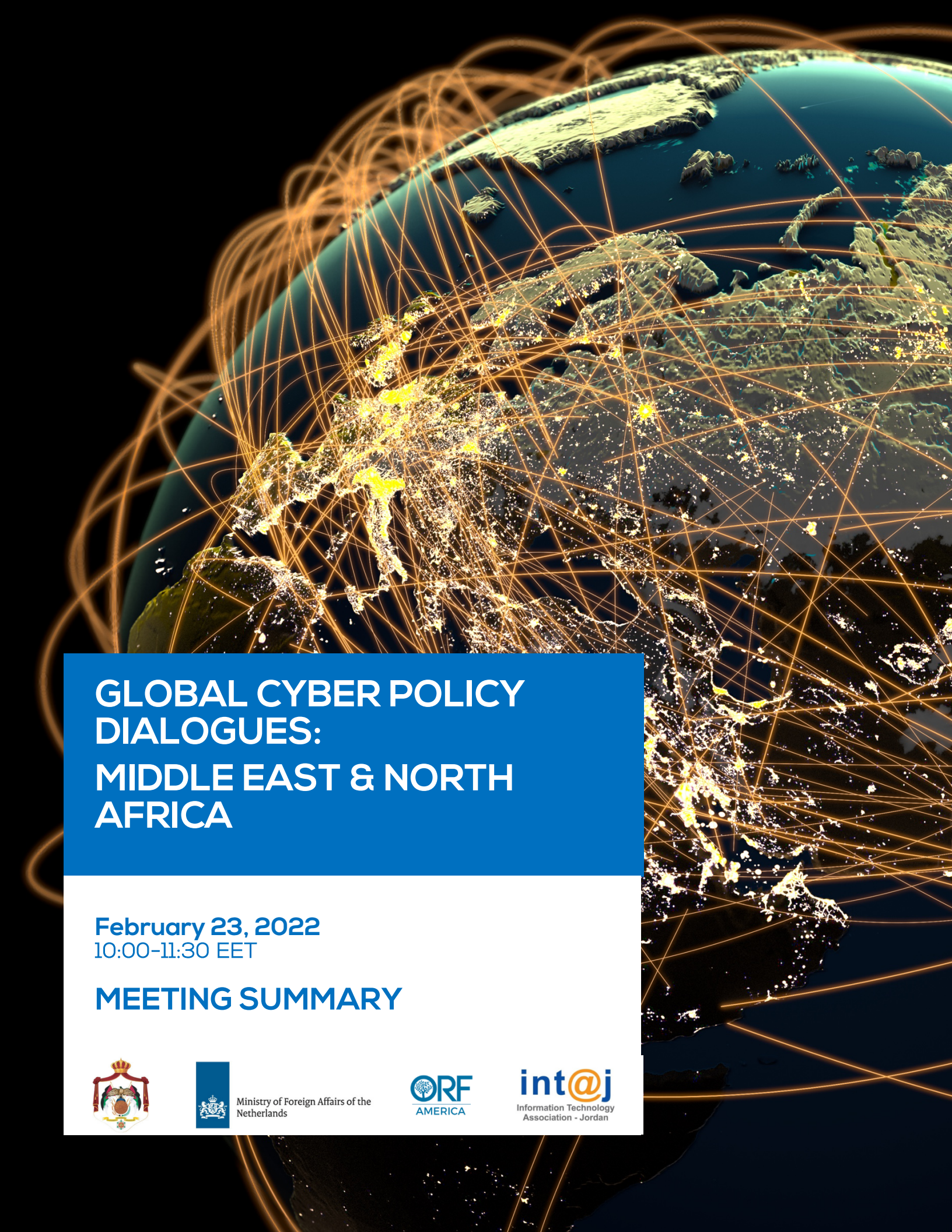

GLOBAL CYBER POLICY DIALOGUES:

MIDDLE EAST & NORTH AFRICA

February 23, 2022
10:00-11:30 EET

MEETING SUMMARY

Ministry of Foreign Affairs of the Netherlands

ORF AMERICA

int@j Information Technology Association - Jordan

Meeting Summary

On February 23, the National Cyber Security Center of Jordan and the Ministry of Foreign Affairs of the Netherlands, in partnership with Observer Research Foundation America (ORF America) and the Information and Communications Technology Association of Jordan (Int@j) hosted the virtual *Global Cyber Policy Dialogues: Middle East and North Africa* meeting. The meeting focused on three interrelated topics: norms of state behavior in cyberspace, cybersecurity and critical infrastructure, and digital development and transformation. In each of these areas, aspects of implementation of national policies, regional cooperation, and capacity building were examined as well as their interlinkages.

This event is part of a larger Global Cyber Dialogue Series being undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands, which seeks to convene regional meetings 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 at the United Nations and other forums.

The meeting kicked off with opening remarks from **Ahmad Milhim**, Head of the National Cyber Security Center of Jordan and **Nathalie Jaarsma**, Ambassador-at-Large for Security Policy and Cyber of the Ministry of Foreign Affairs of the Netherlands.

A panel discussion followed, featuring speakers who spoke on both national and regional dynamics around a wide range of topics including the importance of a coordinated approach to addressing cyber challenges, the links between digital development and cybersecurity, the role of training and awareness-raising in achieving cyber resilience, and the challenge of terrorist use of ICTs to the MENA region.

Summary of Key Points from the Discussion

Ahmad Milhim opened the meeting with an introduction to the National Cyber Security Center of Jordan (NCSC), which was established one year ago. The NCSC is the top national agency mandated by Jordan's national cybersecurity law to protect national information systems, protect critical infrastructure from cyber threats, and establish cooperation programs with peer institutions in the region and globally. He outlined the four strategic objectives of the NCSC as 1) enhancing trust and resilience against cyber threats; 2) understanding and disrupting hostile actions taken against Jordan; 3) developing and deploying appropriate capabilities to respond to cyber attacks; and 4) developing the knowledge, skills, and sustainable sovereign capabilities to maintain robust national cybersecurity. Milhim then pivoted to a regional view, highlighting the main challenge of creating a secure, trusted and safe cyberspace for all. He noted that the United Nations and regional organizations have been discussing norms for many years, and that the current challenge is to figure out how to implement them across the globe. Only by implementing the norms can we create a trusted cyberspace. He finished by affirming Jordan's commitment to cooperation in cyberspace, as this is a shared space where cooperation is necessary to achieve open, sincere discussions.

Nathalie Jaarsma followed, echoing points made by Milhim on the role of trust in cyberspace. She noted that the Netherlands' experience in becoming a leading digital nation had demonstrated that a free, open, and secure cyberspace requires carefully balanced interventions by all stakeholders to promote and protect human rights and avoid replicating societal inequalities. While stakeholders are engaged in such governance interventions, there are two important elements to consider, which revolve around trust: the technical element and the human element. The technical side of trust is citizens' and companies' trust in the security of the digital solutions they rely on in everyday life, including the security of their personal data. The human side of trust is

trust between citizens, companies, and governments that allows for the building of a flourishing digital economy and ecosystem. Both sides of trust are mutually reinforcing and this requires the policy community to be involved in technical processes and vice versa. This improves the ability to address threats and implement policies, and underlines the need to have good collaboration between departments within governments and with other stakeholders. Jaarsma concluded by highlighting three principles that contribute to building trust in cyberspace. First is predictability, which is promoted through the implementation of norms and confidence-building measures as outlined in the normative framework elaborated at the UN, and by cooperation and information sharing across borders. Second is transparency, which can reduce the risk of misperception between actors in cyberspace. States can contribute to transparency by publishing their interpretations of how international law applies in cyberspace. The third principle is inclusivity which is necessary for any international framework to be implemented effectively. She mentioned the importance of local communities taking ownership of cyber capacity building efforts, and that the Global Forum on Cyber Expertise (GFCE) is a leading example of an inclusive approach in this regard and all are invited to participate.

After the opening remarks, a panel of experts tackled issues around norms of state behavior in cyberspace, cybersecurity and critical infrastructure, and digital development and transformation, featuring the following speakers:

- **Omar Nahar**, Ambassador, Ministry of Foreign Affairs of Jordan
- **Nada Khater**, Head, Digital Policies, Ministry of Digital Economy and Entrepreneurship of Jordan
- **Mohammed Aldoub**, Cyber Security Consultant and Trainer
- **Ahmad Elayyan**, Manager, FinCERT Unit, Central Bank of Jordan
- **Yusuf Rousan**, Director, Cyber Policies and Compliance, National Cyber Security Center of Jordan
- **Nidal Bitar**, CEO, Information and Communications Technology Association of Jordan

The panel was moderated by **Bruce W. McConnell**, Distinguished Fellow, ORF America. The following sections highlight key themes from the discussion.

Coordination—both within states and internationally, including with the private sector and civil society—is crucial to addressing cyber threats.

Omar Nahar set the tone for the panel discussion by emphasizing the interconnected nature of cyberspace. No nation's critical infrastructure is safe in isolation, he said, as cyberspace is a shared space. Building common understanding to achieve international agreements is required for cyber resilience and digital prosperity, and Nahar noted the work of the UN to achieve consensus on three tracks: norms of responsible behavior, combating cybercrime, and developing export control mechanisms on offensive cyber capabilities. He highlighted how cybersecurity is intertwined with other threads that bind states, meaning that if the political, economic, or military ties of states are at odds then their cyber relations will also be. This is related to the trend (and necessity) of countries adopting institutional approaches to cyber and integrating it into their diplomacy.

Yusuf Rousan also emphasized the importance of cooperation on cybersecurity as he discussed Jordan's efforts in this regard. In particular, he noted that, through the National Cyber Security Center, Jordan encourages exchanges of best practices on governance and cybersecurity structures, standards, national critical infrastructure protection, as well as computer emergency response team (CERT) cooperation. The center also convenes joint education, exercises and trainings, and workshops. Bruce McConnell asked about efforts to promote cross-border cooperation between CERTs. Rousan noted that Jordan is working on cooperation between agencies on the national level and laying the groundwork for eventual cooperation with regional CERTs and agencies. Ahmad Elayyan added that, in the finance sector, international CERT cooperation is already

happening. The Central Bank of Jordan established a CERT for the financial sector, FinCERT, which is planning to work internationally with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the international CERT network, FIRST. Jaarsma endorsed FIRST as a trusted network that the Dutch National Cyber Security Center also works with. She noted that working through challenges together has contributed to trust within networks, particularly in the technical community. Other networks, such as the points of contact network established in the OSCE are still working on building those trusted relationships. Nahar endorsed the idea of points of contact networks as a way for officials to contact each other in a timely manner on both technical and policy matters. Mohammed Aldoub echoed the point about the value of technical networks and relationships. He noted that official channels of communication are often more reserved and slower, and cybersecurity issues need to be handled fast. He pointed to the existence of trusted relationships between cybersecurity professionals, who will often use private relationships and channels such as WhatsApp to communicate and fast-track such issues in a crisis. While official channels are important, it can be valuable to have this unofficial layer on top of the official processes. This is happening within the Gulf region, but also with partners in Southeast Asia, the U.S., and EU.

Nahar acknowledged that technology companies and other actors have a big stake in digital global affairs and governments must engage with them. This topic of collaboration with the private sector was mentioned by many speakers. Jaarsma noted that while governments tend to think in terms of regulations—which are needed, the reality is that the majority of the Internet is owned by the private sector. Thus, a multistakeholder approach to cyberspace governance is crucial. She noted the responsibility of governments to identify what kinds of values they want to see reflected in cyberspace, which should correspond to the kinds of regulations they enact, but also cautioned against over-regulation. Both Jaarsma and Nidal Bitar emphasized that regulations can be used to encourage growth and innovation. To illustrate the importance of innovation, Bitar shared the example of Int@j's cybersecurity start-up incubator, which was launched recently and encouraged the public sector to be more involved in these kinds of initiatives. He also noted that regulations should take into account awareness, rapid response, agility, and trust.

The links between digitization and cybersecurity must be recognized and strengthened.

Nada Khater spoke about digital transformation in Jordan, highlighting the connection between the digital development community and the cybersecurity community. She pointed out that the growth of the Internet and digital technologies present opportunities for Jordan and other countries. Technology can support Jordan's prosperity agenda through social mobility and inclusion. However, an information society and its various e-services cannot exist without cybersecurity and respect for human rights. Similarly, Nidal Bitar warned that the more digital transformation happens, the more the prospective threats grow. Bruce McConnell noted that this was highlighted during COVID as more services and activities moved online and new threat nodes became evident. Ahmad Elayyan agreed, sharing that the remote work and e-services offered during the pandemic changed how financial services conducted their threat modeling as new entry and exit points were opened up.

Mohammed Aldoub also spoke to the impact of the COVID-19 pandemic on cybersecurity as well as broader digitalization policies. He noted that existing laws governing the permission to record something were tested as people had to figure out how they applied to online meetings. He emphasized that the law is usually slow to catch up to realities on the ground, and countries should be encouraged to review policies and tools put in place during the pandemic. For example, Kuwait is currently in the process of turning off various tracking apps used for contact tracing.

The role of capacity building in the digitization/cybersecurity intersection was also raised by several speakers. Khater emphasized that building capacities in emerging technologies is part of digital transformation and includes elements such as establishing curriculums to ensure that future talent is developed, and creating

training and career paths for cyber professionals. Cybersecurity capacity is about more than just technology, it is the human element that makes the difference and must be invested in. Bitar also endorsed the need for more cyber training and capacity building on all levels, including starting in primary school. In this context he also raised the potential of public-private partnerships again, as important mechanisms for enhancing cyber capacities and also ensuring a link between digitization and cybersecurity. He encouraged governments to consider the need to encourage innovation when designing regulations and other rules in the cyber realm.

Training and awareness are key to achieving cyber resilience.

Building on the above-mentioned linkages between digitization and cybersecurity, many speakers raised the need to ensure adequate training in cybersecurity and resilience and raise awareness about cybersecurity issues at all levels, from the political to the everyday user/citizen. Mohammed Aldoub addressed this in his remarks, noting the need for pipelined education programs focused on cybersecurity through the university level. He also applauded programs that put communities at the center, citing bug bounty programs that have been established in the region. Ahmad Elayyan also took up this theme, elaborating on the experience of the Central Bank of Jordan (CBJ). The CBJ established FinCERT to strengthen cybersecurity protections at the sectoral level. The CBJ is also establishing a procedural cybersecurity framework that will serve as a risk mitigation measure and assessment tool to identify gaps in current cybersecurity procedures. Yusuf Rousan also spoke to Jordan's experience building up its cyber resilience. He noted that Jordan was one of the countries that recognized cybersecurity and its impact on national security early, and that part of the NCSC's vision is a Jordan that is confident, secure, and resilient to cyber threats. He noted that Jordan does face cyber challenges, including skills shortages and lack of cybersecurity awareness.

The threat of extremism and radicalization fueled by disinformation and technology is a challenge for the MENA region.

Another important challenge facing Jordan and the broader region was mentioned by Yusuf Rousan: the use of ICTs by radicals and extremists to spread their ideology. He noted that this threat highlights the need to take an integrated approach to cyber threats and that all countries must do their best to share capacities that make cyberspace more resilient and limit chances for terrorist groups to act through the cyber domain. Mohammed Aldoub also mentioned this challenge, particularly in the context of speech and content laws. COVID has led to the broadcast of university lectures online. This change creates a new context for speech and expression traditionally permitted within the physical spaces of universities in Kuwait. Nahar also called on governments to be aware of the ways in which the younger generations are more tech savvy and thus the need to address extremism and radicalization before it can hit these succeeding generations.

Looking Ahead

In an effort to contribute to the move from discussion to action, the following areas were identified for further engagement:

1. **Identifying or building mechanisms for regional cooperation.** Jordan is in the midst of building its national cybersecurity institutions and cooperative mechanisms. Cooperation with peer institutions was identified as next up on the agenda. Future engagements could include organizing a regional workshop for CERTs to exchange best practices and strengthen relationships. Another effort could focus on supporting the implementation of elements of the normative framework such as the creation of points of contact network for the MENA region, or identifying other avenues for regional cooperation, building on informal networks that already exist, and the formal institutions and capabilities being set up within governments.

2. **Establishing and evaluating regional approaches to countering radicalization and extremism, particularly the intersections with technology.** The use of ICTs by extremist groups was cited as an important challenge for the region, and there are several ongoing initiatives to address aspects of this issue, including the UN norm on international cooperation to address terrorist use of the internet and ICTs (2015 GGE norm d). A future effort could examine existing efforts to address this challenge, identifying best practices, and room for improvement, including capacity gaps, while fully respecting human rights and fundamental freedoms.
3. **Creation of a capacity building agenda for the region to address training and awareness gaps and facilitate partnerships between countries.** While it is clear that several countries are undertaking institutional and integrated approaches to cybersecurity challenges and digitalization, attention could be devoted to facilitating a more regional approach that addresses the cross-border nature of cyber threats. A more in-depth effort focused on regional capacity needs and as well as existing strengths could result in a regional capacity building agenda that facilitates two-partnerships between countries in the region and more broadly.
4. **Exploration of the role of the private sector.** The role of the private sector and the need to engage private companies was a common theme in this meeting. More meaningful conversation with the private sector could be useful in furthering implementation of the international framework for cyber stability and addressing cybersecurity challenges. A series of engagements that bring together private sector actors from a variety of industries could provide a stage to explore the opportunities for partnerships, and impacts of international agreements on private businesses as well as their role in implementation.