Global Cyber Policy Dialogues: Western Balkans

June 1-2, 2022
Skopje, North Macedonia

MEETING SUMMARY

Republic of North Macedonia
Ministry of Defence

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

METAMORPHOSIS
Foundation for Internet and Society

On June 1-2, 2022, the Observer Research Foundation America (ORF America), in partnership with the Ministry of Defence of North Macedonia, Ministry of Foreign Affairs of the Netherlands, and Metamorphosis Foundation, held an in-person roundtable in Skopje, North Macedonia as part of its Global Cyber Policy Dialogues series. The meeting focused on improving the security and stability of cyberspace and building cyber capacity in the Western Balkans in several key areas. The first day brought donors, recipients, and implementers together to discuss ways to improve coordination among donors who are funding cyber capacity projects in the region. The second day focused on enhancing cyber norms and defense, improving resilience through computer emergency response team (CERT) cooperation, combating cybercrime, and addressing disinformation. The meeting brought together over 50 participants from Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia, representing government, civil society, academia, multilateral institutions, and the private sector.

A virtual preparatory meeting held in April 2021 brought to light three central challenges which laid the groundwork for this event. First, while Western Balkans economies are integrating ICTs into their governments, defense strategies, infrastructure and daily life, capacities to ensure the security and integrity of these technologies still need improvement. Second, the region is facing an increasing number of threats, including cybercrime, disinformation and the militarization of cyberspace, which threaten stability and trust among Western Balkan economies and with their neighbors. Third, there is a need for more political engagement on cybersecurity and stability issues, including prioritizing cybersecurity matters and allocating adequate resources. These gaps can be narrowed through partnerships with donor governments, provided such efforts are coordinated and provide targeted, context-specific assistance. Importantly, trust underpins all efforts to address these challenges. This includes trust that technologies are not prone to vulnerabilities, trust that governments are treating data responsibility, and public trust in institutions.

Accordingly, the in-person conference aimed to build on the virtual meeting by addressing how to strengthen trust in key areas and address four critical challenges facing the Western Balkans region: cyber defense, cyber resilience, cybercrime, and information disorder. In an effort to improve donor coordination, a pre-meeting roundtable was held to review previous inter-donor discussions, solicit input from recipient organizations to identify priorities, and explore concrete ideas to deconflict initiatives.

This two-day event was the first in-person roundtable convened as part of the Global Cyber Dialogue Series, a project undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands. This project consists of regional meetings which seek to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity building initiatives. These meetings are intended to complement ongoing international-level cyber processes, such as the United Nations Open-ended Working Group and Ad Hoc Committee on Cyber Crime.

The discussions took place under the Chatham House Rule. Opening remarks for the meeting were provided by Dragan Nikolić, State Secretary of the Ministry of Defence of North Macedonia and Nathalie Jaarsma, Ambassador-at-Large for Security Policy and Cyber of the Ministry of Foreign Affairs of the Netherlands. The first day was moderated by Franziska Klopfer, principle programme manager in the Europe and Central Asia Division at the Geneva Centre for Security Sector Governance (DCAF). The second day was moderated by Bruce W. McConnell, distinguished fellow at ORF America.

June 1: Donor Coordination in the Western Balkans

To support more effective capacity building, the June 1 pre-meeting roundtable explored ways to increase donor and implementer coordination, which had been identified as a need for the region during the virtual meeting in April 2021. After opening statements by Franziska Klopfer (Geneva Centre for Security Sector Governance), Kristo Põllu (EUCyberNet), and Chris Painter (Global Forum on Cyber Expertise), the first session focused on best practices to improve cooperation and avoid duplication at every level, especially considering the number of actors involved in the region and the dynamic nature of the cyber field. There are currently dozens of projects being funded by Western governments and other organizations, with no formal mapping of these efforts to ensure synergies or reduce duplication. Participants identified one way to reduce redundancy at the regional level by building on existing efforts such as those currently undertaken by EUCyberNet, the Regional Cooperation Council, and the Global Forum on Cyber Expertise (GFCE). Several participants underscored the need for greater coordination at the national level within recipient countries to enable them to be stronger partners and project a coherent set of needs in discussions with donors. Future dialogues may consider looking at moving beyond discussing the necessity of coordination to focusing on ways to promote synergy between projects.

The second session opened with remarks by Vojtěch Hons (Directorate-General for Neighbourhood and Enlargement Negotiations, European Commission) and Monika Lekić (e-Governance Academy), and looked at a study conducted by Directorate-General for Neighbourhood and Enlargement Negotiations and implemented by e-Governance Academy which examines the capacity needs of the Western Balkans region. The study was driven by local experts and focused on advancing digitization, prioritizing areas including: institutional frameworks, legislation, incident management, computer emergency response team (CERT) capacity, education, and cybersecurity awareness. The study will inform the design of a new capacity building program, scheduled for 2023, to be sponsored by the European Commission. The EU's interest is to solidify cyber governance frameworks, leverage donor activity, and is driven by national strategies. The study identifies priorities, including national-level leadership (including legislation), risk and crisis management, threat intelligence sharing, and incident reporting (including transnational cyber exercises). During the discussion, some participants emphasized the benefits of community building and engaging on a multistakeholder basis to include youth, small cyber companies, and civil society. Others noted the importance of having sustained national institutions to maximize long-term benefits.

The call from both donors and implementers for more coordination of cyber capacity building efforts means there is room for more sustained projects to fill this gap. Organizations like the GFCE are planning to address this by organizing several meetings that aim to reach consensus amongst stakeholders on what the most urgent coordination issues are, identify ways to address these, agree on a way forward, and implement the outcomes.

June 2: Global Cyber Policy Dialogue: Western Balkans

Cyber Defense

The first session of the day sought to bridge the gap between the cyber diplomatic community and national cyber defense organizations. Participants explored the links between cyber defense strategies, including critical infrastructure protection, and the implementation of diplomatic agreements on the normative framework for cyberspace and confidence-building measures. The Organization for Security and Co-operation in Europe (OSCE) has agreed on confidence-building measures to reduce the risk of conflict created by the use of ICTs. Similarly, in 2015, the United Nations Group of Governmental Experts (UN GGE) released norms of responsible

state behavior in cyberspace to address threats from the use of ICTs by states and to reduce the risks to international peace and security by improving trust among states and overall stability in the domain. The United Nations Open-ended Working Group (UN OEWG) reaffirmed these norms in its 2021 report, and these norms have been endorsed by the UN General Assembly.

The session began with remarks by Andrijana Gavrilović (DiploFoundation; GIP Digital Watch), Mentor Vrajolli (Kosovar Centre for Security Studies), Ivana Tatar (Parliament of Montenegro), and Alenka Gorgieva (Ministry of Defence of North Macedonia). The discussion highlighted how the lack of policy capacity in the Western Balkans has hindered the region's participation in shaping and implementing the normative framework for cyberspace being discussed at the international level. A participant noted that of the 1,394 statements delivered at the UN OEWG, only four were made by governments from the Western Balkans region. Impediments to greater participation include a shortage of resources allocated to cyber defense as well as a lack of lawmaker awareness about the UN processes. In order to address these challenges, participants called for a regional center to educate political officials, the general population, civil servants, critical infrastructure operators, senior executives, and lawyers. A promising development in this regard is North Macedonia's Institute for Cybersecurity and Digital Forensics, which is in its early stages and will contribute to greater education in the region.

Participants acknowledged that the private sector also plays a large role in cyber defense, both in building capacity and marshaling its existing capabilities to various ends. The Ukraine-Russia war was cited as an example. Ukraine has mobilized civilian IT personnel to assist with cyber defense in response to the Russian invasion, raising questions about how best to involve the private sector when considering controversial practices such as "hack back." The discussion emphasized that all activity must adhere to international law and that the roles of government and citizens should be clear. Other concrete recommendations included creating a base of experts and volunteers that can be utilized when needed through national strategies, as well as improving vulnerability disclosure processes and setting up a mechanism to share information on threats quickly and efficiently. Future discussions can also explore specific mechanisms to expand public-private partnerships to strengthen defense while adhering to international law.

Cyber Resilience through CERT-to-CERT Cooperation

The capacity of and cooperation between computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs) is key to cyber resilience, particularly for critical infrastructure, information sharing, and incident response. Building CERT capacity and promoting cross-border and cross-sector cooperation was identified as a priority for capacity-building efforts in the April 2021 virtual meeting. To help increase CERT capacity in the Western Balkans, this session promoted peer-to-peer exchanges between CERT representatives and private and civil society actors involved in cyber resilience regarding such topics as best practices, information on threats, incident response, and CERT operations.

The session began with remarks by Serge Droz (Federal Department of Foreign Affairs of Switzerland; Forum of Incident Response and Security Teams), Franziska Klopfer (DCAF), and Aleksandar Acev (Agency for Electronic Communications of North Macedonia). The discussion looked at how collaboration in the region had brought different CERTs together and created new communities. This is partly the result of the work by DCAF, which has been bringing CERTs together through joint exercises, information exchanges, incident response collaboration, and other peer-to-peer exchanges. It was noted that peer-to-peer exchanges have been particularly effective and should continue. DCAF is looking to continue increasing cyber resiliency within individual countries by promoting internal cooperation between CERTs and other actors including internet service providers (ISPs). Areas for future discussion include how to increase the region's capacity to collect and analyze threat and incident information, facilitate information sharing on incidents, and better methods of sharing confidential information while protecting the identity of victims of cyber attacks.

Trust was identified as a key challenge for CERT effectiveness. In order to share sensitive information or call upon a CERT during an emergency, it must be a trusted entity. Stakeholders must trust that information shared will not be used in a harmful manner and that the CERT has the capacity and expertise to act. Actively building trust and creating relationships between different stakeholders in the region and getting constituents actively involved in the CERTS should continue. A potential challenge is the practice of some governments to use CERTs in a law enforcement capacity. The dual responsibilities of being both a law enforcement agency and a first responder for computer emergencies work at cross purposes: CERTs cannot effectively fill both roles and should avoid taking on a law enforcement role in order to remain trusted actors.

A shortage of human resources also poses a challenge to increasing CERT capacity. While methods of attracting and retaining talent–such as internships, competitions, and conveying the opportunity to do meaningful work–are well-known, implementation has fallen short. To help address this, governments need to see cybersecurity personnel issues as national security issues. The United States Department of Homeland Security was given as an example here: it has received special hiring privileges that place extra value on cybersecurity professionals. As in the first session on cyber defense, a lack of education was again noted as a challenge to increasing capacity. Lawmakers need to be educated on the mandates, purpose, and value of CERTs in order to properly allocate resources to them.

Combating Cybercrime

This session provided an overview of how a new international cybercrime treaty could complement the Budapest Convention on Cybercrime and other means of addressing cybercrime given the increasing use of technology by criminal groups and the ability to exploit cryptocurrency to maintain anonymity. The session began with opening remarks by Kristina Evgo (OSCE Mission to Serbia) and Predrag Puharić (University of Sarajevo) as well as an introduction to the cybercrime work of the United Nations by Nathalie Jaarsma (Ministry of Foreign Affairs of the Netherlands).

Participants discussed how crime is a big business with organized criminal elements now having a large stake in cybercrime schemes. One milestone in the evolution of cybercrime that was noted is the potential for lethality: a ransomware attack against a hospital in Germany delayed care that may have resulted in the death of a patient. The merging of disinformation and cybercrime also creates new challenges. For example, fraud can be facilitated by fake ads that appeal to potential victims, especially as it is easy to disseminate fake information through social media platforms. Similarly, disinformation and cybercrime can be mixed in with digital hate speech. When working towards solutions to cybercrimes, attention must be paid to this and the numerous other intersecting issues.

One challenge that many participants touched upon was the limitation of current legal procedures to adequately deal with cybercrimes. In most countries in the region, only the victim of the crime can report the incident, which artificially limits reporting as people may not know they are a victim of a cybercrime or there may be a stigma to admitting to falling for fraud. Even after a crime is reported, prosecutors need to decide to investigate further and then gather enough evidence to bring the case to court. This process creates many bottlenecks for resolving such crimes, as there is a learning curve and specific capacities are needed for collecting and handling digital evidence. Another challenge cited for law enforcement is that the procedures are different in each country, so in cases of international fraud, obtaining the help of foreign law enforcement agencies can be difficult.

Speakers identified various possible solutions to help address these challenges in the region. One speaker called for increasing regulations on cryptocurrency, establishing an oversight committee for data, exchanging information through international cooperation, and enlisting the private sector to help in dismantling cybercrime networks. Multiple participants called for increasing the amount of cybercrime units in law enforcement. Participants also looked toward cyber hygiene and creating a culture of awareness among the government and general population as a means to help combat cybercrime. Another idea was to better utilize data and metrics, such as financial loss and reported cases, to help shape solutions. Participants suggested that laws be updated to accommodate the nature of cybercrime. Many of these solutions require the aid of legislators. At the same time, it was noted there is a frustrating lack of communication between legislators, law enforcement officials, and judiciaries on how to move forward. Many of these solutions begin with educating legislators and judges, and promoting better communication between these disparate, interdependent bodies. Future discussions could examine methods for improving such communication.

Information Disorder

Digitally manipulated media and disinformation undermine people's trust in governance, institutions, media, science, healthcare, and each other, both in the Western Balkans and globally. Internet trolls and large internet platforms can generate a profit through fake websites that fuel cybercrime. Disinformation campaigns have already contributed to hybrid conflicts and societal polarization. In order to improve trust in the digital ecosystem, and social and political life, these challenges need to be addressed. Such work is part of ensuring a free, open, and secure cyberspace that is resilient to cyber threats and that protects human rights. This session gave partners an opportunity to present regional and local activities undertaken since the 2021 virtual meeting to better understand and address the information disorder challenge.

The discussion began with remarks by Filip Stojanovski (Metamorphosis Foundation), Viola Keta (Faktoje), and Anida Sokol (Mediacentar Sarajevo). The speakers are responsible for many initiatives focused on fact-checking to counter disinformation in the region, such as the Metamorphosis-led regional project Western Balkans Anti-Disinformation Hub: Exposing Malign Influences through Data-Driven Watchdog Journalism, which is supported by the Kingdom of the Netherlands, the Truthmeter.mk fact-checking service, which includes debunking social media disinformation, and the development of the Anti-Disinformation Network for the Balkans. Faktoje engages with various constituencies to promote media literacy, and Mediacentar Sarajevo supports the education of journalists and audiences on how to verify information in different media.

One overarching challenge has been the current financial model of media outlets which has distorted the incentives to fact-check. For instance, some editors do not fact-check because fact-checked content can reduce views and corresponding profits. This helps create a culture that resists fact-checking and puts journalists in a difficult situation, especially when they are pressured to be the first to publish a story and prioritize maximizing the number of views their articles receive. Consequently, inaccurate information is published, and then amplified as it is circulated throughout the region. This, in turn, reduces the public's trust in journalists, media, and news outlets. It can also make journalism seem to be an unattractive career, reducing the number of journalists. Further discussions might explore ways to increase funding transparency and promote more transparent funding structures for media and news outlets.

Disinformation itself is not a new phenomenon and existed before the Internet and digital media. Combating it now requires looking at its evolving nature and addressing how it has manifested differently in contemporary society. First, social media has created information bubbles where people of disparate views congregate in echo chambers, facilitated by algorithms that curate content. Additionally, the nature of disinformation has changed rapidly, becoming much more targeted. A potential way this may occur is to "hack" a public figure, by

influencing them through financial contributions or blackmail to spread disinformation to their audience. Further discussions might more closely examine how disinformation has changed with new technologies.

Potential solutions should keep in mind that many laws in the region explicitly ban censorship, causing reluctance among legislators to enact social media regulations. However, high-level policy regulations, such as those developed by the EU, have helped regulate social media platforms in ways designed to de-incentivize information disorder. Potential regulation of social media outlets may be more effective at the EU level.

Concluding Remarks

Concluding remarks at the end of the conference provided an overview of themes from the dialogue, including the normative framework and cyber defense, CERT cooperation and the role of CERTs, shortages of education and awareness, and a lack of trust. Lack of equitable access, the need for a better vision and leadership at all levels, increased transparency, and better laws and policies were other themes that appeared throughout the meeting. On a positive note, the numerous existing challenges have created support for common action, an increasing level of cooperation, and greater opportunities for participation throughout the region. The discussions identified some areas for potential future efforts and research, which we have outlined here.

Donor Coordination:

- **Sustained communication amongst donors**: Regular meetings to improve awareness of the various ongoing and planned projects can help funders coordinate efforts to ensure projects are cumulative rather than duplicative, as well as identify opportunities for concrete collaboration. Organizations like the GFCE and EUCyberNet with existing convening infrastructure and cyber capacity building networks could be explored as platforms for such dialogue.
- **Move from coordination to synergy**: The next step beyond just increasing awareness of what other funders are doing in the region is for funders to identify synergies—opportunities for their projects to produce reinforcing and cumulative outcomes.
- **Improve mapping of cyber capacity efforts in the Western Balkans**: Regular dialogue as suggested above will contribute to greater awareness of the full picture of cyber capacity building projects taking place in the region. However, maintaining a living document or utilizing a platform to share and track projects could contribute to better coordination and engagement in existing projects.

Cyber Defense:

- **Improve education about cyber challenges and the normative framework at the regional level**: The lack of awareness was cited as a central challenge in adequately participating in or implementing the normative framework, as well as a barrier to connecting the international conversations to national defense efforts. Future efforts could examine the potential for a regional center to educate political officials, the general population, civil servants, critical infrastructure operators, senior executives, and lawyers about cyber challenges. Exploration of the regional role for existing centers, such the North Macedonia Institute for Cybersecurity and Digital Forensics, could also be useful.
- **Greater understanding of the role of the private sector in cyber defense**: The private sector is involved in cyber defense as the Ukraine-Russian war demonstrates. More research on the ways in which the private sector engages in national cyber defense work, and the applicable international law, could help clarify mechanisms for public-private partnerships that respect international law.
- **Develop and implement vulnerability disclosure processes**: Responsible reporting of ICT vulnerabilities is encouraged in the UN normative framework for cyberspace (UN GGE norm 13j). In order for this to take place at the international level, governments must have processes in place at the national level, which requires effective cooperation with the private sector. Future discussions could focus on

convening relevant stakeholders from the private and public sector in the Western Balkans to outline best practices and establish such processes where they do not yet exist.

- **Engage civil society and non-governmental stakeholders to create a more resilient society**: Civil society organizations have an important role to play in building resilience to cyber threats, which is a key component of cyber defense. In particular, this is because they are best placed to reach vulnerable groups through awareness-raising and education, generating and sharing knowledge, capacity building and creating links of cooperation between various stakeholders in society, including state institutions and the private sector.

Cyber Resilience through CERT-to-CERT Cooperation:

- **Implement creative solutions to the human capacity issues**: The lack of human resources was cited as a main challenge to improving CERT capacity. Special hiring policies, initiatives like internships or competitions could be used to help fill this gap. Future efforts could focus on examples of best practices and help Western Balkan CERTs and ICT agencies design programs or initiatives to address the talent recruitment and retention challenge.
- **Clearly define the roles of CERTs**: CERTs can only be useful if they are trusted as a source of emergency help. To promote that trust, governments should make clear the mandates of CERTs and avoid using them for activities outside of their mandate, such as law enforcement.
- **Greater education for policymakers**: Convening workshops for lawmakers on the role and utility of CERTs can help increase understanding about the critical role these entities play in cyber cooperation and resilience. Greater awareness amongst policymakers can lead to better national cyber policies that respect the role of CERTs and allocate adequate resources.
- **Continue peer-to-peer exchanges**: The value of peer-to-peer exchanges like the ones convened by DCAF and others was reaffirmed during the meeting. Continuing these mechanisms–and disseminating takeaways and lessons learned throughout the regional stakeholder community–will be important going forward.

Combating Cybercrime:

- **Improve education and communication among criminal justice actors**: Workshops that bring together legislators, law enforcement officials, and judiciaries can improve communication among these groups, which was cited as a main challenge to adequately addressing cybercrime. Bringing in best practices including on digital evidence handling, writing cybercrime laws that respect human rights, and effectively hold criminals to account, or digital forensics could be useful to improve education as well. Regional exchanges can also help build trust and facilitate relationships that are necessary to fight such borderless crimes.
- **Examine intersections with disinformation**: The ways that disinformation can enable or enhance cybercrime was highlighted at the meeting. More in-depth research into these intersections can help lawmakers design policies that address both cybercrime and information disorder in more effective ways.
- **Discuss mechanisms for practical regional cooperation**: International cooperation is necessary to combat cybercrime effectively, as crimes in cyberspace often cross and transcend borders. However, impediments cited often include different national standards and processes, and a lack of understanding of these differences. Facilitating dialogue at the regional level focused on improving the avenues for practical cooperation across borders could help establish channels of communication and mechanisms for responding to cybercrime.

Information Disorder:

- **Address the current media funding models**: Opaque funding sources and profit models that incentivize speed and views over accurate reporting contribute to the spread of disinformation in the region.

Roundtables that bring together civil society and media stakeholders, as well as regulators, could address ways to increase funding transparency and discuss different profit models and incentive structures.

- **Continue to improve understanding of the evolution of disinformation**: Research into how this phenomenon has utilized or adapted to new technologies can help better understand the policy tools needed to effectively address the digital aspects of the disinformation challenge.
- **Invest in a systemic approach**: A systemic approach is needed to build a culture of critical thinking and social dialogue at all levels, starting with the education system, the relationship of institutions and stakeholders in all sectors, as well as at the family and individual level. Such an approach will help overcame the lack of knowledge and skills, polarization and political bias, and address susceptibility to conspiracy theories disinformation in the Western Balkans, which can be exploited by foreign malign influences and their domestic proxies.