Global Cyber Policy Dialogues: Western Balkans

September 20-21, 2023

Skopje, North Macedonia

MEETING SUMMARY

Republic of North Macedonia
Ministry of Defence

ВОЕНА АКАДЕМИЈА

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

METAMORPHOSIS
Foundation for Internet and Society

On September 20-21, 2023, the Observer Research Foundation America, in partnership with the Ministry of Defence North Macedonia - Military Academy “General Mihailo Apostolski,” the Ministry of Foreign Affairs of the Netherlands, and Metamorphosis Foundation, hosted an in-person Global Cyber Policy Dialogue in Skopje, North Macedonia. This multistakeholder meeting brought together over sixty participants from government, civil society, academia, and the private sector from across the Western Balkans. The meeting was designed to foster genuine, open dialogue among stakeholders from different sectors and backgrounds, and included representatives from Albania, Bosnia and Herzegovina, Kosovo[1], Montenegro, North Macedonia, and Serbia.

This meeting built on results achieved at a prior, in-person roundtable, held with representatives from government, civil society, and the private sector in Skopje in June 2022, and an earlier online session in April 2021. These earlier meetings addressed donor coordination, cyber defense, CERT cooperation, information disorder, and combating cybercrime.

The September 2023 in-person conference provided an additional opportunity to break down barriers regionally, nationally, and across sectors, facilitated mutual engagement on influencing United Nations (UN) processes, bolstered stakeholder collaboration, and stimulated networking. Themes included the importance of capacity building, information sharing, transparency, multistakeholder engagement, norms implementation, and training initiatives to address specific educational needs. The event included a table-top exercise on cross-border communication during a cyber-induced crisis in the Western Balkans and four, moderated, roundtable conversations about donor coordination and capacity building, defending and responding to cyber attacks, UN norms implementation and cyber diplomacy, and intragovernmental coordination on cybersecurity. Participants also received a briefing on North Macedonia’s progress fighting disinformation.

The dialogue began with opening remarks from North Macedonian deputy prime minister in charge of good governance policies Slavica Grkovska and included a reception on the evening of day one hosted by the Dutch Ambassador to North Macedonia where the delegates connected and shared perspectives and viewpoints on an informal basis. All working sessions were conducted in roundtable format under the Chatham House Rule to maximize participation and diversity of viewpoints.

This dialogue was convened as part of the Global Cyber Policy Dialogue Series, a project undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands, which seeks to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity building initiatives. These meetings are intended to complement and inform ongoing international-level cyber norms processes, such as the UN Open-ended Working Group on Security of and in the Use of ICTs (OEWG) and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Ad Hoc Committee).

Day 1 - September 20, 2023

Welcoming remarks were provided by Slavica Grkovska (Deputy Prime Minister in charge of Good Governance Policies of North Macedonia), Vladimir Anchev (State Secretary, Ministry of Defence of North Macedonia), Maartje Peters (Head of the Taskforce International Cyber Policy at the Ministry of Foreign Affairs of the Netherlands), and Mitko Bogdanoski (Dean, Military Academy "General Mihajlo Apostolski").

The opening speakers emphasized that state-on-state conflict is now a reality in cyberspace. In response, democratic governments in the Western Balkans have to work to strengthen the resilience of citizens and institutions, prevent cyber attacks, protect personal information, and counter disinformation. For example,

[1] 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.

following a public awareness campaign, North Macedonia has seen a surge in registrations with CERTs and cybersecurity training signups. Partnerships and coordination with NATO, the European Union, the United States, and other actors have proven valuable for North Macedonia and other Western Balkan governments in meeting these threats.

Officials explained that following the Russia-Ukraine war, cyber attacks have been conducted in tandem with kinetic warfare. Capacity building is essential to improve whole-of-society resilience. And that will require investments in cyber defense and public awareness. Governments, through the UN, have agreed on norms of responsible state behavior for countering malicious actors in cyberspace. Two speakers emphasized that human rights in cyberspace are an imperative. Bridging the digital divide and expressing new laws in a digital society with layered connections between citizens and government, companies and government is critical to building trust in order to produce an open, free, secure, and inclusive cyberspace.

Table-Top Exercise: Cross-border Communication in the Western Balkans in Times of Cyber Crisis

The Centre for Humanitarian Dialogue organized a table-top exercise to test regional responses to an abstract, major cyber incident that stressed government, industry and civil society at both the operational and policy levels. The exercise built on the realization that the Western Balkans is undergoing accelerated digitization across all segments of society, and that following a string of incidents, cybersecurity has entered the debate at the highest political levels.

Key takeaways included that informal networks at the technical and civil society levels can work well for managing lower-tier cyber problems. However, to prevent unwanted escalation of a serious incident, diplomatic communication and political dialogue are required. These are most efficient if based on previously established relationships of trust. The exercise also illustrated a need for states to put in place cyber crisis management plans that identify in advance actions to be taken, assign responsibilities, and delineate crisis mitigation and management mechanisms. It brought out a need for communication redundancy, since a cyber incident may affect telecommunications in unexpected ways – from low tech to high tech.

Participants noted that international understanding of how international law applies, norms of responsible state behavior in cyberspace, cyber confidence-building measures, and an international cyber capacity-building architecture are all still under development. They found that regional organizations are key to ensure an open, secure, stable, accessible and peaceful environment in which states and civil society can benefit from the immense opportunities for societies across the globe that information and communication technology presents.

Donor Coordination and Capacity Building Needs

Significant progress has been made in donor coordination and capacity building, but there remains work to be done in donor, recipient, and implementer coordination in the Western Balkans. The donor coordination and capacity building needs discussion focused on improving information sharing between domestic, regional, and international organizations, transitioning to an implementation phase for beneficiary projects, reflecting time sensitivities, and ensuring that donors have effectively coordinated their strategies and streamlined assessments to avoid overwhelming beneficiary agencies. With more than 200 multistakeholder members and partners from all regions of the world, the Global Forum on Cyber Expertise (GFCE) is one platform that is well positioned to support this effort. In terms of needs, governments in the region have awoken to the policy imperative to devote funding and resources to cybersecurity considerations as a result of attacks suffered in the Western Balkans from malicious actors in the last 18 months.

Opening remarks were made by Dimitar Bogatinov (North Macedonia Military Academy), Vojtěch Hons (Directorate-General for Neighbourhood and Enlargement Negotiations European Commission), Franziska Klopfer (Geneva Centre for Security Sector Governance (DCAF), Orhan Osmani (International Telecommunication Union), and Gilles Schwoerer (Ministry for Europe and Foreign Affairs of France). The session was moderated by Tereza Horejsova (Global Forum on Cyber Expertise).

On the donor side key guidance included: leveraging existing portals for reporting projects (and reviewing them), such as the Cybil Portal, and ensuring that donors know points of contact for coordination and what metrics to utilize for measuring success. Information sharing between organizations is often inadequate, so this requires curating communication channels for deconfliction to avoid redundancy of programs. In short, capacity building for coordination represents an important focal point for future work. Finally, data accuracy from governments remains an ongoing challenge in the Western Balkans making private sector involvement essential to mitigate lack of data. At the same time, all actors should recognize that emphasizing standards improvement during capacity building is both beneficial and achievable. Joint trainings, interoperability, and legal frameworks can be established even while other project areas are under review. The new Western Balkans Cyber Capacity Center (WB3C) established in Montenegro should play a key role in this effort.

Time was identified as a key factor in several cross-cutting ways. Setting up standard operating procedures cannot happen during a response to a crisis - it must be done in advance. Also, despite improvements, there is still a lack of tools for Western Balkan governments to approach donors and too often donors make last minute requests for proposals out of fiscal considerations. Funding in a rush is difficult to absorb if recipients lack the structure to receive and administer it. Finally, ensuring that implementation meetings and trainings still allow actors on the ground in the region sufficient time to implement projects is critical.

The Western Balkans region is no stranger to post-conflict reconstruction in recent decades and so is uniquely positioned to evaluate the strengths and weaknesses of international donor aid. One key idea from a strategy perspective for all donors, particularly for EU members, is to consider the contributions not as charitable “donations” but as “investments” in capacity that have mutual benefit and tangible, positive effect on EU and donor interests. These investments both enhance regional and international cybersecurity and strengthen integration and collaboration with the European Union. Viewed as investments, donors' mutual buy-in and threshold of effort to ensure their success will likely be greater.

Concurrently, input from beneficiaries will likely evolve to become more selective, based on what they believe will make a difference to enhancing aspects of their cybersecurity. Donor governments have to be willing to listen and act in a supporting role for needed specifics.

Day 2 - September 21, 2023

The three sessions and a briefing on the second day were moderated by Bruce W. McConnell, Distinguished Fellow at ORF America. Welcoming remarks were provided by Azir Aliu, Minister of Information Society and Administration of North Macedonia, who encouraged the participants to think through cybersecurity efforts as a multifaceted set of challenges, and to frame solutions through coordination, training programs, and connections with other states both neighbors and global.

Defending and Responding to Cyber Attacks

The Western Balkans exposure to cyber attacks has intensified during the Russia-Ukraine war, reinforcing the need to further solidify elements of national cyber defense. A massive cyber attack against Albania by a third party in July 2022 highlighted the region’s vulnerability to attacks against public services and critical infrastructure. Spillover attacks crossing borders with collateral consequences are a matter of experience now and societies have to be better prepared to mitigate and prevent them.

This session began with remarks by Mergime Ajdini (Ministry of Defence of North Macedonia), Pavlina Pavlova (CyberPeace Institute), Kujtim Kryeziu (Sentry), Milan Sekuloski (e-Governance Academy), Blazo Georgievski (J6 of the Army, North Macedonia), and Rexhion Qafa (National Authority for Electronic Certification and Cyber Security of Albania). The following points emerged during those remarks and the ensuing discussion.

Pre-planned attacks designed to “prepare the battlefield” for traditional warfare have become more common in military practice. Preventing attacks against civilian infrastructure, for example hospitals, stands out as a significant concern, particularly when they affect vulnerable communities. Greater efforts to prevent escalation in cyberspace should become a key goal for the international community and the Western Balkans region. The Organization for Security and Co-operation in Europe’s framework for addressing these issues through cooperation to counter this class of threat is a model worth considering. Denial of human rights and disruption of critical information infrastructure and e-commerce platforms are no longer hypothetical in the region.

A second theme of discussion was the role of private companies in modern armed conflict and in cybersecurity. For example, decisions by firms like Starlink to permit (or not) the use of commercial satellites to supplement states’ military capabilities, can have strong effects on the battlefield. Whether or not to allow or encourage sales of commercial drone and UAV technology and their underlying software provides a similar concern. The commercialization of cyber threats is on the rise. Moreover, blurred lines between groups (hacktivists or cyber criminals) and states reinforce the need for better attribution capability.

A third topic focused on the merits of developing offensive cyber capabilities to enhance cyber defense, particularly for smaller states. Many participants agreed that developing offensive capabilities to enhance the efficacy of red team exercises was worthwhile, but strictly to improve cyber defense via stress testing. Participants also concurred that any deployment required respecting existing international law and using tools under responsible and ethical international norms, including transparency, accountability, proportionality, and discrimination in use of force. Discussions over active cyber defense are underway and abiding by international humanitarian law is essential with the impact of artificial intelligence looming. One participant proposed that in the future regions like the Western Balkans could encourage “e-safe” labeling on cyber tools to create a safer cyber environment.

The North Macedonian MOD’s experience underscored several important lessons for implementing defense capabilities for smaller or developing economies: unity of command, established legal authority, clarity in scope of responsibility, the importance of multiple incident response teams, and the benefit of international cooperation through NATO and harmonization with Network and Information Systems (NIS) standards.

Regarding governance, improving national and regional response capabilities represents the best path forward but will require clear eyed assessments by leaders in the Western Balkans, trust, and international cooperation. A critical mass of expertise and some trusted networks, like those in Serbia, exist across the region to accomplish this, but such progress will require a political and legal framework that enables coordinated vulnerability disclosure and more robust incident response capabilities. One on-going project, funded by the European Union, is focused on four pillars - cyber governance and awareness, legal and regulatory frameworks, risk management and computer security incident response team capacity building. There are others underway also. Additional investments and complementary efforts are needed. Vulnerability disclosure frameworks represent an area for future exploration in the region.

UN Norms Implementation and Cyber Diplomacy

The Western Balkans are part of an ongoing global process for the implementation of agreements on the normative framework for cyberspace – in particular, norms for responsible state behavior under the UN 2021-2025 OEWG. In addition, the global community has chosen to address cybercrime through the UN Ad Hoc Committee process. This panel explored opportunities and obstacles to increased engagement from Western Balkan stakeholders in cyber diplomacy.

Opening remarks were made by Denisa Asko (Public Prosecutor's Office of Albania), Vladimir Radunović (DiploFoundation), and Marica Ristevska (Ministry of Foreign Affairs of North Macedonia).

During the UN OEWG fifth substantive session in July 2023 the OEWG's annual progress report ultimately was adopted by consensus, but there was significant disagreement before reaching that point. Footnote diplomacy was the only way forward to address a group of states' concerns led by Russia. One key takeaway was that the Western Balkans can do more by coordinating views as a region to maximize impact. This is similar to previous experience in post conflict coordination where, by pooling views in UNESCO, the region was more effective on the issues of greatest importance. Participants explained that from a national and regional perspective, continuing to advocate that smaller states and developing economies receive support for response and recovery to ICT incidents is critical. Attendees flagged that ensuring that cyber capacity building continues at pace, that the global point of contact directory is implemented, and that multistakeholder engagement progresses, especially to bridge gaps on policy, legal, and technical issues, are regional priorities.

At the Ad Hoc Committee on Cybercrime, the slated final session will take place in February 2024. Negotiations are continuing with word-by-word critique and major disagreements persist. Implementation of the agreement, if it goes into effect, will be a real challenge, including for the Western Balkans. Policymakers in the region should be thinking about the legal requirements for harmonizing legislation and law with a new international accord on cybercrime.

Zooming out to look at the larger picture in cyber diplomacy, Western Balkan governments are focusing on digitalization in terms of economic development more than cybersecurity. Important issues arising at the United Nations – artificial intelligence and personal data protection – lack strong Western Balkan voices. Providing an explanation of vulnerabilities and proactively identifying common regional interests represents one path to progress. Participants argued that implementing confidence building measures and adopting norms are practical steps members of the region should be taking now to avoid escalation. Public private partnerships at both the national and regional levels can reduce vulnerabilities in hardware and software and provide a basis for sharing experience on the international stage.

One challenge raised was human resources. Initiatives like the Women in Cyber Fellowship program have had a tangible impact on representation for the Western Balkans at UN negotiations, but more is needed. Developing a cadre of experts and cyber specific training within each state's diplomatic corps needs to be a priority. Moreover, some senior leadership do not understand the topics so they avoid the issues. Finally, cybersecurity training for lawmakers responsible for NIS adherence or authorizing new cyber authorities is essential because these policies shape governments' negotiations.

Broadly, at these negotiations the varying capacities of foreign ministries and governments suggests that the Western Balkans needs to harness non-governmental organizations (NGOs) and academic representatives through multistakeholder tie-ins, briefings, and intersessionals. Greater integrated ICT expertise would help ensure that diplomats do not always have to wait for instructions from capitals if they have stronger knowledge and trust.

Briefing from North Macedonia: Progress Fighting Disinformation

Following the onset of the Russia-Ukraine war, the Western Balkans has been exposed to a heightened level of disinformation from a variety of actors seeking to sow instability by exploiting fissures in society. This information session presented concrete examples of progress from North Macedonia, such as the Western Balkans Anti-Disinformation Hub's work building societal resilience, and NATO's collaboration with the North Macedonian Ministry of Defence's Public Affairs Regional Centre to train communications officers throughout Europe.

The briefing was provided by Aleksandar Jovanovski (Ministry of Defence of North Macedonia), Filip Stojanovski (Metamorphosis Foundation), and Ilija Zhupanoski (Office of the Prime Minister, Government of North Macedonia).

The main takeaway for governments in the Western Balkans based on North Macedonia's experience fighting disinformation is that it requires a whole-of-society approach. When North Macedonia's initial steps generated a backlash, civil society worked to raise public awareness and build trust among different stakeholders. Metamorphosis Foundation crafted a coalition of think-tanks and NGOs from North Macedonia. Two years of consultations with groups outside of civil society formed the basis for the recommendations that were accepted by the government of North Macedonia, which included the creation of a National Strategy for Building Resilience to Malign Influence of Disinformation in its Work Plan for 2024. On methodology, a systematic approach based on inclusiveness that acknowledges high polarization and fragmented ideas has proved to be a workable approach. Implementation is ongoing, but the Western Balkans Disinformation Hub Project supported by the Kingdom of the Netherlands is a key component of the regional approach moving forward to counter disinformation, alongside capacity building efforts supported by the European Union.

The North Macedonia Public Affairs Regional Centre's (PARC) partnership with NATO and ministries of defense - particularly the United States - has been fruitful to build counter disinformation capacity and resilience. This has included building public knowledge, training of trainers, dialogue, executing training obligations, and general awareness raising. The center has supported North Macedonia, Bosnia and Herzegovina, and others in this effort. The organization developed media literacy capability and was structured to tackle disinformation. There are two teams - one on reactive analysis, the other proactively discrediting through transparency. The focus is on providing facts and the intent is to avoid confrontation, so attribution, while undertaken, is generally a lower priority. They also offer courses to the public affairs offices to NATO - focused on detecting and discrediting disinformation.

The biggest challenge for North Macedonia's government and society has been countering efforts by Russia, regional and domestic anti-democratic forces to create distrust in Western countries, in NATO, and the European Union. This strategy is based on exploiting windows of opportunity through different stakeholders to influence policy, media, journalists, and social media in order to shape the narrative on certain issues through disinformation. Adopting a bottom-up approach domestically driven by civil society has proven worthwhile. Obstacles remain - the government's ability to involve all stakeholders is limited, changes in political leadership could alter the thrust of the effort, but several steps have been taken to improve international cooperation. A memorandum of understanding has been signed with the United States on disinformation, North Macedonia is collaborating with NATO and the Estonian government, and there is a process underway to establish a Center of Excellence with the EU on this topic.

Intragovernmental Coordination on Cybersecurity

As governments in the region increase capacity and enhance cybersecurity capabilities to address issues across the spectrum of cyber threats, many new agencies, institutions, and legislative authorities have been established. However, communication and coordination within national governments across multiple organizations' jurisdictions are an ongoing challenge. This session aimed to identify best practices and practical examples of what has worked for interagency coordination in cyberspace and examine how governments can shape communication processes through public facing institutions to reflect and absorb input from the various stakeholders essential to creating durable cybersecurity.

The opening remarks for this session came from Leonora Hasani (Geneva Centre for Security Sector Governance (DCAF), Amir Husić (Ministry of Security of Bosnia and Herzegovina), Maja Lakušić (Regulatory Authority for Electronic Communications and Postal Services of Serbia (RATEL), and Maartje Peters (Ministry of Foreign Affairs of the Netherlands).

Coordination within and among governmental institutions on cyber can be enhanced by a comprehensive national strategy. This typically requires a new legislative approach. Most of the successful models establish supported and supporting agencies, with clear roles and responsibilities. Participants described how agencies need to have a mandate, but in practice things are often foggier. Existing responsibilities should not radically change, but be adapted to circumstance and cooperation with operators and service providers is essential. Getting operators to comply with authorities, measures, and standards leads to trust and deeper cooperation. Having one organization lead the way can reduce the time to implementation, especially when collaborating with external implementers in capacity building to share best practices for knowledge transfer, digital forensics and vulnerability sharing. Governments have to be cognizant of both horizontal and vertical approaches to coordination among and within agencies.

Divisions within the governance structures of several Western Balkan governments have made coordination challenging. For example, in Bosnia and Herzegovina attempts to coordinate public private partnerships face barriers such as expensive market conditions, limited resources, and rising costs of leveraging cyber expertise in the private sector. In some cases, cooperation with academic experts has proven more cost effective. In Serbia, efforts to harmonize with key directives, including the European Union Agency for Cybersecurity (ENISA)'s NIS2 directive, are also underway. Cyber relevant agencies now do have their own CERTs to draw on, and are required both to distribute info in the network and send critical information to the national CERT. Simultaneously, special CERTs for key private sector companies in Serbia have been established, especially in critical information infrastructure, that are also required to send information with the national CERT. Belgrade still faces challenges in facilitating the creation of operations teams assembled to respond to and address high level cyber incidents in ad hoc fashion.

In the Netherlands, government came together across ministries recently to write the national cybersecurity strategy in conjunction with academia and the private sector because effective strategy in this area requires external knowledge. The three major CERTs were integrated into one organization and sharing is mandated. Information shared about the status of ongoing incidents has led to a degree of reciprocity whereby companies will share data and details back with the government. This effort takes significant resources and time to do well. Coordination has been changed with the creation of a national cybersecurity council - multistakeholder group with all of the government. Meetings of this group were able to flag and attempt to manage resulting problems. The approach has been to develop circles of trust by sector, starting with banking and financial institutions. In addition to enhanced coordination and NIS2 implementation, the Dutch government invited ethical hackers to engage and test systems as red team actors. Exchange programs between private sector companies for two- three years of civil service may help with development and alleviate the government's brain drain problem.

Takeaways, Recommendations, and Areas for Research

Subsequent concluding discussion among the participants identified the following key takeaways and areas for potential future projects and research.

Donor Coordination and Capacity Building Needs

- Continue conversations and coordination about capacity building among donors, including with other stakeholders. Provide a platform to identify synergies, update on ongoing initiatives and lessons learned as well as deconflict where necessary.
- Streamline capacity assessments to avoid overwhelming beneficiary agencies and verify that assessments are shared for transparency and improvement.
- Recipients should communicate clearly on their priorities, needs and gaps, ensuring that efforts are complementary and projects can be planned for and carried out efficiently, allowing enough time and resources.
- Donors should view their contributions as mutually beneficial long-term investments in capacity that facilitate common objectives and interests.

Defending and Responding to Cyber Attacks

- Spillover of cyber attacks into civilian infrastructure has detrimental effects on human populations, especially vulnerable communities. Fostering restraint and preventing escalation of attacks affecting public services and civilians should represent a key goal for the international community and the Western Balkans.
- New actors are emerging in armed conflict. Cyber criminal and hacktivist groups have started to play a larger role during the conflict in targeting Ukraine and neighbors. Cyber defenses for societies must be calibrated accordingly. The rise of private corporations as actors in global conflicts, such as Starlink, has unique implications for cybersecurity in both capabilities and attribution.
- Effective incident response is the backbone of cyber defense capability. Resources must be directed to this area. During a regional cyber crisis, informal cross-border networks for communication among practitioners may not suffice to manage escalating international tensions. At the same time, deliberate consideration of the role of offensive cyber capabilities is important, and their adoption must be dictated by international law and respect for norms.
- Establishing legal and regulatory frameworks for internal and cross-border vulnerability disclosure is essential to mitigating threats and incentivizing responsible and collaborative behavior among cyber professionals.

UN Norms Implementation and Cyber Diplomacy

- Achieving Western Balkans goals with respect to international cyber and UN negotiations requires cooperation. Proactively shaping cyber through diplomacy offers better return and outcomes. Experience demonstrates that the region has more clout internationally and can achieve desired outcomes in its interests when it speaks with one voice.
- Diversity and inclusion efforts enhance national capabilities but need sustainment.
- Developing a cadre of experts within each diplomatic corps is a priority. Consider drawing cyber ambassadors who have relevant experience. Provide training and capacity building for policy makers and legislative representatives to increase awareness of the importance of these diplomatic issues. Leveraging NGO and academic expertise through forums and expanded multistakeholder engagement can fill expertise gaps.
- Governments need to begin to consider the implications of implementing a cybercrime treaty and harmonizing their laws if the Ad Hoc Committee on Cybercrime produces a “final” convention in 2024.

Fighting Disinformation

- Whole-of-society approaches driven organically from the bottom have had success in countering disinformation. Mere consultation with multiple stakeholders does not guarantee success.
- Effective approaches to disinformation in the short term may focus less on attribution and more on sharing transparent and publicly available counternarratives to build trust in society.
- Upgrading the legislation in the Western Balkans with EU regulations is crucial, especially harmonization with the Digital Services Act (DSA), the Digital Market Act (DMA) and upcoming policies on artificial intelligence.
- Expanding on the EU's Digital Services Act to ensure that web posts are viewable in chronological order rather than based on link spamming or algorithms driven by upvotes can minimize disinformation.

Intragovernmental Coordination on Cybersecurity

- Information sharing and coordination provide challenges both within and among agencies and departments. Messaging and training around cyber hygiene has proven one effective way to transmit cybersecurity messages across a disparate bureaucracy.
- Establishing circles of trust can aid governments in absorbing contributions from external actors, including in the private sector and civil society.
- Public private partnerships are critical to bridging data or information sharing gaps in addressing problems. Personnel exchange programs between private sector companies and government for 18-36 months may help with development and alleviate regional brain drain for each sector.
- If governments are unable to secure private sector expertise due to higher costs to address problems, academia and NGOs may represent a more fruitful path in some instances to get consultation and input on complex problems and also distribute and receive information.