CYBER SECURITY ACADEMY

23—27 SEPTEMBER 2024 / ČSOB
RADLICKÁ 333/150, PRAHA 5

Prague Security Studies Institute

In cooperation with

National Cyber and Information Security Agency NÚKIB

Main partners

British Embassy Prague

ČSOB

risksight

GENERAL INFORMATION

Dress code: Smart Casual

Location: As we will always have to be accompanied to the building, it is necessary to be on time. The meeting point is by the Chestnut statue, right in front of the Radlická (metro line B) station exit!

CSA 2024 format: All of our lectures are governed by Chatham House rules, which means that participants can use the information they receive, but will not reveal from whom they received it.

Meals: Coffee, tea and snacks will be available on site. Lunch is not provided. It is possible to use the La Fresca restaurant, which is located on the CSOB premises – card payment is preferred to ensure faster check-in. The premises also offer the option of heating your own food, or ordering food to be delivered according to your own preference.

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

MONDAY, SEPTEMBER 23RD, 2024

08:20 **Meet at the meeting point next to the statue in front of B-line metro station Radlická**

08:45–09:00 **Opening remarks by Robert Smith, British Embassy in Prague**

09:00–10:30 **Introduction to the Cybersecurity Domain**
Jonáš Papoušek
(National Cyber and Information Security Agency)

The lecture will focus on the definition of basic concepts in the field of cybersecurity (cyberspace, cybercrime, vulnerabilities, threats and incidents), the national strategy of cybersecurity, and the role of the state in the cybersecurity domain.

Jonáš Papoušek works as a legal advisor of the Governmental CERT (Computer Emergency Response Team) in the Czech Republic's National Cyber & Information Security Agency, where he focuses on ransomware threats and legal aspects of ethical hacking. He specializes in various legal areas such as law of cybersecurity, criminal law and international public law. In 2017 he received his master's degree in Law at Masaryk University in the Czech Republic with a focus on procedural aspects of criminal law. In 2016–2018 he worked in the legal department specializing on church restitutions. In the years 2018–2022, he worked as an assistant to the judge designated for criminal proceedings at the Municipal court in Brno.

10:45–12:15 **Cybersecurity in the Avionics Industry**
Tereza Toufarová
(Cyber Forces Command)

The lecture provides a brief summary of the principles of avionics development, an introduction to the principles of certification standards and safety requirements. It focuses on the specifics of cyber security as applied in avionics development and required by certification authorities. In the course of the lecture, you will learn, among other things, a brief history of the integration of cyber security principles into the processes used in aircraft certification, as well as recent development news.

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.

12:30–13:45 **Lunch break**

14:00–15:30 **Digital Identity**
Jiří Bulan
(RaulWalter CZ)

Formerly paper, now computers. But how can identity be trusted in the age of the internet? How do you verify that you are who you say you are? Jiří Bulan will explain how digital signatures, passports and chip ID cards work. He will focus on the example of Estonia, where they work with digital identity on a daily basis. Thanks to this work, Estonia is leading digital governance; Estonian citizens can even vote online in democratic elections.

Jiří Bulan is an independent consultant in the field of RFID, digital identity, cryptography and smart cards. Jiri has integrated technological solutions for biometric passports and a variety of eID cards produced in the United Kingdom, Ireland, Sweden, Lebanon or Jordan. He worked for the Czech state services before starting a digital identity business.

15:45–17:15 **Armed Crisis as a Catalyst for Technological Development**
Tereza Toufarová
(Cyber Forces Command)

This lecture was created to explain and depict the field of defense technology from a slightly contemplative and more humanistic perspective at the request of Charles University as part of the course 'Crisis as Opportunity.' It is a reflection on connections that are familiar but not necessarily obvious: an analysis of the correlation between armed conflict and human invention and progress throughout history. The lecture concludes with a look at current technological and warfare developments.

TUESDAY, SEPTEMBER 24TH, 2024

09:00–10:30 **Information Warfare in Cyberspace**
Adrián Szabó
(Cyber Forces Command)

This lecture will outline the history, terminology and current trends in information warfare in cyberspace, with specific examples from recent years.

Adrian Szabó is a specialist serving in the 92nd group of Cybernetic Warfare. His background is in linguistics and international development, focusing on the transition processes of various systems of government. Adrian is stationed in the Center of information warfare in cyberspace, which 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 the enemy's information influence in cyberspace, and planning and implementing active countermeasures.

10:45–12:15 **Open Source Intelligence Workshop**
Adrián Szabó
(Cyber Forces Command)

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!

12:30–13:30 **Lunch break**

14:00–15:30 **Usage of the AI in Influence Operations**
Jindřich Karásek
(Trend Micro)

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 a senior cyber threat researcher at Trend Micro. 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.

15:45–17:15 **Military Implications in Cyberspace**
Jakub Fučík
(Cyber Forces Command)

The development of communication and information technologies leads not only to new possibilities and opportunities to improve the well-being of society, but also to dependence on these technologies. From a strategic perspective, cyberspace represents a new dimension where state and non-state actors compete with each other to promote their own interests – often at the expense of others. From this perspective, malicious cyber activities represent new threats (and tools) that have a negative impact not only in the digital domain but also in physical dimensions. Cyber defense and cyber security are thus becoming an integral part of public and private interests. This presentation will focus on the military implications of cyberspace and their impact on the nature of contemporary armed conflicts.

Kpt. Mgr. et Mgr. Jakub Fučík Ph.D. studied international relations and law. He worked as an academic at the Centre for Security and Military Strategic Studies at the University of Defence and as a secretary of the professional journal Defence and Strategy. Since 2021, he has been a member of the Army as a senior officer of the Planning Division of the Cyber Forces and Information Operations Command Staff. He completed a foreign course "International Law of Military Operations" at the Defense Institute of International Legal Studies and a research internship at the NATO Defence College. He is active in System Analysis and Studies/NATO Science & Technology Organization panels and workshops and represents the Czech Republic in European Defence Agency Captech "Information."

WEDNESDAY, SEPTEMBER 25TH, 2024

09:00–10:30 **Cyber Attacks in the Banking Industry**
Milan Zrcek
(ČSOB)

The lecture will focus on cyber attacks through all possible digital channels, which will be illustrated by individual examples. A large portion of the presentation will be devoted to current tactics of fraudsters such as "phishing" sites or various applications. These examples will be discussed in detail so that participants can defend themselves in the future and understand the methods of these scammers.

Milan Zrcek is an experienced expert in the field of information security, where he focuses on devising IT security strategy, coordinating cyber security and control programs, risk assessment and implementation of Data Loss Prevention solutions. He previously worked as a consultant and information systems auditor at PwC. He graduated with a degree in Information Management from the University of Economics in Prague.

10:45–12:15 **Role of Cyber Activism in the Cyber Warfare of the 21st Century**
Adéla Klečková
(PRINCEPS)

Heroic guerilla elves taking down hordes of dark trolls in an ideological conflict over the future of humanity? This is no fantasy novel but the beginning of a talk about the "cyber elves" – a group of cyber activists fighting against propaganda, disinformation campaigns and internet trolls. This is a story of the growing importance of individuals in 21st century conflicts. This is a story about bravery and hope that can shine through the darkest corners of the cyber underworld.

Adéla Klečková is a Senior Cyber Risks Fellow at PRINCEPS Institute, TEDx Speaker, CIDOB 35 under 35 young tech leaders, and was featured in Forbes NEXT. She focuses on conflicts in cyber space and the role of non-state actors. She was the first analyst to introduce the movement of the cyber elves to the Czech expert community. Adéla is a recipient of the ReThink.CEE Fellowship with the German Marshall Fund, which she was the first woman from the Czech Republic to receive. She is also a member of the Digital Sherlocks Network founded by the Atlantic Council, specializing in advanced methods of open source investigation. Adéla graduated summa cum laude from the War Studies Department at King's College London.

12:30–13:30 **Lunch break**

14:00–15:30 **Europe Fit for Digital Age: EU's Role in Digital Diplomacy at Global Stage**
Eva Dokoupilová
(Ministry of Foreign Affairs)

Digital technologies have brought new opportunities into the lives of people around the world. However, their fast development can bring about challenges if they are not developed securely and in line with specific standards. EU's role in digital diplomacy at multilateral, regional and bilateral level is also ever increasing, with the aim for the EU to become a key actor in global digital discussions alongside tech giants such as US and China, as well as land a strong role in this area of foreign policy in the current dynamic geopolitical context. The work towards these goals is also ongoing internally within the EU, with the Member States and EU institutions such as the EEAS and Commission, having to face an urgent decision on how to strengthen EU's influence in global digital matters.

During her studies at Masaryk University in Brno, where she studied International Relations, Eva was a trainee at Czech MFA, Office of the Government, Czech mission to OSCE, as well as an EUDEL Trainee in OSCE. Right after finishing her Master's degree, she joined the Czech diplomatic service where she became a national expert on cyber and digital diplomacy in EU and OSCE, including during the CZ PRES of Council of the EU. In the last year, she was seconded to the EEAS where she was responsible for multilateral digital files with particular focus on negotiations of UN Global Digital Compact. Currently she is a Digital Diplomacy Coordinator at Czech MFA responsible for EU digital diplomacy within Czechia and externally. Apart from digital and cyber diplomacy, she worked on OSCE's political and security files with focus on UA conflict, on human rights and she is an active election observer.

15:45–17:15 **Building a Culture of Security Awareness**
Vladimíra Žáčková
(MSD Czech Republic)

Discover the significance of integrating cybersecurity into an organization's culture and how to empower employees to identify and address 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.

THURSDAY, SEPTEMBER 26TH, 2024

09:00–10:30 **Hacking as a Profession**
Martin Leskovjan
(Actum Digital)

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 is a Lead Auditor of Information Security Management and security consultant at Actum Digital, and is a KB specialist at the Faculty of Mechanical Engineering of CTU. 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.

10:45–12:15 **Borderless Domain Calls for Borderless Cooperation: When Cybersecurity Meets its International Needs**
Jakub Maděránek + Michaela Prucková
(National Cyber and Information Security Agency)

In an increasingly interconnected world, cybersecurity has become a global issue that transcends national borders, necessitating robust international cooperation. Organizations such as NATO and the EU have recognized this need, enhancing joint cyber defenses, sharing intelligence, and developing coordinated strategies, policies, and legal frameworks. The United Nations, along with other global fora, contributes to setting international norms and fostering collaboration among a diverse range of countries. Bilateral initiatives and cooperative projects, particularly with third countries, also play a pivotal role, ensuring that no nation is left vulnerable in a borderless digital domain. This collective effort is crucial in addressing sophisticated cyber threats that affect global security, economic stability, and democratic institutions.

Ms. Michaela Prucková is a legal and policy officer in the National Cyber and Information Security Agency (NÚKIB) of the Czech Republic, covering the international cybersecurity agenda of the North Atlantic Treaty Organization (NATO) and the European Union (EU). She has been part of the EU Cyber Resilience Act proposal negotiations, and focuses on various cyber security-related topics such as supply chain security, quantum security and 5G security. She co-leads the drafting of the EU ICT Supply Chain Security Toolbox, and coordinates the Cyber Defence Pledge on behalf of the Czech Republic.

Mr. Jakub Maděránek is a policy officer in the National Cyber and Information Security Agency (NÚKIB) of the Czech Republic, previously leading the Bilateral Cooperation

Unit and covering topics from Cyber Capacity Building (CCB) to cybersecurity agenda of other international fora such as the Organization for Security and Cooperation in Europe (OSCE).

12:30–13:30 **Lunch break**

14:00–15:30 **Russian Capabilities in Cyberspace and War in Ukraine: Impacts and Implications**
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 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.

15:45–17:15 **Cyber Threats and Financial Crime: Using AI to Prevent and Detect Financial Fraud and Money Laundering**
Lucie Novotná
(Resistant AI)

The first part of the session will cover the methodologies and approaches used by regulated financial institutions to prevent or detect financial crime. The session will outline the types of cyber attacks which lead to financial fraud, such as phishing.

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.

18:00–20:00 **Reception at the British Embassy**
180/14 Thunovská, Praha 1
Dress-code: Business casual

FRIDAY, SEPTEMBER 27TH, 2024

09:00–12:15 **Strategic Cyber Security Exercise**
Markus Münzer, Lauri Almann
(RiskSight)

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 main moderator and Lauri Almann as co-moderator. No technical knowledge is required for this type of exercise.

12:15–13:00 **Lunch break**

13:15–14:30 **Final Evaluation, Completion of the Online Questionnaire, Awarding of Certificates, Official Closing of the Academy**

CYBER SECURITY ACADEMY
23—27 SEPTEMBER 2024