European
Cyber Conflict
Research
**Incubator**

# Application Guide

A Step-by-Step Guide to Applying for Google.org's Cybersecurity Seminar Grants

**James Shires & Max Smeets**

**3 January 2024**

# About Us

The European Cyber Conflict Research Incubator CIC (ECCRI CIC) advances the interdisciplinary study of the impact of digital and emerging technologies on global affairs, in Europe and beyond. ECCRI CIC exists to conduct, facilitate and promote research and education on these issues for policymakers, industry, civil society, and the general public. ECCRI CIC is a UK community interest or not-for-profit company (CIC), with its assets tied to the European Cyber Conflict Research Initiative (ECCRI), a UK registered charity. The Initiative also encourages and supports high-quality original research, enabling researchers to communicate their findings to policymakers and the general public. The Initiative runs a wide range of projects, from small writing workshops to larger conferences, where scholars and practitioners can discuss the latest developments.

# Table of Contents

# About the Authors

## James Shires

James is the Co-Director of both the European Cyber Conflict Research Incubator (ECCRI CIC) and the European Cyber Conflict Research Initiative (ECCRI). He is also a Fellow with The Hague Program on International Cyber Security. He was previously a Senior Research Fellow in Cyber Policy at Chatham House and an Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden. He has written widely on issues of cybersecurity and international politics, including cybersecurity expertise, digital authoritarianism, spyware regulation, and hack-and-leak operations. He is the author of The Politics of Cybersecurity in the Middle East (Hurst/Oxford University Press, 2021), and co-editor of Cyberspace and Instability (Edinburgh University Press, 2023).

## Max Smeets

Max is the Co-Director of the European Cyber Conflict Research Incubator (ECCRI CIC) and the European Cyber Conflict Research Initiative (ECCRI). He is also a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich.

His scholarship focuses on cyber security, strategy and risk. He is the author of 'No Shortcuts: Why States Struggle to Develop a Military Cyber- Force' (Oxford University Press & Hurst Publishers, 2022) and co-editor of 'Deter, Disrupt or Deceive? Assessing Cyber Conflict as an Intelligence Contest' (Georgetown University Press, 2023) and 'Cyberspace and Instability' (Edinburgh University Press, 2023). He is currently writing a book on ransomware.

In 2023, he co-founded Binding Hook, a media outlet at the intersection of technology and security. Max is an affiliate at Stanford University's Center for International Security and Cooperation (CISAC) and an associate fellow at Royal United Services Institute (RUSI). He also lectures on cyber warfare and defense as part of the Senior Officer course at the NATO Defense College in Rome.

# Overview

Google.org is collaborating with ECCRI CIC to offer enhanced learning and job opportunities in the field of cybersecurity through the European Cybersecurity Seminars program.

This initiative is aimed at students from selected European universities. These students will have the opportunity to apply their learned skills in practical settings, which will not only help them advance in their abilities but also positively impact their local communities.

Here, we provide a step-by-step guide on how to set up and apply for a Google.org Cybersecurity Seminar grant. This guide will assist you through the process, making sure you have all the necessary information to successfully apply for this opportunity

**Step 1**

Check Eligibility Criteria

**Step 2**

Faculty Champion

**Step 3**

Institutional Support

**Step 4**

Develop Seminar

**Step 5**

Collaboration Assessment

**Step 6**

Mitigate Liability Risks

**Step 7**

Estimate Budget

**Step 8**

Apply

# Step 1 Check the eligibility criteria

European Cybersecurity Seminar grants are only available to universities in one of the following seven countries:

- France
- Poland
- Romania
- Ukraine
- Germany
- Greece
- Czechia

Higher education institutions that are not universities are eligible to apply, as long as their primary purpose is education and most of their courses are open to applications from the general public. Examples include polytechnic institutes, vocational or professional colleges, or military or diplomatic academies. For simplicity, we refer to universities throughout this document.

Eligible applicants must be nonprofit, meaning that the organization’s mandate stipulates that it cannot make a profit or that all profits must be reinvested in the academic or educational purposes of the institution.

# Step 2 Faculty Champion

The second step in applying for a Google.org Cybersecurity Seminar Grant is identifying and assigning the role of the 'Faculty Champion' to a Principal Investigator (PI). This individual must be a permanently employed (tenured) or tenure-track member of the university's academic staff, and is crucial in spearheading the application process for the university.

The PI not only submits the application but also ensures that it reflects the university's vision for enhancing its cybersecurity education. The quality of the application depends on how well the PI communicates this vision and the proposed plan's benefits to both students and the broader community.

# Step 3 Institutional Support

In this step, the application must secure wider backing from the university.

It is essential that the Principal Investigator's proposal has the full support of the institution. Such support is a testament to the project's viability and the university’s commitment to advancing cybersecurity education.

Applications require close coordination within the university, ensuring that the selected application carries the weight of the institution's endorsement and is well-aligned with its overall educational goals.

To ensure full university-wide support, each PI can submit only one application, and a university may be part of only one application, whether as the main applicant or as a sub-granted or sub-contracted institution (more details on this below).

# Step 4 Develop and design your Cybersecurity Seminars

Applicants must craft Cybersecurity Seminars that not only align with the university's infrastructure and vision but also meet specific impact metrics.

Cybersecurity Seminars should realistically aim to train at least 200 seminar students and serve a minimum of 250 local community organizations in preventing cyberattacks by September 2026. The primary measure of success is meeting this impact metric.

Substeps in Developing a Cybersecurity Seminar

## 1. Timing and Design

- Determine whether the Cybersecurity Seminar will be held during term time, as a summer school, or through evening classes.
- To give you an idea of students' and teachers time commitment and the substantive nature of Cybersecurity Seminars, each Seminar should equate to a 5EC component under the European Credit system (roughly 135 hours), with a higher proportion of contact hours (around 50) and a focus on project work with local community organizations.
- Ideally, the first Seminar will be held before the end of 2024.

## 2. Recruitment of Students

- Develop a student recruitment strategy emphasizing diversity, inclusivity, and gender balance.
- Focus on active engagement with underrepresented communities. Please avoid collecting personal data relating to race, religion, or any other special or protected categories.

## 3. Engagement with Local Partners

Illustrate how the seminar will connect students with local community organizations for practical learning experiences.

Examples of partner engagement include:

- **Internship Program**: Practical, hands-on experience in a professional setting as part of the seminar.
- **Hacking Competition**: Competitive events focused on cybersecurity skills, such as ethical hacking or defense strategies.
- **Capstone/Consultancy Project**: A project-based learning experience, simulating real-world consultancy or capstone projects.

## 4. Types of Local Partners

The seminar should engage a variety of local community organizations, such as:

- **Public Entities**: City halls, libraries, schools, etc.
- **Nonprofits**: Homeless shelters, food banks, museums, etc.
- **Local Businesses**: Independent bookstores, family-owned restaurants, local art galleries, etc.
- **Community Organizations**: Sports clubs, cultural heritage groups, scouting organizations, etc.

# **Step 5** Collaboration Assessment

This step involves a critical evaluation of whether collaboration with other educational institutions is required to achieve the desired impact of your cybersecurity seminar program. Applicants must consider the necessity and potential benefits of such partnerships.

Collaboration with other educational institutions is permitted, but does not automatically strengthen an application. Where collaboration is central to an application – especially if an applicant intends to sub-contract or sub-grant some of their grant award to another educational institution – such collaboration should build on existing relationships in relevant areas.

# Step 6 Mitigating Liability Risks in Cybersecurity Seminars

In setting up a cybersecurity seminar, it is crucial to address the liability risks for both the institution and its clients.

Given the real-world implications of the students' actions and recommendations, safeguarding against potential harm and legal repercussions is paramount. This involves a clear understanding of responsibilities for seminar organizers and local community organizations involved, ensuring both parties are equipped to handle engagements with integrity and awareness.

You should involve your university's legal team early in the planning process. The seminar design should fit within the university's risk tolerance.

Additionally, educating students about the inherent risks in defending against cyber threats is a key component of the program. This is especially important when dealing with high-risk scenarios such as working with international or multinational organizations, or more hands-on roles within an organization's technical infrastructure. In such cases, extra precautions, like protecting student identities, may be necessary to ensure their safety and maintain the integrity of the seminar.

# Step 7 Budget Estimation

Step 7 involves creating a comprehensive budget estimation. Successful applicants can receive up to $1,000,000 from Google.org to support the running of Cybersecurity Seminars.

This grant can cover various costs associated with the delivery of courses within the program.

When planning the budget, applicants should consider a range of expenses, such as:

## Faculty and Instructor Compensation

- Payment for faculty and instructors involved in the clinic, which can include compensation for summer sessions.

## Graduate Researcher / Teaching Assistant / Post-doc Support

- Funding for teaching assistants, typically one per semester, who provide instructional support.

## Equipment Needs

- This includes laptops, software, and tools for secure storage and collaboration.

### Curriculum Development

- Costs associated with developing and updating the seminar curriculum.

### Student Involvement

- Expenses for student travel to meet with clinic clients in person, attend conferences, and work as interns.

### Outreach and Promotion

- Allocation for time spent with the institution's communications staff to raise awareness, recruit students, and highlight the successes of the clinic.

In addition to these specific costs, applicants should also consider potential administrative expenses. However, it's important to note that the maximum amount permitted for non-program related costs is 10% of the total grant amount requested.

# Step 8

# Apply for Google.org Cybersecurity Seminars

Applications for the program should be submitted through Submittable. Detailed instructions are available on the Submittable website, and applicants can create an account and collaborate with others on this platform.

Applications will be reviewed by a panel consisting of ECCRI CIC, Google.org, and external experts. Applications will then be recommended by the panel to Google for due diligence checks prior to signing a grant agreement with Google.

Successful applicants will receive cybersecurity education resources by ECCRI CIC and access to Google's technology and expertise. They will also gain access to a diverse and extensive European-wide cybersecurity instructor network, providing valuable mentorship and expertise to help them excel in the field of cybersecurity.

# Timeline and further information

| Opening of Application | Information Workshops: | Deadline for Application Submission: | Notification of Selection | Commencement of the Program |
|---|---|---|---|---|
| November **29, 2023** | January & February **2024** | February **29, 2024** | March **31, 2024** | September **2024** |

Learn more by registering for one of our information workshops via our website. Information workshops will be held on Zoom at the following times (all CET):

**Thursday 11 January 2024, 2-3.30pm**
**Monday 29 January 2024, 3.30-5pm**
**Wednesday 14 February 2024, 10.30am-12pm**

For more information, please visit

**www.cyberseminars.org**

If you have any further queries or need to update your contact details, feel free to reach out via email at:

**contact@europeancyber.org**

European
Cyber Conflict
Research
**Incubator**

European
Cyber Conflict
Research
Incubator

We look forward to receiving your application