European
Cyber Conflict
Research
Incubator

An Analysis of Cybersecurity Education Programs in Europe

Key Findings

James Shires, Max Smeets & Beth Whittaker

10 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.

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. In 2023, he co-founded Binding Hook, a media outlet part of ECCRI 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).

Beth Whittaker

Beth is an Analyst with the European Cyber Conflict Research Incubator (ECCRI CIC). Prior to joining ECCRI CIC she completed an internship with the International Security Programme at Chatham House. Beth holds a masters in Global Security from the University of Glasgow, in addition to an undergraduate degree in Politics and International Relations from the University of Aberdeen.

Introduction

This report presents key findings from an initial assessment of cybersecurity educational programs in eight European Countries: **Czechia**, **France**, **Germany**, **Greece**, **Poland**, **Romania**, **Spain** and **Ukraine**. These countries were chosen because they are all participants in the open call for the Google.org Cybersecurity Seminars program. **The purpose of this assessment is to establish a baseline for advancements in cybersecurity education and identify exemplary programs and practices**.

The assessment covers a wide range of cybersecurity education programs. This includes not just specialized cybersecurity courses, but also general computer science programs and those that mix cybersecurity with policy or business. It also looks at programs that combine different subjects, like artificial intelligence and cybersecurity, and policy courses that have cybersecurity components. The scope of the assessment is limited to university degrees and does not extend to other higher education institutions.

This report elaborates on the following key findings:

1. The availability of cybersecurty degree programs varies across Europe.
2. Cybersecurity degrees retain a technical core but are increasingly interdisciplinary.
3. Around a quarter of universities collaborate with the private sector to provide or enhance cybersecurity degrees.
4. Classroom based learning remains to predominant model for cybersecurity education
5. Few cybersecurity degrees actively promote equality, diversite and inclusion (EDI)

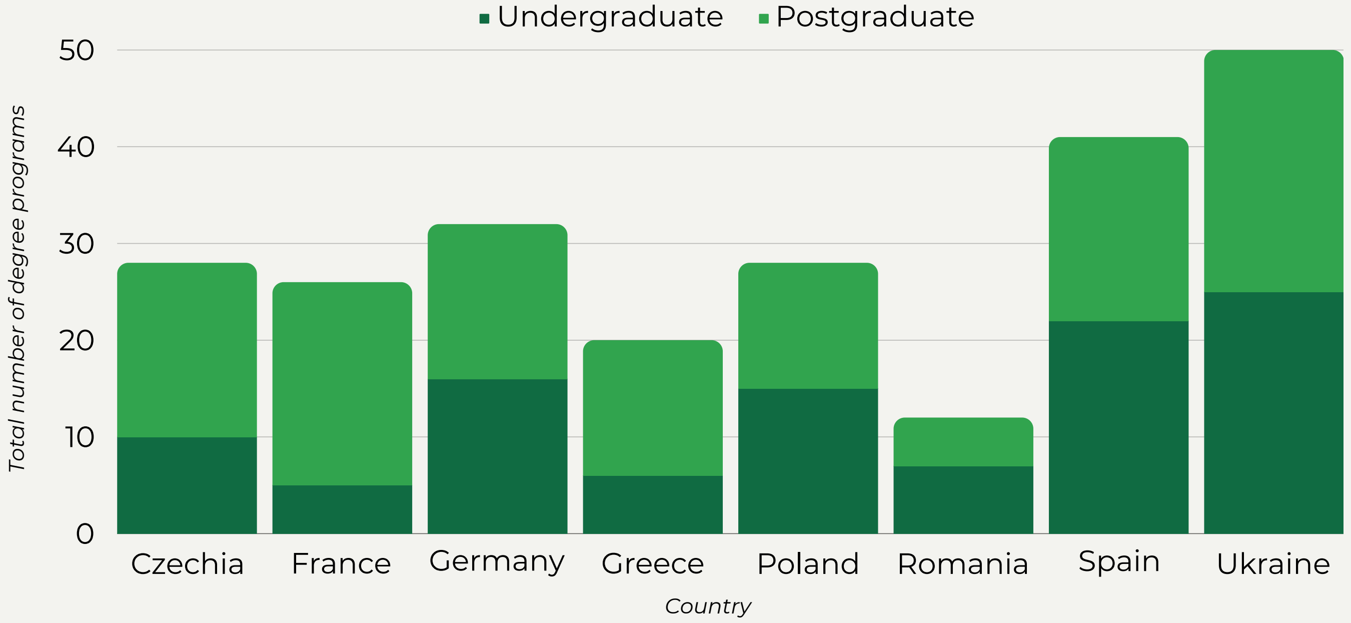
Key Finding 1: The availability of cybersecurity degree programs varies across Europe

Students interested in cybersecurity have multiple options to choose from for their university education.

On average, we found 30 cybersecurity degrees per country across a total of 138 universities. However, the number of available degrees varies across each of the eight countries.

At the upper spectrum, we discovered 50 undergraduate and graduate degrees in Ukraine, 41 in Spain, 32 in Germany, 28 in Poland and Czechia, 26 in France, 20 in Greece and on the lower end, we found a more limited selection in Romania, with just 12 cybersecurity degrees on offer.

Number of cybersecurity, and cybersecurity related, degree programs in each country



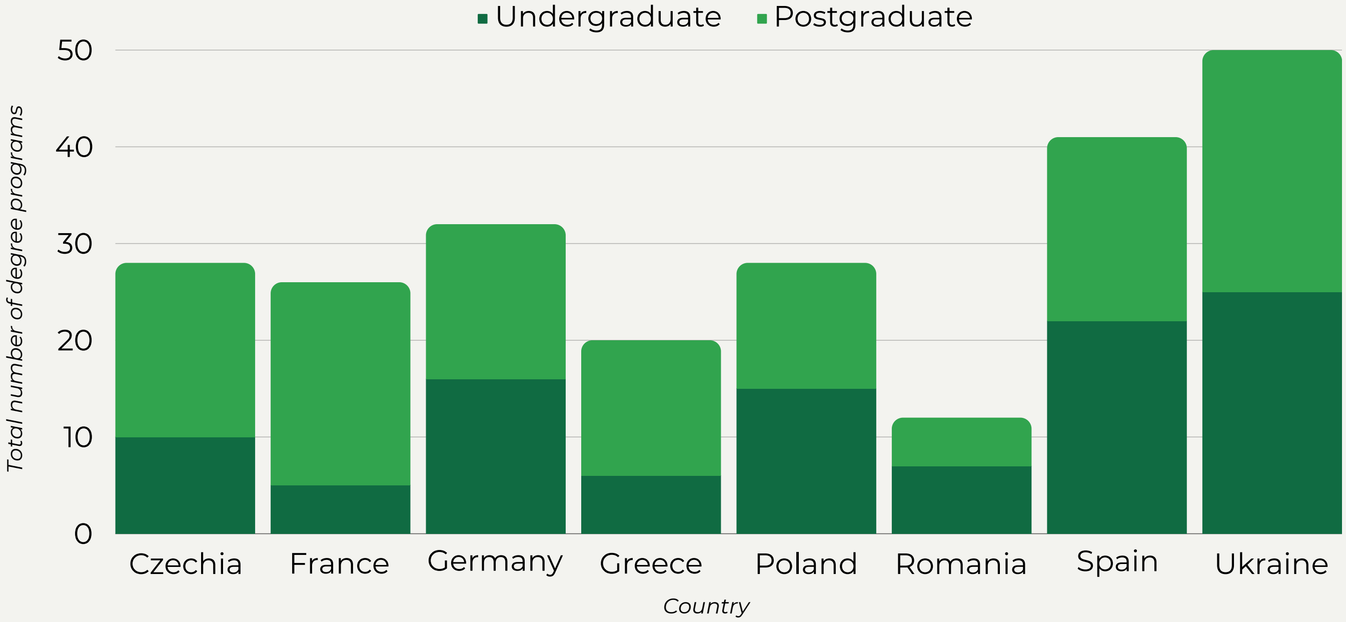
Key Finding 2: Cybersecurity degrees retain a technical core but are increasingly interdisciplinary

Many of the cybersecurity programs we examined have a technical focus, yet still integrate soft skills or social/political aspects of cybersecurity.

Examples include modules on ethics and crime, as seen at the University of Potsdam and the University of Marburg. Similarly, the University of Economics and Human Science in Warsaw, Poland, offers modules in ‘online security of children and adolescents’ and ‘information and hybrid warfare’ as part of their cybersecurity undergraduate program, alongside technical modules in programming and cryptography.

At Brno University of Technology in Czechia, students working towards an engineering degree in cybersecurity can enrol in a ‘Technical Law’ module. Similarly, masters students studying Cyber security at the University of Murcia in Spain will learn the technical skills required to excel in cybersecurity, in addition to the legal nuances. By taking modules covering law and regulation, students will develop an awareness and understanding of the intersection of law and cybersecurity.

Number of cybersecurity, and cybersecurity related, degree programs in each country



Key Finding 3: Around a quarter of universities collaborate with the private sector to provide or enhance cybersecurity degrees

The level of private sector collaboration varies across countries. France and Spain were found to have the highest known partner-engagement, with fewer partnerships indentified from our sample in Czechia, Germany and Ukraine.

From our sample of universities, France and Spain have the highest known partner-engagement with at least 46% of their degree programmes supported by private sector partnerships. In comparison, at least 21% of degree programmes in Czechia and 19% in Germany have known private sector partnerships. However, this assessment of private sector collaboration is limited to public data, meaning that the scope of collaboration is highly likely to be greater than we identified within our sample.

The most recurring partnerships are with multinational companies, including Microsoft, IBM and Cisco. Microsoft and Cisco have public partnerships with universities in Ukraine, Spain and Poland, while Cisco has set up similar partnerships in Greece.

In Ukraine, students at the Simon Kuznets Kharkiv National University of Economics have access to the Microsoft IT academy, and students at Kharkiv National University of Radio Electronics have access to Cisco's Network Academy. Similarly, students at the Mediterranean College in Greece have the opportunity to benefit from Cisco-certified network labs and Microsoft Azure labs, in addition to acquiring the Cisco Certified Network Associate (CNNA) certification.

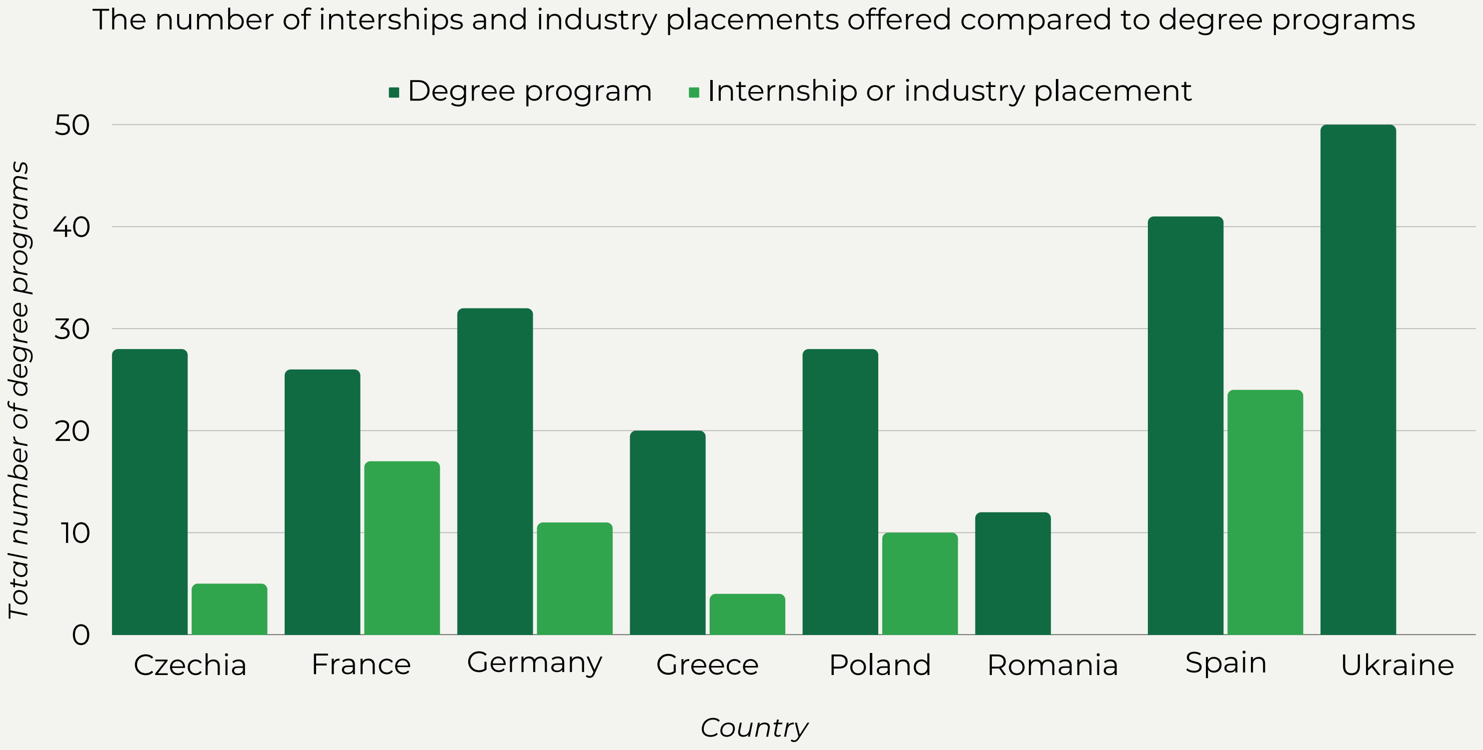
Universities sometimes partner with local businesses, seeking to provide more regional educational opportunities and engagements for students. In France, students at ESIEE Paris, School of Engineering in Electrotechnics and Electronics are granted access to industry placements and industry events through connections with local partners. Likewise in Spain, students studying at the Autonomous University of Barcelona can benefit from the university's partnerships with local and regional industries by acquiring work placements.

Key Finding 4: Classroom-based learning remains the predominant model for cybersecurity education

Across all countries we assessed, most courses take place in a traditional classroom setting with lectures and coursework. The offering of alternative models of education, however, again varies per country.

In France, students can expect to spend a few months of their degree completing an internship, and this is true at both undergraduate and postgraduate level. 65% of degrees researched in France included an internship or industry placement. Spain has a similarly notably high percentage with 59% of degree programs including an internship or industry placement, in comparison to 35% in Poland, 34% in Germany, 20% in Greece and 17% in Czechia, with no known internships or industry placements identified within our sample in Ukraine or Romania.

In France, for example, undergraduate students at the University of Lille's Computer Science complete three months in an internship in the final months of their degree programme, where they apply the knowledge developed during their studies to a business setting. Graduate students in cybersecurity at the Université Grenoble Alpes undertake a five month internship. In Spain, masters students at Mondragon University can complete an optional internship with businesses in both of their two years of study.



In Greece, students at the University of Thessaly can complete an optional internship in their third year. Such internships are intended to benefit both the student and the university: the student can utilise the knowledge and skills they acquire during their studies, while the department strengthens their relationship with the hosting industries. Other examples of non-traditional teaching methods can be found at various universities across Europe. At Saarland University in Germany, undergraduate students have to attend practical sessions in the university's cybersecurity lab. At ESIEE Paris in France, students spend four months working in teams on multidisciplinary projects proposed by industry partners or faculty.

At the Czech Technical University, students have access to an ethical hacking laboratory, named HackingLab, run in partnership with NN Group. The HackingLab grants students the opportunity to practise ethical hacking skills in a controlled environment. In addition to this, the Czech Technical University also runs a Forensic Laboratory and a RFID Laboratory, with the latter focusing on chip card security and other topics.

In Spain at the IE University, students have the opportunity to enhance their learning by participating in a hackathon, in addition to attending a technology immersion week, which provides students the opportunity to interact with and gain exposure to the tech industry.

Key Finding 5: Few university cybersecurity degrees actively promote equality, diversity and inclusion (EDI)

We found only a few programs actively emphasise EDI on their degree program websites or related enrollment materials, or have set up dedicated initiatives aimed at promoting EDI.

Limited data is publicly available regarding the enrollment of students in cybersecurity degree programs. This lack of data makes it challenging to draw definitive conclusions about the characteristics of students in these programs.

There are exceptions to this trend, with BRNO University of Technology being a notable example. BRNO hosts a Summer IT School focused on inspiring school-aged girls in the Czech Republic to learn about computer science. Likewise, in Spain, the University of Lleida includes links to projects which support women in the technology sector, including Google's Women's Techmakers project, on the univers

European Cyber Conflict Research Incubator

europeancyber.org

contact@europeancyber.org