Organization for Security and Co-operation in Europe
Mission to Montenegro

OSCE SLOVAKIA 2019 SLOVENSKO

# National Seminar on Cybersecurity and countering the use of the Internet for Terrorist Purposes and Organised Crimes

**3rd- 4th April 2019, Hotel Verde,**

**Podgorica, Montenegro**

## Wednesday, 3rd April

| | |
|---|---|
| 09:00: 09:30 | **Registration of Participants** |
| 09:30-09:45 | **Opening remarks**<br><br>**Ambassador Maryse Daviet, Head of OSCE Mission to Montenegro**<br>**Ambassador Roman Hloben, Slovak Chairmanship Embassy in Podgorica** |
| 09:45-10:00 | **Seminar Photograph** |
| 10:00-11:00 | Session One<br>**Building confidence in cyberspace between states, including the role of international and regional organizations to reduce the risks of conflict stemming from the use of Information and Communication Technologies (ICTs)**<br><br>In recent years ICTs have added a complex dimension to inter-state relations. Events in cyberspace often leave room for ambiguity, speculation and misunderstanding. The worry is that miscalculations and misperceptions between states arising from activities in cyberspace could escalate, leading to serious consequences for citizens as well as for the economy and administration, and potentially fueling political tensions.<br><br>This presentation will outline the OSCE process to tackle these issues by outlining the sixteen (16) Confidence Building Measures (CBM) agreed by all 57 participation nations. These 16 CBMs are practical, risk-reduction measures designed to enhance transparency and reduce misperception and escalation between states. They include provisions for communication- and information-sharing at the government- and expert-level and for the use of the OSCE as a platform for exchanging best practices, with the aim of increasing inter-state co-operation and stability.<br><br>**Speaker: Mr. Velimir Radicevic , OSCE Department for Addressing Transnational Threats, Project Manager on cyber/ICT security issues** |

| | |
|---|---|
| 11:00-11:15 | Network Coffee Break |
| 11:15-12:45 | Session Two<br><br>**Cyber Audit Management: What you need to know**<br><br>Over the last two to three years, Montenegro authorities have recorded a sharp rise in the number of cyber-attacks, mostly targeting state institutions and media outlets. From only 22 such incidents in 2013, almost 400 were recorded in in 2018. It is no longer possible for cyber-security policies to be purely reactive and it is essential all organizations have the capacity to protect themselves from security breaches and the potentially catastrophic consequences.<br><br>• Assessing cyber operation efficiency – key indicators of capacity in ICB cyber security<br>• Identifying internal controls and regulatory deficiencies within your organization<br>• Understanding the audit checklist practical steps to audit management<br>• Fail to prepare, prepare to fail? How do we get this right?<br><br>**Speaker: Mr. Peter Bátor, Director, Foreign Policy Department Office of the President of the Slovak Republic** |
| 12:45-13:45 | **Networking Lunch** |
| 13:45-15:00 | Session Three<br><br>**Social Media network security**<br><br>The role of social media as a tool to shape national and international politics and policy has evolved significantly in recent years, becoming one of the main information sharing platforms for the developed world. With over three billion social media users worldwide, the potential influence of social media is unprecedented.<br><br>With major concerns of social media vulnerabilities and the potential use of these platforms for disinformation spreading and political distortion, CERT operators are faced with major challenges to ensure that all society members are protected from subversive influencers across the social media, without compromising on individual freedoms.<br><br>This first sessions will focus on how social media has impacted the cyber operator and what this means for government and civilian operators in the future. Key topics that the seminar will focus upon include:<br><br>• How the social media had changed the cyber domain<br>• The approach to security within social media companies<br>• The remit of government cyber regulators within private organization<br>• Demonstrate the impact of social media in influencing and changing population mentality |

| | |
|---|---|
| | • Demonstrate how a cyber secure culture mitigated risk from cyber-attack.<br><br>**Speaker: Mr. Rastislav Kazansky, PhD, The Head of Department of Security Studies, Matej Bel University, Slovak Republic** |
| 15:00-15:20 | **Afternoon coffee and networking** |
| 15:20-16:30 | Session Four<br><br>**A follow up presentation: Reference to education and an early recognition of radicalization and violent extremism which leads to terrorism and the impact of the internet**<br><br>**Speakers:**<br>**Ms. Professor Sonja Tomovic Sundic, PhD, Faculty of Political Sciences , University of Montenegro**<br>**Mr. Adis Balota, PhD, Dean of the Faculty for Information Technology, University of Mediterranean** |
| 16:30-16:45 | Wrap up of day one |

## Thursday, 4th April

| | |
|---|---|
| 09:00-10:15 | Session One<br><br>**Addressing the latest cyber threat landscape & government strategies from a Montenegrin Point of view**<br><br>The primary responsibility is to keep the Montenegro safe and deliver competent government. This Cyber Security Strategy of Montenegro 2018 to 2021 reflects these duties. The document is a bold and ambitious approach to tackling the many threats That Montenegro countenances in cyberspace. Managing and mitigating those threats is a task for us all but the Ministry of Public Affairs (MoPA) recognizes its special responsibility to lead the national effort required. The MoPA also has a special responsibility to the citizen, to companies and organizations operating in the country, and to international allies and partners. There is a need to assure them that every effort made has been to render our systems safe and to protect our data and our networks from attack or interference.<br><br>This introductory session will identify the way forward for all parties.<br><br>**Speaker: Mr. Aleksandar Andjic, Head of the User Support Department, Ministry of Public Administration** |
| 10:15-10.30 | **Coffee Break** |

| | |
|---|---|
| 10:30-11:30 | Session Two<br><br>**Presentation of the OSCE E-learning Module on Countering the Use of the Internet for Terrorist Purposes and future OSCE activities with regard to preventing and countering violent extremism and terrorism online**<br><br>SCAN TO GET THE LINK TO THE OSCE E-LEARNING MODULE<br><br>**Speaker: Mr. Otabek Rashidov, OSCE Department for Addressing Transnational Threats, Action Against Terrorism Unit** |
| 11:30-12:30 | Session Three<br><br>**Investigations and intelligence-gathering from a policing point of view**<br><br>Technological advancements have provided many sophisticated means by which terrorists may misuse the Internet for illicit purposes. Effective investigations relating to Internet activity rely on a combination of traditional investigative methods, knowledge of the tools available to conduct illicit activity via the Internet and the development of practices targeted to identify, apprehend and prosecute the perpetrators of such acts.<br><br>**Speaker: Mr. Jaksa Backovic, Senior Police Inspector I Class, Head of Group for Cyber Crime Investigation, Crime Police Sector, Police Directorate of Montenegro** |
| 12:30- 13:30 | **Networking Lunch** |
| 13:30-15:00 | Session Four<br><br>**Investigations of the Different Components and Protection and Recovery of Forensic Data in Investigations on Countering the Use of the Internet for Terrorist Purposes**<br><br>The experts during this session will present good practices, lessons learned, general guidelines and practical examples of specialized investigative techniques for the gathering of digital evidence stored on the computers or mobile devices utilized, as well as for the investigation of cases where the Internet has been used for terrorist purposes as a facilitator for the incitement, recruitment and training, as well as for |

| | |
|---|---|
| | the planning, communication and execution of acts of terrorism. In addition, the speakers will also highlight the need of closer co-operation between public authorities and the private sector. Investigators must increasingly seek to benefit from such partnerships in order to collect and analyse information from such sources to strengthen their cases for the prosecution of terrorists<br><br>**Speakers from the Forensic Centre of the Police Directorate of Montenegro :**<br>**Ms. Isidora Šljukić, IT Forensic Expert**<br>**Mr. Mladen Mihailović, IT Forensic Expert**<br>**Mr. Slaviša Golubović , IT Forensic Expert** |
| 15:00-15:20 | **Afternoon coffee and networking** |
| 15:20-16:00 | **Closing remarks** |