Global Cyber Policy Dialogues: Western Balkans

June 1-2, 2022
Skopje, North Macedonia

MEETING MATERIALS

Republic of North Macedonia
Ministry of Defence

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

METAMORPHOSIS
Foundation for Internet and Society

Wednesday, June 1

Pre-Meeting Roundtable: Donor Coordination in the Western Balkans

Venue: Members of Parliament Club
Mitropolit Teodosij Gologanov 45
Skopje 1000

13:30-14:00 REGISTRATION

14:00-14:10 OPENING REMARKS

14:10-15:10 SESSION I: BEST PRACTICES FOR COORDINATION

The need for coordination among funders and implementers of capacity building initiatives is evident from the number of previous, ongoing, and planned projects. This session will look at concrete ideas that have emerged from previous coordination discussions and explore opportunities for taking some of these proposals forward to improve communication and transparency among funders, implementers, and stakeholders in the Western Balkans.

Moderator: **Franziska Klopfer**, Principle Programme Manager, Europe and Central Asia Division, Geneva Centre for Security Sector Governance (DCAF)

Speakers: **Kristo Põllu**, Institutional Lead, EU CyberNet
Chris Painter, President, Global Forum on Cyber Expertise Foundation Board

15:10-15:20 NETWORKING BREAK

15:20-16:20 SESSION II: MAPPING AND PRIORITY AREAS

Duplication in aid efforts is often simply a result of imperfect knowledge about what others are doing. A way to mitigate this challenge is through in-depth mapping of projects. Equally important is understanding which areas need the most attention given the priorities of aid recipients. This session will examine the areas of focus for Western Balkan governments and organizations to help donors understand what work still needs to be done. It will also review existing mapping initiatives that show what issues are already being tackled. Avenues for increased regional cooperation on specific issues will be explored.

Moderator:	**Franziska Klopfer**, Principle Programme Manager, Europe and Central Asia Division, Geneva Centre for Security Sector Governance (DCAF)
Speakers:	**Vojtěch Hons**, Policy and Programme Officer, Directorate-General for Neighbourhood and Enlargement Negotiations, European Commission **Monika Lekić**, Head of Project Development, e-Governance Academy
16:20-16:30	**CONCLUDING REMARKS**
19:00-21:00	**RECEPTION**
Venue:	Residence of the Ambassador of the Kingdom of the Netherlands Street 6 A, Number 3, Bardovci, Skopje
18:30	*Transportation will be provided from the **Holiday Inn Hotel** (Boulevard Phillip the Second of Macedon 5, Skopje 1000) to the reception at the Ambassador's Residence. The bus will depart at 18:30.*
21:00	*Return transportation is provided from the Ambassador's residence to the Holiday Inn Hotel.*

Thursday, June 2

Venue: Members of Parliament Club
Mitropolit Teodosij Gologanov 45
Skopje 1000

08:00-08:30 REGISTRATION

08:30-08:35 WELCOME REMARKS

Bruce W. McConnell, Distinguished Fellow, Observer Research Foundation America (Moderator)
Bardhyl Jashari, Executive Director, Metamorphosis Foundation

08:35-09:00 OPENING REMARKS

Dragan Nikolić, State Secretary, Ministry of Defence of North Macedonia
Nathalie Jaarsma, Ambassador-at-Large, Security Policy and Cyber, Ministry of Foreign Affairs of the Netherlands

09:00-10:30 SESSION I: CYBER DEFENSE

In defending themselves and their citizens against malicious activity in cyberspace, states are developing cyber defense strategies and looking to improve capacities in terms of incident response, threat information sharing, and cooperation across borders. There is a need to link these cyber defense efforts with the implementation of diplomatic agreements on the normative framework for cyberspace and the established Confidence Building Measures by the Organization for Security and Co-operation in Europe (OSCE), which improve predictability and trust among states. The 2015 UN GGE norms, recently reaffirmed by the OEWG and GGE in 2021, establish ground rules for state behavior in cyberspace that are meant to improve trust among states and overall stability in the domain. However, much work remains to be done on the implementation of these agreements. This session will explore how the frameworks agreed at the UN and OSCE are relevant for cyber defense strategies and infrastructure in the current geopolitical context, and will look to bridge the gap between the cyber diplomatic community and national cyber defense apparatuses.

Speakers: **Andrijana Gavrilović**, Head of Diplomatic and Policy Reporting, DiploFoundation; Editor, GIP Digital Watch
Mentor Vrajolli, Executive Director, Kosovar Centre for Security Studies (KCSS)
Ivana Tatar, Independent Advisor, Parliament of Montenegro
Alenka Gorgieva, Head of C-4 Sector, Ministry of Defence of North Macedonia

10:30-11:00 NETWORKING BREAK

11:00-12:15 **SESSION II: CYBER RESILIENCE THROUGH CERT-TO-CERT COOPERATION**

A country's cyber resilience requires a systemic approach, involving actors from the private sector, civil society, and government agencies. Key to such resilience, particularly with regard to critical infrastructure, information sharing, and incident response, is the capacity and cooperation between computer emergency response teams, or computer security incident response teams (CERTs or CSIRTs). Building CERT capacity and promoting cross-border and cross-sector cooperation has been the focus of several initiatives in the Western Balkans region, and was identified as a priority for capacity building efforts in the virtual meeting. Facilitating opportunities to exchange best practices and information on threats as well as incident-response and CERT operations, can help increase CERT capacity and strengthen trusted relationships among regional CERTs, as well as other stakeholders. It directly contributes to strengthening the normative framework for cyberspace, in particular norms on critical infrastructure protection and incident response. Building on previous initiatives in the region, this session will create an opportunity for peer-to-peer exchanges between CERT representatives and other private sector and civil society actors involved in cyber resilience, while at the same time exposing policymakers to the technical realities of cyber incident response and related resilience policies.

Speakers: **Serge Droz**, Senior Advisor, Federal Department of Foreign Affairs of Switzerland; Member of the Board, Forum of Incident Response and Security Teams (FIRST)
Franziska Klopfer, Principle Programme Manager, Europe and Central Asia Division, Geneva Centre for Security Sector Governance (DCAF)
Aleksandar Acev, Head of MKD-CIRT, Agency for Electronic Communications of North Macedonia

12:15-13:30 LUNCH

13:30-14:45 **SESSION III: COMBATING CYBERCRIME**

As life in the Western Balkans (and globally) becomes more digitized, there are more avenues for cyber criminals to exploit. Building resilience against cybercrime includes preventative measures (e.g., building cybersecurity into IT infrastructure, fostering awareness and good cyber hygiene practices among users, and devoting resources to threat detection, prevention, and response) as well as measures to catch and hold criminals accountable. This includes ensuring there is specific legislation in place as well as safeguards to protect human rights and fundamental freedoms online, and building capacity among law enforcement and the judiciary to handle digital evidence and investigate cybercrime cases. In the context of a recently launched UN Ad Hoc Committee to negotiate a universal cybercrime convention, as well as regional initiatives to combat cybercrime, this discussion will look to identify avenues for regional cooperation in the fight against cybercrime while also guarding against creeping definitions of cyber criminality and protecting human rights in the online space.

Speakers: **Kristina Evgo**, Senior Organized Crime Advisor, Organized Crime Unit, Security Co-operation Department, OSCE Mission to Serbia
Predrag Puharić, AcCSIRT CEO and Chief Information Security Officer, Faculty for Criminal Justice, Criminology and Security Studies (CSEC), University of Sarajevo

14:45-15:15 NETWORKING BREAK

15:15-16:30 **SESSION IV: INFORMATION DISORDER**

Digitally manipulated media and disinformation continue to be an issue in the Western Balkans as well as globally, undermining people's trust in governance institutions, independent media, science and healthcare, and each other. Fake websites fuel cybercrime, and disinformation promoting extremist views and clickbait have been revealed to generate a profit for Internet trolls as well as large Internet platforms. Orchestrated disinformation campaigns have already played a role in hybrid conflicts and societal polarization. Addressing this problem is necessary to improve trust in the digital ecosystem, as well as social and political life more broadly. Discussion on this issue is important to the broader conversation about how to ensure a free, open, and secure cyberspace, in which citizens and organizations are resilient to cyber threats and in which human rights are protected. This session will be an opportunity for partners to present regional and local activities undertaken since the virtual meeting to better understand and address the information disorder challenge.

Speakers: **Filip Stojanovski**, Director, Partnership and Resource Development, Metamorphosis Foundation
Viola Keta, Editor in Chief, Faktoje
Anida Sokol, Media Researcher, Mediacentar Sarajevo

16:30-17:00 **CONCLUDING REMARKS**

17:00-18:00 **RECEPTION**

Venue: Garden, Members of Parliament Club

The Observer Research Foundation America in partnership with the Ministry of Defence of North Macedonia, the Ministry of Foreign Affairs of the Netherlands, and Metamorphosis Foundation will be hosting an in-person Global Cyber Policy Dialogues: Western Balkans meeting June 1-2, 2022 in Skopje, North Macedonia. This multistakeholder meeting will bring together approximately 40 attendees from Albania, Bosnia and Herzegovina, Kosovo,* Montenegro, North Macedonia, and Serbia, as well as some experts and donor countries from outside the region. Participants and speakers will come from government, civil society, academia, and the private sector.

A first virtual preparatory meeting was held in April 2021 to lay the groundwork for the in-person meeting. It addressed three broad topics: peace and security, cybersecurity and cybercrime, and information disorder. Through the course of the meeting, several trends became clear. First, the Western Balkans are integrating ICTs into their governments, defense, infrastructure, and everyday life. However, the capacity to ensure the security and integrity of the technology still needs improvement. Second, the region is facing a number of increasing threats, including cybercrime, disinformation campaigns, and militarization of cyberspace that threaten stability and trust both among Western Balkan economies and with their neighbors. Third, there is a need for more engagement on the political level in the Western Balkans on cybersecurity and stability issues. This means greater situational awareness of the needs and threats, but also that leaders must act swiftly to prioritize cybersecurity and related matters, and ensure that they are devoting adequate resources to these areas. This highlights an existing capacity gap that is not unique to this region, but must be addressed by appropriate local, regional, and international efforts. Given the interest of other European countries in the cybersecurity and stability of their neighbors in the Western Balkans, there is ample opportunity for partnerships on capacity building. However, such efforts would require increased coordination among donors and assistance that is targeted and context-specific.

An element that underpins all efforts to address these challenges is trust. Users need to trust that technologies are not prone to vulnerabilities, and they also need to trust that governments and companies are treating their data responsibly and not using it unlawfully or to target disinformation and manipulate them. Public trust in institutions and within communities is also impacted by the veracity of information spread online. Actors looking to exploit cyberspace and algorithms for financial or political gain can undermine that trust. Governments need to be able to trust that other countries are not using their digital systems against them, or sponsoring or harboring third party actors using ICTs in malicious ways. Capacity building partnerships also require trust between actors. For their part, companies would also like to trust that governments are not carrying out malicious activity on the infrastructure they own and operate. This meeting will look at trust as an essential element of ensuring security and stability in cyberspace and realizing the economic and social potential of the Internet and digital technologies. Participants will discuss how to strengthen trust in several key areas and address critical challenges facing the Western Balkans region: cyber defense, cyber resilience, cybercrime, and information disorder.

Donor Coordination Roundtable

On the sidelines of the main conference, the Observer Research Foundation America in partnership with the Ministry of Defence of North Macedonia, the Ministry of Foreign Affairs of the Netherlands, and Metamorphosis Foundation will be hosting a donor coordination roundtable.

In 2021, the UN Open-ended Working Group (OEWG) highlighted the importance of needs-based, recipient-led capacity building initiatives, more equal partnerships, and better coordination to reduce redundancies.

* This designation is without prejudice to positions on status and is in line with UN Security Council resolution 1244 and the International Court of Justice Opinion on the Kosovo declaration of independence.

Similarly, the Organisation for Economic Co-operation and Development (OECD) has worked to improve the effectiveness of international aid by promoting principles including ownership, alignment, harmonization, managing for results, and mutual accountability.

Several discussions have identified a need for increased coordination among donors involved in cyber capacity building in the Western Balkans region. At the April 2021 Global Cyber Policy Dialogues: Western Balkans virtual meeting, speakers described some of the many projects underway to build capacity to address cyber challenges, from bolstering cyber diplomacy, to increasing peer learning on cybersecurity, to combating disinformation. It became clear that improved coordination across the initiatives could increase their effectiveness. Since then, other efforts have been undertaken to improve such coordination, including from the Global Forum on Cyber Expertise (GFCE), the Geneva Centre for Security Sector Governance (DCAF), and EU CyberNet. Other organizations could also facilitate regional cooperation on capacity building opportunities for Western Balkans economies, including the Regional Cooperation Council (RCC), the Organization for Security and Co-operation in Europe (OSCE), and the International Telecommunication Union (ITU).

This pre-meeting roundtable on June 1 will bring together countries from outside the region that are currently or are planning to be engaged in cyber capacity building in the Western Balkans, representatives of government agencies in the Western Balkans, implementing civil society organizations, and the private sector. Building on the OEWG and OECD, the event will review previous coordination discussions, solicit input from recipient organizations to identify priorities, and explore concrete ideas to deconflict initiatives, including finding opportunities for synergies. Particular emphasis will be on specific mechanisms for continued coordination among donors and recipients going forward, and supporting the work of existing fora that can serve this coordinating function.