UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Report of the International Security Cyber Issues Workshop Series

Acknowledgements

Financial support for the **International Security Cyber Issues Workshop Series** was received from the Governments of the Netherlands and the United States of America.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to 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 the author. They do not necessarily reflect the views or opinions of the United Nations or the sponsors of this project.

The report was drafted by James Lewis with support from Kerstin Vignard.

Table of Contents

Report of the International Security Cyber Issues Workshop Series

The work of the United Nations (UN) Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is the focal point for the international discussion of cybersecurity. The GGE reports of 2010, 2013, and 2015 set the negotiating agenda for cybersecurity, launched a series of efforts at capacity and confidence building, and altered the political landscape for international cooperation by recognizing the centrality of the UN Charter, international law and national sovereignty for global cooperation. To build on this success and maintain momentum, the UN has scheduled a fifth round of GGE meetings to begin in August 2016.

Progress has not come easily. Achieving consensus in the GGEs is a demanding task, given the compressed time for discussion and negotiation, the complexity of the subject, and the range of national views. GGE outcome documents have been shaped by complex negotiations on balancing freedom of expression with terrorist use of the Internet, on the nature and legitimacy of cyberattack, and by the larger tension between national sovereignty and universal values. These are core issues that arise repeatedly.

In light of this complexity, it may be useful to provide an overview of key issues that have shaped GGE discussions. In 2016, the UN Institute for Disarmament Research (UNIDIR) and the Center for Strategic and International Studies (CSIS) organized three expert workshops to open and broaden the discussion of international norms for responsible State behaviour in cyberspace and to identify new ideas to support further progress by the international community. The first focused on identification of new norms, the second on the application of international law, and the third on ways to manage the spread of malicious cyber tools. The intent was to build on past progress and to expand the space for international agreement on measures to increase stability and security in cyberspace.

I. UN Groups of Governmental Experts

The UN began its discussion of information security in 1998, with the adoption by the General Assembly of a resolution proposed by the Russian Federation.[1] This put cybersecurity[2] on the General Assembly's agenda for the first time. The most important venue for discussion of this issue has been the GGEs convened by the Secretary-General at the request of the General Assembly. There have been four GGEs convened on developments in the field of information and telecommunications in the context of international security: 2004–2005, 2009–2010, 2012–2013, and 2014–2015.[3] A fifth GGE is scheduled for 2016–2017.

The process for establishing a GGE begins with a recommendation from the UN's First Committee (Disarmament and International Security) to the General Assembly that it pass a resolution requesting the Secretary-General, "with the assistance of a group of governmental experts", to undertake a study and "to submit a report on the results of the study to the General Assembly" at a later session.[4] The resolution details the Group's mandate, which, to a large extent, serves as its work plan.

The mandate for the Group, as well as its size and number of sessions, are crafted in consultations and negotiations in the First Committee. Considerations include both political and budgetary aspects. The first three GGEs had experts from 15 nations, the 2015 GGE had 20 members,[5] and the upcoming 2016–2017 group will have 25.

The UN Office for Disarmament Affairs serves as the Secretary to the cyber GGEs. UNIDIR has been the Consultant to all but the 2005 GGE. The Secretary helps to administer the Group, while the Consultant is responsible for synthesizing the Group's discussions, preparing drafts of the report and advising the Chair.

GGEs are composed "on the basis of equitable geographical distribution". The five permanent members of the Security Council traditionally have a seat on all GGEs, and the remaining seats are allocated by UN regional grouping. States often send an official request for a seat on a GGE of particular interest to them, and might even lobby at the highest levels of the Secretariat for a place at the table. The Office of the High Representative for Disarmament has the task of proposing the Group's composition to the Secretary-General, taking into account not only geographical and political balance, but a demonstrated interest in the topic, the number of times that a country has served on other GGEs, whether they are currently serving on a different GGE, etc. Occasionally a government might decline to participate in a GGE if it believes it lacks the personnel or expertise necessary for the work.

Once the countries have been identified, they are asked to nominate an expert to participate in the GGE. In almost all cases, these experts are government officials. There was a mix of experts in the early GGEs on information security, some with diplomatic and others with technical backgrounds. Over time, the composition of the experts has changed, as nations

[1] General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/53/70, 4 January 1999.

[2] The term "cybersecurity" will be used throughout this text, without prejudice to other terms that include "information security" and the more accurate but cumbersome "information and telecommunications in the context of international security".

[3] GGEs are typically referred to by the year that they concluded and thus the year of their report.

[4] While this document is concerned with the GGEs focused on cybersecurity, the First Committee establishes GGEs with relative frequency. Topics addressed by GGEs range from the relationship between disarmament and development, to confidence-building measures in outer space, to fissile materials, among others.

[5] The countries represented on previous GGEs are listed in Annex 1.

have moved to select experts with diplomatic, arms control, or non-proliferation experience. Experts from technical backgrounds can be “left behind” in the sometimes intense diplomatic negotiations that accompany a GGE.

Each GGE selects a Chair from among its members. A strong and skilful Chair is vital to the success of the group. The Russian Federation chaired in 2005 and 2010, Australia in 2013, and Brazil in 2015. While it is the experts who sit at the table (there are no “delegations”), some experts are accompanied by advisers. In the recent GGEs, legal advisers have been particularly common.

The Group, guided by the Chair and shaped by the mandate included in the General Assembly resolution, largely determines its own agenda and work plan. Work, particularly commenting on drafts and informal consultations, is often conducted intersessionally.

Most GGEs meet for four one-week sessions.[6] The Group holds its meetings in the UN format, sitting for six hours a day (from 10 a.m. to 1p.m., and then again from 3 p.m. to 6 p.m.), with simultaneous interpretation into all six official languages of the UN. The GGE’s meetings are closed and there are no publicly available meeting summaries. The closed door format is essential for the frank discussion that GGEs require to find agreement. Thus there are also no observers—whether representatives from other governments, non-governmental organizations, the private sector or international organizations such as the International Committee of the Red Cross. On more than one occasion it has been suggested that the International Telecommunications Union (ITU), the UN specialized agency responsible for developing technical standards for information and communications technologies (ICTs), might be invited to observe the group. However, the General Assembly mandates place the work of the GGEs squarely in the realm of international security and disarmament and thus not as a technical exercise.

That the GGE falls under the UN’s First Committee has important implications for how the Group interprets its mandate, by focusing and narrowing the scope of the task. The First Committee is a Main Committee of the General Assembly and is allocated agenda items on disarmament and international security. GGEs have decided after multiple discussions that issues that are not under the purview of the First Committee—such as espionage, Internet governance, development and digital privacy—are not the focus of the Group’s work. While terrorism and crime are important topics for understanding cybersecurity, previous GGEs have limited themselves to calling for greater cooperation among States, while deciding that detailed discussion of these topics and the development of recommendations for them is best done in other UN bodies.

The GGE Reports

The GGEs have been the most important vehicles for setting the global agenda on cybersecurity. Each of the GGEs made valuable progress towards international agreement on responsible State behaviour in cyberspace. GGEs operate by consensus—the whole group must agree upon the report in its entirety. There are GGEs that have failed to do so—the first GGE in 2004–2005 is a notable example.

In case of inability to reach consensus, the Chair transmits a purely procedural report to the Secretary-General, listing the members of the group and the meeting dates. In cases of consensus, the Chair transmits the text of the report to the Secretary-General, who

[6] The 2005 and 2013 GGEs met for three one-week sessions.

transmits it to the General Assembly. The Group asks Member States to, for example, "actively consider" the recommendations within the report and how they might be implemented. The First Committee generally "welcomes" the GGE report and, in the words of the 2015 resolution, calls on Member States to be "guided in their use of information and communications technologies by the 2015 report".[7] The recommendations of the GGEs are not legally binding on Member States. GGE reports provide valuable advice and suggestions to the General Assembly, the Secretary-General, and to Member States as they consider how best to move forward the discussion of security and stability in cyberspace.

One underappreciated constraint on GGE reports is that, as an official document of the UN General Assembly, they have a word limit that includes the report summary, the Secretary-General's forward, the Chair's letter of transmittal, and a list of the experts, in addition to the text of the report itself. Taking these into account, often only 4,000 or 5,000 words are available for the actual body of the report.

The first GGE on information security, meeting in 2004–2005, was unable to agree on a report.[8] Two fundamental issues reportedly divided the group: disagreement over how to characterize the threat posed by State exploitation of ICTs for military purposes; and whether the discussion of ICT security should focus solely on the ICT infrastructure or include information content as well.[9] The 2010 report,[10] although short, established the international negotiating agenda for cybersecurity as it called for the international community to undertake work to develop norms of responsible State behaviour, confidence-building measures, and action to build cybersecurity capability on a global basis.

The 2013 GGE[11] created the normative framework for international cybersecurity by stating that the UN Charter, international law, and the principles of State sovereignty applied to cyberspace. The General Assembly resolution on the report "welcomes the effective work" of the GGE and the report. It "takes note" of assessments and recommendations contained therein. The 2013 report reshaped the political context for discussing cyberspace by upending the widely held but mistaken view that the Internet was "global commons". The idea of a borderless cyberspace that grew out of millennial thinking on the future of international relations was an impediment to negotiations and agreement and it introduced confusion over the role of States and their responsibilities. It is now widely accepted that the Internet has borders and depends on a physical infrastructure that is subject to sovereign control. The recognition of sovereignty usefully embeds international discussion of cybersecurity in the existing framework for obligations, State practice, and understandings among States.

The 2015 report[12] expanded the work of 2013 on norms, the application of international law and confidence-building measures. In a stronger endorsement than that of 2013, the General Assembly welcomed the report and called upon Member States to be guided in their use

[7] General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/70/237, 30 December 2015, paras 1, 2a.

[8] The Group's procedural report is contained in General Assembly, *Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, UN document A/60/202, 5 August 2005.

[9] See United Nations Office of Disarmament Affairs, *Developments in the field of information and telecommunications in the context of international security*, ODA Fact Sheet, July 2015.

[10] General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010.

[11] General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/68/98*, 24 June 2013.

[12] General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015.

of ICTs by the recommendations laid out therein. Among the norms recommended by the 2015 GGE are that States should cooperate to prevent harmful ICT practices and should not conduct or support ICT activity that damages or impairs critical infrastructure. The report called for the increased exchange of information and assistance to aid in the prosecution of terrorist and criminal use of ICTs, noting that States should guarantee full respect for human rights, including privacy and freedom of expression.

The mandate for the upcoming GGE, contained in resolution 70/237, tasks the GGE "to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them", including "how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States", and "confidence-building measures and capacity-building" measures.

II. Some Fundamental Issues

Several broad issues have been recurring themes in the discussions of every GGE—the nature of malicious cyber actions, terrorism and content control, attribution of malicious cyber actions, and the nature of the Internet and its implications for sovereignty. Resolution of these issues is far in the future and will require much more discussion and debate. The challenge for each group has been to craft consensus language that addresses each issue, and sometimes this requires very general language or a discussion that takes note of the issue without taking a position.

The Nature of Malicious Cyber Actions

An issue that arises frequently in discussions of cybersecurity is the nature, scope and effect of a cyberattack or other malicious cyber action. An adequate understanding of the nature of malicious cyber actions is particularly important for the GGE's work, given the centrality of the concepts of "use of force" (which appears in Article 2.4 of the UN Charter) and "armed attack" (Article 51). While these concepts are central to the discussion of cybersecurity they are also exceptionally difficult to define, in part because the nature of cyberattacks is itself subject to wide variation.

Most experts agree that there have been thousands of incidents of cyber espionage and cybercrime (the most costly usually victimize financial institutions). In contrast, there have been perhaps a dozen incidents of countries using cyber tools for political coercion, and perhaps only three or four incidents that experts would qualify as the use of force or armed attack—these have involved physical destruction, and there is an implicit threshold generally held among nations that a cyber incident that produces physical destruction, casualties, or death would qualify as the use of force.[13]

These terms, "use of force" and "armed attack", are drawn from the UN Charter, in Articles 2.4 and 51. The experience of the GGEs has shown that it is preferable to use these two terms, grounded as they are in international law, than the imprecise term "act of war".

[13] Both government and non-governmental sources maintain their own resources for classifying cyber incidents. For example, CSIS maintains a rolling list of "significant cyber incidents" since 2006 which helps to indicate the breadth and scope of malicious cyber activity. See "Significant Cyber Events", CSIS, July 2016, https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-events

Deciding what is an act of war is a political decision reserved to the individual State. Reaching international agreement on what qualifies as the use of force or an armed attack remains a crucial problem for international negotiation and agreement on cybersecurity.

Malicious cyber actions can have a range of effects. “Denial of service” attacks flood the target computer network with huge amounts of traffic, causing a temporary disruption of services. Denial of service attacks are basic in that they do not involve gaining access to the target computer. Many nations do not regard denial of service actions as attacks but rather as a noisy and annoying form of online protest. More damaging attacks gain access to the target network and disrupt data or services (“disruptive incidents”), perhaps erasing data. The most damaging attacks, of which there have been only a handful, cause physical damage. These attacks gain access to the target network or computer and disrupt services, but also cause physical destruction (the most famous example being Stuxnet). A few experts have suggested that in some instances a cyberattack could produce an effect equivalent to that of a weapon of mass destruction.

Denial of service attacks do not involve entry to the victim computer, which is the hallmark of more advanced attacks. In simple terms, more advanced cyberattacks involve the covert insertion of malicious software onto the target computer. This malicious software, when run by the target computer, creates damage or disruption. The most damaging attacks require the most skill, and these skills are not generally available to non-State actors (although this may change at some point in the future). The most damaging attacks also tend to be precise, tailored to affect specific software and computer systems. The caveat to this precise nature of truly damaging cyberattacks is that some States possess damaging or disruptive capabilities that could have mass effect, but an attack that could produce mass effects faces both technical and operational constraints that suggest that such attacks are unlikely to occur.

There is a general, if implicit, understanding (derived from existing international law and practice) among many nations that this last category (physical destruction) could qualify as an armed attack or use of force, particularly if there are casualties as a result of the event. There is also general agreement that denial of services incidents would not usually be considered an armed attack or the use of force. However, disruptive incidents (the middle category) fall into a grey area and there is no consensus on the level of disruption they would need to cause to qualify as the use of force. Nations have been reluctant to establish precise definitions, noting that the terms “armed attack” and “use of force” are themselves not precisely defined in the Charter. However, in the physical world an armed attack or the use of force is usually obvious and a weapon can be easily defined and identified. The same is not true for actions in cyberspace and this can complicate the discussion of security issues and the application of international law—but not to the point where further progress on norms for responsible behaviour and stability are impossible to develop.

The Internet and Cyberspace

One important fact that shapes GGE discussions is that there is now a clearer understanding of the nature of the Internet and cyberspace, an important change since many of the initial assessments from the technical and Internet communities were in error. It is not a global commons, it is not independent of sovereign control, and its core technologies change very slowly. The Internet depends entirely on a physical infrastructure that is subject to national jurisdiction. Each nation can apply its laws to its national network infrastructure, consistent with its international commitments on human rights and trade. The idea of a global commons was an illusion created by the ease and speed of connectivity to sites in other countries, and one of its chief drawbacks is that calling cyberspace a commons muddled and diminished State responsibility for security, enforcement of laws, and protection of the public good when no other actor had the capabilities or right to provide these public functions.

In addition to the physical infrastructure of the Internet, there is the "logical infrastructure", the protocols or rules embodied in computer programmes that govern computer and network operations and allow for seamless connectivity. These include the Transmission Control Protocol and the Internet Protocol (TCP/IP), which are networking protocols that allow devices to connect, and the Domain Name System (DNS), which is a hierarchical addressing system that provides a "name" for every device connected to the Internet and allows Internet users to send traffic to each other. These protocols and systems were developed years ago, provide stable and reliable connectivity, and have proved to be easily scalable from a few million users to several billion.

Concern over political control of the DNS system is misplaced and reflects a misunderstanding of the Internet's architecture, which was designed not to have any single point of failure (and thus also lacks any single point of control). It is globally distributed (for security reasons). There are thirteen top level domains in this hierarchical system, but there are also hundreds of "root servers" distributed around the world and not controlled by any government or private entity. The non-profit organization ICANN[14] acts as a coordinating body to ensure compatibility among Internet addresses and a subsidiary body, the Internet Assigned Numbers Authority (IANA), ensures technical coordination among servers.

The global nature of the Internet and the interconnectivity of the root servers means, however, that there is a degree of interdependence in the logical infrastructure. There have been three reported "denial of service" attacks against the DNS system, in 2002, 2007 and 2015. The built-in redundancy of the DNS system prevented the attacks from having serious consequences. Protecting the infrastructure of the Internet has been a topic of discussion in the GGE for the development of additional norms, the idea being that nations would make the commitment not to damage the global infrastructure and avoid disrupting its operation.

Attribution and Evidence

One central dilemma for the application of international law to cybersecurity is the difficulty of attributing the source of a malicious action. Many diplomatic and legal remedies are predicated on being able to establish culpability; this can be difficult in cyberspace. Malicious actors take advantage of the ease with which identity can be misrepresented or concealed in cyberspace. This is changing for the better, but slowly and unevenly. A few private companies now have the ability to attribute malicious actions through forensic investigation, and a few countries have developed strong attribution capabilities using both forensic investigation and their national intelligence capabilities. Forensic investigation involves examining the malicious code left on the victim's computer and tracking, when possible, both the source of the malicious code, the destination to which stolen information is sent, and the location of the "command-and-control" servers that carry out the attack. Attribution remains difficult and is not always possible, but it is much more possible than it was a few years ago.

[14] Internet Corporation for Assigning Names and Numbers.

One dilemma for international negotiations is the uneven distribution of attribution capabilities among nations. A very small number of the leading technological powers have strong attribution capabilities, resulting from both strong domestic information technology industries and advanced intelligence capabilities.

Most other nations, both developed and developing, do not have similar capabilities. There have been proposals to remedy this situation by creating an international institution like the World Health Organization (WHO) or the International Atomic Energy Agency (IAEA) that would investigate and determine attribution for the international community. However, this suggestion, while attractive in an academic setting, is in fact impractical and unimplementable. Cyberattacks, unlike a disease, are not a natural phenomenon but are, rather, the consequence of intentional human action. Thus investigations of the "origin" of an outbreak will be hindered by at least one party not wanting the investigation to succeed. In the case of the IAEA, there is a near-universal treaty that constrains the development of nuclear weapons and tasks the agency to administer safeguards to verify that States fulfil their non-proliferation commitments. There is no similar political agreement to constrain cyberattacks and the most powerful actors are unlikely to cooperate in investigating their own actions. Perhaps the most apt analogy would be that of the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO), which established an international monitoring system designed to detect a nuclear explosion conducted anywhere on Earth. Similar to the IAEA, the work of the CTBTO is grounded in a treaty regime[15] that expresses clear prohibitions as well as provides legitimacy for the establishment of the global monitoring network.

Sovereignty

Key concepts—self-determination, sovereignty and legitimacy—shape the expectations of populations and elites in countries around the world for Internet governance and cybersecurity. Sovereignty is the foundation of the international system, but it is a dynamic concept that evolves in reaction to political forces and technological change. The Internet, with its seamless and rapid connectivity and its ability to disseminate ideas and opinions readily to a global audience, affects sovereignty and at first seemed to undermine it. However, cyberspace is being "normalized" and is no longer seen as a unique space where existing rules do not apply. In cyberspace, sovereignty means that national laws apply to networks located in a country's sovereign territory, subject to its international commitments. National sovereignty, and the rights and responsibilities that come with it, is an essential element for defining responsible State behaviour in cyberspace and for developing international commitments to increase stability and security. States are responsible for their actions and the actions of their citizens, as well as for actions taken from within their sovereign territory.

With the recognition that cyberspace is based on physical infrastructure located in sovereign territory, the concept of sovereignty has become progressively more influential in the development of a cooperative approach to international cybersecurity. Sovereignty reshapes international expectations about cyberspace, reflecting an emerging consensus that responsible State behaviour is derived from existing international norms and commitments as they apply in the physical world. However, sovereignty is not absolute. International agreements constrain it. In particular, the UN Charter, the Universal Declaration of Human Rights, and the agreements establishing the World Trade Organization, are all agreements by which nations have voluntarily surrendered some of their sovereign rights.

[15] Although the treaty has yet to enter into force, the International Monitoring System is completely operational.

The applicability of national sovereignty to cyberspace is no longer in contention. The debate is now over the scope and nature of sovereignty, the extraterritorial application of national laws (particularly when citizens of one State view material hosted on websites in another State), and the balance between national sovereignty and universal values. While there is general agreement that States have the same responsibility for cyber actions as they do for actions in any other realm, some States seek to expand (or restore) their sovereign authority, in reaction to what they see as interference in their internal affairs, while others seek to defend existing "universal" commitments. Powerful tensions between sovereignty and universal values shape GGE discussions, as do differing national views of the scope of sovereignty and the extraterritorial application of national laws to online activities. As with other issues, achieving consensus requires finding a balance between opposing views. The essential conclusion, however, is that cyberspace is not a unique domain but one where the existing rights and responsibilities of States apply, and one task for the GGE is to articulate the nature of the application of sovereignty as it applies to cybersecurity.

III. International Cybersecurity Workshop Series

To help prepare for the next GGE and to identify areas of common understanding and of divergence on cybersecurity issues, CSIS and UNIDIR held a series of three expert workshops in 2016 to open and broaden the discussion of international cybersecurity by mixing diplomats, researchers, and technical experts in a conversation on the GGE, which heretofore had been largely closed to outside communities. The first workshop focused on the identification of new norms, the second on the application of international law, and the third on ways to manage the spread of malicious cyber tools. The objective of the series was to build on past progress and to expand the space for international agreement on measures to increase stability and security in cyberspace.

The workshop series was attended by participants from selected UN Member States, the private sector, non-governmental organizations, and the academic community. The involvement of non-governmental actors in this preliminary process was both unprecedented and helpful, bringing a wider range of views to the issues raised by GGE reports. The sections below give highlights of the key points arising from the discussions. The workshop agendas are found in Annex II.[16]

Workshop 1. International Norms for Cybersecurity (Geneva, 9–10 February 2016)

An international norm is an expectation among governments as to how each will behave. The focus of international negotiations on cybersecurity for the last six years has been the creation of norms for responsible State behaviour and extending current international commitments and law into cyberspace. The international discussion of norms is at a transitional moment. A new negotiating dynamic, driven by broader participation and by contending concepts of cybersecurity is likely to make reaching consensus in the next GGE more challenging.

Non-Western nations, including members of the G-77 and the Non-Aligned Movement (NAM), rightfully expect to play a larger role, and bring to these discussions different views on sovereignty, international law and arms control. Recent NAM statements in the General

[16] Additional materials from the workshops are available at http://www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series.

Assembly call for intensification of efforts to "safeguard cyberspace from becoming 'an arena of conflict' and ensure its peaceful use to contribute to social and economic development".[17]

The themes of disarmament, peaceful use of cyberspace, sovereignty and economic development will have an increasingly prominent place in international discussions. Some nations prefer an approach based on disarmament and the avoidance of arms races or militarization over one that seeks to extend the laws of armed conflict into cyberspace. There will be proposals to expand government control of the Internet. That more countries are concerned about cybersecurity is positive, but it means that future discussions of norms will need to encompass a broader range of ideas. An approach to norms based on arms control and non-proliferation was a valuable starting point for cybersecurity discussions, but it needs to evolve to accommodate new technologies and a broader group of international stakeholders.

The GGEs have been the focal point for progress on global cybersecurity norms. The 2010 report laid out the negotiating agenda by proposing that the international community focus on norms, confidence-building measures, and capacity building. The 2013 report reshaped the political landscape relating to cyberspace by affirming the application of international law, the UN Charter and the principle of State sovereignty to cyberspace. The 2015 report proposed a significant set of voluntary norms and confidence-building measures, including an agreement not to attack critical infrastructure in peacetime, to promote supply chain integrity, and to respond to requests for assistance. The report also "took note" of a country's right to take measures consistent with the UN Charter and international law (including the inherent right of self-defence).

Some outside experts have suggested that the next GGE should consider new norms, including a commitment to protect the critical infrastructure and the "public core" of the Internet, further extension and clarification of the application of existing international law, and perhaps agreement to constrain commercial espionage in cyberspace. While specific norms have been proposed by academics, the private sector, as well as international initiatives led by "like-minded" States, it will be for individual GGE members to decide whether to introduce these ideas into the next GGE discussion.

This first workshop reviewed progress in the development of norms for responsible State behaviour in cyberspace. Drawing on the norms recommended in the last GGE report, the workshop discussed what additional norms may be necessary to limit the risk of unintended consequences in peacetime and protect the underlying infrastructure of the Internet.

The first panel, on the development of international norms of behaviour in cyberspace, began by examining international perspectives on the norms that have been, or could be, considered by the next GGE. Overall, the panel concluded that the increased interest from a broad range of countries is promising but requires renewed efforts to promote these nations' cybersecurity policy awareness and technological capacity in order to avoid skewed risk perceptions between countries of different capabilities. The more that developing countries can be brought into the international process and made to feel that they have a stake and role in the shaping of norms, the greater the chances that the GGE's proposals and recommendations will be adopted. While the issue of sovereignty will continue to arise, the panellists agreed that it is likely that most States would be able to find common ground

[17] "Cyber Warfare, unchecked, could topple entire edifice of international security, says speaker in First Committee at conclusion of thematic debate segment", *General Assembly Meetings Coverage*, 29 October 2014, http://www.un.org/press/en/2014/gadis3512.doc.htm

in norms on how States can cooperate to protect critical infrastructure in nation States and for the Internet as a whole.

Panellists pointed out that the discussion of norms is just as important for developing countries as for developed countries, since they are growing equally dependent on ICTs and the Internet. These countries not only see sovereignty in terms of non-intervention but also as an obligation to protect what is within their own national space. Experience has made them aware of the importance of cyberspace, but in terms of common understanding, developing countries are at very different levels and expectations vary among regions. GGE norms are and can be supplemented at the regional level, where differences in capacity, investment, and political sensitivities are more readily accommodated. Other speakers noted that differences in risk perception are linked to different capabilities.

The second panel featured technologists' perspectives, and explored what technological norms might be feasible. It focused on how the norms developed by the GGE, especially those prohibiting the targeting of critical infrastructure, could be deepened and made more explicit. Of primary concern was the vulnerability of the Internet's architecture, with the targeting of a root server largely agreed upon by the panellists to be an attack constituting the disruption of critical infrastructure. Attacks on the DNS and protocol vulnerabilities were also suggested as further examples of attacks that could be explicitly referenced through norms.

The panellists noted that State policies to promote technological or data sovereignty become a problem if they interfere with routing protocols, highlighting the complex interplay between technology, commercial interests and security, and the potential for unintended consequences to global security from such policies. The norms developed by the 2015 GGE, especially those prohibiting the targeting of critical infrastructure, could be expanded to avoid this. A starting point might be for States to agree to avoid cyber operations that damage "essential civilian infrastructure".

The technologists also emphasized the importance of preserving trust and in creating norms that prevent States from undertaking destabilizing actions. Trust is the core of how the Internet functions, and this trust is undermined if weaknesses in the core protocol are exploited. The panel discussed the idea that the Internet can be seen as a global public good (both the Internet protocols and technical infrastructure). The panellists suggested that there could be agreement on norms concerning the protection of the public core of the Internet against unwarranted interventions by States. The next GGE might consider language on state responsibility to protect the core infrastructure and logical layer of the Internet. One important outcome of this panel discussion is the realization that the tech community is speaking a completely different language to that of the policy community, and that further progress may require development of a "common dialect" for technologists, diplomats, and researchers.

The third panel noted that the GGE's format has evolved over time—with an expansion of the group and a growing awareness of earlier reports. The result, however, is that the GGE format may no longer be adequate to accommodate the interests of the international community as a whole in this issue, since accommodating these interests may require a more formal mechanism for the discussion of the issues that cyberspace creates for international security—one that is anchored in the UN system, that is more inclusive and more transparent.

How sovereignty applies in cyberspace was a recurring theme in these discussions. States are anxious about fulfilling their responsibilities in this new area of public and international interaction and are adopting new rules and technologies that provide them with greater control. What we are seeing now is the extension of sovereignty into cyberspace, which used to be largely shielded from sovereign control by the belief that it was a commons. This extension is now unavoidable given many States' perception that the risks to public interests created by the Internet require their intervention. Panellists urged the GGE to consider how, in an environment of expanding national control, to safeguard the global, interconnected nature of cyberspace and to consider ways to promote and support the security and stability of its global qualities.

Some panellists asserted that it is essential to engage the private sector in the development of cyber norms. They also argued that it is important to think about norms as broadly as possible and avoid being narrowly focused on norms specific to peacetime only. New approaches to international cybersecurity could propose mechanisms for monitoring and sharing information on the threat landscape, engaging the private sector, and building capacity to enable countries to implement norms, particularly norms designed to address the risks to stability and peace from actions in cyberspace below the level of armed conflict.

The final panels considered the future of efforts to build international cyber norms, concluding that the most important outcomes the GGE could achieve would be the promotion of capacity building, the establishment of mechanisms to preserve stability and limit the threat of escalation, and the adoption of broadly accessible language to reach a diverse constituency of both States and private partners. The greatest immediate benefits would be found in norms relating to actions below the level of armed conflict in cyberspace. The panellists also touched on the topic of attribution, with some maintaining that attribution had been almost entirely solved as a problem, while others maintained that it is still not possible to determine technical attribution firmly enough to enable political attribution.

The GGEs have recommended norms that (a) define responsible behaviour by States in cyberspace, (b) apply existing international commitments for conflict and human rights, and (c) agree to restrict the use of force against infrastructure where the consequences could be particularly devastating to cyberspace itself. Further progress on norms will be difficult but not impossible.

There was broad agreement among participants that the next GGE could usefully consolidate and refine norms agreed in previous GGEs. While some suggested that the GGE might be better served by focusing on deepening existing norms rather than introducing new ones, the general sense was that more work on norms to protect critical infrastructure would be useful. Future norms might also address non-proliferation of malware and protecting the IT supply chain, and the further elaboration of mechanisms to preserve stability and reduce the risk of escalation.

Workshop 2. The Application of International Law in the Context of International Cybersecurity (Geneva, 19–21 April 2016)

This second workshop brought academic and non-governmental experts together with government policy and legal experts to discuss how international law applies to State conduct in cyberspace, one of the more difficult issues that will confront the next GGE. It also examined whether the discussion of the application of international law has advanced sufficiently to allow for meaningful progress to be made in international negotiations. The central conclusion is that this discussion has not made sufficient progress, given significant political differences on how cyber conflict should be approached in the international system.

To help prepare for further work, this seminar examined salient issues in the application of international law to cybersecurity and State responsibility in the context of disarmament and international security. The intent was to better inform future discussion and provide a range of views from non-governmental experts.

Discussion in the workshop made clear that how to apply international law to cyberspace is not a straightforward choice, as it involves decisions on how malicious cyber actions relate to the concepts of force and attack, the implications for cybersecurity of agreements on human rights, the nature of sovereign responsibility, and the always contentious issue of how to address terrorist use of the Internet. Differing national legal traditions and perspectives further complicate the discussion.

The ground-breaking report of the 2013 GGE emphasized the importance of international law, including the UN Charter and the principle of State sovereignty, as critical to firmly placing cybersecurity in the existing framework of laws and understandings that govern State relations. The 2013 report called for further work to develop common understandings on the application of existing international law and norms, rules and principles for responsible behaviour by States. This was reflected in the mandate of the 2014–2015 GGE, which requested that the Secretary-General and a new GGE continue to study, inter alia, how international law applies to the use of ICTs by States.

How international law applies has been one of the most difficult and contentious issue for the international community to address. Some nations argue that existing international law is inadequate and that new laws must be developed. There are differing views on the nature of armed conflict in cyberspace, the best way to prevent it, and on the application of the principles found in the Hague and Geneva Conventions, including the obligation for States to use cyber techniques in a manner consistent with the laws of armed conflict. Some frame the legal question in the broader tension between national sovereignty and universal commitments, such as the Universal Declaration of Human Rights.

Other re-occurring issues of contention include the application of Articles 2.4 and 51 of the UN Charter to cyberspace, the level of evidence and attribution needed for the assignment of State responsibility, and the application of the right to self-defence or countermeasures by injured States. Additional areas of contention include the role of neutrality and violations of third party sovereignty, cyberattacks by non-State actors, and the implications created by State sovereignty for cybersecurity and responsible State behaviour. The fact that there are divergent views held by governments on these issues is reflected in what appears—and does not appear—in the consensus GGE reports.

How States choose to respond to a cyber incident is, of course, ultimately, a political decision, but such decisions are usefully guided by international law and agreement. Norms remain the focus of GGE efforts, but there is an interplay between norms and international law that shapes the discussion. In the words of the 2013 report, "The application of norms derived from existing international law … is an essential measure to reduce risks to international peace, security and stability". The work of the GGE on the application of international law, while not binding, provides a useful foundation for further discussion and ultimately negotiation on how to promote security and stability in cyberspace.

The first panel noted that there remain differences in the interpretation and application of international law in practice, especially for actions that fall below the threshold of force. These would involve actions that did not cause physical damage or human casualties. The cyber actions that may pose the greatest risk to stability, such as destruction of data, fall into a grey area when it comes to the application of international humanitarian law (IHL), the branch of international law that deals with the conduct of war. These are coercive actions that "destroy" or damage intangible objects, but are not regarded as a clear use of force or an "armed attack".

In the words of the 2015 report, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs". Panellists discussed the principle of due diligence as it applies to State behaviour. Due diligence requires States to ensure that their territory is not used for harmful actions directed against other States. A State is obliged to "take all available measures" and "do all that could be reasonably expected of it" in a specific circumstance. If a State takes all feasible and reasonable measures but is unable to prevent an internationally wrongful act, then there is no violation of principles, but there may still be an obligation to notify and cooperate. While States cannot have absolute knowledge of all things happening within their territory, there are precedential standards based on whether a State knew or ought to have known about a particular activity or action on its territory. There is also a responsibility for States to take preventive measures that are in accordance with their international obligations to protect cyber and critical infrastructure. The challenge for the next GGE will be to strike the right balance on State responsibilities if it is to further develop norms on due diligence.

There was contention over the extent to which the due diligence principle applies to cyberspace—some participants mentioned that due diligence only matters in the law of countermeasures and recommended that the GGE not concern itself with developing obligatory language that would expand the scope of international law; others felt that States already have the obligation to "take all available measures", including cyber means to pre-emptively protect cyber and critical infrastructure. During the discussion, some developing country representatives argued that international law "does not work in our favour", and is perceived as a "net" to control them.

There was also contention over the utility of the work of informal, limited-membership groups to define the application of international law to cyberspace. While some argued that these issues are best left to lawyers to decide among themselves, others, including GGE experts, contended that without agreement among States at the political level, it will be impossible to reach definitive conclusions.

Panellists focused on what they identified as the crucial issues of evidence and attribution, asking how a nation would prepare itself to justify a response or to present evidence (whether at the Security Council, bilaterally or to the international community). States are neither technologically nor politically prepared to do this. Evidence involves identifying the facts to which international law would apply. Attribution of the source of an action contrary to international law and the commitments of States is often a problem for international security but the attribution problem is exacerbated in the case of cyberspace. Attribution is critical for the application of international law, but varying attribution capabilities and differing standards of proof among States complicate the assignment of responsibility for malicious cyber actions.

The second panel highlighted that the 2015 GGE report made significant progress in forging common national views on rules in peacetime, yet found it difficult to establish consensus on the application of international law in wartime. There were also limits to the topics that the GGE covered, based on the mandate given to the group by the First Committee. Workshop participants discussed the value of including legal advisers in the GGE discussions. Legal advisers provide accuracy in the discussion of law, but this accuracy must be used carefully. GGE reports are determined through negotiation and compromise, and ultimately these reports are political, shaped by State interests and achieved by consensus at a political level. Consensus reports are often reached through constructive ambiguity, not legalistic precision.

In the third panel on the law of armed conflict and use of force and armed attack in cyberspace, panellists concluded that IHL applies to cyberwarfare in a *jus in bello* context, where IHL offers protection to civilians. However, they noted that an explicit agreement stating that States should not engage in cyber operations against civilians or essential civilian infrastructure could be useful. The panel concluded that attribution was paramount for the application of IHL, but difficulties arise given the varying capabilities and standards of proof among different States. There was also some debate as to whether cyberattacks constituted "use of force" when they did not lead to physical damage.

There was some discussion of countermeasures, an element of international law that has yet to figure in a GGE report. Some suggested that the next GGE should consider a norm that would read: "the victim State may take actions not involving the use of force in response (or retaliation) to a malicious cyber action by another State". A countermeasure could, for example, entail the Security Council imposing sanctions on the attacking State in order to strengthen and maintain international peace and security.

The third panel discussed how IHL applies to cyber operations when they occur during armed conflict. IHL "regulates the conduct of parties engaged in an armed conflict". IHL sets forth prohibitions and limitations—it is not about legitimization of the use of force. IHL applies in both international and non-international conflicts. It seeks to protect civilians and minimize suffering. It is clear that IHL applies to new weapons, methods and means of warfare.[18] The vast majority of IHL obligations are relatively easily to transpose to cybersecurity. There is a need, however, to clarify some issues when it comes to the application of IHL, including how it applies to cyber operations without kinetic impact or to "attacks" that only affect data. There was discussion as to whether existing international law already addresses State activity in the context of warfare, with panellists arguing that what is needed is agreement on activities below the (still implicit and not formally defined) threshold for the use of force.

Panellists pointed out that, contrary to the claims of some States that embedding the conversation in IHL somehow "legitimizes" cyberwar, IHL sets forth necessary and useful prohibitions and limitations on the use of force and attack in cyberspace. This recurring debate reflects differing understandings of the effects of cyberattack (and in particular whether a cyberattack could produce mass effects similar to those of weapons of mass destruction), as well as the nature of risk in cyberspace, which some argue comes as much from content as from an attack itself.

While discussion of human rights is not part of the GGE's mandate, the fifth panel touched upon interesting linkages among the full range of cybersecurity issues. In the final panel, the experts concluded that the GGE was a useful platform for discussing expected State behaviour and guidelines for norms. The GGE can build cooperation and establish confidence-building measures (CBMs). However, the panellists agreed that more clarity

[18] Article 36 of Additional Protocol I of the Geneva Conventions.

among States on the application of international law was needed to ensure that States were in compliance with their existing commitments.

Workshop 3. Managing the Spread of Cyber Tools that can be used for Malicious or Unlawful Purposes (Geneva, 15–16 June 2016)

The 2015 GGE report included a recommendation that "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions". This workshop explored precedents from non-proliferation for the creation of norms and for the establishment of mechanisms to constrain the use of cyber tools for malicious and unlawful purposes. ICTs have characteristics that pose a number of challenges to efforts to control the spread of tools that can be used for malicious purposes. These include the relative ease and speed with which capabilities can be transferred, as well as the dual-use nature of many cyber tools that also play a critical role in strengthening cybersecurity. The workshop placed this discussion in the larger context of efforts to promote international security in cyberspace.

Experts from industry and the research community discussed current trends in the spread of cyber capabilities that can be used for malicious purposes—these capabilities spread and expand so rapidly as to challenge any effort to control them, how they are being used, and what effects they create. The discussion provided a broad range of views from experts on how cyber capabilities are spreading and possible means to address the challenges that they pose. One fundamental question is whether and when it makes more sense to focus on cyber capabilities or effects. A second relevant distinction worth considering may be weighing the merits of an "export control/non-proliferation" approach versus an arms control approach, and the value of controlling the spread of tools that can be used for malicious purposes (drawing on the precedent of controlling dual-use technologies) versus banning certain capabilities and tools entirely.

There was general agreement that the international community should find some way to control the spread of malicious software tools. However, as the workshop progressed it became increasingly clear that controlling malicious cyber tools using a traditional non-proliferation approach would be extremely challenging. By its nature, new technology can be disruptive, but that in itself does not make the spread of such technology destabilizing. Moreover, there can be significant costs associated with any effort to manage the spread of technologies—including those that can be put to harmful uses. For example, many tools that can be used for malicious purposes can also be necessary for critical network defence and cybersecurity research purposes. There is a risk that impeding the transfer of such items would harm those beneficial objectives.

There was also discussion of how cyberattacks are often highly tailored, designed for a specific target, and thus limit the potential for indiscriminate effect. Since indiscriminate effect is a characteristic of weapons of mass destruction and other banned weapons, the question for cybersecurity may need to focus more on the intent of attacks rather than their effects.

The workshop provided an opportunity for an exchange of views on the aspects of the spread of cyber tools that pose the greatest threats to international cyber stability, and to identify key goals that efforts to manage the spread of such capabilities could pursue. The workshop discussed some of the unique challenges to such an effort that governments should take into account. Such challenges include the dual-use nature of the technology, which makes it difficult to determine whether a particular transfer is intended for harmful or beneficial purposes, and the fact that the global nature of the Internet means that information can be transferred almost instantaneously, making transfers of cyber capabilities difficult to monitor or interdict.

The discussion considered a number of existing mechanisms that have been used to address the spread of other potentially harmful items. For example, the Global Initiative to Combat Nuclear Terrorism (GICNT) is a voluntary regime that seeks to build capacity and cooperation among States to combat nuclear terrorism. Another example is the Proliferation Security Initiative (PSI), a global framework of States that commit to disrupt transfers of weapons of mass destruction, their delivery systems, and related items to and from States and non-State actors of proliferation concern. There are also useful examples of government cooperation with the private sector to secure hazardous materials and sensitive data. While none of these examples provide an exact formula for efforts in the cyber arena, they offer useful lessons.

Perhaps the existing mechanism most relevant to cybersecurity is the Wassenaar Arrangement, a multilateral regime that was established in 1996 to promote international security by regulating the transfer of conventional weapons and related dual-use goods and technologies. Participating States recently agreed to establish controls on malicious cyber tools, yet these new controls have created controversy due to definitional problems regarding what is being “caught”. The Wassenaar Arrangement already controls some kinds of software, but its controls are designed to capture software related to military equipment or controlled production technology—essentially linking the software to military or dual-use hardware (such as the software to run machine tools needed to produce military aircraft parts). This makes it easy to define the scope of controls and the software being captured, but it may also make Wassenaar less useful as a tool to manage access to software products that are not linked to military hardware. Additionally, while agreements like the Wassenaar Arrangement set a useful precedent that might, with care, be extended to cybersecurity, any extension must be mindful of the fact that there may be unintended consequences of further regulation.

Participants in this workshop concluded that the non-proliferation or export control model is likely to be ineffective to control access to these ubiquitous cybersecurity technologies for two reasons. The definitional issue means that there is a real risk that a definition that captures malicious software tools will also capture legitimate products and may inadvertently stifle innovation. Second, any control would be difficult to implement, given the ubiquity of production and the ease of creating malicious software, and could simply shift production to a less regulated or illicit market.

It might be possible to identify a small number of end uses or end users to which governments could restrict exports, while freely permitting sales for legitimate uses and users. Alternative strategies for reducing the availability of dangerous capabilities could also be appropriate. Such strategies include market-based mechanisms, like “bug bounty” programmes, that are aimed at identifying and reducing the number of undiscovered vulnerabilities that malicious cyber actors could develop into tools that they exploit themselves or sell on the illicit market. Other strategies could focus on software or hardware design, reducing the ability of malicious actors to repurpose dual-use products for malicious purposes.

Lastly, the workshop discussed broader efforts to promote stability in cyberspace, including efforts of the GGE to reach consensus on the applicability of international law to cyberspace and certain peacetime norms, as well as bilateral and multilateral efforts to develop CBMs. Participants considered how efforts to control the spread of cyber tools that could be used for malicious purposes could fit into these efforts and, conversely, to discuss how development of certain peacetime norms or CBMs could feed into a larger strategy to address the spread of such tools. Since many cyber norms focus on effects (e.g. harm to critical infrastructure), the workshop considered how a focus on effects—rather than capabilities—may be appropriate in the context of the discussion.

The first panel focused on defining who the predominant actors in cyberspace are, their respective roles, what constitutes an attack in cyberspace, and how these acts can (if possible) be controlled. The second panel analysed to what extent a non-proliferation regime can be successfully implemented in the cyber realm while meeting realistic expectations. The third panel discussed the parallels between nuclear and cyber non-proliferation, and determined that there are many similarities but also that cyberspace is a unique domain that has many independent attributes. As cyber actors need not possess expensive or rare material, proliferation is harder to control. The fourth session examined how to approach attacks in cyberspace given the tools that are currently available, what gaps are there in current strategy, and the effectiveness of regulation. The fifth panel focused predominantly on how to define a malicious cyber tool.

Panellists repeatedly noted that creating a balance among human rights commitments, law enforcement, commercial concerns and international security in relation to cybersecurity is a complex problem. Some panellists even asked how much cybersecurity is an arms control issue, given the variation in actors and capabilities, and the effect of the action taken.

Looking to the future, it may be worth considering the establishment of some kind of open working group to ensure that the conversation among diplomats, technologists and researchers continues. All parties have varying interests, and the involvement of non-State actors, while necessary to some degree, will complicate the discussion. The trends that need to be watched include not only attacks on critical infrastructure, but the increased risks created by reliance on the Internet and cyberspace. Eventually, the deployment of malware could lead to the loss of life: aside from this observable standard, it is difficult to determine the metrics of a cyber arms race because it is not observable in the same way as in the case of other weapons.

Future Discussions on International Cooperation in Cybersecurity

Looking back on the GGE process, it has been remarkably successful since 2010. It has helped catalyse international interest in cybersecurity. The more that developing countries can be brought into the international process and made to feel that they have a stake and role in the shaping of norms, the greater the chances that GGE recommendations will be implemented. Expanding this interest will require renewed efforts to promote not just technical capacity-building efforts, but efforts to increase policymaking capacity in countries around the world.

At the conclusion of the 2015 GGE, many commentators and participants asked whether the process had reached the end of its utility. In some ways, part of the rationale for holding another GGE is the difficulty the international community faces in identifying an alternative way forward in relation to international cybersecurity. Over time, the GGE process has evolved into a proxy for negotiations between States, and there have been suggestions that it might be time to move these discussions to a more regular diplomatic process, such as within the Conference on Disarmament, or a body similar to the UN Office for Outer

Space Affairs Committee on the Peaceful Uses of Outer Space (COPUOS), or by creating a new, open-ended working group. Each of these offers its own advantages, such as being more inclusive or transparent, but also disadvantages, such as a record of ineffectiveness in reaching agreement.

One question the 2016 GGE could usefully ask itself is what would the best vehicle for reaching greater international agreement. New models for multilateral dialogue on cybersecurity beyond the GGE have yet to be widely discussed, and the 2016 GGE may need to consider the issue of how best to take forward—in a more formal, inclusive and transparent manner—the work of building stability and security in cyberspace.

Annex I. List of Member States of the previous Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

2005	2010	2013	2015
Belarus	Belarus	Argentina	Belarus
Brazil	Brazil	Australia	Brazil
China	China	Belarus	China
France	Estonia	Canada	Colombia
Germany	France	China	Egypt
India	Germany	Egypt	Estonia
Jordan	India	Estonia	France
Malaysia	Israel	France	Germany
Mali	Italy	Germany	Ghana
Mexico	Qatar	India	Israel
Republic of Korea	Republic of Korea	Indonesia	Japan
Russian Federation	Russian Federation	Japan	Kenya
South Africa	South Africa	Russian Federation	Malaysia
United Kingdom of Great Britain and Northern Ireland	United Kingdom of Great Britain and Northern Ireland	United Kingdom of Great Britain and Northern Ireland	Mexico
United States of America	United States of America	United States of America	Pakistan
			Republic of Korea
			Russian Federation
			Spain
			United Kingdom of Great Britain and Norther Ireland
			United States of America

Annex II. Agendas from workshop series

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

International Security Cyber Issues Workshop Series:
The Future of Norms to Preserve and Enhance International Cyber Stability

9–10 February 2016
Room XI, Palais des Nations, Geneva, Switzerland

Tuesday, 9 February 2016

9:15 – 10:00 Registration and coffee

10:00 – 10:15 Welcoming remarks

Jarmo Sareva, *Director, UNIDIR*
James Lewis, *Director and Senior Fellow, CSIS*
Wouter Jurgens, *Cyber Coordinator, Ministry of Foreign Affairs, The Netherlands*

10:15 – 11:00 Introductory Keynotes: An Overview of the Development of Norms in the GGE

FU Cong, *Ambassador for Disarmament Affairs of the People's Republic of China to the United Nations, Geneva*
Andrey Krutskikh, *Special Representative of the President of the Russian Federation for International Cooperation in Information Security (statement delivered by Ms N. Sokolova)*
Michele Markoff, *Deputy Coordinator for Cyber Issues, United States Department of State*

11:00 – 13:00 Session 1. International Perspectives on Norms

Moderator — James Lewis
— *How do expectations for cyber norms vary among regions and countries?*
— *How does increased interest from a broad range countries reshape the norms discussion?*
— *Where are the friction points among differing national and regional views?*
— *What do we seek to protect?*
Oleg Demidov, *PIR, Russian Federation*
Elina Noor, *Institute of Strategic and International Studies, Malaysia*
Zahid Jamil, *Developing Countries' Centre on Cyber Crime (DC4), Pakistan*
Katherine Getao, *Ministry of Information, Communications and Technology, Kenya*
Frédérick Douzet, *Chaire Castex de cyberstratégie, France*
Tobias Feakin, *International Cyber Policy Centre, ASPI, Australia*
So Jeong Kim, *Electronic and Telecommunications Research Institute, Korea*

13:00 – 15:00 Lunch Break
Coffee available in front of the meeting room at 14h30

15:00 – 18:00 Session 2. Technologists Perspectives and Ideas for Future Norms

Moderator — Wouter Jurgens
— *What norms best promote stable operations?*
— *Can norms protect the underlying infrastructure of the Internet Itself?*
— *What is feasible and what is desirable for international cybersecurity norms?*
— *How do political norms fit with the existing structure of governance and technology?*
— *Can one verify compliance with norms?*

Olaf Kolkman, *Internet Society (ISOC)*
David Conrad, *Internet Corporation for Assigned Names and Numbers (ICANN)*
Dennis Broeders, *Scientific Council for Government Policy, The Netherlands*
Klée Aiken, *Asia Pacific Network Information Centre (APNIC)*
Marilia Maciel, *Fondação Getúlio Vargas (FGV), Brazil*

18:00 – 19:30 Reception

Wednesday, 10 February 2016

10:00 – 10:30 Welcome Day II

Kerstin Vignard, *Deputy Director, UNIDIR*
Nur Hayuna Abd Karim, *Principal Assistant Secretary of Cyber and Space Security Division, National Security Council, Malaysia*
Olivia Preston, *Assistant Director, Office of Cyber Security and Information Assurance, Cabinet Office UK*

10:00 – 13:00 Session 3. The Future of Norms — Beyond Arms Control

Moderator - Eneken Tikk-Ringas

— *What are the lessons for cyber norms from other regimes?*
— *What is the future of the norms discussion in terms of venue (or venues), format, content?*
— *What are the goals for norms? Stability? Disarmament? Rules for conflict?*
— *What additional norms would limit the risk of unintended consequences in peacetime?*
— *Can "internet governance" and "international security" be separate discussions?*

Cheri McGuire, *Symantec*
Alex Klimburg, *The Hague Centre for Strategic Studies, The Netherlands*
Paul Nicholas, *Microsoft*
Henry Fox, *Cyber and Space Policy International Security Division, Department of Foreign Affairs and Trade (DFAT), Australia*
Mika Kerttunen, *Cyber Policy Institute, Estonia*
Camino Kavanaugh, *Center on International Cooperation, NYU*
John Mallery, *Massachusetts Institute of Technology*

13:00 – 15:00 Lunch Break
Coffee available in front of the meeting room at 14h30

15:00 – 15:10 Afternoon kick-off

Ricardo Mor, *Ambassador-at-large for Cybersecurity, Ministry of Foreign Affairs and Cooperation, Spain*

15:10 – 17:45 Session 4. Colloquium: Building a Normative Structure for Cyberspace

— *How do we advance the global discussion of norms?*
— *What are good outcomes in the GGE and elsewhere?*
— *How do we define responsible state behavior for cyberspace?*

Panel moderators and all invited speakers

17:45 – 18:00 Closing remarks

This workshop is organized by UNIDIR and CSIS
with support from the Governments of the Netherlands and the United States

UNIDIR
UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

International Security Cyber Issues Workshop Series:
The Application of International Law in the Context of International Cybersecurity

19–21 April 2016
Room XXIV, Palais des Nations, Geneva, Switzerland

Tuesday, 19 April 2016

9:15 – 10:00 *Registration and coffee*

10:00 – 10:15 **Welcoming remarks**

Jarmo Sareva, *Director, UNIDIR*
James Lewis, *Director and Senior Fellow, CSIS*

10:15 – 10:30 **Keynote Remarks**

Andrei Krutskikh, *Special Representative of the President of the Russian Federation for International Cooperation in Information Security*

10:30 – 13:00 **Session 1. Overview of International Law as It Applies to State Conduct in Cyberspace in Peacetime**

— How does international law define responsible State behavior in cyberspace?
— How can existing law best be applied to cyberspace and to State conduct in peacetime?
— Are there useful precedents from other areas of international law that can be applied to cyberspace?
— What are the most important questions to consider in the application of international law for responsible State behavior and cybersecurity?

Moderator — James Lewis
Duncan Hollis, *Associate Dean for Academic Affairs & James E. Beasley Professor of Law, Temple University School of Law*
Jayantha Fernando, *Director, Legal Affairs, ICT Agency of Sri Lanka*
Catherine Lotrionte, *Director of the Institute for Law, Science and Global Security, Georgetown University*
Karine Bannelier-Christakis, *Associate Professor of International Law, Université Grenoble-Alpes*

13:00 – 15:00 ***Lunch Break***
Coffee available in front of the meeting room at 14:30

15:00 – 18:00 **Session 2. Issues in International Law at Previous UN GGEs**

Moderator — James Lewis
Legal advisors from Australia, China, Germany, the United Kingdom and the United States who have supported national expert in previous GGEs

18:00 – 19:30 **Reception, 8th Floor Delegates' Restaurant**

Wednesday, 20 April 2016

Coffee available in front of the meeting room at 9:30

10:00 – 13:00 Session 3. The Law of Armed Conflict, and the Implications for the Use of Force and Armed Attack in Cyberspace

— How should we clarify the concepts of use of force and armed attack in cyberspace?
— What are the determinants of necessity and proportionality?
— How do concepts like proportionality, distinction and discrimination apply?

Moderator — Nils Melzer
Liis Vihul, *Senior Analyst, Law and Policy Branch, NATO Cooperative Cyber Defence Centre of Excellence*
William Boothby, *Former Air Commodore and Deputy Director, Legal Services, Royal Air Force, UK*
Terry Gill, *Professor of Military Law, University of Amsterdam & Netherlands Defence Academy*
David Simon, *Counsel, Sidley Austin LLP*
Michael Schmitt, *Director, Stockton Center for the Study of International Law, United States Naval War College*

13:00 – 15:00 Lunch Break
Coffee available in front of the meeting room at 14:30

15:00 – 18:00 Session 4. Sovereignty, State Jurisdiction, Territorial Integrity and Non-Intervention

— How does the application of sovereignty shape responsible State behavior?
— What are the limitations of the concept of territorial integrity for cyberspace?
— What is the nature of State jurisdiction over cyber activities and infrastructure?
— How can the concept of neutrality be applied in cyberspace?
— What may be done to respond to violations of the principle of non-intervention?

Moderator — Sean Kanuck
Anatoly Streltsov, *Deputy Director, Institute for Information Security Issues, Moscow State University*
Arun Mohan Sukumar, *Head, Cyber Initiative, Observer Research Foundation*
Eneken Tikk-Ringas, *Consulting Senior Fellow, The International Institute for Strategic Studies*

Thursday, 21 April 2016

Coffee available in front of the meeting room at 9:30

10:00 – 13:00 Session 5. International Humanitarian Law, Cybersecurity and Human Rights

— How is the development and use of new technology shaped by IHL?
— What cyber actions could justify the use of force in self-defense?
— What are the requirements for evidence and attribution?
— How should we think about combatant status and participation in hostilities?
— How do the doctrines of countermeasure and necessity apply?
— What is the relationship between data protection (and privacy) and cybersecurity?

Moderator — Kerstin Vignard
Elina Noor, *Director, Foreign Policy & Security Studies, Institute of Strategic and International Studies (ISIS) Malaysia*
Laurent Gisel, *Legal Adviser, International Committee of the Red Cross*
Nohyoung Park, *Director, Cyber Law Center, Korea University*
Gary Brown, *Professor of Cyber Security, Marine Corps University*

13:00 – 15:00 Lunch Break

Coffee available in front of the meeting room at 14:30

15:00 – 18:00 Session 6. Conclusions: Applying International law to the use of ICTs by States

— Where are there significant differences and can they be resolved?
— What would be a good outcome of a future GGE?
— Where are the most promising areas for progress?
— What does the international community need from the application of international law in cyberspace?

Moderator — James Lewis
Anatoly Streltsov, Nohyoung Park, Arun Mohan Sukumar, Duncan Hollis,
Jayantha Fernando *and* ***Elina Noor***

This workshop is organized by CSIS and UNIDIR
with support from the Governments of the Netherlands and the United States

UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

International Security Cyber Issues Workshop Series:
Managing the Spread of Cyber Tools for Malicious Purposes

Provisional Agenda

15–16 June 2016
Room XII, Palais des Nations, Geneva, Switzerland

Wednesday, 15 June 2016

9:15 – 10:00 *Registration and coffee*

10:00 – 10:15 **Welcoming remarks**

Jarmo Sareva, *Director, UNIDIR*
James Lewis, *Director and Senior Fellow, CSIS*

10:20 – 13:00 **Session 1. Current Trends in Malware and Cyber Tools**

Moderator — James Lewis
Trey Herr, *Fellow, Belfer Center at the Harvard Kennedy School*
Caroline Baylon, *Information Security Research Lead, AXA*
Bill Wright, *Director, Cybersecurity Partnerships, Symantec Corporation*
Bill Marczak, *Senior Researcher, Citizen Lab*

13:00 – 15:00 ***Lunch Break***
Coffee available in front of the meeting room at 14:30

15:00 – 18:00 **Session 2. Managing the Spread of Cyber Tools:**
What are the Concerns? What are Realistic Goals? What are the Challenges?

— Which aspects of the spread of cyber tools pose the greatest threats to international cyber stability?
— What would be appropriate goals for efforts to manage the spread of such capabilities?
— What are the unique challenges to such an effort that governments should take into account?

Moderator — Kerstin Vignard
Angela McKay, *Director, Government Security Policy and Strategy, Microsoft*
Edin Omanovic, *Research Officer, Privacy International*
Jeremy Otis, *General Counsel, Eniram Ltd.*
Sico van der Meer, *Research Fellow, Clingendael Institute*
Ben Wagner, *Director, Centre for Internet and Human Rights*

18:00 – 19:30 **Reception, 8th Floor Delegates' Restaurant**

Thursday, 16 June 2016

Coffee available in front of the meeting room at 9:30

10:00 – 12:00 Session 3. Lessons from Non-Proliferation

- What insights might be drawn from other regimes and initiatives such as the Global Initiative to Combat Nuclear Terrorism, the Proliferation Security Initiative, and the Wassenaar Arrangement?
- What are the limitations of these sorts of approaches in the cyber context?

Moderator — Kerstin Vignard
Philip Griffiths, *Head of Secretariat, Wassenaar Arrangement*
Rajiv Nayan*, Senior Research Associate, Institute for Defence Studies and Analyses*
Benjamin Hautecouverture, *Senior Research Fellow, Fondation pour la recherche stratégique*

12:00 – 13:00 Session 4. Curbing Cyber "Proliferation" and Promoting Stability in Cyberspace

- What strategies exist for reducing the availability of dangerous capabilities?
- Are they delivering satisfactory results?
- How might they be improved or expanded?
- How might efforts to control the spread of cyber tools that could be used for malicious purposes fit into ongoing stability activities?
- Is it helpful to focus on effects—rather than capabilities—in the context of this discussion?

Moderator — James Lewis
Wen Baihua, *Associate Professor, PLA National Defense University*
Elaine Korzak, *National Fellow, Stanford University*
Tim Maurer, *Associate, Carnegie Endowment for International Peace*
Heli-Tiirmaa Klaar, *Head of Cyber Policy Coordination, European External Action Service*

13:00 – 15:00 Lunch Break
Coffee available in front of the meeting room at 14:30

15:00 – 16:45 *Session 4 continued*

16:45 – 17:45 Session 5. Lessons and Outstanding Questions

- This session provides an opportunity for participants to share perspectives on the issues covered during the workshop and identify topics or questions that might bear further discussion or research

Moderators — James Lewis and Kerstin Vignard
Speakers from each panel

17:45 – 18:00 Closing remarks

This workshop is organized by CSIS and UNIDIR
with support from the Governments of the Netherlands and the United States

UNIDIR
UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

Report of the
International Security Cyber Issues Workshop Series

The work of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is the focal point for the international discussion of cybersecurity. Achieving consensus in a GGEs is a demanding task, given the compressed time for discussion and negotiation, the complexity of the subject, and the range of national views. GGE outcome documents have been shaped by complex negotiations on balancing freedom of expression with terrorist use of the Internet, on the nature and legitimacy of cyberattack, and by the larger tension between national sovereignty and universal values. These are core issues that arise repeatedly.

In light of this complexity, in 2016, the UN Institute for Disarmament Research and the Center for Strategic and International Studies organized three expert workshops to open and broaden the discussion of international norms for responsible State behaviour in cyberspace and to identify new ideas to support further progress by the international community. The first focused on identification of new norms, the second on the application of international law, and the third on ways to manage the spread of malicious cyber tools. The intent was to build on past progress and to expand the space for international agreement on measures to increase stability and security in cyberspace.