UNIDIR

UNIDIR Cyber Stability Conference 2017

ICTs in the Context of International Peace and Security

Current Conditions and Future Approaches

UNIDIR RESOURCES

Acknowledgements

Support for the 2017 Cyber Stability Conference was received from the Governments of Germany and Switzerland.

About UNIDIR

The United Nations Institute for Disarmament Research—an autonomous institute within the United Nations—conducts research on disarmament and security issues. 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 the 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's activities are funded by contributions from governments and donor foundations.

About the Annual Cyber Stability Conference

UNIDIR's annual Cyber Stability Conference presents an ongoing opportunity for stakeholders to discuss how to take pragmatic steps towards a more stable and predictable cybersecurity environment, with a specific focus on the risks of escalation in times of conflict, and the implementation of transparency and confidence-building measures.

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 the delimitation of its frontiers or boundaries.

The views expressed in this publication are the sole responsibility of UNIDIR. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR's sponsors.

The report was drafted by Sebastian Michael Mueller.

www.unidir.org

UNIDIR Cyber Stability Conference 2017

ICTs in the Context of International Peace and Security: Current Conditions and Future Approaches

Conference Report

11 October 2017, UN Headquarters, New York City, USA

Introduction

The ongoing digitalization of almost all aspects of life offers enormous opportunities, including for economic growth, social development and scientific progress. However, the technological dependencies give rise to new potential vulnerabilities. Critical infrastructure, government communications, military assets and electoral processes—to name just a few key services—are increasingly dependent on information and communication technologies (ICTs). ICTs and their use by States and other actors have thus become a matter of international peace and security. Consequently, the international community has undertaken a number of initiatives in order to ensure an open, secure, stable, accessible and peaceful ICT environment. These efforts include discussions held in international, regional and bilateral fora on a normative framework for responsible ICT use, confidence-building measures (CBMs), capacity building and more.

At the United Nations, this has led to the establishment of five Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGEs) since 2004. They have produced three consensus reports in 2010, 2013 and 2015, which form the basis of discussions both at the UN and elsewhere. As the most recent group concluded its work in June 2017 without reaching consensus on a substantive report,[1] some of the most contentious issues of the debate on international cyber security remain unresolved. In particular, the progress made in the 2013 and 2015 reports on the question of how international law is to be applied to States' use of ICTs could not be repeated. Interpretations of how ICTs challenge fundamental concepts such as self-defence, international humanitarian law (IHL) and counter-measures in cyberspace differ.

Beyond the UN, a number of regional organizations and multilateral fora have incorporated cybersecurity matters into their agendas. They have become important venues for continued discussion on these urgent topics of international peace and security, both as sources for innovation and implementation of agreed measures.

Despite the relevance of the processes at the UN and elsewhere to both governmental and non-governmental experts, these efforts have remained poorly understood. UNIDIR's annual Cyber Stability Conference serves the purpose of not only allowing for an expert discussion but also awareness raising among interested stakeholders that were hitherto less involved. Given the unique nature of the ICT environment, stability in cyberspace can only be achieved through the cooperation of all stakeholders.

[1] A procedural report was published as UN document A/72/327.

The Annual Cyber Stability Conference

This was UNIDIR's fifth annual Cyber Stability Conference. The 2017 conference, like previous events in the series, provided a forum for representatives of governments, international and regional organizations as well as civil society to discuss issues pertaining to the international security dimension of ICTs. Until now, the annual Cyber Stability Conference had been held only in Geneva. This year's iteration took place at UN Headquarters in New York on the margins of the First Committee of the General Assembly. The conference took place only a few months after the 2016–2017 GGE had concluded its work without reaching a consensus. It thus provided an opportunity to assess the current situation and discuss possible ways forward. A particular focus was placed on exploring divergent views regarding the application of international law to States' use of ICTs and on how to continue the international debate, in particular the role of the UN, going forward.

Proceedings

Welcoming Remarks

- **Jarmo Sareva**, Director, UNIDIR

Mr Sareva convened the fifth annual Cyber Stability Conference, noting the important timing of the event. The GGEs had altered the political landscape on cooperation in cyberspace, with the 2015 report setting a normative agenda. Furthermore, General Assembly Resolution 70/237 had called upon Member States to be guided by the recommendations of that report. However, over the past year, the fifth GGE had attempted to build upon this progress but concluded without consensus. The First Committee would now consider how to best take the issue forward to ensure a stable and secure cyber environment for all countries as well as the role of the UN in this endeavour.

This year's conference intended to take the next step in the debate through its three panels. The first would discuss the GGE process and cyber within the UN system as it relates to international peace and security. The second panel would discuss divisions in the international community on cyber issues, particularly on how international law applies. The topic of the final panel would be future work both in the UN and beyond.

Mr Sareva reminded participants of UNIDIR's longstanding contribution to the theme of ICTs and international security: from the annual Cyber Stability Conference, to serving as the consultant to the UN GGEs, as well as through analysis such as the 2013 *Cyber Index*, which was currently being transformed into an interactive online tool for policy makers.

Opening Remarks

- **Izumi Nakamitsu**, United Nations Under-Secretary-General and High Representative for Disarmament Affairs

High Representative Nakamitsu welcomed that UNIDIR's annual conference was being held during the First Committee in New York, noting the timeliness of the conference given that the international community is at a critical juncture on how to deal with particular uses of ICTs in international security matters. She also noted that this topic is a top priority of the UN Secretary-General.

Any discussion of the future must take into account past achievements. In this regard, she commended the Chair of the most recent GGE, Mr Karsten Geier of Germany, for his energetic and tireless effort to achieve consensus. As next steps are deliberated, it is important to keep in mind that the three consensus GGE reports serve as a foundation upon which to build. The validity of the 2015 GGE report was without question given the unanimous call in General Assembly resolution 70/237 that Member States be guided by its recommendations. These reports contain a lot of valuable material, for instance on the application of international law, norms, CBMs and capacity building.

One possible way forward for States to consider is to focus on raising awareness of these achievements and consider how to operationalize them. With the support of the Government of Singapore, the UN Office for Disarmament Affairs (UNODA) has started preparing an online training course to that end.

While the size of the GGEs had grown over the years—with initially 15, then 20, then 25 governmental experts—less than 25% of the 193 Member States of the United Nations had participated in the GGE process. Cybersecurity concerns all States and therefore it was perhaps time for a more inclusive space for discussion.

The conference would also consider a path forward. While States had confirmed that the security dimension of ICTs was their responsibility, it was nonetheless important to identify ways to involve the private sector. It is impossible to find an effective solution to the challenges at hand without these stakeholders.

Despite different views expressed within the GGE, all States need an open, accessible, secure and peaceful ICT environment. Cyberspace is becoming increasingly unstable and dangerous. For instance, recently an entire country had been taken off the grid, Wannacry had affected several countries and there was a trend towards manipulating information, so-called "fake news" campaigns. These events had destabilizing effects in several regions of the world. As a consequence, the international community needed to rally together to address these concerns.

In conclusion, the High Representative urged States to engage in sincere dialogue. It is necessary to build upon the work already done and she assured participants that her office is committed to working with Member States in this undertaking.

Session 1: Reviewing the State of Play

- **James Lewis**, Vice President, Center for Strategic and International Studies (Moderator)
- **Kerstin Vignard**, Deputy to the Director, UNIDIR
- **Camino Kavanagh**, Senior Visiting Fellow, Department of War Studies, King's College London

James Lewis opened the first session by introducing the two panellists: Kerstin Vignard, who served as consultant in all but one of the GGEs and Camino Kavanagh, who was a consultant to the 2016–2017 GGE. He also recalled his experience in the three GGEs that led to the 2010, 2013 and 2015 reports. Together the three speakers in this first session represented the consultancy teams of four of the five UN GGEs.

Ms Vignard recognized that UNIDIR has been privileged to serve as consultant to all but the first GGE. The consultancy team and the Secretary of the group (a staff member from UNODA) are the only people inside each meeting of the GGE not associated with a national expert—so they have considerable and unique knowledge about the GGE process from a neutral perspective. Thus the institutional knowledge represented on this panel was truly unique.

In 1998 Russia sponsored the first General Assembly resolution on ICTs and international security. It is hard to imagine today, but at first Russia had to convince many States of the relevance of the topic. While the first GGE, meeting in 2004–2005, could not reach consensus, the 2010 iteration did, and its report—despite its brevity—included a number of key topics. The 2013 report then set the normative agenda of the GGE process, its greatest achievement being the affirmation of the application of international law to States' use of ICTs. The 2015 report added a number of norms, while less progress was achieved on how international law applied to this field.

The mandate for the 2016–2017 group had clearly set the objective of clarifying and operationalizing the 2015 report. Despite its failure, there were fruitful discussions on a number of topics, such as hybrid threats, CBMs and capacity building. Unfortunately, little progress seemed possible on international law and future work. In this regard, she suggested that readers of GGE reports should keep in mind that GGE reports represent negotiated outcomes. Thus it is often more telling what is not in the report, than what is. If one looks at the 2015 GGE report through this lens, one can already see the divergent views. For instance, the group only took "note" of principles of humanitarian law, rather than agreeing on a stronger statement, such as the group agreeing that principles of IHL are applicable in the cyber domain.

Ms Vignard noted that the GGE process is generally poorly understood both outside the UN and even among Member States because the only public information about them are the mandate at the beginning and the report at the end. The GGEs are a closed process without records or the participation of other States, the private sector, or external experts. Thus those outside the process are left to "fill in the blanks" and "read between the lines", which over the years has led to a number of inaccuracies becoming accepted as fact.

Regarding whether the GGEs are an appropriate format for taking forward discussions on the international security dimensions of cyber, she stated that in her view the cyber GGEs could not go on indefinitely. She gave two examples why. First, she argued that instead of serving as an incubator leading to a wider "process"—as GGEs do on other topics—the cyber GGEs themselves became the process. As GGEs have a limited membership, a growing number of States are feeling excluded. In addition, with the changing composition of the group, it was becoming increasingly difficult to hold the line on past GGE achievements. Not all new members to the group believed that the reports were cumulative; rather they believed that issues from past reports could be reopened.

Before turning to the next panellist, **Mr Lewis** echoed Ms Vignard's comment that the consensus reports were the outcome of bargains, some of them not always logical to external observers. He offered the example of the topic of capacity building in the 2010 report, which was the result of a deal between members as only one State had insisted on including it. Since then it has been a full section in all subsequent reports.

Ms Kavanagh highlighted the complementarities of the GGE process with other processes, with the framework for stability established by the GGEs being increasingly picked up by other organizations and actors.

In parallel to the work at the UN, regional organizations had begun to address cybersecurity in a robust way. The OSCE, for example, has established an Informal Working Group and agreed on a number of cyber confidence-building measures. Deliberations on topics related to cybersecurity were also increasingly prominent in the ASEAN Regional Forum, the Shanghai Cooperation Organisation, the Organization of American States, the European Union, the BRICS grouping, the G7 and G20.

Despite this progress, challenges remain: the management of existing and potential threats; expectations after the failure of the most recent GGE; open questions on how to maintain dialogue on issues where consensus remains elusive; implementing what has been already agreed; and capturing the interest of the general public.

Within the UN framework, the work of the GGE is complementary with other processes, such as those considering the relationship between cyber and terrorism, crime, development and human rights. Ms Kavanagh presented a schematic of the UN entities addressing different facets of cyber issues: international peace and security, human rights, and economic and social development (see Figure 1). This mapping is part of a recent UNIDIR study she authored, considering the UN actors involved in this topic as well as recommending steps for more strategic UN engagement. [2]

Looking forward, she suggested that the UN could focus on four activities:

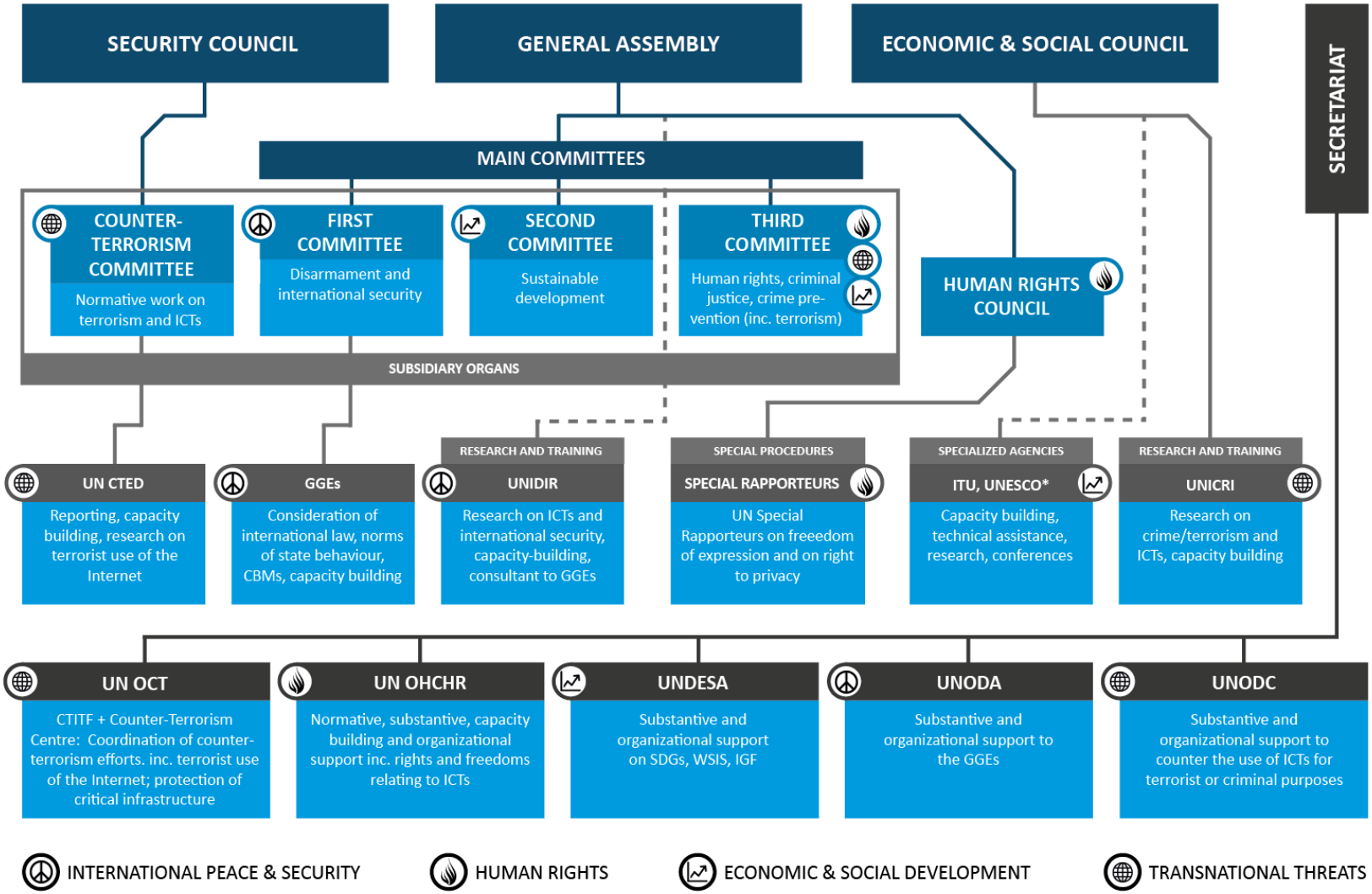
- Awareness raising;
- Capacity building;
- Good offices; and
- Reviewing existing tools.

Reacting to the presentations, **Mr Lewis** asked whether actors other than States could truly address the international security dimension of cyber issues. He asked Ms Vignard what role she saw for the private sector.

Ms Vignard replied that across the board on emerging technology issues, the private sector is in many ways more forward leaning than States on normative development. She pointed to Microsoft's initial proposed norms for State behaviour and its more recent proposal for a "Digital Geneva Convention". That said, States continue to consider that international security issues remain their *domaine réservé* yet reality demonstrates that managing and mitigating cyber threats requires working with the private sector—and States need to find a more productive way of engaging with them on these issues.

[2] *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, UNIDIR, 2017, bit.ly/UNIDIR_UN_Cyberspace.

Figure 1. ICT's international peace and security, and the principal organs of the United Nations



** Specialized agencies are autonomous and are coordinated through ECOSOC at the intergovernmental level*

Ms Kavanagh added how there was an existing body of work on how to include civil society in the development and implementation of such frameworks.

Once the floor was opened for comments, discussion focused on whether or not there was an overlap or disconnect between the different international processes handling various aspects of cyber-related issues—in particular, the relationship between the GGE process and the World Summit on the Information Society and the Internet Governance Forum. In addition, participants exchanged views on the distribution of responsibility for stability in cyberspace —was this solely a governmental responsibility or did other actors, such as the private sector, have responsibilities as well? It was argued that the respective roles of States and the private sector would need to be better understood and that topics not related to international peace and security might be more easily suited for multi-stakeholder approaches.

Session 2: Perspectives on How International Law Applies

- **Kerstin Vignard**, Deputy to the Director, UNIDIR (Moderator)
- **Duncan Hollis**, Professor of Law and Associate Dean for Academic Affairs, Temple University
- **Arun Mohan Sukumar**, Head of the Cyber Security and Internet Governance Initiative, Observer Research Foundation
- **Pavel Karasev, Senior Researcher**, Institute of Information Security, Moscow State University
- **Elina Noor**, Director of Foreign Policy and Security Studies, ISIS Malaysia

Ms Vignard opened the session by introducing the panellists and describing how the discussion on the application of international law to States' use of ICTs was the area where national perspectives remain far apart.

Mr Hollis began by offering the participants three words that represented the most contentious issues in the debate on cyber and international security: "Sartre", "baby carriage" and "horse".

"Sartre" signified the existential challenges in the debate. How should one deal with those that say that international law does not apply? The 2013 GGE report stated that international law was applicable. The 2015 report added additional thoughts on a number of subcategories of international law. Nonetheless, existential questions remained, namely on self-defence, IHL and due diligence. Agreement on these would require consensus on whether international law exists in cyberspace and criteria as to when and how it is to be applied.

The "baby carriage" was drawn from the famous Fuller–Hart debate of 1958, where the example of whether a statute banning "vehicles" from a public park would apply to a baby carriage. Would something that is not explicitly mentioned still be covered by a given regulation? A number of issues in the cyber debate related to this problem. Among those were the questions of how international law is applied in the cyber domain to the concepts of use of force and sovereignty. Default rules of interpretation are necessary but difficult to arrive at—as the GGE process has shown.

Finally, "horses" stemmed from the expression "law of the horse" coined by Judge Frank Easterbrook in the mid-1990s. Easterbrook argued against the idea of developing a specific subset of law dedicated to cyber issues. He illustrated this point by stating that there exists no single "law of the horse", despite the fact that we have many laws that are applicable to horses—purchasing horses, damages caused by horses, licensing horses, etc. The argument being that a specific rule was not always necessary as general rules could be applied instead. There are two camps in the debate on the application of international law to States' use of ICTs. The first advocates for using existing

international law, complemented by evolving State practice, for instance on counter-measures. In contrast, others see the necessity for a "law of the horse", which would be achieved first through norms and eventually new legal instruments.

Mr Sukumar contextualized his comments by reminding participants that international law was not an end in itself but was rather to be applied in a specific context. The greatest leaps in creating regimes and common understandings of international law had occurred during times of tension.

Following on from the discussion of session one, the responsibility of ensuring cyber stability is clearly with States as they are the ones possessing cyber "weapons". The divergence on how international law is applied to cyberspace may not have arisen had the implications of cyber weapons for strategic stability been addressed beforehand. In terms of the balance of power, cyber weapons did not introduce a fundamental change but rather expanded options at the disposal of States within that balance. This, however, was negative for small States since stronger ones now had a new tool for coercion. This development is linked to the discussion on international law, with smaller and emerging States fearing they will be left out of a debate dominated by the great powers.

Cybersecurity also has a strong impact on those States that do not produce hardware or software. This increases these economies' vulnerability as most of them do not have agencies capable of effectively mitigating cyber threats. Furthermore, data is often times stored outside of the country, which can impede domestic law enforcement.

In conclusion, he urged emerging countries to engage in the discussions on international law. The GGE process had created an epistemic community. However, small and emerging countries had hitherto not been part of this community.

Mr Karasev emphasized that a shared understanding of international law is the basis of achieving stability in cyberspace. Furthermore, the focus of the international community should be to prevent incidents from occurring and the use of ICTs for military purposes.

The GGEs demonstrate a consensus in the international expert community on certain basic issues, including the obligation to abide by basic principles of international law. There is also agreement that the ICT environment is an area of international relations that is different from the traditional domains due to its manmade nature. The virtual nature of processes within that domain contributes to the problem of attribution.

Therefore, the expert community should seek to prevent the use of ICTs for military or terrorist purposes. At the same time, however, there is still no consensus on how to improve the effectiveness of the legal framework. In his view, such efforts should focus on the negotiation and adoption of universal treaties on the application of principles, norms and rules for responsible State behaviour as well as on the implementation of CBMs. Furthermore, it is essential to clarify the scope and essence of international obligations and defining the limits of sovereignty in the ICT environment. One idea for increased practical cooperation could be joint investigations of incidents by national Computer Emergency Response Teams (CERTs).

In addition, the security of imported products is a vital topic that needs to be addressed. Other issues that need to be tackled are cybercrime, possibly by updating the Budapest Convention, and interference in the internal affairs of States via cyber means.

Working groups, for instance within the International Law Commission, could appropriately address all the aforementioned issues. Such groups could bring together experts on the respective topics and prepare draft documents. He noted that the more topics that a group is mandated to discuss, the harder it may be to negotiate them. For this reason, he suggests that only similar topics should be discussed in the same group, for instance legal questions regarding sovereignty or the UN Charter to be dealt with by legal specialists.

Ms Noor stated it was important to take into consideration the perspectives of small and developing States. Smaller States tend to uphold the principles of international law as they need to rely on it given their lack of other capabilities. Yet while there is agreement on the applicability of international law, there is disagreement on how it should be applied.

Small States face particular challenges. Issues such as cybercrime or content, which could undermine the stability of the State, are often more pressing to them and hence prioritized. Oftentimes, representatives of smaller States are intimidated by technical discussions and have yet to develop relevant technical capacity. As participants in discussions on cybersecurity from developing countries often lack a basic understanding, enhanced sensitization to increase their understanding of the matter is needed. The recent regional workshop organized by UNIDIR, the Center for Strategic and International Studies, and Singapore is a good example of this practice. One of the main hindrances to greater participation of small and developing States in cyber matters are internal structural difficulties—it is often unclear which agency or individual is responsible for the portfolio.

Due in part to their resource constraints, developing States legitimately focus on those topics that pose the most direct threat to their stability. For this reason, addressing cybercrime and content issues, including disinformation, have priority. On the other hand, traditional security issues such as arms control are seen by smaller States as the remit of major powers. In her view, smaller States have legitimate concerns about how international law is not equally applied.

In the discussion period regret was expressed that new ideas and initiatives by the private sector are not taken up by governments, despite the failure of the GGE process to produce consensus on how international law applies.

Concern was also expressed about the reluctance of small States to engage on the international security dimension of cyber. Another intervention clarified that while the international security aspects of ICTs are not necessarily the top priority of small States, this does not mean they are not significant to them—sometimes it is a question of first engaging them through capacity-building efforts. One participant highlighted that the Forum of Small States could be useful in this regard, given its broad membership.

Another topic in the discussion period was the strong differences among countries in the understanding of fundamental aspects of international law. In addition to the issues already mentioned, one participant highlighted how IHL provides a great example of why a new cyber treaty was needed. Without such an instrument, it would be impossible to know, for instance, whether hospitals were protected in case of a conflict in cyberspace.

The effect of cyber capabilities on the balance of power was also raised. While the same set of States involved in the traditional balance currently dominate the cyber field, new cyber leaders will emerge over time.

Session 3: Looking Ahead–Where Do We Go from Here?

- **Karsten Geier**, Head of the Cyber Policy Coordination Staff, German Federal Foreign Office (Moderator)
- **Belisario Contreras**, Cyber Security Program Manager, Organization of American States
- **Patricia Lewis**, Research Director for International Security, Chatham House
- **Shen Yi**, Associate Professor, Department of International Politics, Fudan University
- **James Lewis**, Vice President, Center for Strategic and International Studies (CSIS)

Mr Geier, who had served as the Chair of the 2016–2017 GGE, opened the session by asking panellists to address some of the dilemmas introduced in the preceding exchanges. These included the relationship between the role of the State for international security and the role of private actors in the virtual realm of cyberspace, calls for more awareness raising and inclusive fora while ensuring effectiveness, and the lack of consensus due to very different ideas on international law. He also asked panellists to share their thoughts on possible future paths in the UN and elsewhere.

Mr Contreras started out by saying that there were good reasons for the existence of both international and regional organizations. Regional arrangements are unique, fulfilling different roles in their respective parts of the world according to the needs of their members. That said, cross-regional fertilization can be very beneficial. For example, the work of the OSCE in part inspired the establishment of a working group on cooperation and confidence building in the OAS.

Capacity building is particularly important in the regional context as many States and regional organizations need to understand their role in a global system of cybersecurity. In many countries, there is lack of human, financial and technical resources as well as know-how in the field of ICT security. He stressed that even failures offer valuable lessons and experience.

Mr Geier commented that while rules for State behaviour were developed at the global level in the UN, having confidence that States would abide by these rules is equally important and that regional organizations are often the best-placed fora for such confidence building.

Looking ahead, **Ms Lewis** first considered the existing UN formats that could be used to continue the international discussion on ICTs in international peace and security. Beginning with what had so far been the forum of choice, she cautioned against rushing to establish a new GGE. States need some time to absorb and operationalize what has already come out of the GGE process. Increased outreach is necessary, both to States and non-State actors, in order to assist with this before a new GGE starts. A second option would be an open-ended working group under the auspices of the General Assembly. Importantly, its mandate would need to be limited in some way and all States should feel welcome to participate. The outcome of such a group could lead to a new GGE with a more specific mandate or a different way forward. A third option would be to incorporate the topic of cybersecurity into the work of the Conference on Disarmament.

She suggested that when assessing options to take the international discussion forward, criteria to consider includes: the inclusiveness and transparency of a process, whether the option allowed for the participation of non-governmental actors, the perceived legitimacy of the format, and finally the possible outcomes of the respective process. She then briefly described six additional proposals:

1) The establishment of a **UN Special Representative for ICT Security**. Reporting to the Secretary-General, this person could be the system-wide "face" on cyber issues, be a champion of building capacity in developing countries, and help to facilitate increased collaboration between the international and regional levels.

2) The establishment of a **UN Advisory Board on ICT Security** modelled after the Secretary-General's Advisory Board on Disarmament Matters. It could report directly to the UN Secretary-General and be complementary to the establishment of a Special Representative.

3) The establishment of a **UN CERT**, which would serve in an advisory capacity, building knowledge on cybersecurity throughout the UN system and one that States could use as a technical resource.

4) Negotiation of a **Code of Conduct for Cyberspace**, similar to other already established codes on other topics, or promote the adoption of regional or internationally harmonized legislation.

5) The establishment of a **Committee on the Peaceful Uses of ICTs** analogous to the Committee on the Peaceful Uses of Outer Space (COPUOS). COPUOS has done a lot of valuable work in a potentially difficult field, including on confidence building, through its different committees covering legal and technical issues. Such a committee could be established under the General Assembly or in a different setup, preferably in Geneva given other relevant bodies and institutions in that city. It could focus on capacity building, as well as develop normative and legal frameworks.

6) Lastly, **reframing how the cyber security issue is discussed**. One proposal for such a reframing is through the lens of *information integrity*, the confidence in the security and authenticity of information received. Framing the issue in the context of *attribution* could also help. Attribution of a cyber incident can be difficult, and the private sector could have valuable experiences to draw upon. *Cyber terrorism* is also a potential framework through which to approach the issue of international cybersecurity.

In her view, there is a lack of appetite in the international community to continue the GGE process, despite most States agreeing on the importance of continuing the work in the UN in some fashion.

Mr Shen stated that the fundamental question of the debate on cyber in international security was how to govern cyberspace given the myriad of threats. In his view, the most significant threat is a conflict between great powers as a result of a mis-attributed cyber incident caused by a non-State actor.

In tackling such challenges, multilateral arrangements are of great significance. Hopefully the UN can transfer its legitimacy from traditional security issues into the cyber field. In order to achieve stability in cyberspace, ensuring the equality of States—a key concern of China—was important. Also, "cybersecurity" needs to be clearly defined. In this regard, he pointed to the different positions of China and the United States, in particular on the issue of content. The issue of "fake news" demonstrates that content is indeed a relevant security concern. The UN should therefore facilitate discussions on definitions of key terms to ensure a common understanding among States.

Information- and knowledge-sharing mechanisms are needed to counter the proliferation of malware. Thus an institutional mechanism for information sharing or distribution of software patches to known vulnerabilities are two practical roles for an international cyber entity.

Mr Lewis recalled 25 years ago, there were grave warnings about the potential of a "Cyber Pearl Harbor", and yet such an event has yet to occur. Self-preservation through national defence remains the primary concern of States, which justifies their focus on the security aspect of ICTs, despite the existence of other important issues, such as privacy.

Mr Lewis asked whether the process on cybersecurity should be reserved for the UN or if there are alternative venues. The process would be significantly quicker if only great powers were to participate. Most diplomatic achievements begin with support by the great powers, with some

prominent exceptions such as the ban on anti-personnel landmines. There is also the question of involving actors other than States, such as the private sector, in such a process.

Some general principles akin to those for the global financial system agreed at Bretton Woods may be achievable. While many ideas brought to the discussion are sensible, he felt that it was impractical to consider initiatives that do not have the support of the key cyber players. He raised the possibility that perhaps it would take a real cyber crisis before there would be a breakthrough in international agreement.

Mr Lewis believes that there is not a single approach to discuss cybersecurity. There is a need for discussions at a global forum, involving all States and—if possible—also the non-State actor community. At the same time, discussions among likeminded States are necessary. Lastly, there needs to be a mechanism for opponents to engage with each other. While many different mechanisms and fora exist, only few really allow for formal agreements constraining State behaviour.

The discussion period highlighted the role and contributions of regional and like-minded organizations, in operationalizing norms and providing venues for discussion between both friends and adversaries. It also brought to the fore the limitations of negotiated outcomes, which tend to represent the lowest common denominator of agreement. Some felt that efforts among likeminded deliver results meeting a higher standard. Lastly, there was discussion around whether it was useful to distinguish between the "weaponization" of code (such as Stuxnet) to create specific damage of physical objects or digital systems, and the more frequent sorts of cyber operations (hacking, spoofing, intrusion, intelligence gathering, etc.). It remained an open question as to whether dealing with these issues separately at the international level would be more or less effective than the current approach which addresses them together. Lastly, reacting to some of the proposals presented by panellists, such as the establishment of an organization for attribution, the general feeling in the room was that it is unlikely Member States would be willing to bear the necessary financial burden to allow for their realization.

Closing Remarks

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

Bringing the conference to a close, **Ms Vignard** once more thanked participants for their active engagement and expressed her hope that they found the presentations thought provoking. She brought to the attention of participants the previously mentioned UNIDIR report mapping how the international security aspects of cyber issues are dealt with throughout the UN system.[3] Lastly, she thanked the Governments of Germany and Switzerland for sponsoring the event.

[3] Ibid.

Annex. Biographies of Panellists

Belisario Contreras is the Cyber Security Program Manager at the Organization of American States (OAS). He has over 10 years of experience in government and security initiatives, particularly in the Latin America and the Caribbean region. Mr Contreras has played a key role in the development of cybersecurity capacities in the Americas. He has led the design, planning and execution of cybersecurity initiatives, including: Development of National Cyber Security Strategies and Policies; Creation and Development of Computer Emergency Response Teams (CERTs); Provision of Technical Training; Implementation of Crisis Management Exercises; Capacity building on Critical Infrastructure Protection (CIP); and Cyber Security awareness.

Karsten Geier is head of the Cyber Policy Coordination Staff in Germany's Federal Foreign Office and served as Chair of the 2016–2017 Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. A career Foreign Service officer, Mr Geier has held a variety of posts both at home and abroad. He has served in South-Eastern Europe, Brussels (at Germany's Representation to the European Union) and Washington, D.C. (including as exchange officer in the US Department of State). His most recent assignment abroad led him to New York, where he helped set up the European Union Delegation. Mr Geier subsequently worked at Germany's Mission to the United Nations. In the context of Germany's membership of the UN Security Council, he chaired numerous meetings of the Committees set up under Security Council resolutions 1267 (Al Qaida Sanctions) and 1988 (Taliban Sanctions). Karsten Geier was Germany's member of the 2014-2015 GGE. He represents his country in the OSCE's Informal Working Group on the Risk of Conflict Stemming for the Use of Information and Communication Technologies.

Duncan B. Hollis is Professor of Law and Associate Dean for Academic Affairs at Temple University Law School. He is editor of the award-winning *Oxford Guide to Treaties* (Oxford University Press, 2012) as well as a series of articles on securing cyberspace, including (with Martha Finnemore) "Constructing Norms for Global Cybersecurity," which was recently the lead article in the *American Journal of International Law*. A former Attorney-Adviser at the US Department of State, Professor Hollis is a Non-Resident Scholar at the Carnegie Endowment for International Peace, a member of the American Law Institute, and an elected member of the Juridical Committee of the Organization of American States.

Pavel Karasev is Senior Researcher at the Institute of Information Security Issues at Moscow State University (IISI MSU). Dr Karasev's research interest is the political dimension of ICT use in international relations, varying from issues of cyberwarfare, to problems of terminology, to filtration of objectionable content and application of international law to cyberspace. He has authored numerous reports and articles on issues of information security, cybersecurity, and international information security. He holds a doctorate in political science.

Camino Kavanagh is a Senior Visiting Fellow at the Department of War Studies, King's College London. She served as a member of the consultancy team to the 2016–2017 UN Group of Governmental Experts (GGE) on ICTs in the Context of International Peace and Security and is lead consultant to the OSCE on a project relating to Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of ICTs. She is also involved in a number of policy-related initiatives on ICTs and emerging technologies as they relate to conflict, terrorism and crime. Dr Kavanagh's PhD was awarded by the Dept. of War Studies, King's College London in 2016 and focused on information technology, sovereignty and the state, a topic that remains a core focus of her research activities. She is a Member of the Global Initiative on Transnational Organized Crime.

James Andrew Lewis is a senior vice president at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. His government experience includes work on Asian politico-military issues, as a negotiator on conventional arms and technology transfers, and on military and intelligence-related technologies. Dr Lewis led the US delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was a member of the consultancy team to the UN Group of Government Experts on Information Security for the successful 2010, 2013, and 2015 sessions. He has served on several Federal Advisory Committees, including as chair of the Committee on Commercial Remote Sensing, as well as member of the Committees on Spectrum Management and International Communications Policy, and as an adviser on the security implications of foreign investment in the United States. He received his PhD from the University of Chicago.

Patricia M. Lewis is the Research Director, International Security at Chatham House. Her former posts include Deputy Director and Scientist-in-Residence at the Center for Non-proliferation Studies at the Monterey Institute of International Studies; Director of UNIDIR; and Director of VERTIC in London. Dr Lewis served on the 2004-2006 WMD Commission chaired by Dr Hans Blix; the 2010-2011 Advisory Panel on Future Priorities of the OPCW chaired by Ambassador Rolf Ekeus; and was an adviser to the 2008-2010 International Commission on Nuclear Non-proliferation and Disarmament (ICNND) chaired by Gareth Evans and Yoriko Kawaguchi.

Elina Noor is Director of Foreign Policy and Security Studies at ISIS Malaysia. She was previously a key team member of the Brookings Institution's Project on US Relations with the Islamic World in its formative years post-September 11, 2001 and researched WMD terrorism at the Center for Nonproliferation Studies, Monterey Institute of International Studies in Washington, DC. Her policy interests include US-Malaysia bilateral relations, cyber warfare and security, radicalization and terrorism, and major power relations. Her commentaries have appeared in local and foreign media, including *The New Straits Times*, BFM, the *New York Times* and Al-Jazeera. She currently serves on the Global Commission on the Stability of Cyberspace.

Shen Yi is an associate professor in the Department of International Politics, School of International Relations and Public Affairs at Fudan University in Shanghai. Dr Shen heads the university's newly established Cyberspace Governance Research Center focusing on the cybersecurity and cyberspace governance related issues. Since 2009, he has focused on Sino-US cybersecurity relationship and global cyberspace governance. He has written numerous short commentary pieces for newspapers, including The Global Times and Wen Hui. He has also published several academic papers analyzing America's cyberspace strategy and his book *The National Cybersecurity Strategy of United States* was published in 2013. In 2016, he was one of the ten representors to participate the Conference on Cybersecurity and Informatization hosted by President Xi Jinping. Dr Shen holds a PhD in international politics from Fudan University.

Arun Mohan Sukumar heads the Observer Research Foundation's Cyber Security and Internet Governance Initiative and is the Co-Chair of CyFy: The India Conference on Cyber Security and Internet Governance. He is the elected Vice Chair of the Asia-Pacific Regional Internet Governance Forum. He was the non-governmental representative in India's official delegation to the Tallinn Manual consultations to articulate laws of armed conflict in cyberspace. Mr Sukumar is a member of the World Economic Forum's Global Future Council on the Digital Economy and Society. He has previously served on the editorial board of *The Hindu*, and is a lawyer by training. He holds a Master's degree from the Fletcher School of Law and Diplomacy, Tufts University, where he was the Douglas Dillon Fellow, and the recipient of the Leo Gross Prize for Outstanding Student of International Law.

Kerstin Vignard is Deputy to the Director and Chief of Operations at the UN Institute for Disarmament Research, where she advises the Director and leads the Institute's work on emerging security issues. Ms Vignard served as a member of the consultancy team to four of the five UN GGEs on Developments in the field of Information and Telecommunications in the Context of International Security. Since 2013, she has led UNIDIR's work on the weaponization of increasingly autonomous technologies.

UNIDIR

UNIDIR Cyber Stability Conference 2017

ICTs in the Context of International Peace and Security

Current Conditions and Future Approaches

Reports issued in recent years by the United Nations Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security have been a significant achievement on international security issues in cyberspace. However, the most recent GGE concluded its work in June 2017 without reaching consensus. As Member States will need to consider how best to build upon the last consensus GGE report (2015) in order to promote a peaceful, stable and secure cyber environment for all nations, this year's conference provided an opportunity to take stock and consider next steps for enhancing cyber stability at the international level.