

New Threats and Secure Communication

Prague, September 21–22, 2023
CEVRO Institute, Jungmannova 17, Prague

The Conference is organized by the Prague Center for Transatlantic Relations, CEVRO Institute under the auspices of the US Embassy in Prague and Vít Rakušan, The First Deputy Prime Minister of the Czech Republic and Minister of the Interior

The Russian aggression in Ukraine has dramatically changed the security situation in the world. Russia deliberately acts against stability in politics, the economy and society in democracies. China questions the international order. China and Russia coherently intend to weaken the influence and unity of the West. Confrontation and rivalry are gaining ground in the new spheres. The threat of confrontation has expanded to the cyber sphere and space. Economies, state administrations and ensuring citizens' security are increasingly dependent on critical information infrastructure. Our enemies subject our critical infrastructure in cyberspace to attacks, seize crucial and sensitive information, and endanger the stability and functioning of our strategic information and communication systems.

The conference will target new security threats to critical infrastructure in different fields with a particular focus on digital and telecommunications. We will discuss connectivity as an essential requirement for national security and vulnerability to disruptions of communication infrastructure. Following best practices, we will also examine the practical solutions based on government and private sector cooperation. The expert workshops on Friday, September 22, will dive deeper into secure high-capacity critical communications infrastructure and discuss its cybersecurity, public procurement or Dedicated Networks for First Responders, Public Protection and Disaster Relief (PPDR).

New Threats and Secure Communication

Prague, September 21–22, 2023

September 21

9:30

WELCOME REMARKS

by **Vít Rakušan**, *The First Deputy Prime Minister and Minister of the Interior, Czech Republic*
and **Bijan Sabet**, *US Ambassador to the Czech Republic*

9:50

KEYNOTE REMARKS

by **Mircea Geoaană**, *Deputy Secretary General, NATO (live stream)*

10:10

SPECIAL ADDRESS

by **Dita Charanzová**, *Vice President of the European Parliament*

10:25

PANEL 1: NEW SECURITY THREATS,

moderated by Daniel Koštoval, Senior Fellow, PCTR

In addition to “traditional” threats such as military aggression, thanks to the boom in new technologies and the revolution in communication technologies, new threats appear that, when used in a concentrated manner, can disrupt or even threaten the functionality of entire states and ensure the functioning of society. Moreover, some states like Russia and China are willing to use these technologies to achieve their political goals, and at the same time, it is not yet a clear crossing of the line between peace and war. Cyberspace is a typical example. In addition, the development of new technologies, such as quantum technology in IT and communication, means a significant threat to existing systems. Whoever adopts this first will be able to act effectively on an unprecedented scale and in a very short time.

Tomáš Pojar, *National Security Advisor, Czech Republic*

Peter Ptáček, *COO, ICZ, Czech Republic*

Lt Gen Karel Řehka, *Chief of the General Staff of the Armed Forces, Czech Republic*

11:35–11:50 COFFEE BREAK



CEVRO INSTITUTE
[school of political studies]



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



New Threats and Secure Communication

Prague, September 21–22, 2023

11:50 **PANEL 2: SECURITY THREATS AND CRITICAL INFRASTRUCTURE RESILIENCE**

moderated by Lucie Kadlecová, PWC Czech Republic/PRCP

New threats mean an entirely new quality of threat, especially for critical infrastructure. The scale and speed of infrastructure disruption can leave a state unable to act, let alone defend itself. Therefore, the robustness and endurance of critical infrastructure is a significant task for the future to preserve our ability to defend ourselves, i.e. to protect our sovereignty and independence.

Martin Durčák, Chairman of the Board of Directors, ČEPS a.s., Czech Republic

Lukáš Kintr, Director, The National Cyber and Information Security Agency, Czech Republic

Martin Schieffer, Head of Unit Counter-Terrorism, European Commission, DG HOME

13:00–14:00 **BUFFET LUNCH**

14:00 **PANEL 3: CONNECTIVITY AS AN ESSENTIAL REQUIREMENT FOR NATIONAL SECURITY**

moderated by Michal Wojnar, PWC Czech Republic

This panel aims to discuss connectivity's critical role in national security as the underlying layer for all essential critical functions. According to a study by RAND Corporation, if communication infrastructure is disrupted, it is one of the critical functions most likely to cause a cascade of failures since other functions depend on it for its operations. The panellists will discuss the dependence of critical functions on connectivity and how to mitigate the associated risks.

Col Radek Haratek, Commander of Information and Cyber Forces in the Czech Republic

Jorge Laurel, Chief, Enduring Security Framework, NSA Cybersecurity Collaboration Center, US

Joseph M. Wassel, CEO, FirstNet Authority, US

15:15–15:35 **COFFEE BREAK**

15:35 **PANEL 4: VULNERABILITY TO DISRUPTIONS OF COMMUNICATIONS INFRASTRUCTURE**

moderated by Jiří Kalemba, Prostor Radio

To protect critical communications infrastructure and withstand the demands of a new generation of critical functions, an increased focus on the network architecture and operational and security parameters of critical communications infrastructure is necessary. This needs to be supplemented by an increase in data capacities, using state-of-the-art technologies and enabling sharing by all government departments, dynamic capacity allocation, and setting robust security policies. If communications infrastructure is to be fully functional and protected, robust cyber protection and full physical and geographic redundancy are also necessary.

Pavel Hadrbolec, CFO, T-Mobile Czech Republic

Lori J. Smith, *fmr.* Area Vice President, Public Sector & FirstNet, AT&T

Juraj Šedivý, CEO, CETIN Group

17:00 **GLASS OF WINE**

New Threats and Secure Communication

Prague, September 21–22, 2023

September 22

Expert workshops moderated by **Bela Virag**, *Managing Partner, Head of Arthur D. Little Austria*

9:00

RESILIENT, SECURED COMMUNICATIONS INFRASTRUCTURE IN A MODERN FUNCTIONAL STATE

Jorge Laurel, *Chief, Enduring Security Framework, NSA Cybersecurity Collaboration Center*

David Lund, *BroadWay Coordinator, European Commission DG Home*

Soumen Ganguly, *Partner, Altman Solon (online)*

Lori J. Smith, *fmr. Area Vice President, Public Sector & FirstNet, AT&T*

Czech National Cyber and Information Security Agency Representative (tbc)

10:00

DEDICATED NETWORKS FOR FIRST RESPONDERS, PUBLIC PROTECTION AND DISASTER RELIEF (PPDR)

Max Brandt, *Policy Officer Critical Communication, European Commission, DG HOME*

Jeff Bratcher, *CTO FirstNet Authority, US*

Robert Sloan, *fmr. Chief Operating Officer, AT&T FirstNet, US (online)*

Bohdan Urban, *Ministry of the Interior of the Czech Republic*

11:00–11:20 COFFEE BREAK

11:20–12:30 PUBLIC PROCUREMENT OF COMMUNICATIONS INFRASTRUCTURE SERVICES

Michael Berkholtz, *Senior Manager, Technology Lifecycle Services,*

Office of Enterprise Technology Solutions, Information Technology Category (ITC)

in GSA's Federal Acquisition Service (online)

Jan Ďoubal, *National Agency for Communication and Information Technologies, Czech Republic*

Nicholas West, *Acting Director, Office of GSA Acquisition Policy,*

Integrity & Workforce, Office of Government-wide Policy (online)