CYBER STABILITY CONFERENCE

STRENGTHENING GLOBAL ENGAGEMENT 2019

SUMMARY REPORT

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

UNIDIR's Security and Technology Programme is supported by the Governments of the Netherlands, Norway and Switzerland.

Garrett Hinck, Junior Fellow, Nuclear Policy Program and Cyber Policy Initiative at the Carnegie Endowment for International Peace, served as rapporteur for the conference. Oleg Demidov of UNIDIR also contributed to this report.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to a variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and Governments. UNIDIR activities are funded by contributions from Governments and donor foundations.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning

www.unidir.org

CONTENT

1 Introduction 1

2 Summary of Discussions 2

Opening and Welcoming Remarks 2

Spreading the Benefits of a Secure and Stable Cyberspace 2

Building Productive Multi-Stakeholder Engagement 3

Operationalizing Norms with the Private Sector and Technical Communities 4

Building Cyber Stability within the United Nations Framework: The Way Forward 5

3 Key Takeaways 7

Multi-stakeholder Engagement 7

Complementarity of the GGE and OEWG Processes 7

Operationalizing Norms 8

Future Progress on Norms 8

Capacity-Building 9

Annex 1 Agenda 10

List of abbreviations

CBMs	confidence-building measures
GGE	Group of Governmental Experts
ICT	information and communications technology
OEWG	Open-Ended Working Group

1 Introduction

Conflict related to information and communications technologies (ICTs) is a matter of deep and growing international concern for both State and non-State actors. In 2018, the Secretary-General warned that, "malicious acts in cyberspace are contributing to diminishing trust among States".[1] At its seventy-third Session, the General Assembly established two processes focused on ICT-related issues in the context of international peace and security: a sixth Group of Governmental Experts (GGE)[2] and, for the first time, an Open-Ended Working Group (OEWG).[3] These two Member State-led processes are in the company of a variety of other processes underway in the international environment, some multi-stakeholder, some very specialized. In the last year alone, States and non-State actors have announced additional initiatives on this issue, such as the Paris Call for Trust and Security in Cyberspace and the Cybersecurity Tech Accord. These efforts show mounting international interest in ICT-related international security issues but raise questions about how such initiatives could be complementary to the multilateral processes in a productive way.

At the United Nations, the GGE and OEWG build on work on "developments in the field of information and telecommunications in the context of international security" going back to 1998 and five previous GGEs. Three consensus reports from the GGEs now form the basis for many discussions of these issues in other forums and contexts. In particular, the 2013 GGE's consensus report recognized that international law and the Charter of the United Nations are applicable to cyberspace, and the 2015 GGE report put forward a list of 11 voluntary and non-binding norms for responsible State behaviour in cyberspace. These two outcomes have become the basis for global discussions on norms and responsible State behaviour. However, in 2017, the fifth GGE did not reach consensus on a report. The establishment of the sixth GGE and the OEWG provides opportunities for resuming momentum for advancing discussions at the multilateral level of ICT-related issues in the peace and security context and broadening the conversation to include more stakeholders.

Strengthening global engagement was thus the key focus of UNIDIR's 2019 Cyber Stability Conference, held in New York on 6 June 2019. The conference brought together over 120 representatives from government, the private sector, the technical community, academia, and civil society to explore how the GGE and OEWG could advance efforts to promote a secure and stable cyberspace, how multi-stakeholder engagement can contribute to these efforts, and how private sector actors and technical communities can operationalize existing norms; and to map the way forward for ensuring and strengthening cyber stability within the United Nations framework. Through the lens of these topics, participants discussed the mandates of the GGE and OEWG, how both processes could produce complementary outcomes, and how capacity-building can contribute to strengthening global cybersecurity.

This summary report identifies the main issues discussed as well as key takeaways from the conference.

[1] *Securing Our Common Future: An Agenda for Disarmament*, United Nations Office for Disarmament Affairs, 2018.

[2] See General Assembly, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/RES/73/266, 2 January 2019.

[3] See General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/RES/73/27, 11 December 2018.

2 Summary of Discussions

OPENING AND WELCOMING REMARKS

- **Kerstin Vignard**, Deputy Director, UNIDIR
- **Izumi Nakamitsu**, Under-Secretary-General and High Representative for Disarmament Affairs

As cyber threats to international peace and security mount across the globe, engagement among States and other actors should be strengthened to confront them. The establishment of the GGE and OEWG show that States are convinced of the urgency of the challenge and taking steps to address it, even if there are significant disagreements about how best to do so and with whom.

As so much is at stake in these processes, both speakers encouraged participants to consider three factors that will enhance the possibility of successful outcomes: 1) building on past work, 2) developing a strategic vision for global cyber stability, and 3) providing opportunities for input and ensuring that the views and concerns of a broad range of relevant stakeholders are taken into account.

Against this context, speakers at the conference's opening provided a substantive highlight of a number of issues falling under the scope of these three action items. Thus, for building on past work, the speakers noted that the cumulative record of the past five GGEs provides a nascent but coherent framework for addressing existing and emerging cyber threats, application of international law to cyberspace activities, voluntary norms of state behavior, and confidence-building measures (CBMs).

In order to build a strategic vision for global cyber stability, the speakers encouraged Member States to consider how they can ensure that the OEWG and GGE contribute to complementary outcomes, with the High Representative suggesting that perhaps the OEWG could focus on CBMs and implementation while the GGE could focus on more technical issues. Another message to the Member States from the speakers was to think of a longer-term vision of multilateral cybersecurity discussions after the end of the OEWG and GGE processes, and how States could advance cyber stability in different forums and consider the views of coming generations in these efforts.

Finally, with regard to including all relevant stakeholders in a transparent and inclusive process, the speakers focused on how private sector and technical actors can work with the public sector to strengthen cybersecurity. Several recent initiatives by private sector actors were mentioned, including the Cybersecurity Tech Accord and the Charter of Trust, that could be complementary with the already agreed GGE norms. It was also noted that the OEWG, through the mechanism of intersessional consultations, provides States and the private sector with an opportunity to come together for the first time in a United Nations process to move multistakeholder engagement on these issues forward.

SPREADING THE BENEFITS OF A SECURE AND STABLE CYBERSPACE

- **James Lewis,** Senior Vice President and Director, Technology Policy Program, Center for Strategic and International Studies (moderator)
- **Frédérick Douzet,** Professor, French Institute of Geopolitics, Paris 8 University; Center GEODE
- **Nora Mulira,** Board Member, Uganda Communications Commission
- **Tim Maurer,** Co-director of the Cyber Policy Initiative, Fellow, Carnegie Endowment for International Peace

Incentives for States to engage in discussions on cyber stability in order to come to consensus on principal issues was a major theme of the session. Participants discussed what might motivate agreement in the OEWG and GGE and ensure productive cooperation between the two processes. The worsening threat environment might have the positive effect of putting more pressure on States to come to agreement, especially as threats in areas such as the financial sector have come to affect both developed and developing States. Some suggested that the current environment is not conducive to finding common ground on fundamental norms and principles, many of which are grounded in national identity and deeply held societal values where compromise is rarely accorded. Some panellists also identified the issue of State responsibility, including the scope and limitations of competencies and obligations of States in cyberspace, as a potential area for fruitful discussions and cautioned against focusing solely on armed conflict.

The interdependencies between cybersecurity and development could be an entry point and incentive for more States to participate in the discussions. Growing dependence on ICTs for economic growth due to global and cross-sectoral digital transformation means that all States have an interest in a stable cyber environment. Some panellists discussed how those States that are "newcomers" to the United Nations-led multilateral cybersecurity discussions could contextualize work on cybersecurity in the context of their social and economic development. The speakers agreed that the communities discussing cybersecurity and development mostly operate in silos and without coordination between them. Exploring the interdependencies and mutual impacts of cybersecurity and social and economic development was emphasized as another potential area of work for the OEWG, especially in terms of how momentum within the private sector might be harnessed to promote development goals.

BUILDING PRODUCTIVE MULTI-STAKEHOLDER ENGAGEMENT

- **Alex Grigsby**, Senior Associate, Macro Advisory Partners LLP (moderator)
- **Kerry-Ann Barrett**, Cyber Security Policy Specialist, Cyber Security Program, Inter-American Committee against Terrorism, Secretariat for Multidimensional Security at the Organization of American States
- **Olaf Kolkman**, Chief Internet Technology Officer, Internet Society
- **Sheetal Kumar**, Programme Lead, Global Partners Digital
- **Jan Neutze**, Senior Director, Digital Diplomacy and Head, Cybersecurity and Democracy Team, Microsoft

Multi-stakeholder engagement can enrich efforts for cyber stability in multiple ways, contributing to multilateral processes and discussions, as well as adding value outside of them. However, those ways could be different and specific for each of the stakeholder groups, ranging from the private sector and civil society, to regional organizations and others. This panel considered operationalization of cyber stability and cybersecurity policy norms led by stakeholders other than States.

Recent private sector initiatives such as the Cybersecurity Tech Accord were mentioned in the context of its responses to the evolving technology and threat landscape. According to some panellists, the companies leading such initiatives consider not just what rules are needed, but also how the multi-stakeholder community can advance towards the objective of a more peaceful cyberspace. A particular emphasis was placed on strengthening linkages between private sector efforts and cybersecurity capacity- and confidence-building activities at the regional level. As an example, the discussants highlighted that private actors have contributed to the proposal of a set of cybersecurity CBMs to the Organization of American States' ongoing consultations and have become an important part of capacity-building efforts in the Americas.

Civil society plays a variety of roles in efforts and processes aimed at strengthening cyber stability—from research to raising awareness. There is a clear interest from civil society to be actively involved at an early stage in discussions or processes in order to effectively leverage their expertise and share the concerns of their stakeholders. Finally, with regard to the technical community's role, it was emphasized that it could add necessary realism and so provide a nuanced understanding of the complexity of the technological environment to multilateral discussions on ICTs and cybersecurity, including those taking place within United Nations forums.

Another key theme concerned the challenge of building trust and the importance of transparency. One concrete example of a trust-building measure is the sharing of national points of contact on cybersecurity policy and sharing of national policies and legislation at the regional level. The question remains whether there is sufficient trust for such initiatives to be scaled to the international level. The need for greater transparency and clarity in States' cybersecurity-related decision-making, legislation and policy-making processes was emphasized. UNIDIR's Cyber Policy Portal and other publicly available information sources were held up both as reference tools, but also as mechanisms encouraging transparency by consolidating the cybersecurity policies, structures and doctrines of States.

OPERATIONALIZING NORMS WITH THE PRIVATE SECTOR AND TECHNICAL COMMUNITIES

- **Oleg Demidov**, Researcher, Security and Technology Programme, UNIDIR (moderator)
- **Anne-Rachel Inné**, Executive Director of Government Affairs and Public Policy, American Registry for Internet Numbers
- **Chris Nissen**, Director, Asymmetric Threat Response and Supply Chain Security, The MITRE Corporation
- **Andy Purdy**, Chief Security Officer, Huawei Technologies
- **Eva Schulz-Kamm**, Global Head of Government Affairs, Siemens

Norms, rules and principles of responsible behaviour are only one pillar of a broader cyber stability ecosystem, which also includes capacity-building efforts, information-sharing mechanisms, CBMs and cooperation frameworks. The panellists highlighted how efforts beyond the multilateral frameworks contribute to putting norms into practice and how their added value for norm-building processes could be better leveraged. The discussion focused on the specific examples of ensuring security and integrity of ICT supply chains, responsible disclosure and reporting of vulnerabilities in ICT products, and protection of critical information infrastructure.

The panellists highlighted the experience of regional internet registries, such as the American Registry of Internet Numbers, in encouraging best practices among network operators and providing training for policymakers on a wide range of issues such as Internet governance and protection of the Internet infrastructure from cyber threats. Another example given of a cooperation mechanism was MITRE's "Deliver Uncompromised" initiative on supply chain integrity, which is designed to address third-party risks in an untrusted ICT environment.

Trust and accountability were stressed as fundamental prerequisites for the implementation by the private sector of cybersecurity norms and cooperation frameworks. Particular emphasis was placed on how independent third-party review of source code of ICT products could be a way for moving toward objective and transparent mechanisms for the evaluation of cybersecurity risks. The Charter of Trust initiative promoted by Siemens was highlighted as a mechanism that operationalizes the 2015 GGE norm on supply chain integrity by committing its 16 members and their suppliers to baseline supply chain security principles and putting in place mandatory security requirements supporting these principles. Participants also discussed how measures such as information-sharing and setting global standards for security of ICT products, their source code, and supply chains could form the basis for strengthened collaboration among governments and industry on cyber stability.

BUILDING CYBER STABILITY WITHIN THE UNITED NATIONS FRAMEWORK: THE WAY FORWARD

- **Kerstin Vignard**, Deputy Director, UNIDIR (moderator)
- **Jovan Kurbalija**, Executive Director, Secretariat of the Secretary-General's High-Level Panel on Digital Cooperation
- **Izumi Nakamitsu**, Under-Secretary-General and High Representative for Disarmament Affairs
- **Guilherme Patriota**, Special Representative of Brazil to the Conference on Disarmament (video address)

The GGE and OEWG will shape the course of multilateral debates on cybersecurity norms, CBMs and international cooperation on cybersecurity for the coming two years. In addition, there is an increasing emphasis throughout the United Nations system to respond to ICT-driven challenges and to promote a stable cyber environment from which all States can benefit. The vision for and objectives of these efforts led by both the United Nations Secretariat and Member States, as well as their coordination and potential synergy, was the key subject of the discussion at the session.

The discussions demonstrated that there are distinct and sometimes incompatible views on the appropriate division of labour between the OEWG and GGE. Considering the overlap in the language of the two mandates and the limited time accorded to the processes (three and four weeks respectively), a primary challenge for each group will be to adhere to their mandates while not duplicating discussions across both forums. Early buy-in to a coherent division of labour will set up the processes for more productive discussions and maximize the possibilities of two successful processes.

Member States and other interested actors should carefully consider the "value added" by each format and on which issues progress is more likely to be made in a small, closed-door format versus an inclusive and more transparent one.

Various distributions of topics have been proposed. For example, as the OEWG's mandate includes all States as well as a mechanism for engagement with non-State actors such as the private sector and civil society, capacity-building and building productive multi-stakeholder cooperation are an obvious "value added" of the OEWG setting.

The closed-door limited membership of the GGE will inevitably make it a more State-centric conversation. The GGE will also address the perennially divisive topic of international law—its mandate states that national positions on international law can be annexed to the group's report. This is unlikely, however, to keep the topic from being a significant part of the Group's discussions as it has been in each of the five previous GGEs. Drawing on the regional consultations included in the GGE's mandate, the GGE will have rich sources of information to consider how existing norms, rules and principles are being operationalized in different regions.

The two State-led processes are part of a larger, but somewhat poorly understood, ecosystem of other United Nations Secretariat and international initiatives. Some panellists noted that the United Nations can play an important convening role in a divided community with multiple stakeholder groups and that this extends beyond the two processes to efforts like the Internet Governance Forum, the World Summit on the Information Society, and efforts to tackle cybercrime. The Secretary-General has demonstrated personal engagement on these issues—actions to promote cyber stability feature prominently in his Agenda for Disarmament. The Secretary-General has also offered his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace. In order to make the United Nations organization more responsive and better equipped to support Member States on these issues, the Secretariat has recently undertaken an internal mapping exercise on cyber expertise throughout the organization.

In July 2018, the Secretary-General established the High-level Panel on Digital Cooperation as a multi-stakeholder expert group tasked to advance proposals to strengthen cooperation in the digital space among governments, the private sector, civil society, international organizations, academia, the technical community, and other relevant stakeholders. The Panel’s report, released the week after UNIDIR’s Cyber Stability conference, identifies a number of relevant issues and mechanisms for addressing cybersecurity and digital stability challenges. In particular, the Panel highlighted three major gaps: the lack of bridges between forums that cover digital-related issues; the lack of reliable data, metrics, and evidence on which to base policy efforts and interventions on digital security cooperation; and the lack of inclusion of relevant stakeholders such as developing countries, indigenous communities, women, the young and elderly, and those with disabilities.

The conference concluded with the recognition that 2019 starts a new chapter in international efforts to build a more stable and secure cyber environment. All stakeholders have the opportunity through the OEWG and GGE to contribute to this objective.

3 Key Takeaways

MULTI-STAKEHOLDER ENGAGEMENT

For the moment, the different communities within the cybersecurity ecosystem—**States, the private sector, the technical community, civil society, and other actors—remain quite distinct**. There was wide agreement that multi-stakeholder engagement will be an increasingly important aspect of successful cyber stability efforts. The question is **how to ensure that this engagement is not simply a catchphrase**. In order to align expectations in any multi-stakeholder process, it seems necessary to first raise awareness about the United Nations processes before moving into specific consultations in order to ensure that actors with technical and other expertise understand the policy framework already in place.

At the same time, this engagement goes both ways. There remains room for governments to step up their commitment by holding more consultations with other actors. More regular engagement with the technical community could address concerns that there could be a gap between what is negotiated at the policy level and its technical implementation and implications. The opportunities presented by the **OEWG consultations** with industry, non-governmental organizations and academia **should not be missed by both participating governments and interested stakeholder groups**.

COMPLEMENTARITY OF THE GGE AND OEWG PROCESSES

All stakeholders have a role to play and interest in ensuring that the two processes and their outcomes are complementary. As the OEWG and GGE will run in parallel, a primary objective is **to have a consensus report at the end of each process**. While recognizing the similarity of their mandates, for practical purposes and to ensure that their outcomes do not undermine or contradict each other, the OEWG and GGE should **focus on the unique characteristics of each process and their different membership compositions** to take the lead on various topics. For instance, the OEWG's mandate includes a focus on building relationships and drawing on the expertise of non-State actors such as the private sector and civil society. A complementary goal for this closer engagement could be **prioritizing the role of cybersecurity capacity-building in the OEWG process,** so that States could harness the benefits of engagement with non-State actors with mature skills, technical knowledge and capacities. Another approach to leveraging a productive "division of labor" between the two processes might be the **GGE to take the lead on CBMs among States while drawing on the efforts of regional organizations to operationalize existing norms**.

A widely shared concern is **the risk of the two processes arriving at contradictory outcomes**. Discussion focused on how bridges could be built between the two processes in terms of information exchange, coordinating the division of topics, and ensuring communication and cooperation at the level of their Chairs and Secretariats. For instance, the GGE's Member State consultations could be an opportunity for the OEWG to feed into the GGE's discussions. **States with less cyber capacity that have not taken part in previous GGEs will have a forum to articulate their security concerns in the OEWG**—and these are likely to be less homogenous than the concerns focused on in the GGEs thus far. The OEWG could therefore add more nuance to the international understanding of how cyber instability affects States and regions differently.

Another approach to ensuring synergy and coordination between the processes could be to encourage the 25 GGE experts to also participate as part of their OEWG delegation. This idea might resonate with the logic of coordination between the Chairs of both processes.

OPERATIONALIZING NORMS

A major theme of discussion was how to operationalize existing norms of State behaviour. An increasing number of governments are articulating their views on how international law applies in cyberspace, which will be an important framework for operationalizing norms. The work in the GGE and OEWG to discuss the "competencies and obligations of States" could contribute positively to **developing a common understanding of how the GGE norms build on States' existing obligations under international law**. Another potentially fruitful input into the two processes might be legal analysis of past cyber incidents to determine which norms were violated, thereby strengthening the understanding of how international law applies to cyberspace activities.

Yet, **the actors that operationalize cyber norms are not just States but also the private sector and other non-State actors**. In this regard, international efforts need to be promoted beyond norms to include objective and transparent mechanisms that enable levying of consequences against those that violate such norms. One approach to this could be **considering how incentives for private actors can be used to reduce cybersecurity risks**.

These discussions also pointed to a question of how the international community might go about putting these ideas into practice. While the GGE and OEWG may be able to arrive at consensus on broad principles, it may be **more difficult to find agreement on the details of implementation**, which are often regionally or nationally specific in nature. Further, in this regard open processes like the OEWG may offer the awareness-raising benefit of promoting an open discussion of the different ways that norms can be operationalized.

Some actors named within the GGE norms, particularly critical infrastructure providers, are unaware of the GGE recommendations altogether. Therefore, **awareness-raising in communities outside of government is a crucial first step to operationalizing existing norms** and creating a larger community of interested actors that can hold their governments accountable to their commitments. The authority and credibility of the United Nations and the knowledge resources it can provide, such as the training modules being developed by the Office for Disarmament Affairs, can make a significant contribution to raising awareness on cybersecurity norms, diplomacy tools and other instruments.

Finally, **how will the international community organize itself to respond to violations of norms?** What would be the role of the Security Council in responding to a violation of norms? A topic for further discussion should be how would the Security Council exercise its authority under article 39 of the Charter of the United Nations to determine if a threat to or breach of the peace or act of aggression had occurred in cyberspace.

FUTURE PROGRESS ON NORMS

Whether the GGE and OEWG should consider additional norms to those agreed by the GGE in 2013 and 2015 was a key topic of discussion. One view is that **there may be room for new norms**, which could build on proposals from non-State groups such as the Global Commission on the Stability of Cyberspace and from the Paris Call. These new norms could include, for example, protection of the "Public Core of the Internet" or highlighting the protection of particular sectors, such as the financial sector. However, others have recalled that these specific norms (and others) were discussed in previous GGEs and thus it might be worth reflecting on why they did not receive consensus when previously proposed.

One particularly contentious topic was whether a new norm might focus on "malicious content". **Content-related security issues are highly politicized** and States may wish to weigh the risks of bringing these issues to the current multilateral processes considering the limited duration of their mandates. However, there is a desire on the part of some States to discuss this topic and therefore—if it is decided to not address it in the current processes—States might consider the appropriate venue and format where the relationship between security and content could be discussed. Some have articulated a further risk that the focus on malicious digital content could accelerate the fragmentation of the Internet. In this regard, it is useful to recall that these issues have been acknowledged in previous GGE reports while focusing the content of the reports themselves on issues within the purview of First Committee.

There are several **counter-arguments to the idea of developing additional norms.** One is that existing 2013 and 2015 GGE norms already form a solid foundation for responsible State conduct in cyberspace and that the focus of cyber stability efforts should turn to operationalizing and enforcing these norms. Those advocating this position state that having an increasing number of proposed norms that are divorced from actual State practice and thus not operationalized actually undermines the value of the already agreed—and perhaps somewhat neglected—norms. Second, there is a risk that **opening discussions of additional norms could lead to undermining the existing consensus encompassed by the package of the GGE norms**, as well as to excessive regulation of cyberspace and the curtailing of online freedom. Instead, time should be spent focused on considering how best to implement and enforce the existing normative framework.

CAPACITY-BUILDING

Capacity-building is a shared goal of the United Nations cyber norm-building processes and for cybersecurity policy efforts and initiatives undertaken by other actors—for instance, by regional organizations and within the technical community. While there has been a variety of capacity-building activities undertaken around the world, **the OEWG offers the opportunity to hear from a larger group of States about their cybersecurity concerns and thus to better tailor future capacity-building efforts**.

Some have suggested that there may be value in **shifting the framing of capacity-building from cybersecurity to cyber readiness**, a more comprehensive and flexible paradigm encompassing cyber hygiene and digital literacy, cyber resilience and other components.

At the conference, UNIDIR presented its Cyber Policy Portal, a reference tool containing cybersecurity policy information about each Member State. Participants highlighted this as an important tool for building awareness of policymakers of national legislation and strategies in other States. The Portal and similar tools also promote transparency and thus serve as **an incentive for States to share information about their cybersecurity policies, legislation and institutional developments**.

Annex 1
Agenda

Welcome and opening remarks

- **Kerstin Vignard,** Deputy Director, UNIDIR
- **Izumi Nakamitsu,** Under-Secretary-General and High Representative for Disarmament Affairs

Session 1 | Spreading the Benefits of a Secure and Stable Cyberspace

- **James Lewis,** Senior Vice President and Director, Technology Policy Program, Center for Strategic and International Studies (moderator)
- **Frédérick Douzet,** Professor, French Institute of Geopolitics, Paris 8 University; Center GEODE
- **Nora Mulira,** Board Member, Uganda Communications Commission
- **Tim Maurer,** Co-director of the Cyber Policy Initiative, Fellow, Carnegie Endowment for International Peace

Lightning talk | Using the Cyber Policy Portal to Prepare for the OEWG and GGE

- **Oleg Demidov**, Researcher, Security and Technology Programme, UNIDIR

Session 2 | Building Productive Multi-Stakeholder Engagement

- **Alex Grigsby**, Senior Associate, Macro Advisory Partners LLP (moderator)
- **Kerry-Ann Barrett**, Cyber Security Policy Specialist, Cyber Security Program, Inter-American Committee against Terrorism, Secretariat for Multidimensional Security at the Organization of American States
- **Olaf Kolkman**, Chief Internet Technology Officer, Internet Society
- **Sheetal Kumar**, Programme Lead, Global Partners Digital
- **Jan Neutze**, Senior Director, Digital Diplomacy and Head, Cybersecurity and Democracy Team, Microsoft

Lightning talk | Overview of the GGE and OEWG Processes

- **Gillian Goh,** Cyber Team Leader, United Nations Office for Disarmament Affairs

Session 3 | Operationalizing Norms with the Private Sector and Technical Communities

- **Oleg Demidov**, Researcher, Security and Technology Programme, UNIDIR (moderator)
- **Anne-Rachel Inné**, Executive Director of Government Affairs and Public Policy, American Registry for Internet Numbers
- **Chris Nissen**, Director, Asymmetric Threat Response and Supply Chain Security, The MITRE Corporation

- **Andy Purdy**, Chief Security Officer, Huawei Technologies
- **Eva Schulz-Kamm**, Global Head of Government Affairs, Siemens (VTC)

Session 4 | Building Cyber Stability within the United Nations Framework: The Way Forward

- **Kerstin Vignard**, Deputy Director, UNIDIR (moderator)
- **Jovan Kurbalija**, Executive Director, Secretariat of the Secretary-General's High-Level Panel on Digital Cooperation
- **Izumi Nakamitsu**, Under-Secretary-General and High Representative for Disarmament Affairs
- **Guilherme Patriota**, Special Representative of Brazil to the Conference on Disarmament (video address)

Concluding remarks

- **Kerstin Vignard**, Deputy Director, UNIDIR

CYBER STABILITY CONFERENCE

Strengthening global engagement was the key focus of UNIDIR's 2019 Cyber Stability Conference, held in New York on 6 June 2019. The conference brought together representatives from government, the private sector, the technical community, academia, and civil society to explore how the GGE and OEWG can advance efforts to promote a secure and stable cyberspace, how multi-stakeholder engagement can contribute to these efforts, and how private sector actors and technical communities can operationalize existing norms; and to map the way forward for ensuring and strengthening cyber stability within the United Nations framework. Through the lens of these topics, participants discussed the focuses of the GGE and OEWG, how both processes can produce complementary outcomes, and how capacity-building can contribute to strengthening global cybersecurity.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH