Global Cyber Policy Dialogues: Western Balkans

April 15, 2021
15:00 CEST

MEETING SUMMARY

ORF AMERICA

Republic of North Macedonia
Ministry of Defence

Ministry of Foreign Affairs of the Netherlands

METAMORPHOSIS
Foundation for Internet and Society

Meeting Summary

On April 15, 2021 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 the Global Cyber Policy Dialogues: Western Balkans meeting. The event was organized to further discussions around building capacity in the Western Balkans to address key cyber challenges related to peace and security, cybersecurity and cyber crime, and information disorder. ORF America looks forward to continuing to cooperate with these and other organizations working in the region to advance a common cyber improvement agenda.

This event was part of a larger Global Cyber Dialogue Series being organized by ORF America and the Ministry of Foreign Affairs of the Netherlands which seeks to convene regional dialogues 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 norms processes, such as the United Nations Open-ended Working Group (OEWG) and Group of Governmental Experts (GGE).

The April 15 meeting featured speaker contributions on three broad topics: peace and security, cybersecurity and cyber crime, and information disorder. Over 70 representatives from government, civil society organizations, the private sector, and academia attended the event.

The following sections briefly summarize the speaker contributions and characterize the discussions, which took place under the Chatham House Rule. The discussion was moderated by Bruce W. McConnell, Distinguished Fellow at ORF America.

INTRODUCTORY REMARKS

Radmila Shekerinska Jankovska, Minister of Defence of North Macedonia

In the process of its accession to NATO, North Macedonia undertook efforts to improve its cyberspace capabilities and defenses. However, governments face problems of slow, bureaucratic processes and a lack of coordination between agencies and offices, and in cyberspace, being slow means failing. The first year of North Macedonia's NATO membership was also the year of the coronavirus pandemic, and this context heightened the importance for the government to do more in the cyber context.

Over the past year, North Macedonia has made progress on improving its cybersecurity, but there are two examples that show how vulnerable its institutions remain. First, North Macedonia experienced a cyber attack on its election infrastructure during the 2020 elections, which took place amid growing populism, widespread proliferation of fake news, and a difficult political context with many things at stake—all during a pandemic. An attack carried out on the website of the state election commission caused a loss of confidence, although fortunately it does not seem to have produced great mistrust in the outcome of the elections. This incident demonstrated vulnerabilities in areas that the government may not have paid sufficient attention to in the past. The second example is the case of a user on Twitter, who posed as an EU expert and harshly criticized North Macedonia's performance and institutions. This illustrated how malicious actors can use social platforms to attempt to undermine the EU accession process.

Governments must be vigilant against such threats and act quickly. We must learn how to respond quickly in a way that is based on data and facts. Cyber patterns are changing, and if we do not adapt quickly enough, we

will fail. This is a current debate within NATO, as the focus of the alliance shifts more toward cyberspace. The Ministry of Defense is working on implementing a cyber defense strategy, and is looking to be more involved with NATO efforts to combat cyber threats. Change requires cooperation with our allies and neighbors.

Nathalie Jaarsma, Ambassador-at-Large, Security Policy and Cyber, Ministry of Foreign Affairs of the Netherlands

Cyber risks experienced by the Western Balkans countries are also risks to the EU, and we must cooperate to find solutions to these threats. Many of the threats the region is facing, including cyber attacks, cyber crime, and disinformation, are not new. The good news is that there are many opportunities to increase our cooperation in the digital domain, including through processes at the United Nations, the Organization for Security and Co-operation in Europe (OSCE), NATO, EU, and the Global Forum on Cyber Expertise (GFCE). The first step is making sure that cyber is higher on the public and political agenda, which is one of the goals of this meeting.

Success with our global and regional efforts to promote stability between states in cyberspace will depend in the long run on our ability to implement capacity building measures. That is why the Netherlands puts a strong emphasis on capacity building and founded the GFCE, a multistakeholder forum which brings together needs, resources, and expertise of public and private partners to build capacity to address cyber issues on both the technical and policy levels.

PEACE AND SECURITY

Vladimir Radunović, Director, E-diplomacy and Cybersecurity, DiploFoundation

There are three trends that we need to understand better in the Western Balkans to more effectively address cyber priorities:

1) Digitalization of life: Governments have been introducing new e-services, laws, and policies and the COVID pandemic has accelerated this trend. There is no separate "cyber" anymore—everything is connected to the digital domain in some way creating real-world risks where everything is a target. Thus, the approach to cybersecurity needs to be a whole-of-government and whole-of-society approach.
2) Politicization of cybersecurity: Cyber attackers are well-organized, well-resourced, and sometimes backed directly by states. Attacks can be sophisticated with high impacts on businesses, state secrets, and critical infrastructure. At the same time, most attacks are conducted under the threshold of armed conflict, and are difficult to attribute. The risks are high: They are political, economic, and societal and require a strategic approach to mitigate.
3) Militarization of cyberspace: States are developing cyber armaments, including in the Western Balkans, but there is no transparency about what is happening. We know all about what missiles countries have, but little about military cyber capabilities. There is also a lack of transparency about policies for how these tools will be used, which leads to a lack of predictability and in turn raises the risk of escalation and conflict rising from cyber attacks.

There is some good news in terms of addressing certain risks associated with these trends, including the existence of global and regional processes about "rules of the road" and how international law applies in cyberspace, for example at the United Nations in the form of the OEWG and GGE. There are also regional processes, for example, in the OSCE, as well as multistakeholder initiatives such as the Paris Call for Trust and Security in Cyberspace, the Geneva Dialogue, and the GFCE, but Western Balkans countries are not present in these discussions. The countries in the region need to strengthen foreign policy and diplomatic efforts on cyber issues. There is not a clear understanding of the political risks, policies to deal with those risks, or connection

among agencies and countries, as well as overall capacities, particularly within foreign affairs ministries. The lack of presence from the Western Balkans in international processes reflects the failure to prioritize these issues at the political level. We need to improve capacity within the Western Balkans and start a regional dialogue on these topics.

Chris Painter, President, Global Forum on Cyber Expertise (GFCE) Foundation

Cybersecurity issues need to be mainstreamed as a core policy issue throughout government. It is unfortunate that Western Balkans countries have not yet developed cyber expertise in their foreign ministries. We don't need a massive cyber attack with horrific consequences for these issues to gain traction—enough bad things are already happening. It is necessary for countries to start raising these issues at the political level with each other. If a country puts cyber threats on the agenda of a bilateral meeting with another country, it will become a priority for both countries.

Capacity building is also critical. The GFCE is a multistakeholder group that is trying to help build cyber capacity and take forward some of the decisions agreed at the UN and other multilateral cyber processes, to make sure countries are able to develop national strategies that reflect the political importance of these issues. However, from this region, only Serbia is a member of the GFCE. We welcome other Western Balkan countries to join. It is important that countries have the capacity and expertise to participate in these international processes, because if you're not actively participating, other people are steering your future.

CYBERSECURITY AND CYBER CRIME

Vilma Tomco, Director General, National Authority for Electronic Certification and Cyber Security of Albania

The pandemic has shown us how moving activities online provides more opportunities for cyber criminals, and thus also demonstrated the importance of cybersecurity expertise. Establishing national computer emergency response teams (CERTs) and adopting national strategies are the most important elements for a country's efforts to enhance cybersecurity. National cyber strategies must include all actors (national banks, police, as well as defense agencies and CERTs). Such strategies should focus on protecting critical information infrastructure and establishing relationships between these actors.

Another important part of cybersecurity efforts is improving awareness among citizens at all levels, from children to adults and senior citizens, about the threat of cyber crime and steps they can take to protect themselves. The National Authority for Electronic Certification and Cyber Security of Albania has set up a website for citizens to report illegal online content (e.g., illegal gambling and child sexual abuse material), and an e-game to teach children what to do when they encounter an issue online. This has proven successful and is being distributed for teachers to use in the classroom.

INFORMATION DISORDER

Filip Stojanovski, Director, Partnership and Resource Development, Metamorphosis Foundation

Disinformation in the region is being used as part of hybrid warfare, as a non-military means to defeat one's enemy. Distrust in democratic systems and institutions contributes to the success of these campaigns, and multistakeholder cooperation is key to addressing them. The pandemic has also created a situation ripe for disinformation, as it increased widespread mistrust of government institutions with citizens suspecting that governments were misrepresenting data related to the pandemic, or failing to be transparent about justifications for lockdowns and other restrictions.

Metamorphosis Foundation has been working on combating disinformation for over a decade, approaching the issue from a human rights perspective. Metamorphosis' efforts began with political fact-checking of digital and social media outlets, and then expanded to include fact-checking traditional media outlets and trying to improve journalistic education, and then expanded again to address disinformation spread through word of mouth. In addition to fact-checking programs, Metamorphosis' activities have included building capacity in cybersecurity, journalism, and the public to understand the issues around disinformation and improve critical thinking. It also created a regional network (antidisinfo.net) to combat cross-border disinformation. Disinformation has the potential to impact many countries and unless it is addressed at a systemic level it will continue to have adverse effects on societies.

Nikolaos Panagiotou, Associate Professor, Peace Journalism Lab, School of Journalism and Mass Communications, Aristotle University of Thessaloniki

There are many good initiatives in the Western Balkans to address disinformation, but what is missing is coordination of these efforts. In combating disinformation, we are facing entities that are well-organized and structured. We need to have a strong network to effectively deal with these threats.

Fake News Hunters is one example of an effort to combat disinformation across borders. This initiative started in 2020, and was not focused on fact-checking, because we saw that despite the existence of good fact-checking sites and initiatives, people were still willing to believe and distribute fake news stories. Instead, Fake News Hunters seeks to complement other efforts by analyzing the discourses that allow fake news narratives to circulate and flourish and comparing and contrasting them in different countries. An important element of this work was to analyze the discourses upon which fake news can be built, and alert societies to potential disinformation campaigns. In its analysis, Fake News Hunters found that the five top stories in the countries under examination were identical. We are dealing with entities that have a specific aim in spreading fake news: attacking democracies, breaking down trust in democratic institutions, and promoting a positive image of their own countries or entities. This was especially clear in fake news stories spread to enhance positive images of certain countries' COVID vaccines.

It is clear that the response to disinformation campaigns should not just be technological, but requires strengthening democracy and related institutions, and working through cross-border networks.

CONCLUDING REMARKS

Franziska Klopfer, Project Coordinator, Europe and Central Asia Division, Geneva Centre for Security Sector Governance (DCAF)

The speakers and discussion at the meeting brought out four main points, which are also reinforced by DCAF's own efforts in the region.

First, any progress on cybersecurity has to be context-specific and targeted. One assistance model cannot be applied to all countries in the Western Balkans, as many countries in this region have made progress on various aspects of cyber capacity and policy, and any additional support should work with the capacities already in place.

Second, cybersecurity is an issue that transverses many policy areas, and it is important to mainstream it across the policy landscape. Capacity should be developed in all policy areas to work on cyber-related issues. In particular, capacity must be developed in cyber diplomacy, in order to give countries an opportunity to engage in the international processes such as the OEWG and GGE. At the present, cybersecurity is not yet at the highest political priority.

Third, it is important to seize opportunities to engage in regional and international cooperation on cybersecurity matters, including disinformation. Working together at the political level on one issue can advance cooperation on others such as implementing cyber norms and confidence-building. Regional cooperation on capacity building provides an opportunity for Western Balkans countries to learn from the experiences of their peers. Countries should consider joining the GFCE or perhaps explore ideas such as creating a Western Balkans regional hub for cyber capacity building.

Fourth, there is a need for greater coordination at the level of donors and implementers. There are many actors in the region, including the Regional Cooperation Council, the OSCE, the U.S., U.K., the Netherlands, and ITU. It is important to think about ways these actors can coordinate their efforts to avoid overlap and redundancies. Solutions could include setting up networks of organizations that work on similar issues, creating pooled funds for projects, or formalized discussions between donors and implementers.

RESOURCES SHARED DURING THE MEETING:

- The OSCE online course on Confidence Building Measures in Cyber: elearning.osce.org
- DCAF's cyber capacity building project for the Western Balkans, which held its final conference in March 2021: https://dcaf.ch/cyber-resilience-and-cybersecurity-capacity-building-western-balkans
- GFCE website: www.thegfce.org
- The GFCE Cybil portal that collects information on projects, best practices and other resources for cyber capacity building: https://cybilportal.org/actors/gfce/
- The Digital Watch observatory run by the Geneva Internet Platform provides information and updates on the UN Open-ended Working Group and Group of Governmental Experts: https://dig.watch/processes/un-gge
- Western Balkans Digital Summit is a high level event where cyber is one of the main streams of discussion: https://digitalsummitwb6.com/about-the-digital-summit/
- Diplo's Cybersecurity Diplomacy online course: https://www.diplomacy.edu/courses/cybersecurity-diplomacy
- "Inside Cyber Diplomacy" podcast that discusses international developments related to cybersecurity and relevant negotiations: https://www.csis.org/podcasts/inside-cyber-diplomacy
- Digital Communication Network Southeast Europe Hub: http://dcn-see.org/
- Peace Journalism Lab: http://pjl.jour.auth.gr/welcome/
- Website of the Critical Thinking for Mediawise Citizens - CriThink project launched by Metamorphosis Foundation. The project aims to promote media literacy as a basis for preserving the right of citizens to have different opinions, by stimulating a culture of critical thinking, pluralism of opinions and democratic values: https://crithink.mk/
- Metamorphosis Foundation's political fact-checking and discourse analysis website: Truthmeter.mk
- Anti-Disinformation Network for the Balkans: antidisinfo.net