Report: Countering Fake News and Protecting Cyber Space

ELF Project: Liberals Fighting Disinformation
Venue: Prague, Czech Republic
Date: 15th – 16th November 2018
Organizer: Adéla Klečková, Friedrich Naumann Foundation Pragu
Participants: See Attached

Business Breakfast:

Cyber and information security is one of the major challenges faced by states and companies at the time of the expansion of information and communication technologies. This issue was dedicated to the working breakfast organized by the European Liberal Forum on 15 November 2018, in cooperation with the Institute for Politics and Society and the Friedrich Naumann Foundation. GLOBSEC expert expert Katarína Klingová and CyberGym Europe security analyst Jan Sharadin presented the speech as speakers. The discussion was moderated by analyst of the Institute for Politics and Society Roman Máca.

In the area of cyber-security and information security, a number of shortcomings appear in both states. "The Slovak Republic, as compared to the Czech Republic, lacks a national security audit that would point to safety gaps." Katarína Klingová said. She also added that the current legislation, which was created for cyber security in Slovakia, only transposes EU standards. Therefore, they do not have a sufficient level for the public-private cooperation factor or a greater emphasis on transparency issues.

Jan Šaradin considers the low level of awareness and deficiencies in internal communication, among others, for entities operating critical and important information infrastructures as a major problem. "There is no obligation for penetration testing in the Czech Republic and there is also no standardization in the protection of infrastructure in response to threats. The nature of the attackers has changed, relying solely on the software is not enough. "Says Šaradin. In this context, the recent cyber attacks on foreign affairs in the Czech and Slovak Republics were also discussed. Jan Šaradin pointed out that it is very challenging to find the attackers after a long time and that the attention should therefore be drawn to the recognition of the techniques and methods of the attacks. The establishment of Security operation and Cyber Defense Centers in a multinational corporations environment as well as the emergence of specialized cyber security professions in universities is considered a positive trend.

Discussion also focused on information security and the fight against misinformation disseminated in the Internet environment. Katarína Klingová pointed to a recent GLOBSEC public opinion poll on fake reports and conspiracy theories. According to a survey of approximately 10 million people in the Central European region, they regularly visit disinformation media. The results also show that the most vulnerable to accepting conspiracy theories are in Slovak V4 space. "53% of Slovaks believe there are secret societies that want to achieve worldview. 55% of Czechs disagree with this statement. 52% of Slovaks also believe that Jews have a great influence on the control of institutions, 67% of Czechs disagree with this claim. When questioned about the attack on the World Trade Center on September 11, 2001, 74% of young Czechs aged 18-24 disagreed with the assertion that the US government executed this attack, with only 38% of the young Slovaks believing it, "Klingova said. It also pointed out that the Czech Republic joined the initiative of the Center for Excellence in Combating Hybrid Threats (Hybrid CoE) and that the Center for Counter Terrorism and Hybrid Threats works at the Ministry of the Interior, while similar projects are missing in Slovakia. She also said that a number of media and non-governmental organizations have been working in both countries. However, Slovakia's problem is how the public administration responds to the threatened threats.

At the end of the discussion, both speakers named major cyber and information security challenges. According to Katarína Klingová, Slovakia is calling for a comprehensive approach in the area of strategic communication, which would include all components of public administration. Further enhancement of cyber security capabilities and creation of an action plan, including ongoing evaluation, allowing to deal effectively with changes in the environment. Jan Šaradin pointed out the importance of introducing mandatory penetration tests, especially for critical and important information infrastructures. Furthermore, the need to improve organizational measures, including continuing education, as well as the development of cyber security programs.

Workshop

The goal of…