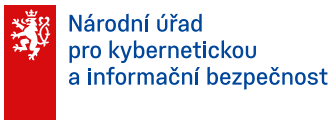
CYBER SECURITY ACADEMY
21–25 SEPTEMBER 2026
KAROLINSKÁ 707/7, PRAGUE 8-KARLÍN

Prague Security Studies Institute

UNDER THE AUSPICES OF



MAIN PARTNERS

2026 CYBER SECURITY ACADEMY

Dear Participants, it is our pleasure to welcome you to the 9th edition of PSSI's Cyber Security Academy.

We hope you enjoy the days ahead — from the lectures and discussions with our distinguished speakers to the opportunity to meet and connect with fellow participants, both during the Academy and at the Thursday reception. We hope you will also be able to explore Prague and its many charming spots.

Should you have any questions or concerns, please reach out to the Program Manager.

PRACTICAL INFORMATION

Dress code Smart Casual; with an exception of the Thursday reception at the British Embassy, which calls for Business Formal.

Venue The Academy will take place at the SentinelOne premises, in the Missouri Park complex (Karolinská 707/7, Prague 8-Karlín). We kindly ask all participants to respect the workplace environment and behave appropriately.

Themes Lectures and workshops are organised around four thematic pillars – one will be covered each day. You may look forward to Cyber Basics & Diplomacy; Tools, Techniques & Operations; Era of AI; and Cyber Threat Landscape. The program is complemented by a hands-on simulation of an international cyber crisis on Friday.

Format All lectures are held under the *Chatham House Rule* – participants are free to use the information received, but may not disclose the identity or affiliation of any speaker or participant.

Refreshments Coffee breaks will include beverages and light snacks. Lunch is not provided, but participants are welcome to explore the nearby dining options, bring their own food to heat on the premises, or order delivery.

Feedback After the final lecture on Friday, all participants will be asked to complete an anonymous evaluation form. Your honest feedback will help us improve future editions of the Academy and enhance the participant experience. Certificates of completion will be distributed afterwards.

Notice Photos and videos will be taken during the Academy for promotional purposes.

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.

PROGRAM SCHEDULE

MONDAY, SEPTEMBER 21ST

08:30 Meet-up

08:55 Opening Remarks (*Tomáš Procházka)*

09:00 Introduction to the Cybersecurity Domain (*Jonáš Papoušek)*

10:45 Building Cyber Resilience Through International Cooperation *(Vladěna Sasková)*

12:15 Lunch Break

13:45 Russian Capabilities in Cyberspace and War in Ukraine: Impacts & Implications *(Michael Myklín)*

15:30 Ice-Breaking Non-Pub Pub Quiz

TUESDAY, SEPTEMBER 22ND

09:00 The Deaf Spy: How Intelligence Adapts When It Can No Longer Listen *(Petr Vancl Hochberger)*

10:45 The Edge of Tomorrow – Technologies Rewriting Warfare Thinking *(Tereza Toufarová)*

12:15 Lunch Break

13:45 OSINT Essentials – from Theory to Practice *(92nd Cyber Warfare Group)*

15:30 OSINT Workshop *(92nd Cyber Warfare Group)*

WEDNESDAY, SEPTEMBER 23RD

09:00 Cyber Threats and Financial Crime: Using AI to Prevent and Uncover Illicit Financial Flows *(Lucie Novotná)*

10:45 Endpoint – the AI agent That Never Sleeps *(Lukáš Ciasnoha & Jakub Jiříček)*

12:15 Lunch Break

13:45 Diverse Palette of Opportunities in Cyber *(Václav Kotyk & Silvia Kusá)*

15:00 Usage of AI in Influence Operations *(Jindřich Karásek)*

THURSDAY, SEPTEMBER 24TH

09:00 Anatomy of an Intrusion: How Offensive Operations Actually Work *(Markéta Petrtýlová)*

10:45 Hacking as a Profession *(Martin Leskovjan)*

12:15 Lunch Break

14:00 The CISO-less Future: When Security Runs Itself *(Martin Leskovjan)*

18:00 Reception at the British Embassy

FRIDAY, SEPTEMBER 25TH

09:00 Double Session: Strategic Cyber Security Exercise *(Markus Münzer & Lauri Almann)*

12:30 Final Evaluation & Certificate Ceremony

13:30 Conclusion & Farewell

MONDAY, SEPTEMBER 21ST

Cyber Basics & Diplomacy

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

08:55 **Opening Remarks**
Tomáš Procházka *(PSSI Alumnus; Cyber Attachée in Washington, D.C., National Cyber and Information Security Agency)*

09:00 **Introduction to the Cybersecurity Domain**
Jonáš Papoušek *(NÚKIB – National Cyber and Information Security Agency)*

The presentation introduces the audience to cybersecurity. It explains key concepts, the characteristics of cyberspace, the main types of threats, and the actors behind them. Using examples, it illustrates the impact of both intentional and unintentional system disruptions. It also distinguishes between cybersecurity, cyber defence, and cybercrime. The final section presents the role of the state, the Czech institutional framework, the National Cybersecurity Strategy, and NÚKIB's role as the coordinating, regulatory, and expert authority.

Jonáš Papoušek is a Legal Advisor to the Governmental CERT at the National Cyber and Information Security Agency of the Czech Republic (NÚKIB). In his work, he focuses on the legal aspects of cyber incident and vulnerability handling, coordinated vulnerability disclosure (CVD), and ethical hacking. He is also involved in designing and developing the legal and procedural frameworks that support the operation of the national CERT. His areas of expertise include cybersecurity law, criminal law, and public international law.

10:45 **Building Cyber Resilience Through International Cooperation**
Vladěna Sasková *(NÚKIB – National Cyber and Information Security Agency)*

Today, more than ever, international cooperation in cybersecurity is essential for ensuring the stable provision of essential services and strengthening the security and resilience of both the state and society. This lecture provides a comprehensive overview of international cooperation from the perspective of a national cybersecurity agency. It focuses on the main areas of cooperation, the identification of key partners and the benefits of working with them, as well as the practical challenges and outcomes of coordination with international counterparts. Participants will understand why international cooperation matters and what benefits it brings in terms of national security and collective resilience.

Vladěna Sasková leads the Department of International Cooperation and the European Union at NÚKIB, where she and her colleagues coordinate cooperation with foreign partners from around the world. Focusing on the EU and NATO, as well as on bilateral partnerships with like-minded countries, she ensures that NÚKIB is respected worldwide, consulted on various cybersecurity topics, and contributes its expertise wherever relevant.

12:15 **Lunch Break**

13:45 **Russian Capabilities in Cyberspace and War in Ukraine: Impacts & Implications**
Michael Myklín *(NÚKIB – 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.

15:30 **Ice-breaking Non-Pub Pub Quiz**

TUESDAY, SEPTEMBER 22ND

Tools, Techniques, & Operations

09:00 **The Deaf Spy: How Intelligence Adapts When It Can No Longer Listen**
Petr Vancl Hochberger *(Defence & Intelligence Consultant)*

How does intelligence really work inside NATO? We will start by looking at how intelligence is collected and shared within the Alliance and challenge several common myths about what NATO can and cannot do. We will then look mainly at SIGINT. Why it has been so important for decades and how new technologies, encryption and changing communication habits have reduced some of its traditional capabilities. Through several practical examples, the speaker will show how OSINT and data from commercial providers can help fill some of these gaps. The lecture will also show why modern intelligence is becoming less about separate intelligence disciplines and more about combining different types of data.

Petr Vancl Hochberger is a Defence & Intelligence Consultant with more than 14 years of experience in intelligence, data and technology. He began his career in Military Intelligence, where he later became Deputy Chief of the Special Analysis Department. He also served at NATO Headquarters as Chief of the Intelligence Section and as an adviser to SACEUR on SIGINT. After leaving the military four years ago, he moved into the private sector, where he has held senior roles in technology companies and led data strategy in a multinational corporation. His work today focuses on intelligence, data analytics, technology and the practical use of complex data for decision-making.

10:45 **The Edge of Tomorrow – Technologies Rewriting Warfare Thinking**
Tereza Toufarová *(Czech Armed Forces)*

This lecture will explore how technologies that are increasingly ubiquitous in our everyday lives can be harnessed for warfare and military operations. It will examine how the current technological and societal landscape is transforming not only capabilities on the battlefield, but also the way military operations are planned, approached, and understood.

1st Lt. Ing et BcA. Tereza Toufarová is a professional soldier, a member of the 92nd Cyber Warfare Group of the Information and Cyber Forces, where she serves as Commander of the Development Centre. She joined the army after nine years of experience in the development of control software and avionics for the American company Honeywell, where, among other things, she was involved in the certification of aircraft systems and worked for many years as a project engineer. In her personal time, she manages a choir and the Czech branch of the Society of Women Engineers, with which she organizes the SHE Award competition for female students of technical universities, and is interested in other activities supporting women in technical fields, such as the Women4Cyber initiative in Czechia.

12:15 **Lunch break**

13:45 **OSINT Essentials – from Theory to Practice**
92nd Cyber Warfare Group *(Czech Armed Forces)*

The lecture 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.

15:30 **OSINT Workshop**
92nd Cyber Warfare Group *(Czech Armed Forces)*

WEDNESDAY, SEPTEMBER 23RD

Era of AI

09:00 Cyber Threats and Financial Crime: Using AI to Prevent and Uncover Illicit Financial Flows
Lucie 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 – 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 and the most prominent trends, 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.

Lucie is the Head of the Solutions team and a technical Product Manager for a Transaction Monitoring product at Resistant AI. She is responsible for finding the best ways to leverage AI for AML and anti-fraud purposes. Lucie has over 10 years of experience with anti-financial crime (AFC) and financial regulation. In her role at Resistant AI, she combines her previous experience as a compliance officer, as an AFC policy advisor to the public sector, and as a financial crime lead on an AML & fraud tech solution. She holds a master's in International Security from SciencesPo Paris with a focus on nuclear proliferation and international law, and a bachelor's in Political Science from the London School of Economics. Lucie speaks fluent Czech, Italian, and Russian.

10:45 Endpoint – the AI agent That Never Sleeps
Lukáš Ciasnoha & Jakub Jiříček *(SentinelOne)*

AI is no longer on the security roadmap – it is already in every department, and attackers got there first. This session covers both halves of that problem. We open with what AI has actually changed for the adversary: agentic AI as a new attack surface, deepfake-grade social engineering, prompt injection, data and model poisoning, and the shadow AI quietly leaking company data. We then trace how AI compresses every stage of the attack lifecycle, from initial access to weaponization and evasion, with real examples from this year's threat research. The second half turns to the defense: how machine-learning detection at the endpoint still decides most outcomes, which capabilities are worth demanding from any vendor, what agentic investigation looks like when Purple AI works an alert end to end in minutes instead of hours, and how Prompt Security governs the AI your own people and applications already use. Technical, vendor-specific where it matters, and grounded in what actually shipped.

Following the presentation, we'll hold a live threat-hunting challenge "Mortal vs. Machine" in which a seasoned human threat hunter (the "Mortal") goes head-to-head against a CSA student with no prior security background (the "Machine"), armed only with SentinelOne's Purple AI. Both sides will be given the same real-time incident response and detection scenario and race to investigate, hunt down indicators of compromise, and reach the right call. The exercise will offer students a hands-on introduction to working with an AI assistant in a live

security context, while showcasing how far novice-plus-AI can go against deep human expertise - no prior experience with the platform required.

Lukáš Ciasnoha is a cybersecurity specialist with over 12 years of hands-on experience in incident response, digital forensics, and SOC operations. His work centers on coordinating decisive action during active incidents, reconstructing attacker activity through digital forensics, and building effective detection workflows for security operations centers. He also brings expertise in threat hunting, malware analysis, and security consulting, translating technical risk into practical next steps for organizations. Since February 2026, Lukáš has been a crucial part of SentinelOne's Wayfinder Threat Detection & Response organization, leading MDR teams in Czechia and Poland. He holds multiple GIAC certifications.

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.

12:15 Lunch break

13:45 Diverse Palette of Opportunities in Cyber
Václav Kotyk & Silvia Kusá *(SentinelOne)*

Let's move beyond general titles to explore the distinct specializations within the cybersecurity field! Speakers Silvia Kusá 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, in the ever-changing AI era, and enable attendees to strategically prepare for their future in the industry.

Václav Kotyk has dedicated the past 11 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.

Silvia Kusá is a Senior Full Stack Technical Recruiter with 10 years of experience in talent acquisition, specializing in sourcing and hiring technical talent across the cybersecurity and technology sectors. She has built her career supporting engineering and technical teams in startups, scale-ups. Currently leads full-cycle technical recruiting at SentinelOne, where she has been based in Prague since February 2024. She is an active member of the Czech cybersecurity community, regularly attending and supporting events such as Security BSides Prague and Women in Cyber. Silvia holds a degree from the University of Economics in Bratislava.

15:00 Usage of AI in Influence Operations
Jindřich Karásek *(Rapid7)*

This lecture focuses on the use of artificial intelligence 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.

THURSDAY, SEPTEMBER 24TH

Cyber Threat Landscape

09:00 Anatomy of an Intrusion: How Offensive Operations Actually Work
Markéta Petrtýlová *(MSD Czech Republic)*

The lecture follows a realistic intrusion from the first reconnaissance to the moment the attacker's objective is reached, and explains why such operations keep succeeding. It introduces who conducts offensive operations today, and what artificial intelligence has genuinely changed for attackers and defenders. A case study of a deepfake-enabled executive fraud closes the practical part.

Markéta Petrtýlová is an Attack Automation Engineer at MSD, focused on advancing cybersecurity through automation, cloud security, and AI security research. Her work centers on developing attack automation capabilities, conducting threat research, and exploring the security implications of rapidly evolving AI technologies. With a background in both DevOps and cloud security, she brings experience from global organizations including MSD, IBM, and Microsoft. Markéta holds both a Bachelor's and a Master's degree from the Faculty of Information Technology at the Czech Technical University in Prague.

10:45 Hacking as a Profession
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.

12:15 **Lunch break**

14:00 **The CISO-less Future: When Security Runs Itself**
Martin Leskovjan *(Penta Hospitals CZ)*

The lecture will present a vision of a fully autonomous ISMS, in which automation and AI ensure the complete execution of security measures, analyze risks, respond to incidents, and remediate vulnerabilities they discover themselves. It will explore the technological and process prerequisites an organization must meet to transition from "manually" managed security to security driven by data, automation, and artificial intelligence. We will discuss the foundations on which a healthy (and therefore automatically manageable) ISMS must be built, and why the biggest obstacle is not technology, but the organization itself and the way it is struc-tured and managed. We will also look at how professionals interested in pursuing a career in IT security in the AI era should develop their skills so that their roles are not ultimately taken over by autonomous security management.

18:00 **Reception at the British Embassy**

Location: **180/14 Thunovská, Prague 1-Malá Strana**
Dresscode: **Business Formal**

FRIDAY, SEPTEMBER 25TH

09:00 **Strategic Cyber Security Exercise (Double Session)**
Markus Münzer & Lauri Almann *(RiskSight)*

During this exercise, participants will address a scenario of a gradually escalating international crisis in cyberspace. Topics such as situation assessments, stakeholder communication and large-scale business decisions will be tackled. Participants 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 Lauri Almann and Markus Ilmar Münzer. No technical knowledge is required for this type of exercise. The exercise is going to take place on the strategic cybersecurity exercise platform STRATEX.

Markus Ilmar Münzer is the Chief Executive Officer of RiskSight, a cybersecurity trainings and exercises company, delivering cyber awareness trainings and operational to policy level cyber exercises internationally to customers in the government, defence, critical infrastructure, private and academic sectors. Person-

ally, Markus fronts the cyber exercises business line of RiskSight, having participated in the design, development execution and analysis of more than 75 exercises, where he has delivered projects in Europe, Asia, Africa and Latin-America, including for NATO CCDCoE, European Defence Agency, Microsoft US and EU, International Committee of the Red Cross. He is a long-standing member of the EU Cyber Net Expert Pool. Markus holds a bachelor's degree in Business IT from TalTech, Estonia as well as a Chief Information Security Officer and Information Security Auditor certificate from the IT-Academy, governed by TalTech.

Lauri Almann is Co-Founder and Chairman of the Supervisory Board of CybExer Technologies, a deep-tech AI assurance and cyber-range company providing high-fidelity digital twins for testing and training in 40+ countries, including defense, banking and critical infrastructure. An international speaker, he has managed and contributed to major cyber exercises for EU Presidencies, NATO, EDA, NATO CCDCoE, financial institutions and sovereign customers.

From 2004–2008, he was Permanent Secretary of Estonia's Ministry of Defence, overseeing its management. In that capacity, he co-founded the NATO CCDCoE, led defense innovation initiatives including Estonia's first drone program SWAN, and oversaw major air defence, surveillance, armored vehicle, artillery and infrastructure programs, such as the NATO HNS airfield in Ämari. He previously served as Legal Adviser and Special Adviser to the Defence Minister, advised on procurement and intelligence reform, participated in Estonia's NATO accession talks, and served as a diplomat in Brussels, St. Petersburg and Kyiv.

He helped draft key defence legislation, oversaw drafting of Estonia's first Cyber Security Strategy, and coordinated the Ministry's response to the 2007 cyberattacks, . Since 2022, he has served on the Executive Board of the Estonian Association of ICT, responsible for cybersecurity; since 2023, on Estonia's AI Council. He holds a distinction-level LL.M. from Georgetown University as a Fulbright Scholar and is admitted to the New York State Bar.

12:30 Final Evaluation & Certificate Ceremony

13:30 Conclusion & Farewell

CYBER SECURITY ACADEMY
21–25 SEPTEMBER 2026
KAROLINSKÁ 707/7, PRAGUE 8-KARLÍN

Prague Security
Studies Institute