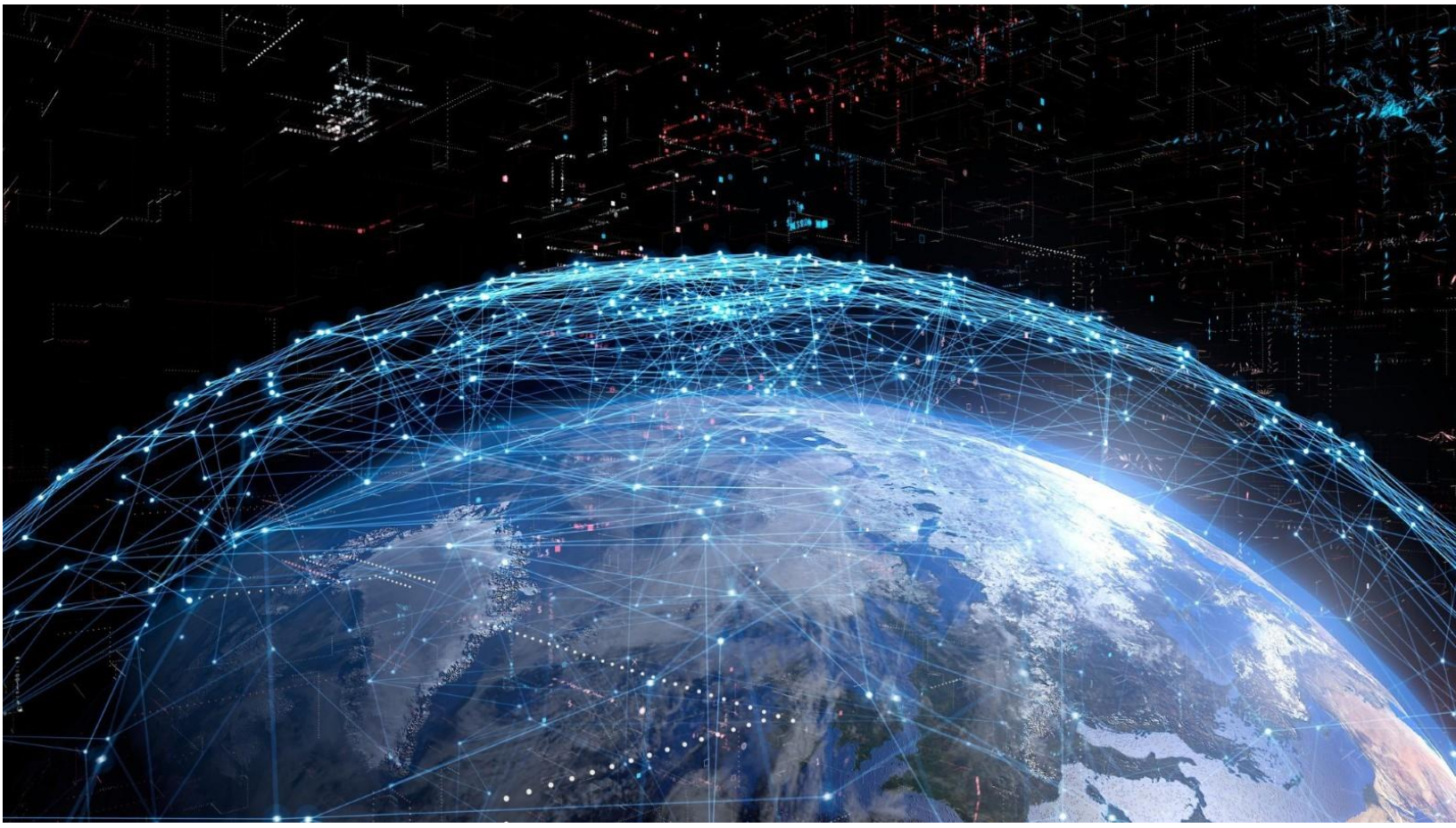
KELLEY SCHOOL OF BUSINESS
Executive Education

INDIANA UNIVERSITY BLOOMINGTON
SPACE GOVERNANCE LAB

Space Cybersecurity

Professional Certificate Program



The Indiana University Bloomington Space Governance Lab, together with the Kelley School of Business - Executive Education, launched a new Space Cybersecurity Professional Certificate Program, in collaboration with the public and private sectors

Background: The Emerging Space-Cyber Nexus and the Urgent Need for Skilled Personnel

Space has long been a dangerous and uncertain domain. There are few places where cybersecurity and resilience are so critical to mission success than space. A traditional, on the ground cybersecurity event may mean temporary service outages and delays, but is physically reachable by cybersecurity personnel to mitigate the risk. In contrast, a cyber event impacting assets in space has the potential to go undetected for long periods of time, delivering inaccurate or dangerous data to critical infrastructure, users, and other services. While key US adversaries have proven capabilities to destroy satellites using Anti-Satellite missiles (ASATs), the major risk to satellites is from cyberattacks, which are easier and cheaper to launch and provide plausible deniability. Space cyber-attacks are a low-risk, high-yield tool and the perfect asymmetrical weapon, the kind of which were launched by states, criminal organizations and terrorist groups. Due to the reliance of advanced militaries and modern economies on space-based infrastructure, its disruption might cripple the military and bring the economy to a standstill. In our daily lives we might see disruption of our ability to navigate, use credit cards and ATMs and even TV and the internet. The war in Ukraine, dubbed the first space-cyber war demonstrated these challenges, when on the eve of the Russian invasion, the satellite services that ViaSat, an American company, provides to Ukraine were disrupted. This new combined space-cyber warfare theatre is emerging as the primary battlefield for superpowers in the 21st century, and commercial space companies are also targets.

Now more than ever, the US Space Force and the space industry—and all firms that work within it—are in desperate need of space cybersecurity professionals who understand the space domain as well as the unique challenges it presents. Indeed, while terrestrial cybersecurity methods can apply to ground stations, the space segment presents new challenges. Currently, the US is almost completely lacking skilled space cybersecurity personnel. Indiana University Bloomington therefore decided to pioneer a program that would train the first generation of space cybersecurity experts.

Program Description

This is the first program, in the United States and globally, to offer training in the cybersecurity of space assets. At the end of the program, participants would have the capacity to develop and see the implementation of an organization-wide policy and measures on space cybersecurity. They will gain an in-depth understanding of the cyber threats to space assets, the different types of space cyberattacks, and the systems and applications at higher risk. They will learn protective strategies and tools as well as the legal requirements and industry best practices. They will be introduced to the available support from the government and industry organizations. They will further learn how to respond to an incident. The program promotes innovation and cyber resilience in aerospace while also providing the opportunity to be part of a network of space cybersecurity professionals.

This Program is geared towards existing and would be chief information security officers (CISOs) of space companies and government agencies, as well as advanced students of cybersecurity interested in a career in the space sector.

Hours & Credits

This is a 10-weeks, 30 hours program.

This is a stand-alone program, graduates of which will earn a Digital Badge if they attend 80% of the sessions and take either the Space Cybersecurity Quiz or the Space Cyberattack Postmortem and pass with a score of 80% or more.

In addition, participants may earn 3 credit hours towards IU's prestigious 12-credit hour Kelley School of Business graduate certificate in Cybersecurity Management or 30-credit hour Master's of Science in Cybersecurity Risk Management degree. To earn the 3 credit hours, participant will need to (1) attend all sessions, and (2) take both the Space Cybersecurity Quiz and the Space Cyberattack Postmortem assignments and pass with a score of 80%.

Schedule & Place

In each of the 10-weeks we will have a 1-hour synchronous teaching via Zoom + 1-2 of asynchronous work.

The schedule includes a mix of synchronous lectures and discussions, asynchronous pre-recorded presentations, home readings, and assignments to provide a comprehensive learning experience for the participants.

Week	Topic
1.	**Introduction to Space Cybersecurity** ○ Space assets as critical infrastructure and prime targets ○ The unique cyber vulnerabilities of space systems ○ Space systems as system of systems (ground control, space segment, etc.) ○ The emergence of the space-cyber nexus and the escalatory cycle of its militarization ○ The first space-cyber war and its ramifications ○ The market for space cybersecurity
2.	**Law and Policy of Space Cybersecurity** ○ International space law and cyber law and the international law of space-cyber warfare ○ U.S. space laws and regulatory framework for cybersecurity regulation ○ Presidential Memoranda: Space Policy Directive-5—Cybersecurity Principles for Space Systems ○ The Bills in Congress on space cybersecurity
3.	**Compliance: frameworks and standards** ○ U.S. frameworks and standards on cybersecurity of space systems (DHS/CISA, FBI, NIST) ○ German technical standards on cybersecurity of space systems ○ Towards an ISO standard for cybersecurity of space systems ○ Implementation and compliance: ➢ compiling regulations into an organization-wide policy ➢ navigating the complexities of multiple relevant authorities and instruments

4.	**Designing and Implementing a Mitigation Strategy & Secure by Design** ○ Secure by Design: embedding cybersecurity at the design phase of systems and processes so they are foundationally secure ○ Designing a cybersecurity policy for space organizations ○ Preparing and implementing effective mitigation strategies ○ Testing mitigation strategies with real-world scenarios
5.	**Threat Identification** ○ The importance of threat identification for business and services continuity ○ Proactive threat identification methods ○ Identifying space cybersecurity vulnerabilities and threats ○ Analysis of past incidents (ViaSat etc.)
6.	**Space Attack Research and Tactic Analysis (SPARTA)** ○ Using cybersecurity matrices and the SPARTA method for space-cyber TTP analysis ○ Applying SPARTA in the space-cyber context.
7.	**Verification & Validation (including Risk Analysis)** ○ Verifying that the space system's requirements are correctly defined ○ Validating that the space system correctly implements the required functionality and security requirements ○ Performing Risk Assessment: documenting potential risks and the policies adopted to mitigate them
8.	**Business Continuity, Mission Assurance, and Redundancy** ○ Redundancy and preventive measures in space cybersecurity ○ Implementing resilience measures in space systems ○ Incident response ○ Ensuring mission-critical operations and maintaining vulnerable assets during disruptions
9.	**Space Systems Security & SOC** ○ Systems security of space systems and services ○ The unique challenges of securing the space segment ○ The three pillars - People, Process, and Technology ○ SOC (security operations center) for space systems: monitoring operations, and detecting, investigating and responding to incidents ○ SOC - in house or outsource?
10.	**Cross-Sector Collaboration on Space Cybersecurity: Government, Military, Industry, Academe** ○ Cross-sector collaboration: importance and tools ○ Tapping into the Knowledge Pool on Space Cybersecurity ○ The importance of information sharing in space cybersecurity ○ The Space ISAC (Space Information Sharing and Analysis Center) ○ How to draw from the experience of other space actors and leverage shared information for better practices

Eligibility Requirements

The program does not require prior cybersecurity education or technical proficiency.

Each application will be evaluated on its merits.

Tuition & Scholarships

The tuition is $ 3,995.

Full and partial scholarships are available to all participants! Follow this link to apply.

Registration

For additional information and registration visit the program's webpage.

Faculty

In order to train the first generation of space cybersecurity personnel, IU Bloomington invited experts from the government and industry to complement its already leading cybersecurity faculty.

1.1 IU Faculty

- Professor Scott J. Shackelford, Executive Director, Center for Applied Cybersecurity Research
- Professor Eytan Tepper, Director, Space Governance Lab & Space Cybersecurity Program Director

1.2 External Faculty

- Professor Gregory Falco, Cornell University Sibley School of Mechanical and Aerospace Engineering
- Henry Danielson, CISSO, CSWAE, CDRE,CIHE, Technical Advisor, California Cybersecurity Institute & Lecturer/Adjunct Professor Liberal Arts, Cal Poly, California
- Brandon Bailey, Senior Project Leader for the Cyber Assessments and Research Department, The Aerospace Corporation
- Nick Saunders, Chief Cybersecurity and Data Officer for Government Systems, ViaSat
- Scott Nelson, (Colonel, Retired), Cyber Workforce Initiatives, Information Operations, and Academic Engagement, U.S. Cyber Command / Department of Defense
- Michael Campanelli, Area Practice Leader – Department of Defense, Amazon Web Services
- Erin Miller, Executive Director, Space ISAC