



CYBER SECURITY ACADEMY
22-26 SEPTEMBER 2025
KAROLINSKÁ 707/7, PRAGUE 8-KARLÍN



IN COOPERATION WITH



MAIN PARTNERS





PSSI'S MISSION

The mission of the Prague Security Studies Institute is to help safeguard and strengthen the individual freedoms and democratic institutions of the countries in Central and Eastern Europe and beyond. The Institute also seeks to illuminate select unconventional threats emanating from authoritarian governments that challenge the transatlantic alliance and other partners globally, especially in the economic & financial and space domains. PSSI is dedicated to the education and training of new generations of security-minded students and young professionals, including through its programmatic activities and growing academic network in the Czech Republic and abroad.



MONDAY, SEPTEMBER 22ND

08:30 Meet-up in front of the Missouri Park entrance

08:55 Opening Remarks

Berta Jarošová (Cyber Attachée in Washington, D.C., National Cyber and Information Security Agency)

09:00 Introduction to the Cybersecurity Domain

Foundations of Cybersecurity

Šárka Hurych (National Cyber and Information Security Agency)

The lecture will introduce key concepts in cybersecurity (cyberspace, cybercrime, vulnerabilities, threats, and incidents), outline the national cybersecurity strategy, and discuss the role of the state in the cybersecurity domain.

Šárka Hurych is a legal and policy officer at the Czech Republic's National Cyber and Information Security Agency (NÚKIB), where she focuses on cybersecurity strategy and policy. Alongside her legal and security expertise, she is developing a specialisation in the intersection of cybersecurity and psychology and is currently completing a bachelor's degree in psychology. She holds master's degrees in law from Charles University in Prague and in international security from Sciences Po Paris. She has gained experience in Czech institutions and international organisations, including the Ministry of Defence, the Office of the Public Defender of Rights (ombudsman), the EULEX Mission in Kosovo, the Permanent Mission of the Czech Republic to the United Nations in New York, and UNHCR.

10:45 Cyber Threats and Financial Crime: Using AI to Prevent and Uncover Illicit Financial Flows

Cyber Threat Landscape

Lucie Rehák-Novotná (Resistant AI)

Financial crime (money laundering, fraud, sanctions evasion, etc.) is the enabler of all organised crime in the world. Terrorism needs to be fuelled by money, drug cartels are driven by profit – the financial crime is at the core of this all, and it flows through our banking and payment systems. This session will cover the fundamentals of financial crime, offering an overview of the systems financial institutions currently use to detect and prevent it, the potential of AI to help with a much-needed revolution in this area, and highlight possible career paths for those interested in combating financial crime.

Lucie is an AML and Fraud Solution Engineer at Resistant AI, helping clients leverage the power of advanced machine learning for transaction monitoring and anti-fraud purposes. She has experience with anti-financial crime (AFC) and financial regulation. She combines her previous experience as a compliance officer from Goldman Sachs, as an AFC policy advisor to the public sector, and as a financial crime lead on an AML & fraud tech solution. Lucie has advised governments and policy stakeholders on the design of regulation & supervision, including on topics of anti-corruption, beneficial ownership transparency, AML, and business integrity.



12:30 Lunch Break

13:30 Building a Culture of Security Awareness

Vladimíra Žáčková (MSD Czech Republic)

Foundations of Cybersecurity

Discover the significance of integrating cybersecurity into an organization's culture and how to empower employees to identify and address cyber security threats. Uncover the psychology behind falling for phishing attacks and explore practical strategies for prevention. Gain insights into best practices for building and maintaining security awareness programs to create a more resilient workforce and mitigate the risks associated with insider threats and human error.

Vladimíra Žáčková is a Cybersecurity Awareness Specialist at MSD, where she is responsible for creating and executing strategies to enhance cybersecurity awareness on both a global and local scale. After gaining experience as an IT auditor and consultant, she transitioned her focus to information and cyber security with particular emphasis on governance, internal communication, and employee training. Currently, she is dedicated to promoting cybersecurity for the general public and within corporate environments.

15:15 Ice-breaking Non-Pub Quiz

TUESDAY, SEPTEMBER 23RD

09:00 OSINT Essentials – from Theory to Practice

92nd Cyber Warfare Group (Czech Armed Forces)

Tools, Techniques & Operations

The presentation will outline OSINT as a discipline, describe its features and introduce the most commonly used tools. Specific examples of OSINT used in the field will culminate in a set of practical case studies that will test the audience's OSINT skills.

The center of information warfare in cyberspace is designed to build capabilities and conduct active and highly effective operations of the Czech Armed Forces in cyberspace and in the information space. The Centre's primary task is assessing the factors of an enemy's information influence in cyberspace, planning and implementing active countermeasures.

10:45 OSINT Workshop

92nd Cyber Warfare Group (Czech Armed Forces)

Tools, Techniques & Operations

12:30 Lunch break



13:30 **Offensive Cyber Operations**

Tools, Techniques & Operations

Tomáš Siřínek (Czech Armed Forces)

Offensive cyber operations (OCO) are tools of modern statecraft and strategy. The nation-states exploit digital vulnerabilities not only for espionage, but also to disrupt, degrade, deceive, or destroy adversary systems in ways that can influence political decisions, military outcomes, or generally to achieve national strategic goals in a competing international environment. For some, OCO are perceived as a low cost/high-reward capability. Are they though?

Tomáš Siřínek currently heads the Cyber Testing Group and is Deputy Commander of the Cyber Engagement Center at the 92nd Cyber Warfare Group.

15:15 **Cyber Threat Intelligence at a Glance**

Cyber Threat Landscape

Lucie Kadlecová (PwC, PRCP IMS FSV UK)

In today's rapidly evolving threat landscape, a purely reactive security posture is no longer sufficient. This presentation will demystify the fundamentals of Cyber Threat Intelligence (CTI), explaining how it transforms raw data about emerging threats into contextualized, evidence-based, and actionable intelligence. We will explore the core principles of the intelligence lifecycle and highlight its critical importance in understanding adversary motivations, tactics, and infrastructure. Attendees will leave with an understanding of how an effective CTI programme enables organizations to shift from a reactive to a proactive defense, facilitating more informed strategic decision-making, and a significantly strengthened overall security posture against sophisticated cyber threats.

*Lucie works as a manager in the Global Threat Intelligence Team at PwC and as a post-doctoral researcher at the Peace Research Centre Prague, Charles University, focusing on the non-technical aspects of cybersecurity. She was previously a Fulbright visiting scholar at the Massachusetts Institute of Technology (MIT) in Cambridge, USA and worked at the Czech National Cyber Security Centre. She holds a PhD from Charles University and an MA from the War Studies Department at King's College London. She is the author of the book, *Cyber Sovereignty: The Future of Governance in Cyberspace*, published by Stanford University Press (2024).*

WEDNESDAY, SEPTEMBER 24TH

09:00 **Hacking as a Profession**

Tools, Techniques & Operations

Martin Leskovjan (Penta Hospitals CZ)

In this session, you will delve into penetration testing, or ethical hacking. You will learn about the ethical and legal principles and methodologies used in this field, the most common types of tests, testing tools and procedures, as well as the unexpected pitfalls that practical verification of system resilience can bring. A separate part of the lecture will be devoted to the most



effective type of cyber attack, which is an attack on wetware (humans). It will introduce the basic procedures and principles of testing using social engineering methods.

Martin Leskovjan has held several cyber-related positions in his career, including Lead Auditor of Information Security Management, Senior Security Consultant at Actum Digital or KB specialist at the Faculty of Mechanical Engineering of the Czech Technical University. He co-founded and led the Czech team of Citadelo, a company focused on penetration testing and audits. He also co-founded Parallel Polis, an organization focused on crypto technology and its impact on society. His profession leads him to look for weaknesses in all systems, so he has also worked on cryptocurrencies, internet privacy, and antifragile structures such as anonymous crypto markets. Currently, he holds the post of Chief IT Security Officer at Penta Hospitals CZ.

10:45 Stopping Modern Cyberattacks in the AI Era *Peter Lechman & Jakub Jiříček (SentinelOne)*

Applied Cyber Security

As cyber threats become more sophisticated with the rise of AI, a new approach to defense is needed. Peter Lechman will discuss the evolution of security from antivirus to EDR and XDR, and finally, to SentinelOne's vision for comprehensive protection, through a unified, AI-powered SIEM. He will also outline the critical role of AI in modern products and services, discuss the risks of Shadow AI, and how one can secure enterprise users and their data when interacting with large language models.

Following the discussion, Jakub will bring that vision to life with a live demonstration - and walk you through a detailed analysis of the Scattered Spider group and their successful attacks on companies like MGM. He will show you firsthand how today's cyber products like SentinelOne's Singularity Platform provide enterprises with the visibility to detect and stop these attacks, and how users can leverage capabilities like Purple AI to perform powerful, natural-language threat hunting to proactively secure their organization.

Peter Lechman has over 20 years of experience in the information and communication technology (ICT) sector. He began his career at Cisco, where he spent seven years in various sales positions, managing key accounts across the Czech Republic. In 2014, he became the first representative for Palo Alto Networks in Eastern Europe. During his tenure, he successfully built and led a sales team in the region, and in his last three years, he contributed to the development of sales channels in Eastern Europe, Turkey, and the Commonwealth of Independent States (CIS) region. Since September 2022, he has served as the Regional Sales Director for Eastern Europe at SentinelOne, with the goal of strengthening the company's position as a leader in endpoint security.

Jakub Jiříček is an experienced professional in IT and cybersecurity with over 25 years of experience. Throughout his career, he has gained valuable expertise as a systems engineer, technical sales specialist, and consultant. He has participated in numerous significant security projects for both corporate and government entities. He has worked for companies such as Symantec and Palo Alto Networks. Currently, he serves as the Lead Solutions Engineer for SentinelOne in the Eastern Europe region. Jakub holds a degree in Computer Science and Networks from the Czech Technical University in Prague (ČVUT FEL).



12:00 **Diverse Palette of Opportunities in Cyber**

Václav Kotyk & Ana Friesen (SentinelOne)

Applied Cyber Security

Let's move beyond general titles to explore the distinct specializations within the cybersecurity field! Speakers Ana Friesen and Vaclav Kotyk from SentinelOne's Talent Acquisition team will outline the essential skills and mindsets required for success in areas like: threat research & detection, SecOps & MDR, red teaming, internal infosec or developing cybersecurity SW products. This session is designed to provide a clear overview of the diverse landscape of cyber careers, and enable attendees to strategically prepare for their future in the industry.

Ana Friesen is the leader of Sentinelone's Technical Talent Acquisition team. With a decade of experience in Recruiting, she has been a foundational part of the company's success in the region, helping it grow from just a handful of people to almost 400 employees today. As employee number two at SentinelOne's Czech site, she has been a key player in the company's growth.

Václav Kotyk has dedicated the past 10 years to headhunting and building talent communities at Société Générale, and currently SentinelOne. Fueled by his passion for the security field, gained through cyber podcasts or hiring cyber talent across EMEA, he has kicked off local research community meetups "CyBeer" and participates in organizing Security BSides Prague conference.

12:30 **Lunch break**

13:30 **Cyber Diplomacy & Capacity Building: A National Agency's Perspective**

Tomáš Procházka (National Cyber and Information Security Agency)

Cyber Diplomacy & Geopolitics

This lecture provides a comprehensive overview of international cooperation from the perspective of a national cyber agency. It examines how government institutions engage with foreign partners to address emerging threats in cyberspace and to build resilient infrastructures. Drawing on real-world case studies, the lecture delves into two key areas: cyber diplomacy, including trust building, and policy coordination; and cyber capacity building, focusing on training, technical assistance, and institutional development in partner countries. Participants will gain insights into the practical challenges and benefits of working with international counterparts and discover how these partnerships enhance national security and improve collective cyber resilience.

Tomáš Procházka leads the Bilateral Cooperation Unit at the National Cyber and Information Security Agency, where he focuses on cyber diplomacy and capacity building. In his previous role as a desk officer, he managed relations with the United States, the United Kingdom, and Canada, as well as capacity-building projects with countries across Latin America, Africa, and the Middle East.



15:15 **Cyber Partnerships from the International Frontline**

Cyber Diplomacy & Geopolitics

Veronika Kolek Netolická (Cyber Attachée in Canberra, National Cyber and Information Security Agency)

Veronika serves as the Cyber Attachée for the Indo-Pacific at the National Cyber and Information Security Agency. Previously, she was the Head of the National Strategy and Policy Unit, where she led the development of the current National Cyber Security Strategy and initiatives on supply chain security. She holds a master's degree in Security and Strategic Studies from Masaryk University in the Czech Republic, where she is also pursuing her Ph.D. with a focus on cybersecurity threats and risks. In 2018, she completed a long-term research stay at Ho Chi Minh University of Technology in Vietnam. Additionally, Veronika is an alumnus of the Program on Cybersecurity Studies at the George C. Marshall Centre in Germany and graduated from the Young Leaders Program at the National Graduate Institute for Policy Studies in Japan with a master's in Public Policy in 2021.

THURSDAY, SEPTEMBER 25TH

09:00 **Russian Capabilities in Cyberspace and War in Ukraine: Impacts and Implications**

Cyber Diplomacy & Geopolitics

Michael Myklín (National Cyber and Information Security Agency)

The Russian Federation is among the states with the most advanced offensive capabilities in cyberspace. Until the start of the war in Ukraine, these capabilities were generally used for cyber espionage and occasional experiments in cyber sabotage. This modus operandi changed with the start of the war, particularly in the application of wartime cyber attacks. This lecture will focus on the summary of Russian capabilities, analysis of their application during the conflict, and the implications for NATO and EU states.

Michael Myklín is the director of the Central Analytics Department at the National Cyber and Information Security Agency (NÚKIB) of the Czech Republic. The department is responsible for crafting analytical materials about cyber attacks and trends in cyber security for decision-makers and Czech and foreign administrative bodies.

10:45 **Usage of AI in Influence Operations**

Cyber Diplomacy & Geopolitics

Jindřich Karásek (Rapid7)

This lecture focuses on the use of artificial intelligence (AI) in influence operations. It explores how AI can be used to optimize influence operation strategies in the realms of politics, economics, and public opinion. The presentation will focus on specific examples and techniques that allow for better understanding and influencing target audiences.

Jindřich Karásek is Lead security researcher at Rapid7. His research work focuses on cognitive warfare, cyber espionage and cyber threats or intelligence. He is also a security data scientist, known as a 4n6strider.



12:30 Lunch break

13:30 Strategic Cyber Security Exercise (double session)

Markus Münzer & Lauri Almann (RiskSight)

Applied Cyber Security

During this exercise, participants will address a scenario of a gradually escalating international crisis in cyberspace. They will be able to put into practice their theoretical knowledge acquired in the previous days of the Cyber Security Academy. The exercise will be led by Markus Münzer as the main moderator and Lauri Almann as the co-moderator. No technical knowledge is required for this type of exercise.

18:00 Reception at the British Embassy

Location: **Thunovská 180/14, Praha 1**

Dresscode: **Business**

FRIDAY, SEPTEMBER 26TH

10:45 The Deaf Spy: How Intelligence Adapts When It Can No Longer Listen

Petr Vancl Hochberger (Tovek)

Cyber Threat Landscape

SIGINT, the long-reigning queen of intelligence disciplines, is gradually fading, and OSINT is unexpectedly taking its place. We are witnessing the most significant change in a traditional intelligence discipline since the global adoption of mobile phones. In this lecture, we will look at what this change means in practice. We will discuss the role NATO plays in the world of intelligence, where its limits are, and why countries must ultimately rely on themselves. We will explain why SIGINT has changed and how OSINT helps in the newly created "silence." Using practical examples, we will show why phone numbers are one of the most important identifiers, yet we barely protect them at all. We will examine how this and other personal data are traded on the "grey" data market and what real consequences this has not only for the security of companies but for all of Europe.

Petr Vancl Hochberger began his career in Military Intelligence, where he worked his way up to the position of Deputy Chief of the Special Analysis Department. Here, he focused on the Big Data analysis of multilingual sources with a special emphasis on Chinese and was one of the first to integrate OSINT into certain intelligence processes. He later served at NATO Headquarters as Chief of the Intelligence Section and advisor to the Supreme Allied Commander Europe (SACEUR) for Signals Intelligence (SIGINT). Currently, he leads marketing and business development at TOVEK, where he leverages his experience in data analysis and OSINT in the commercial sector.

12:30 Final evaluation & Certificate Ceremony

13:30 Conclusion & Farewell



CYBER SECURITY ACADEMY
22-26 SEPTEMBER 2025
KAROLINSKÁ 707/7, PRAGUE 8-KARLÍN



Prague Security
Studies Institute