UNIDIR

UNIDIR Cyber Stability Seminar 2016

Taking Security Forward: Building on the 2015 Report of the GGE

UNIDIR RESOURCES

Acknowledgements

Financial support for the 2016 Conference was received from the Governments of the Netherlands and the United States of America.

About UNIDIR

The United Nations Institute for Disarmament Research—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 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 Strategic Technologies Program of the Center for Strategic and International Studies (CSIS)

The CSIS Strategic Technologies Program provides pragmatic, data-driven analysis and recommendations written for a global audience. Its current research agenda includes projects on security, innovation and the future of the internet. These projects explore the challenges and opportunities of digital technologies and how technology is reshaping politics, international security, and innovation. The Program's work on cybersecurity helps define the global agenda and its work, including its Commission on Cybersecurity for the 44th Presidency, continues to shape policy and practice in countries around the world.

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 Daniel Golston. Additional support was provided by Elena Finckh and Julie Wald.

www.unidir.org

UNIDIR Cyber Stability Seminar 2016

Taking Security Forward: Building on the 2015 Report of the GGE

Seminar Report

17 June 2016, Geneva, Switzerland

Introduction

Cyber technologies have revolutionized the way societies around the world interact, their myriad applications altering every aspect of our lives. At the same time, these technologies provide high strategic value and, as such, carry with them some destabilizing qualities. This has led to greater calls for international cooperation and dialogue on the implications of cyber technologies for international peace and security. At the highest international level, this contributed to the establishment of the United Nations (UN) Group of Governmental Experts (GGE) process on Developments in the Field of Information and Telecommunications in the Context of International Security (henceforth referred to as the GGE process).

The latest GGE concluded its work in 2015 with the adoption of a consensus report, which was transmitted to the General Assembly as document A/70/174. A new GGE, with an expanded membership, will commence work in August 2016.[1] The 2016 Cyber Stability Seminar, "Taking Security Forward: Building on the 2015 Report of the GGE", sought to take stock of what has already been achieved by previous GGEs and consider what lies in store for the 2016–2017 GGE and beyond.

The GGE process has helped to establish a normative foundation for the international community to build upon as it works towards the shared objective of—in the words of the 2015 GGE report—an "open, secure, stable, accessible and peaceful ICT environment". Achieving stability in the cyber domain will require a collective effort among all stakeholders, as well as understanding and respect for different regional and

1 See UN General Assembly resolution A/RES/70/237.

national equities and interests. It is incumbent upon the international community to pursue constructive and frank dialogue in order to work towards this objective.

The Annual Cyber Stability Seminar

This was UNIDIR's fourth annual Cyber Stability Seminar. The 2016 event, organized with the Center for Strategic and International Studies (CSIS), provided a valuable forum for engaging the range of communities concerned with the international security dimension of cyber issues, including policymakers and representatives of international organizations, regional organizations, industry and civil society. The 2016 seminar took place shortly before the 2016–2017 GGE began its work and was therefore an opportune moment to take stock of the GGE process, consider where the international community should be when the 2016–2017 GGE concludes its work, and explore what a multilateral cyber stability regime may look like in the future.

PROCEEDINGS[2]

Welcoming Remarks

- **Kerstin Vignard**, Deputy to the Director, UNIDIR
- **James Lewis**, Senior Vice President and Director, Strategic Technologies Program, CSIS
- **Ambassador Henk Cor van der Kwast**, Permanent Representative of the Netherlands to the Conference on Disarmament and Disarmament Ambassador at Large

Ms Kerstin Vignard convened the fourth annual Cyber Stability Seminar. She noted that the 2016 seminar was particularly relevant given that a new GGE was scheduled to start its deliberations in August 2016. The GGE had been expanded to 25 members, which was a reflection of the increased international interest in cybersecurity processes at the UN. However, far more countries had expressed an interest in participating in the GGE than could be accommodated, and thus it remained important to provide opportunities and forums for international dialogue as a complement to the GGE process in order to engage as wide a range of States as possible.

Ms Vignard continued by noting that, for over 15 years, UNIDIR had used its unique position in the UN system and its convening power to organize events, expert meetings and regional conferences on issues of cyber stability and security. UNIDIR had supported the GGE process as consultant to the previous three GGEs, and would continue to do

2 This report aims solely to reflect the content of the presentations and discussions and does not necessarily reflect the opinions and positions of UNIDIR, the United Nations, the sponsoring organizations, or supporting States. Listen to the presentations made at the event at http://bit.ly/28Nvjtr

so for the 2016–2017 GGE. Most recently, UNIDIR and CSIS had co-organized a series of three expert workshops that sought to build understanding of key cybersecurity issues—including norms, legal issues, and addressing malicious cyber tools—among previous and future members of the GGE process.[3]

Mr James Lewis welcomed all participants and commented on the fruitful partnership between UNIDIR and CSIS over the years. He saw the current event as the capstone of the 2016 UNIDIR–CSIS expert workshop series and noted that the series had particularly benefited from the presence of both governmental and non-governmental experts. He said that UNIDIR's annual Cyber Stability Seminar was one of the leading forums for discussing cybersecurity at the multilateral level and he looked forward to the presentations and interventions from the audience throughout the day.

Ambassador van der Kwast thanked UNIDIR and CSIS for organizing the event. One of the problems facing the international community in many disarmament forums is the fact that discussions often result in little or no outcome. He expressed hopes that the current meeting would be more fruitful and take security discussions forward, successfully building on what the international community had achieved thus far. Around the world, strategic tensions are increasing and therefore he welcomed constructive dialogue on issues such as norms and international law in the cyber domain, in order to help build common foundations.

Keynote Remarks

- **Andrei Krutskikh**, Special Representative of the President of the Russian Federation for International Cooperation in Information Security
- **Michele Markoff**, Deputy Coordinator for Cyber Issues, United States Department of State

Representing two of the largest and most influential cyber powers, Mr Krutskikh and Ms Markoff explored their respective governments' perspectives on the GGE process, bilateral relations, and recent normative developments in the cyber domain.

Mr Krutskikh began by emphasizing the importance of bilateral discussions and agreements for building mutual understanding. He highlighted the fact that such meetings have achieved a number of successes, such as the establishment of hotlines, and have furthered mutual understanding, for example in the form of intergovernmental or inter-agency agreements and other confidence-building measures.

Mr Krutskikh said that the time was ripe to conclude an incident prevention agreement between the Russian Federation and the United States of America. Such an agreement would clarify response options in more detail. He stressed the importance of establishing clarity on "what to do" should any suspicious activity arise, and of allowing a State to

3 See the report of the workshop series at http://bit.ly/2aIZENC

provide a reliable explanation of events. In this context he emphasized the need for special lines of communication to deal with cyber incidents, noting that normal diplomatic channels are insufficient given the special characteristics of the information space. He welcomed the fact that these sorts of arrangements had been established with Canada, the United Kingdom and Australia, and noted that the Russian Federation would continue to pursue such agreements with other States.

In the absence of an overarching agreement on responsible State behaviour in the cyber domain, he explained that States are obliged to develop a safety net in the form of a network of arrangements and agreements based on bilateral relations. However, he also noted that an inclusive multi-stakeholder approach would ultimately be preferable, to prevent some States from being left out and thus creating a risk of becoming "safe havens" for illicit or malicious cyber activities.

Mr Krutskikh welcomed the growing interest in the work of the GGE, one example being the high number of applications to participate in it. He also welcomed the clear mandate of the forthcoming GGE to develop rules, norms and principles for responsible State behaviour. While the applicability of international law to information space implies the possibility of developing new norms should this be deemed necessary, preference should be given to the identification of existing applicable norms. In this context Mr Krutskikh suggested that the time might be ripe to convene another GGE, led by legal experts, for example within the UN General Assembly's Sixth Committee, to deepen the discussion on how international law applies and to make recommendations to the General Assembly.

Mr Krutskikh advocated for more focus in the GGE's discussions, stressing the risks related to continuously broadening the agenda. It would be more constructive to devise basic rules of behaviour, rather than taking a non-proliferation or a technology control approach. These latter approaches face significant challenges given the dual-use characteristics of cyber tools.

Mr Krutskikh concluded by emphasizing the need to focus on small but realistic steps forward. As a practical way to increase the acceptability of the GGE's work thus far, he suggested that the next GGE should recommend that the General Assembly adopts a resolution consolidating the GGE's most notable achievements. Starting with a voluntary, soft law approach to State behaviour in the cyber domain could provide some initial movement in a positive direction.

Ms Markoff recalled the international community's increasing dependence on networked information systems—this dependence is associated with vulnerabilities to cyber-enabled national infrastructure, and ultimately national security. While recognizing the importance of consulting technical specialists, Ms Markoff noted that foreign policy actors have the primary responsibility for addressing the international peace and security aspects of cybersecurity, as States traditionally bear the primary responsibility for international stability. Rather than trying to control the cyber domain, States should act as stewards working towards the common goal of an open and inclusive cyberspace for the benefit of all. Highlighting the importance of international cooperation, she thanked UNIDIR and

CSIS for organizing the International Security Cyber Issues Workshop Series over the previous seven months.

According to the United States Government, cyber stability is the best way to achieve the common goal of keeping cyberspace peaceful, open and accessible to all. International cyber stability means States have incentives to cooperate and avoid conflict. She asked, how best can we achieve that goal? She noted that there are a number of challenges that need to be addressed to achieve such stability, including the sheer number of actors operating in the cyber domain, persistent issues with attribution, as well as the usability of cyber tools with low lethality and their dual-use nature. In light of these challenges, Ms Markoff stressed the need for a clear understanding of what constitutes responsible State behaviour in cyberspace, for example in the form of declaratory policies, as well as stronger and more resilient national defences coupled with credible response options and increased international engagement to promote principles of responsible State behaviour. She addressed a common criticism according to which norms can only play a limited role, particularly regarding malicious actors that have no intention to abide by them, by affirming that norms are absolutely vital in establishing the boundaries of acceptable behaviour.

Ms Markoff noted that the rules governing the use of force provided by international law, namely international humanitarian law (IHL) and the UN Charter, which guide States in the use of kinetic tools, also apply to State activity in cyberspace. For example, the same care taken in planning the use and targeting of kinetic weaponry must also be applied in cyber-enabled operations, including respect for collateral damage and avoidance of civilian infrastructure. Ms Markoff listed several categories of measures that enhance international cyber stability and reduce risk: (1) *stability measures*, such as additional, voluntary and non-binding norms for State activity in peacetime (so-called peacetime norms); (2) practical *transparency and confidence-building measures* (TCBMs) aimed at reducing uncertainty about State activity; and (3) *cooperative measures* aimed at providing States with the means to prevent and react to cyber incidents.

In conclusion, Ms Markoff stressed the significant role of the GGE and other multilateral processes in cyber stability by recalling important achievements thus far: In 2013, 15 GGE experts reached consensus that existing international law applies in cyberspace.[4] In 2015, the GGE expanded to 20 experts and took a further step by highlighting the applicability of the UN Charter in its entirety. The 2015 GGE report constitutes a significant achievement as it includes recommendations regarding voluntary norms for State behaviour during peacetime. These reports have laid the foundation for two addition milestones in 2015: first, a September bilateral agreement reached between China and the United States on several key cyber issues; and second, the November G20 endorsement of an approach to promoting stability in cyberspace. These developments, along with recent activities by the Organization for Security and Co-operation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN), collectively represent a major step towards promoting a stable cyber domain.

4 See UN document A/68/98.

Session 1. International Law

- **Laurent Gisel**, Legal Adviser, International Committee of the Red Cross (ICRC)
- **David Simon**, Counsel, Sidney Austin LLP
- **Elina Noor**, Director, Foreign Policy & Security Studies, Institute of Strategic and International Studies (Malaysia)

Previous GGEs have affirmed that international law applies in the cyber domain; however, shared understanding of *how* international law applies is still coalescing. This session sought to expose some of the different perspectives and approaches to the key legal questions.

In his presentation, **Mr Gisel** first explored the notions of cyberwarfare and cyberattack. He noted that there currently exist no consensus-based definitions of these terms and that some actors use them to describe actions that rather qualify as cyber espionage or criminal activity. The ICRC understands cyberwarfare to be operations against a computer or a computer system through a data stream, in so far as they are used as means and methods of warfare in the context of an armed conflict as defined under IHL. This can occur either in the form of kinetic operations or, in the absence of kinetic operations, when cyber warfare alone would amount to armed conflict. Though cyber warfare has not led to dramatic humanitarian consequences to date, the ICRC is concerned because cyber technologies can be used to manipulate civilian infrastructure, such as power plants, water supplies or banking systems. Thus the potential for humanitarian consequences is substantial.

Mr Gisel welcomed the fact that the 2013 GGE report affirms the application of international law in the cyber domain. He then explained that IHL imposes important restrictions on cyber warfare comparable to “traffic rules”. Under IHL, for example, the use of indiscriminate weapons is prohibited, as well as attacks on vital civilian infrastructure. Therefore a cyber operation designed to disable indispensable civilian objects (e.g. water supply) is already prohibited under IHL. In addition, Mr Gisel questioned whether a cyber virus could be used in a sufficiently targeted, discriminate and proportional manner. While IHL already prohibits the use of indiscriminate weapons, he suggested that an explicit ban on cyber weapons may be more effective if it were to become apparent that cyber technologies could not be used in accordance with IHL.

Given that State activity in cyberspace poses such novel challenges, Mr Gisel saw these leading to the question of whether existing IHL is sufficient. He affirmed that determining the answer to this question was the responsibility of States. A thorough legal review of new cyber weapons in order to ensure that they comply with international obligations would have great value. In conclusion, he reminded participants of the increasing number of States developing cyber warfare capabilities, which reinforces the urgency of exploring the potential humanitarian consequences. He hoped that the international community could move forward on this issue before the human cost of cyber warfare compelled it to do so.

The next presenter, **Mr Simon**, began by emphasizing that the question of *how* international law applies to cyber operations is not well settled among States, specifically how it applies *below* the threshold of the use of force, even though this is where most cyberattacks are taking place.

First, Mr Simon recalled the core international legal norms that guide the lawful use of force: notably Article 51 of the UN Charter which recognizes States' right to self-defence in the case of an armed attack, and Article 2(4) on the threat or use of force against the territorial integrity or political independence of any State. These guide State behaviour in regard to the threat or use of force. However, he said that the application of such principles is complicated in the cyber domain, as most cyber activity does not rise to the level of an armed attack.

Mr Simon noted that there are other tools available to States to enable them to respond to cyberattacks below the threshold of the use of force, notably countermeasures in response to violations of a State's sovereignty. Mr Simon highlighted that the International Law Commission's 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts contain the most important elements of contemporary doctrine regarding countermeasures. In cases that would neither justify the use of force nor countermeasures, States could still resort to retorsion, including lawful political actions with symbolic impact, such as the withdrawal of an ambassador.

To illustrate some of the legal challenges, Mr Simon presented a few hypothetical scenarios of cyber operations. In the first scenario, a State is conducting a three week-long online national election. Voting takes place on government websites, which experience a distributed denial of service (DDoS) attack. Because such an incident would likely not meet the threshold of an "armed attack" a State would not be allowed to resort to self-defence. However, an affected State could resort to countermeasures, as such interference would constitute an unlawful interference with sovereignty. These countermeasures could include interfering with the computers used to launch the unlawful activities, in order to allow people to vote. He noted, however, that the right to such countermeasures would be limited to the duration of the unlawful interference. In a second scenario, all government computers involved in the command and control structure of a State's nuclear weaponry are irreversibly compromised. In a third scenario, a country's financial sector is disrupted for two days. In these cases, the legal analysis would be more difficult. Would these represent circumstances that merit the use of force? Did the attack interfere with the *domaine réservé* of the State? Could this be considered a coercive act? What would be an appropriate response?

In conclusion Mr Simon noted that considering the wider political context in such cases is extremely important, but he suggested that States will have different answers to these questions. Mr Simon suggested that working through scenarios such as these would help to identify what the potential legal questions may be.

This panel's final presenter, **Ms Noor**, reviewed some key legal terms and their application in the cyber domain. She prefaced her presentation by reminding participants that international law has been drafted over time and has not evolved in a vacuum.

States invoke international law in their activities and, despite the best of intentions, the interpretation of that law is invariably coloured by policy and national interest. She noted that widely differing interpretations were particularly apparent regarding rules about the use of force. In her presentation she illustrated this concern with four examples.

The first example she gave concerned the threshold of the use of force. It is not clear, for example, whether or when a cyberattack would allow for countermeasures, especially when an attack merely results in economic loss. It is also not clear what actions are permissible if an attack emanates from non-State actors. She noted that the notion of an armed attack could be interpreted in a restrictive way, requiring actual physical damage, or in a wider way, including non-kinetic damage that in scale would amount to comparable harm. The second example concerned the persistently challenging topic of attribution. Ms Noor explained that there are three types: technical, political, and legal. The International Court of Justice has generally taken the position that a State must have effective control over an attack for it to be attributable. However, in the cyber domain, Ms Noor explained that this sort of attribution is difficult. Furthermore, attribution of any sort is all the more challenging for less technologically advanced States.

Linked to the attribution issue she moved to her third example, the question of evidence. In the case of a State being accused of conducting a cyberattack, is the burden of proof reversed (i.e. for a State to prove that the attack did not originate from its territory)? Furthermore, what is the standard of proof? What methods for gathering evidence are acceptable? The last issue she covered was that of self-defence, a well-established concept in international law. Ms Noor explained that the invocation of self-defence has a chequered history. She observed a trend in the past two decades of technologically advanced States reserving the right to conduct anticipatory or pre-emptive self-defence operations. This is a controversial development—even more so for the cyber domain, as the arguments for anticipatory self-defence must interpret the conditions of imminent threat more broadly.

In conclusion, she felt that existing international law provides an adequate framework for developing provisions for the cyber domain. Ms Noor recognized that there remain many ambiguities and space for subjective interpretations. However, these can be dealt with openly and systematically and in the process, will provide opportunities for cooperation and collaboration.

During the discussion period, participants pondered the need for a cyber-specific legally binding instrument or whether the existing legal framework was sufficient. One participant remarked that existing international law already addresses State activity within the context of warfare. This participant suggested that the international discussion should move away from the need for a legal treaty governing such activity and instead focus on activities below the threshold of the use of force. Another participant remarked that in conversations around existing treaties banning specific types of kinetic weapons, the idea behind their ban was that these weapons failed a basic legal weapons review because they are inherently indiscriminate. Conversely, cyber operations can be highly tailored. Thus the legal question is shifted away from the notion of effect and towards that of intent.

Session 2. Addressing Malicious Cyber Tools

- **Heli Tirmaa-Klaar**, Head of Cyber Policy Coordination, European External Action Service, European Union
- **Trey Herr**, Fellow, Belfer Center at the Harvard Kennedy School
- **Elaine Korzak**, National Fellow, Stanford University

The 2015 GGE report included a norm that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions". This panel considered how the international community could operationalize this norm, including regulatory questions and definitional challenges.

The first presenter, **Ms Tirmaa-Klaar**, explored the notion of cyber risk and how the European Union (EU) and other actors can address it. She began by arguing that a common understanding of risk in the cyber domain is needed. Risks within the cyber ecosystem are best conceptualized as a three-tiered pyramid. At the top of this pyramid are high-impact/low-probability State-on-State or State-directed incidents. The middle layer is high-end cybercrime that is sometimes State-tolerated. At the bottom of this risk pyramid are low-end risks that damage businesses and societies. The question is how to address these risks? The international community must address these layers both at the same time and separately. For example, one cannot ignore the frequent low-end risks while only focusing on high-impact risks at the top.

While less related to international security, it is the middle and lower portions of the cyber risk pyramid that concern most people—yet States have varied levels of readiness and resilience to respond to these risks. For this reason, the EU has begun a sizeable cyber capacity-building assistance programme for States around the world. In countries with a sound legal cyber framework, this involves discussions with key government abroad to evaluate cybercrime legislation; in other countries, this means engaging and training legislative actors. Training for the judiciary and law enforcement can also be provided. She noted that tackling cybercrime was an urgent task for the international community. The EU programme also focuses on building incident response capabilities, which are especially important in rapidly growing economies with less governmental capacity to address these issues.

Ms Tirmaa-Klaar supported the development of positive norms to encourage responsible behaviour in the cyber domain. Focusing on the regulation of *behaviour* rather than *tools* is all the more important due to the lack of a clear system of verification in cyber operations.

She concluded by affirming that the international community needs to take care of the entire cyber ecosystem: one cannot deal with only one aspect of the threat spectrum. In order to achieve enhanced cyber stability, all three layers of the risk pyramid must be managed at the same time.

Mr Herr began his presentation by attempting to disentangle the various goals within the international community's cybersecurity conversations. He raised three key questions.

The first was *what is it that States want to control or manage*: was it tools, software, malware, actors, effects, capabilities? The second question was *what sort of proliferation do States care about*: was it State-on-State, State-on-non-State actor, or between non-State actors? The final question was *what mechanism would States like to use in order to control the spread of malicious cyber tools*? Furthermore, are non-proliferation activities the appropriate model for doing so? He suggested that non-proliferation processes usually include an existential threat—which is, for example, the impetus behind nuclear non-proliferation processes. However, this scale of consequences does not necessarily translate to the cyber domain. Nevertheless, non-proliferation experiences hold some transferrable lessons.

He noted that at the third UNIDIR–CSIS International Security Cyber Issues Workshop on Managing the Spread of Cyber Tools for Malicious Purposes, the discussion began around export controls then evolved into a larger conversation with two points of agreement. The first was that there exists a key distinction between criminal activity and national security, not solely in terms of content and actors, but in terminology, approach and outcomes. These worlds, however, are linked and dealing with this linkage is important. The second point of agreement was that there is a cyber ecosystem where goods are being bought and sold by a variety of actors. This ecosystem has shown itself to be reactive to new information and structural changes. For example, when a key actor in the trade of malicious cyber tools is arrested, the ecosystem reacts. These points of agreement can prove beneficial in addressing the proliferation of malicious cyber tools.

Mr Herr concluded with a point about malicious cyber tools: they are fundamentally tools of information. The underlying product and the capabilities under discussion are information-based. This has two implications: they can exist in multiple places at once—meaning that exclusivity is difficult; secondly, we own the solutions to the problems we face. In other words, even though we are the potential target of an attack, we control the infrastructure of the attacks and thus the ability to manage these threats rests with us, our States and organizations.

The final presenter for this panel, **Ms Korzak**, explored regulatory questions as regards the proliferation of malicious cyber tools. Echoing Mr Herr's presentation, she suggested the need to focus on *what* the international community is trying to regulate. Is the focus on tools and instruments? What is meant by the word "malicious"? The term "cyber weapon", even though it is frequently used, is defined differently by most actors. A bigger problem still, according to Ms Korzak, is that existing definitions commonly focus on effects or consequences, thus on an *ex post* evaluation, i.e. the damage caused by the cyber weapon. However, regulatory efforts try to identify the tools and technology to be controlled *before* they are used, making most definitions of cyber weapons problematic. In light of this, Ms Korzak explored other ways to address the proliferation of malicious cyber tools. For example, one could explore regulation that focuses on the producer, end user, the use of the tool (including services provided by the producer), or on the notion of intent or motivation.

Furthermore, it is important to address the variety of equities that are necessary to balance in this conversation on malicious cyber tools. These include law enforcement,

international security, human rights, development, industry, and research. Moving forward, one question should be how to weigh these various equities. For example, the Wassenaar Arrangement's 2013 provisions on intrusion software and surveillance technology were in part motivated by human rights concerns, yet were addressed using arms control mechanisms. As there has been an unintended negative effect on the business and research communities, Ms Korzak questioned how to better align the international community's area concern and a mechanism to address the issue.

This led Ms Korzak to her final point on the need for complementarity. There is no single solution to solve the problems faced by the proliferation of malicious cyber tools. A global web of measures is needed, and solutions should range from formal to informal, binding to voluntary, governmental to non-governmental, and domestic to international.

This panel's discussion period explored translatable lessons from extant non-proliferation regimes to cyber stability processes. Some participants highlighted the dual-use nature of cyber tools, which suggests the need to pursue existing dual-use control mechanisms such as the Wassenaar Arrangement. When one participant expressed concern over the exclusivity of the Wassenaar Arrangement (currently 41 members) and the need to expand these provisions to include more States, another responded that the Arrangement was open to any State that fulfils the core obligations detailed in the Arrangement—thus underscoring the strong views and sensitivities surrounding any discussion of control regimes. Another participant noted that control regimes inevitably "catch" some non-malicious purposes, such as research on defensive measures. Numerous participants noted that it is difficult to translate more traditional control measures to the cyber domain. For example, the possession of conventional weapons is easier to verify than in the cyber domain. Due to the ubiquitous nature of the cyber domain and the specific characteristics of cyber capabilities, ascertaining possession of "cyber weapons" is not as clear-cut, and therefore rather than focusing on the control of objects, the international community should address a spectrum of behaviour.

Session 3. Cyber Norms

- **Frédérick Douzet**, Chaire Castex de cyberstratégie
- **Camino Kavanagh**, Senior Adviser, ICT4Peace
- **Madeline Carr**, Senior Lecturer in International Relations, Cardiff University

This panel explored the variety of approaches to norms and normative development in the cyber domain. At present, there are several potential directions for the international community as regards cyber stability processes: some advocate for a treaty-based arrangement much like the outer space security regime whereas others would prefer an arrangement focused on situating controls on cyber conflict within existing IHL. The goal for the GGE process is to define a framework for responsible State behaviour and to promote security and stability in cyberspace; a large part of that will invariably include norms and normative developments.

The first panellist, **Ms Douzet**, provided an international perspective on cyber norms. She began by explaining that the perception of risk and threat varies greatly across countries and is inherently linked to geopolitical context. She and her team have mapped these risks and found great variance. In ASEAN, for example, the risk of conflict escalation relates to territorial disputes paired with the risk of major financial and economic crises. However, there is variance between States within regions. In one State, the number one perceived risk might be terrorism followed by humanitarian concerns, whereas in another it may be climate change. Thus the perception of cyber risk—and the importance accorded to it within each government—varies considerably.

Cyber risk itself is highly complex and transborder in nature; it also feeds into greater arms control and international cooperation conversations. In some communities, it is seen as a new security challenge whereas in others, it is seen as a traditional risk emanating from geopolitical threats. As regards the latter, cyber capabilities are then a tool for States to increase their power, which can reduce the incentives for States to cooperate or share information. Efforts to stabilize the domain are further complicated by the overlap between these two perceptions of cyber risk—and the competing interests that come with each.

Ms Douzet also noted that the perception of cyber risk was inherently linked to disparities between States in terms of cyber capabilities. This includes varying defensive and offensive capabilities and levels of dependency on foreign networks. There are varying levels of development in legal frameworks, cybersecurity strategies and general cyber "maturity". These disparities in turn influence a State's perception of its own vulnerabilities and strengths. Ms Douzet continued by exploring the implications of these perceptions on the elaboration of international norms. She noted that some States place emphasis on conflict prevention whereas others attempt to create a framework for countermeasures, sanctions and pre-emptive strikes for coercive purposes. Some States emphasize sovereign control of information and communication technologies whereas others support the free flow of information. These implications have an impact on what States seek to protect and manage through the elaboration of norms. They further influence the question of whom States seek to pursue dialogue with, i.e. like-minded States, a larger group of States, civil society and/or the private sector.

In conclusion, the international perspective on norms differs considerably due to varying geopolitical realities and the conflation of perceptions of risk and threat. Some of these issues are easy to reconcile; others are more challenging. Ms Douzet reminded participants that technology advances rapidly, and therefore States need to develop norms and reconcile conflicting perceptions before this becomes more difficult.

The next panellist, **Ms Kavanagh**, provided an overview of the voluntary norms enshrined in the 2015 GGE report. This expanded list of norms included important recommendations on, inter alia, attribution, national computer emergency response teams (CERTs), critical infrastructure, and stemming the spread of malicious cyber tools. The question is whether the existing normative corpus for the cyber domain is sufficient or whether the 2016–2017 GGE should focus on identifying new norms. In her view, deepening existing norms would be more valuable than creating new ones at this stage. The list of norms in the

2015 GGE report is a substantial step forward: if all actors were to implement them, it would contribute to greater cyber stability.

However, she noted that challenges remain. For example, less progress has been made on the question of attribution. According to this norm, States should consider all relevant information including the larger context of an event, geopolitics, and the nature and extent of the event's consequences. In addition, attribution difficulties persist. Some form of an international arbitration mechanism has been proposed. Were such a mechanism to be pursued, Ms Kavanagh believed it would be key to determine how such a mechanism would involve technical experts, given the highly technical nature of attribution in cyber operations.

Formulating norms on zones of non-engagement would represent an important step forward in clarifying which types of behaviour are not permitted (for example conducting cyber operations against a State's critical infrastructure or CERT). Many norms in the 2015 GGE report suggest that States have the responsibility to protect their own critical infrastructure and Ms Kavanagh affirmed that many are taking the relevant steps to achieve this. For example, the EU and the United States have agreed on a formal mechanism for the protection of critical infrastructure. This is an important development because such protective requirements have historically been voluntary and therefore it was difficult to ascertain how States were addressing this issue. Resilience measures overall are moving forward in some positive ways.

Ms Kavanagh considered that one of the core tasks of the next GGE will be to examine existing, mutually agreed norms and to determine what has been done to-date, what is missing and what can be developed further. Additionally, it is important to explore how to engage technical experts, civil society and industry in this process. In conclusion, Ms Kavanagh suggested that greater effort will be needed to create an environment conducive to ensuring that mutually agreed norms are respected. Given the shifting geopolitical climate, this is likely to be the most challenging issue, which consequently underlines the importance of TCBMs.

Next, **Ms Carr** began by noting that norms are a social process and the pursuit of norms can be frustrating, tedious, slow, uncertain and, at times, they can also be regressive. In order to facilitate thinking about next steps beyond the GGE she explored different ways of conceptualizing norms.

Ms Carr first focused on how existing and emerging norms can be identified. She noted that norms can emerge from negotiations and discussions like the GGE, but emphasized that they can also emerge from practices without explicit negotiation or recognition. Recognizing norms that emerge from practice is not always easy and is especially difficult in the cyber context. She noted that agency and behaviour can be ambiguous in the cyber environment: it is not always clear where a given action is taking place, or from where it originates. The speed at which things move in the cyber domain complicates this further.

Ms Carr continued by giving an example of how a norm on State practice was made "visible" in the cyber domain. In 2008, the Government of Pakistan asked Pakistan

Telecom to block YouTube access within the country as a result of the site carrying what was considered to be offensive material. Pakistan Telecom attempted to block the site, but mistakenly temporarily blocked YouTube worldwide. This was a technical mistake made at the level of the Border Gateway Protocol (BGP), a fundamental protocol used to route traffic across the Internet. The mistake was recognized and reported immediately. The Government of Pakistan instructed Pakistan Telecom to fix it, which it subsequently did, and the Government then issued an apology. This was not the first time there had been an issue with the BGP. However, this instance, according to Ms Carr, had a political dimension. Within the technical community, it had already been commonly understood that altering the BGP was off-limits, whereas it was not necessarily apparent that this norm also applied to State behaviour. However, the Government's reaction offered evidence that responsible State behaviour extends to the protection of the BGP. This is an example of the "spill over" of a norm into the political domain.

Ms Carr suggested that one can recognize norms not just by what actors agree is acceptable behaviour explicitly, but also by examining actions which actors feel the need to deny, hide or justify. For example, is the need to justify an action necessary because there is a widespread expectation that this type of behaviour should not take place? Ms Carr noted that not every denial or hiding of behaviour indicates a norm a priori. Rather, this was a place to zoom in and determine if there were any normative processes at play. She concluded her presentation by reiterating that norms are a social process whose power stems from the fact that actors internalize them and believe they should behave as these norms dictate.

The discussion picked up on the exploration of norms and whether the next GGE should deepen or expand the existing normative corpus. One participant enquired as to how one can strengthen voluntary norms. Others commented on the appropriateness of the GGE process and the UN as forums for establishing global norms. Several believed that the GGE process was too exclusive to produce global norms. It was noted that the GGE became the focal point for these discussions by default and one participant highlighted the fact that there are other multi-stakeholder forums where these issues are being discussed. One participant raised the critical distinction between a norm and a rule. For example, one party can establish a rule and if they have sufficient power, they can enforce it. A norm, by its very nature, is a social process which parties agree to endorse. Thus norms traditionally evolve in a widely acceptable way, as opposed to rules that may need to be enforced by powerful actors.

Session 4. Looking Ahead: The GGE and Beyond

- **Alexander Klimburg**, Director, Cyber Policy and Resilience Programme, Hague Centre for Strategic Studies
- **YUE Ping**, Deputy Director, Cyber Security Office, Department of Arms Control and Disarmament, Ministry of Foreign Affairs of the People's Republic of China
- **James Lewis**, Senior Vice President and Director, Strategic Technologies Program, CSIS

With a new GGE mandated to start meeting in August, this session explored not only whether the new GGE should deepen or broaden its work, but also what sort of process or mechanism is appropriate in the longer term to deal with the international peace and security dimension of cyber issues.

Mr Klimburg considered how norms interact with one another in the cyber domain. He explained that norms come in various shapes and sizes. There are *regulatory norms* that define what behaviour actors can and cannot do. There are *prescriptive norms* that prescribe actions that are to be taken in certain situations. And there are *constitutive norms* that establish new actors, behaviours and/or interests. He highlighted the fact that there are different norm regimes in the cyber domain, including regimes made by governments and the private sector. One example of a norm regime originating entirely from the private sector was that of operator and content agreements for the routing of Internet traffic. Mr Klimburg stressed that there are a significant number of non-State norms.

Next, he moved to cases of norm collision. Norm collision represents a challenge for global normative processes in the cyber domain. Individual norms exist within all regimes and have no automatic legitimacy across different regimes. Even for a commonly held norm within a community, there can be variations in implementation. But what happens when norms collide? For example, there are various crisis communication instruments around the world that represent a general normative development. However, at the international level, competing regime norms on crisis communication can create confusion and duplication when they collide. To achieve norm coherence, it is important to concentrate on linking regimes around the world to create clusters that further exchange information on norms. It will also be important to invite standing rapporteurs to report back between forums. It may also be helpful to consider arrangements for permanent dialogue between regimes to allow for sustained cross-fertilization.

Ms YUE Ping began her presentation by affirming that it is the shared responsibility of the international community to pursue a global, rule-based cyberspace in order to prevent it from becoming a lawless frontier. With GGE-based dialogue deepening over the years, the UN has made positive progress in this respect. She noted that the previous GGEs have emphasized several principles such as peace, State sovereignty, and the prohibition of the threat or use of force. Additionally, GGE reports made important recommendations on norms, counter-dispute measures and capacity building. The 2016–2017 GGE should

build upon the previous reports and go further, in the hope of making practical and effective recommendations.

Ms YUE explored three points on how best to promote a peaceful and secure cyberspace. The first concerned the relationship between important elements of a ruled-based regime in cyberspace. She suggested that the international community could begin with voluntary norms and build trust towards a legal arrangement. The second point is to identify key issues in terms of priority. In her view, cyberterrorism is one high-priority issue on which the international community should focus. She also highlighted the importance of the protection of critical infrastructure in finance, electricity, communication and transportation. These sectors should constitute the top priority in cyber security, given the possibilities for severe disruption and financial chaos, with devastating consequences. The third and final point concerned capacity-building. The international community should build a cyberspace that is both safe and prosperous. She acknowledged that a country's level of security was also dependent on its level of economic development. Therefore, it will be important to consider boosting economic growth through capacity-building and cooperation, for example on e-business. She concluded by reminding participants that the cyber domain has transformed the world into a global community with a shared destiny and that the aim should be to work on a common, lasting security.

The final panellist, **Mr Lewis**, provided some remarks on the GGE process. Looking back on the process itself, he said that it had been very successful. Upon the conclusion of the 2015 GGE, however, many commentators wondered whether the process had reached the end of its utility. There will be another GGE in part because the international community has yet to agree upon an alternative way forward. The GGE process has evolved into a proxy for negotiations between States. Mr Lewis called for the international community to take a step back and ask whether the current direction is the most preferable. He noted that the question that should be asked is: what is the best vehicle in the coming years for reaching an international agreement on how best to create a secure and stable cyberspace? While the GGE process has been effective thus far, the value of it as a continuing process will depend on whether the 2016–2017 GGE achieves a consensus report, and that report's reception by the international community as a whole.

The discussion period explored the issue of multilateral dialogue on cyber stability beyond the GGE. One participant suggested a model such as that of the Organisation for the Prohibition of Chemical Weapons, with a treaty supporting its programme of work, an attribution mechanism, and a capacity-building role. Another participant suggested that what is created will depend on what the focus is for the international community on cyber stability. If the focus is more on international peace and security implications, then the resultant model would be different than, for example, if the focus were more on a multi-stakeholder global governance approach. Other participants believed that it was premature to establish a larger cyber-specific agency and that it would be preferable to mainstream existing structures and deepen the role of INTERPOL and local cyber agencies on specific topics such as crime. These participants advocated for a concerted focus on building local capacity around the world to ensure greater resilience.

Closing Remarks

In her closing remarks, **Ms Vignard** said it was clear that the international community agreed on the importance of cyber stability, and that progress had been made towards involving an ever greater number of governments in these discussions. However, there remains a full agenda of work ahead—including the 2016–2017 GGE and beyond. She thanked CSIS, the seminar's sponsors, and the participants for the highly constructive and informative seminar.

UNIDIR

UNIDIR Cyber Stability Seminar 2016

Taking Security Forward: Building on the 2015 Report of the GGE

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 significantly altered the political landscape for international cooperation on security issues in cyberspace. The GGE's 2013 Report, which included an agreement among participating states that international law applies in cyberspace, set important precedents for norms and other cooperative measures that will shape future discussion of cybersecurity. More recently, the 2015 Report included a reaffirmation of the applicability of international law, and for the first time, a list of voluntary norms for state in cyberspace during peace time. It also included a norm that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions." A new GGE is slated to begin work in August 2016.

This seminar considered how the international community can operationalize and build upon these consensus reports—and generate momentum for a successful 2016-2017 GGE. The seminar brought together stakeholders from the Geneva diplomatic community, industry, and capital-based policymakers to discuss and explore how to leverage the GGE process to promote a peaceful, stable and secure cyber environment.