INDIANA UNIVERSITY BLOOMINGTON
SPACE GOVERNANCE LAB

INDIANA UNIVERSITY
EUROPE GATEWAY

INSTITUTE FOR EUROPEAN STUDIES
HAMILTON LUGAR
SCHOOL OF GLOBAL AND INTERNATIONAL STUDIES

European Space Cybersecurity Priorities & Capacity Building

Workshop at Indiana University's Berlin Global Gateway

February 26-27, 2026

Workshop Location

Indiana University Europe Gateway
Gneisenaustraße 27
10961 Berlin
Germany

Purpose

The Berlin Workshop on European Space Cybersecurity Priorities & Capacity Building will convene European space professionals from government, academia and industry with a view to co-design a Model European Space Cybersecurity program, fitted European needs, and building on Indiana University's Space Cybersecurity program.

The workshop will integrate data from a survey to be conducted specifically for this purpose, soliciting input from European space cybersecurity professionals from the government, academia, and industry. The workshop will extend "EU-IU collaboration" to create a cross Atlantic partnership on space cybersecurity capacity building, noting the shared threats and opportunities.

Workshop Organizers

The workshop is organized by Indiana University's Space Governance Lab, Institute for European Studies, Europe Gateway, and International Affairs in collaboration with ethicallyhacking.space and the University of Hamburg.

Organizing team:

Scott J. Shackelford, Provost Professor and Associate Vice President & Vice Chancellor for Research, Indiana University Bloomington

Eytan Tepper, Research Professor, Space Governance & Security and Director, Space Governance Lab, Indiana University Bloomington

William O. Ferguson, ethicallyHackingspace (eHs)

Colton T. Ames, Associate Director, Institute for European Studies, Indiana University Bloomington

Annabell Türk, Director, Indiana University Europe Gateway, Berlin

DAY 1

European Space Cybersecurity Priorities

February 26, 2026

A Call to Action

Indiana University has taken on a global mission to extend its established Space Cybersecurity program to the European Union as a means of accelerating the development of EU-specific space cybersecurity capabilities. This mission is built on one common goal: to cultivate a generation of experts across cyberwarfare, research, security operations for space systems, and both commercial and government domains who are equipped to meet the threats and opportunities of tomorrow.

We have selected you based on your demonstrated passion and commitment to advancing this critical topic. You are here because you are a leader, an innovator, and a driver of change in space cybersecurity. We implore you to bring that energy, expertise, and passion into every session of this workshop.

Our objective over these two days is to enable leaders in the strategic, organizational, and governance dimensions of space cybersecurity, in the management of cyber risks to space systems, and in the development of national and regional response capabilities to collaborate openly and ambitiously. Together, we aim to make available existing solutions from the United States while simultaneously supporting the innovation and development of EU-specific capabilities that reflect European regulatory frameworks, operational realities, and strategic priorities.

This is your workshop. The outcomes we produce here will directly shape the Model European Space Cybersecurity Program and the future of transatlantic cooperation in this domain. Be active. Be bold. Be the leaders this mission requires.

Time	Session
11:00-11:30	**Registration and Coffee** Participant check-in and informal networking.
11:30-12:00	**Opening Plenary: Cross Atlantic Partnership on Space Cybersecurity** Overview of Indiana University's space cybersecurity initiatives, including the Space Cybersecurity program, and the cross Atlantic partnership initiative to jointly curate a Model European Space Cybersecurity program and offer it in European NATO member countries via partnerships with academia (e.g., Universität Hamburg and Université Toulouse Capitole) and governments (e.g., BSI, CNES). Introduction of the survey: explanation of the survey's purpose, structure, and how participant responses will inform the afternoon sessions and curriculum design.

	Output: Shared understanding of the goals and methods, including how the sessions will support drafting a European-tailored curriculum.
12:00-12:30	*Lunch* Break for lunch and informal networking.
12:30-13:00	**Survey Completion** Participants complete the survey introduced during the Opening Plenary. The survey captures role-specific perspectives on space cybersecurity priorities, skill gaps, and European regulatory considerations. Responses will be compiled and used to frame the afternoon sessions. **Output:** Completed survey responses ready for integration into afternoon presentations and breakout discussions.
13:00-14:00	**Indiana University Space Cybersecurity Baseline Topics Framed by Survey and European Objectives** Presentation of core domains including architecture and attack surfaces, secure software and firmware, detection and telemetry, resilience and incident response, supply chain assurance, and governance, policy, and compliance. Each domain is compared with survey inputs and European regulatory drivers such as NIS2, ESA and ENISA initiatives, and NATO priorities. **Output:** A comparative map identifying strong alignment areas and elements requiring adaptation.
14:00-14:15	*Break*
14:15-15:00	**Breakouts I: Role-Specific Priorities** Research Track: Review of Section B signals and identification of three leading research priorities. Industry Track: Review of Section C signals with emphasis on workforce shortage areas and skill gaps. Government Track: Review of Section D signals and identification of oversight and competence gaps related to NIS2 and CER obligations. **Output:** Three priority signal maps linking role needs to baseline topics and European/NATO objectives.
15:00-15:15	**NATO Space Cybersecurity Preparedness** A presentation by Professor Eytan Tepper.
15:15-16:00	**Breakouts II: Tailoring to Role Needs** Each group drafts learning outcomes aligned with its priority signals, European regulatory requirements, and the Indiana University baseline domains.

	Output: Draft role-specific learning outcomes.
16:00-16:45	**Plenary Synthesis: Cross-Cutting Needs** Participants integrate learning outcomes across all tracks. Cross-cutting European/NATO expectations are identified, including standards, certification paths, mobility, and intelligence-sharing practices. **Output:** Draft set of core Model European Space Cybersecurity Program learning outcomes.
16:45-17:00	**Wrap-Up** Review of Day 1 outputs, and planning for Day 2. **Output:** Inputs for Day 2 design activities.
18:00	**Dinner Reception** Kreuzberger Himmel, Yorckstraße 89, 10965 Berlin

DAY 2

Model European Space Cybersecurity Program

February 27, 2026

Morning Session: Curriculum Design

Time	Session
8:30-9:00	**Coffee and Networking** Informal discussion and preparation for the design session.
9:00-9:15	**Recap and Decision Criteria** Review of Day 1 outputs including signal maps and draft learning outcomes. Criteria for module inclusion and emphasis are confirmed with attention to European regulatory alignment and role relevance. **Output:** A decision matrix guiding module drafting.
9:15-10:00	**Breakouts III: Academic, Commercial, and Government Pathways for Space Cybersecurity Workforce Capacity Building** "How do we align the next generation with the roles of the future?" Each pathway group develops a structured approach to workforce development that addresses training durations, delivery types, and progression models.

	Groups explore how hackathons, workshops, conferences, and sustained training programs contribute to capacity building within their sector. **Output:** Four pathway proposals: (1) an Academy approach with structured programme durations and certification milestones; (2) an Academic approach with degree integration, research-led training, and faculty development; (3) a Commercial Industry approach with corporate training pipelines, vendor partnerships, and hands-on exercises; and (4) a Government approach with national workforce frameworks, interagency exercises, and policy-driven competency standards. Each proposal specifies recommended training durations and types including hackathons, workshops, and conferences.

Applied Training Session

Space Cybersecurity Foundations - Indiana University Digital Badge Program

This training session delivers the Indiana University Space Cybersecurity Foundations course across three modules. Each module runs for 50 minutes followed by a 10-minute break. Module III features sovereign speakers from partner nations to assist with country-specific content delivery.

Module I: Strategic, Organizational, and Governance Dimensions of Space Cybersecurity

Time	Topic
10:00-10:10	**Introduction and Program Overview**
10:10-10:25	**The Emergence of the Space-Cyber Warfare Domain**
10:25-10:40	**Regulatory Instruments and Standards Landscape**
10:40-10:50	**Organization-Wide Cybersecurity Policy**
10:50-11:00	***Break***

Module II: Managing Cyber Risks to Space Systems

Time	Topic
11:00-11:10	**Cyber Threats to Space Systems**
11:10-11:20	**The Space System Attack Surface**
11:20-11:30	**Secure-by-Design Principles**
11:30-11:40	**Detection, Monitoring, and Situational Awareness**
11:40-11:50	**Incident Response and Resilience Practices**
11:50-12:40	***Lunch***

Module III: Space Cybersecurity Priorities and Emerging Response Capabilities

Time	Topic
12:40-12:48	**The European Space Cybersecurity Landscape**
12:48-12:58	**United States: Space Cybersecurity Standards and Responses**
12:58-13:08	**Germany: Space Cybersecurity Standards and Responses**
13:08-13:18	**France: Space Cybersecurity Standards and Responses**
13:18-13:28	**United Kingdom: Space Cybersecurity Standards and Responses**
13:28-13:38	**European Perspectives: Cybersecurity as a Resilience Mechanism**
13:38-13:48	**Capacity Building in Space Cybersecurity**
13:48-13:52	**Course Conclusion and Next Steps**
13:52-14:00	**Break**

Output: A shared technical foundation suitable for transatlantic and European-wide adaptation.

Assessment: Space Cybersecurity Foundations Quiz

Optional. Participants who attend the Applied Training Session and take the quiz will earn the Indiana University Space Cybersecurity Foundation digital badge.

Time	Session
14:00-14:30	**Multiple Choice Assessment** Ten-question multiple choice quiz covering content from all three modules. A passing score of 70% (7 out of 10 correct) is required to earn the digital badge.
14:30-15:00	**Closing Remarks**

Co-funded by the
Erasmus+ Programme
of the European Union