UNIDIR

The United Nations, Cyberspace and International Peace and Security

Responding to Complexity in the 21st Century

UNIDIR RESOURCES

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.

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 UNIDIR's sponsors.

www.unidir.org

CONTENTS

FIGURES

Acknowledgements

The author would like to acknowledge the thoughtful inputs received on sections in earlier drafts of this study from Madeline Carr (Cardiff University), Paul Cornish (Global Cyber Security Capacity Centre, Oxford Martin School), Sebastian Einseidel (UNU), Martha Finnemore (Georgetown University), Gillian Goh (UN Office for Disarmament Affairs), Duncan Hollis (Temple University School of Law), Jim Lewis (CSIS), Tim Maurer (Carnegie Endowment for International Peace), Jan Neutze (Microsoft), Marc Porret (United Nations Counter-Terrorism Committee Executive Directorate), Rafal Rohozinski (SecDev Foundation), Kerstin Vignard (UN Institute for Disarmament Research), and Xu Yu (UN Security Council sanctions monitoring team).

About the author

Dr. Camino Kavanagh is a Senior Visiting Fellow at the Department of War Studies, King's College London.

She served as consultant to the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security and is lead consultant to the OSCE on a project relating to Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of ICTs. She is also involved in a number of policy-related initiatives on ICTs and emerging technologies as they relate to conflict, terrorism and crime.

Dr Kavanagh has spent more than twenty years working on national and international security issues. She has worked in conflict and post-conflict contexts, including with UN peacekeeping operations and political missions in Africa and Central America and has served as post-conflict reform advisor to governments in Africa, Latin America and Asia. Camino has also managed several high-level initiatives and projects focused on assessing and responding to transnational threats and their impact on security, governance and development and she consults regularly for governments and different international organizations.

Her PhD was awarded by the Department of War Studies, King's College London in 2016 and focused on information technology, sovereignty and the State, a topic that remains a core focus of her research activities. She is a Member of the Global Initiative on Transnational Organized Crime.

Abbreviations

AALCO	Asian-African Legal Consultative Organization
ASEAN	Association of Southeast Asian Nations
ARF	ASEAN Regional Forum
BRIC	Brazil, Russia, India, and China
CBM	confidence-building measure
CI	critical infrastructure
CEIP	Carnegie Endowment for International Peace
CTC	Counter-Terrorism Committee
CTED	Counter-Terrorism Committee Executive Directorate
CTITF	Counter Terrorism Integrated Task Force
ECOSOC	Economic and Social Council
EU	European Union
G7	Group of Seven
G20	Group of 20
GFCE	Global Forum on Cyber Expertise
GGE	Group of Governmental Experts
IAEA	International Atomic Energy Agency
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation of Assigned Names and Numbers
ICT	Information Communications Technology
IGF	Internet Governance Forum
IoT	Internet of things
IP	Internet protocol
IT	information technology
ITU	International Telecommunication Union
ISIL	Islamic State in Iraq and the Levant
IWG	informal working group (OSCE)
MLAT	Mutual Legal Assistance Treaty
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
SCO	Shanghai Cooperation Organization
SDGs	Sustainable Development Goals
UN	United Nations
UNDESA	United Nations Department of Economic and Social Affairs
UNDPA	United Nations Department of Political Affairs

UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UNOTC	United Nations Office of Counter-Terrorism
UNU	United Nations University
US	United States
WSIS	World Summit on the Information Society

Executive Summary

ICT-related issues have been on the agenda of the United Nations for almost two decades, driven by both the positive benefits and the malicious purposes they can be leveraged for. This report is concerned with the UN's response to the latter in the context of international peace and security. It focuses principally on the norm-setting work currently underway within the General Assembly. It outlines where progress has been made in developing a normative framework to shape behaviour in the use of ICTs and ensure stability of the ICT environment, highlighting where challenges and on-going sources of disagreement lie.

The report also discusses linkages and complementarities with other non-UN processes, as well as linkages and complementarities with other items on the UN agenda, directly or indirectly linked to international peace and security. Finally, it identifies how the UN, particularly the UN Secretary-General, might play a role in raising awareness of, supporting and strengthening this on-going work.

Key findings

Enormous economic and social benefits can be leveraged from modern information communications technologies. This fact has been repeatedly acknowledged by States in their commitments to a shared vision of an open, secure, accessible, and peaceful ICT environment.

Yet, despite these benefits and commitments, the world has a serious ICT problem. The source of the problem is not just the technologies themselves, which are prone to vulnerabilities and flaws. Rather, human behaviour is a large part of the problem. Indeed, both State and non-State actors are using cyberspace and related ICT tools, techniques, and capabilities for a range of malicious purposes. The aggregate effect of these "cyber insecurities" is undermining trust in the technologies and related products and services. Moreover, it is undermining trust between governments, with important implications for international peace and security.

The international system has a series of built-in safety valves that can help mitigate existing and emerging threats. In the ICT realm, the development of norms—a standard of appropriate behaviour for actors with a given identity—has emerged as one of the main policy tools of choice, along with confidence- and capacity-building, for responding to such threats. Within the United Nations, Member State action has centred on developing a normative base to shape the behaviour of different actors (States, criminal actors, users, etc.) in both peacetime and in the context of armed conflict in their use of cyberspace and ICTs, thereby ensuring a stable ICT environment. From a political–military perspective, this policy option has included the work of the General Assembly First Committee on Disarmament and International Security, which, through its successive Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security, has facilitated some of the first efforts to reach global consensus on the binding and non-binding norms that apply to the digital environment and the behaviour of States in their uses of ICT. It has also provided a framework for confidence- and capacity-building measures anchored in the principles of cooperation and transparency and aimed at creating a conducive environment for implementing the norms recommended by the GGEs. These efforts have spread to other organizations and forums, where many of the recommendations have been picked up and, at times, added to.

Other important norm-shaping efforts directly or indirectly linked to ICTs and international peace and security have emerged around the other pillars of the UN's work, including with regard to terrorist and criminal use of the Internet and ICTs, and protecting basic human rights and fundamental freedoms from State abuse of ICTs.

Despite many positive developments and this gradual spread of norms, the foundations for establishing a strong normative framework around the use of ICTs in the context of international peace and security appear to be faltering. Indeed, they remain complicated by several overlapping factors:

- persisting **disagreements among States on *how* existing rules of international law apply** to State uses of ICTs. The sources of these disagreements—many of which spill over into other policy areas—lie just as much in different appreciations of the legal issues at hand as they do in perceptions of strategic imbalances in military and civilian IT resources and capabilities and were—to a large degree—what prevented the 2016–2017 GGE from agreeing on a consensus report;
- the sluggishness of some States in **moving beyond mere process to practical implementation** of the recommended norms of State behaviour;
- an equally serious **lack of capacity and resources to implement some of the recommended norms and confidence-building measures**, including for establishing the national structures and mechanisms required to respond to ICT vulnerabilities and risks, and for attributing ICT-related incidents;
- a **lack of awareness by policymakers** in many States of the different normative processes underway within and beyond the UN relating directly or indirectly to international peace and security; and
- a deepening **lack of trust among various stakeholders**, driven in part by broader, non-technological issues affecting relations among States, and which undermines collaboration and cooperation.

If States are sincere in their commitments, they need to strengthen the normative foundations for responsible behaviour in the use of ICTs across policy agendas. This can be achieved by shifting to practical implementation of those norms and measures that have already been agreed upon, helping bridge existing capacity needs, and by ensuring that existing multilateral and bilateral channels are kept open for continued dialogue on those issues on which agreement is less tangible in the immediate term. Moreover, any effort to bridge existing disagreements moving forward will require the existence of a conducive political environment, which realistically can only be achieved by stepping up ongoing efforts to build trust and confidence among States, and ensuring the engagement of other relevant actors in the process.

What role for the United Nations?

The United Nations can play a significant role in supporting these efforts, all of which are crucial to the maintenance of international peace and security. The former UN Secretary-General already raised a number of international ICT/cybersecurity matters in policy statements, suggesting the growing importance of the issue within the Organization. Initial efforts were also made within the Secretariat to coordinate efforts on ICT/cybersecurity-related matters. Yet, in view of global society's increasing dependency on ICTs and the simultaneous increase in their malicious use, engagement on ICT and international peace and security by the top UN official and the United Nations leadership needs to be scaled up.

The current Secretary-General can show leadership, promote and rally support around the achievements resulting from the different normative processes underway across the Organization's principal organs, raising awareness among Member States on what has been achieved, the need to shift from the mere articulation of norms to their adherence and implementation (including through bridging capacity needs), and the need for continued dialogue, trust and confidence building on those issues around which consensus is most difficult to achieve. The following recommendations lay out just some of the areas on which that attention can be focused:

1. Internally, the Secretary-General might consider establishing a nimble and cost-effective internal arrangement for United Nations ICT/Cyber Affairs in order to:

   – Promote coherence between the Organization's multifaceted work on ICTs and international peace and security. Such an arrangement could focus on promoting and projecting—within and beyond the Organization—the positive and common benefits of an open, secure, accessible, and peaceful ICT environment raising awareness of the normative work resulting from the Organization's different bodies, while also flagging those issues that require continued and urgent dialogue and action.

   – Raise awareness among senior UN leadership and staff of i) how existing and emerging ICT-related threats impact their work; and ii) the different normative frameworks and related measures emerging in response. The outcome of these efforts could eventually serve as a strategic framework for assessing the United Nations' comparative advantage in providing technical assistance and capacity-building support to Member States and other actors on issues relating to ICTs and cybersecurity, and in assigning roles and responsibilities among relevant departments and agencies.

International peace and security

2. Regarding ICTs in the context of international peace and security, a possible role for the Secretary-General and the relevant senior leadership could be to:

   – Leverage the momentum generated by the First Committee's GGEs by publicly supporting efforts within and beyond the UN to i) advance implementation of those norms of behaviour that can lead to greater security and stability in cyberspace; ii) encourage Member States to report annually on national views in line with General Assembly document A/53/576; iii) prioritize and promote dialogue on those normative issues on which there has been limited agreement; and iv) promote greater engagement of relevant technological bodies or associations, industry actors, civil society, and academia in these efforts.

   – Work with Member States and other core partners to determine the most legitimate mechanism (annual or bi-annual conference, flanking mechanism, or other) to channel progress made on norms and confidence-building measures at the regional and subregional levels and through the growing number of plurilateral and multi-stakeholder arrangements back into the multilateral process.

   – Actively encourage efforts to foster a conducive environment for the process of norm implementation and adherence, notably by raising awareness of and promoting cooperative measures and confidence-building processes relating to ICTs and international peace and security underway or taking root at the regional level, and leveraging the Organization's preventive diplomacy and crisis management tools to deal with tensions that may emerge between States around the use of ICTs.

- Strengthen the capacity of the Organization's research institutes (such as UNIDIR, UNU and UNICRI) to:
  - organize expert conferences and workshops and produce targeted publications for Member States on existing and emerging ICT vulnerabilities and risks and the technical and policy responses being shaped in response (for instance, UNIDIR's longstanding efforts to deepen discussion through its cybersecurity and stability conference series and its expert workshops)[1];
  - develop sustainable partnerships with external research institutions; and
  - organize thematic debates for Member States involving industry, academia, and civil society.

These same institutions can also help identify linkages and tensions with other areas of the ICT-related normative work on the UN agenda—for instance on terrorism and crime—and study how they are being addressed at the national and regional levels.

They can also be leveraged to assess how ICT are being integrated into the UN's and broader international community's "conflict management toolbox" and to identify where knowledge, capacity and integration gaps lie.[2]

Transnational threats

3. Complex issues relating to how best to deal with transnational threats such as criminal and terrorist use of the Internet often spill over into First Committee processes and discussions relating to ICTs and international peace and security. The United Nations Secretary-General would do the international community a great service by:
   - Encouraging greater awareness-raising of and reporting on current normative processes relating to the use of the Internet for terrorist and criminal purposes, highlighting where progress on implementation has been made, where challenges lie, and how those challenges are being addressed; and
   - Encouraging presentations by experts in relevant committees of the General Assembly on certain issues that straddle different policy areas (for instance, State use of criminal proxies in the context of malicious ICT activity, the potential of terrorists to conduct cyber-enabled attacks against critical infrastructure, etc.), the shifting character of cybercrime, and its implications for international peace and security.

Human rights, development and Internet governance

4. Member States have long acknowledged the indivisible and interdependent relationship between peace and security, development, and human rights. This relationship is equally pertinent as it applies to ICTs, yet requires sustained attention. Moving forward, the United Nations Secretary-General might consider:
   - Supporting the dissemination and socialization of existing and emerging human rights norms, standards, and principles relating to ICTs. The Secretary-General can encourage the relevant UN departments and agencies to work with other organizations and initiatives to

ensure that these norms are mainstreamed across the Organization's existing and evolving capacity-building and technical assistance work. To this end, the UN can promote the inclusion of human rights considerations in national cybersecurity strategy development from the outset rather than as an afterthought;

- Advocating for the engagement of core human rights actors in accompanying implementation of these efforts; and encourage globally recognized technology companies and ICT service and product providers to adopt, implement, and promote the principles and standards they publicly claim to espouse;
- Helping diffuse tensions on internet governance related issues, notably by supporting efforts to strengthening the engagement of all relevant actors in Internet governance-related processes and determining linkages with other relevant areas of work;
- Strengthening on-going efforts to integrate ICTs and emerging technologies into the UN's work on economic and social development, while also highlighting the benefits of these efforts for broader peace and security and the protection of human rights;
- Encouraging the effectiveness and coherence of UN capacity-building efforts, while also ensuring coherence between UN efforts and those other non-UN entities are engaged in. This can involve:
    - strengthening the work of the UN system's Chief Executive's Board for Coordination (CEB), including with regard to identifying relevant linkages and lacunae across the UN system's capacity-building and technical assistance efforts;
    - strengthening relations with other international and regional organizations and with initiatives such as the Global Forum for Cyber Expertise;
    - ensuring that cybersecurity capacity-building efforts pay due attention to key concepts such as risk management and key development principles such as national ownership and responsibility; and
    - engaging different actors to identify gaps, garner lessons, foster cooperation, and continue much-needed dialogue on the tensions between rights and security and the important linkages between development and security.

Given the United Nations' current challenges, influenced in no small measure by important geopolitical shifts as well as the pressing need for reform, these steps can ensure the UN's continued engagement—and comparative advantage—in a field which is of growing importance not only to the maintenance of international peace and security, but also to the protection of human rights and the fostering of economic and social development.

1. Introduction

Cyberspace and cybersecurity

In contemporary understandings, the term “Information and Communications Technology” (ICT) generally refers to computers, computer networks and systems, and disparate information distribution or delivery technologies such as land and submarine cables, satellites, the telephone, and even television.[3] Today, these networks, technologies, and their delivery systems are increasingly referred to as “cyberspace”, the technological substrate of modern societies made up of several interconnected layers—physical, syntactic, semantic, and pragmatic,[4] with the physical and pragmatic layers subject to certain sovereign governmental jurisdiction and controls.[5] Framed by the use of electronics and the electromagnetic spectrum, cyberspace enables “the creation, storage, modification, exchange and exploitation of information via interdependent and interconnected networks using information communication technologies”.[6] While the Internet is often conflated with cyberspace, it is just one part of the global technological substrate. And while it connects more than three billion devices, it is not a singular system, but rather involves many layers of distinct “functions” and “tasks”, the latter carried out by actors as distinct as private industry, technical institutions, States, or through multilateral governmental coordination.[7]

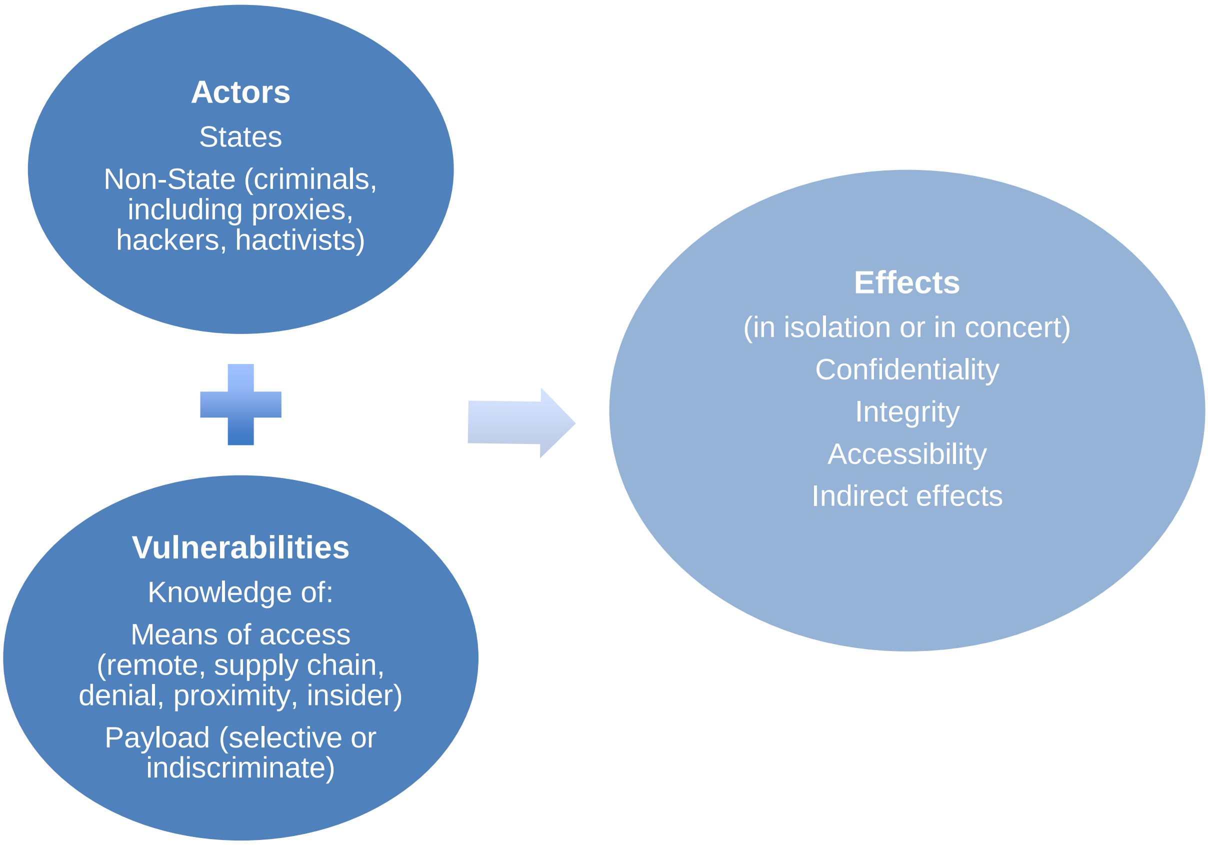
Cybersecurity—efforts to secure ICT—is “the protection of [ICTs] from *unauthorized* access or attempted access”[8] affecting the so-called “CIA” triad of Confidentiality, Integrity and Accessibility of ICT. The “unauthorized access” referred to implies the presence of an adversary, thus capturing intentional threats (e.g., sabotage, destruction) while excluding damage caused by internal computer errors or interoperability problems. The focus on protection of ICTs also excludes security issues associated with the content of ICT communications.[9] However, as the second section of this report suggests, a distinction between such intentional threats and communications content does not always correspond to how States approach cybersecurity (or digital risk) in strategy and in practice.

Background and context

Although networked digital computers emerged during the latter decades of the Cold War, the creation of the World Wide Web in 1989, coupled with global economic liberalization, led to important transformations in the way people communicate and modern societies conduct daily business. The new hyperconnected environment ushered in great expectations during the 1990s: the potential for e-commerce was significant. Moreover, it was expected that many traditional barriers to economic growth and development could be overcome, allowing developing countries to participate on a more equitable footing in the global economy. At the same time, individual citizens would be empowered by technologies allowing them to communicate and organize politically at national and international levels in ways not possible before.

Increasing connectivity, however, did not only bring the prospect of human betterment; it created technological disparities between States and growing vulnerabilities and risks, or what are often described as “cyber insecurities” or “digital uncertainties”.[10] Such insecurities or uncertainties stem from the way different actors exploit ICT vulnerabilities, and the capacity of the targets to minimize the consequences and ensure business continuity. Consequences can be localized or, depending on the severity and the actors involved, escalate to the international level. A digital or cybersecurity threat begins when a specific actor learns about a vulnerability in an ICT, gains access to the technology, and then determines how to exploit the confidentiality, integrity, accessibility "of the activities or the digital environment in which they are carried out or on which they directly or indirectly rely", generating immediate or indirect effects (figure 1).[11]

Figure 1. Cyber insecurities and their effects


Actors
States
Non-State (criminals, including proxies, hackers, hactivists)
Vulnerabilities
Knowledge of:
Means of access (remote, supply chain, denial, proximity, insider)
Payload (selective or indiscriminate)
Effects
(in isolation or in concert)
Confidentiality
Integrity
Accessibility
Indirect effects

The effects of these insecurities are assessed in terms of their impact on the confidentiality, integrity, and availability—of the data and ICT systems and infrastructure.[12] The effects generating significant concern today involve the indirect effects of vulnerability exploitation, i.e. "losses of confidentiality, integrity and availability … designed with some other effect(s) in mind".[13] For some States, the sources of insecurities are not just technical but also relate to content. For instance, the Russian Federation and several other States use the broader term "information security", a much broader concept which relates to the "[p]rotection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information *per se* with respect to its characteristics, such as integrity, objectivity, accessibility and confidentiality".[14] The inclusion of "information *per se*" has been and remains problematic for many States for reasons of law and principle.

The gathering storm of ICT-related insecurities

Initial "insecurities" stemming from ICT vulnerabilities can be traced back to the late 1960s. For instance, in the United States, concerns relating to the protection of private data had become such a concern that the Congress dedicated three days to hearings on "The Computer and Invasion of Privacy" in 1966. There was also a growing realization within the defence sector that vulnerabilities in networked computers could (and would) be exploited by hackers to commit fraud, and steal or manipulate information.[15] Since then, both State and non-State actors have taken advantage of ICT vulnerabilities, the number of economic, national security and human rights issues they implicate increasing in tandem with global society's growing dependence on ICTs, the shifting character of interstate and intrastate conflict, and a shifting international order.

The most common ICT-related incidents remain those committed with criminal intent targeting financial institutions and individual users, including the recent surge in ransomware incidents.[16] Nonetheless, the number of ICT-related incidents involving States are increasing both in number and sophistication. They include State-supported acts of economic and industrial espionage,[17] important data breaches targeting key government agencies and services and multi-national companies and the surveillance practices of technologically sophisticated States as revealed by Edward Snowden,[18] incidents such as the distributed denial of service (DDoS) attack against the US-based domain name service (DNS) provider, Dyn, disrupting daily life and economic activity at significant financial cost, have given cause for further concern.[19] Not only did this attack show how vulnerable so-called Internet of Things (IoT) devices are (this incident leveraged millions of devices as an attack vector) and how difficult it is to defend against such attacks, it also demonstrated the complex web of interests—State and non-State alike—that will likely complicate any long-term solution to IoT vulnerabilities.

Of growing concern are incidents involving acts of sabotage or disruption conducted by State actors or their proxies targeting critical infrastructure[20] and the use of ICTs to meddle in the internal affairs of other States, including with the intent of influencing political outcomes.[21] And while they have yet to occur, governments are increasingly turning their attention to those incidents that may result in loss of human life or significant and lasting damage to industrial facilities and infrastructure providing essential services to the public.[22]

The issue of attribution compounds these "insecurities" since the layered and distributed nature of cyberspace allows actors to either misrepresent or conceal their actions. Thus, both prosecution and deterrence are difficult, regardless of the means used, since such means are "largely predicated on being able to establish culpability".[23] This challenge of attribution is not unique to cyberspace, however, and increasing experience investigating ICT incidents, notably by private sector actors or by cooperation between the latter and law enforcement, has made attribution much more feasible than it was a few years ago. At the same time, regardless of technical progress on reaching attribution findings, actually attributing an incident will likely always be a political decision. In addition, the fact that only a handful of States have advanced attribution capacities and capabilities means that there is limited trust in publicly stated attribution findings, exacerbated by the fact that there are no internationally accepted standards for reaching attribution findings or making attribution claims—issues that will likely remain difficult to resolve in the near term.

In short, the exploitation of ICTs by State and non-State actors has led to growing tensions and waning trust among States, and between States and citizens. In turn, this has produced an increasingly tense politicization of policy debates relating directly or indirectly to ICTs and straddling the three core pillars of the Organization's work: international peace and security, human rights, and economic and social development.

Shaping a response

The distributed and layered nature of cyberspace—particularly the Internet—suggests that efforts to respond to current global ICT insecurities requires significant collaboration and cooperation among different actors at different levels and across borders. The mushrooming of national cybersecurity strategies over the past decade bears witness to the growing awareness of our shared insecurities, the need to shape norms of behaviour, and the need to confirm or assign policy and administrative roles and responsibilities. Research by the Organization for Economic Co-operation and Development (OECD) has shown that cybersecurity is generally approached from four different (and often interdependent) perspectives:[24]

i. technology, which involves a focus on the actual digital environment (often called "information security", "computer security" or "network security" by experts);

ii. law enforcement, and more generally, the legal framework (e.g. for responding to cybercrime);

iii. national and international security (issues ranging from intelligence to the use of ICT in conflict); and

iv. economic and social prosperity (relating to wealth creation, innovation, growth, competitiveness, and employment across economic sectors and other aspects such as individual liberties, health, education, culture, and so forth).

While national strategies may differ on many of these fronts, most imply the prior existence of capacity and resources and a multisectoral and multi-institutional approach involving the public and private sectors as well as significant transborder cooperation and collaboration.[25]

At the international level, the current context has made cooperation and coordination between States on ICT-related insecurities more challenging and agreement on how to govern equally complex policy issues and assigning roles and responsibilities more difficult to attain.[26] It is against this backdrop that norms—both binding legal norms and non-binding political norms—have emerged along with confidence- and capacity-building measures as "the principal policy tools of choice" to meet the shared vision of an open, secure, accessible, and peaceful ICT environment.[27] Many of these norms and measures are aimed at shaping the behaviour of different actors in peacetime and draw on existing rules and principles. A growing number, however, are also aimed at studying not whether but how existing norms, rules and principles—particularly chapters VI and VII of the Charter of the United Nations as well as the Geneva Conventions—can be applied to prevent conflict stemming from State uses of ICTs or restrict the use of ICTs in a situation of conflict.

Norms, ICTs, and international peace and security

The standard definition of a norm as "collective expectations for the proper behaviour of actors with a given identity" implies questions of identity (the grouping at which the norm is directed), behaviour (which can be regulative, generative, or constitutive), propriety (that which defines the behaviour as appropriate or inappropriate), and collective expectations (the social and intersubjective character of the norm).[28] In short, norms "embody powerful expectations that can both constrain and compel actors in world politics", providing "guidance on what is required, permitted or prohibited" and are thus considered to carry moral weight.[29] In international politics, norms "reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States".[30]

Some norms depend on law for their propriety, others are developed with the aim of eventually shaping law, while yet others may emerge from political consensus, culture, religion, even professional training. If initial efforts to articulate a norm and organize support around it are successful, "the norm may reach a 'tipping point', leading to a 'cascade' of the norm and its internalisation (i.e. its implementation)".[31] At the same time, the dynamic process whereby a norm emerges and the behaviour it is prescribing or proscribing is internalized (i.e., adhered to) by the target grouping can be both complex and lengthy.

The current international framework for mitigating the effects of the aforementioned "cyber insecurities" on international peace and security is very broad, with responsibilities and interests spanning different international regimes and involving different norm-shaping and confidence-building processes, as well as significant investment in capacity-building. As with other areas, progress is punctuated by the oft-conflicting positions and interests of State and non-State actors alike, which inhibit cooperation and collaboration, as well as persistent vulnerabilities in ICT.

Within the United Nations alone, several organs are involved in relevant ICT norm-shaping, and confidence- and capacity-building processes (see figure 2). For instance, the General Assembly, its First Committee, and a number of Groups of Governmental Experts (GGEs) have served as a central platform for discussions on the application of binding and non-binding norms of State behaviour to State use of ICTs, covering issues from the application of existing international law to the ICT environment and State responsibilities and duties as they relate to critical infrastructure protection and incident preparedness to confidence and capacity building, and human rights protections.

Also on critical infrastructure protection, the Second Committee has served as the initial home for framing resolutions on the promotion of a global culture of cybersecurity and the protection of critical infrastructure, since taken up by the GGEs. More recently, the Security Council was briefed for the first time, via an open "Arria formula" meeting,[32] on the use of ICTs and international peace and security, including attacks relating to critical infrastructure. The Economic and Social Council (ECOSOC) and the General Assembly's Third Committee have focused on human rights issues resulting from State [ab]uses of ICTs. And while not a cybersecurity risk *per se*, the Security Council and its subsidiary bodies have paid increasing attention to questions pertaining to the use of the Internet and ICTs for terrorist purposes, around which a cooperative framework and a more substantial normative framework are emerging. The General Assembly's Second and Third Committees have also focused on strengthening the normative base for responding to transnational threats such as the use of the Internet and ICT for terrorist or criminal purposes. Meanwhile, several of the Organizations' departments and specialized agencies are also involved in translating some of these norms into practice, providing support to Member States through awareness-raising, guidance, capacity-building, technical assistance, and rule of law-related support.

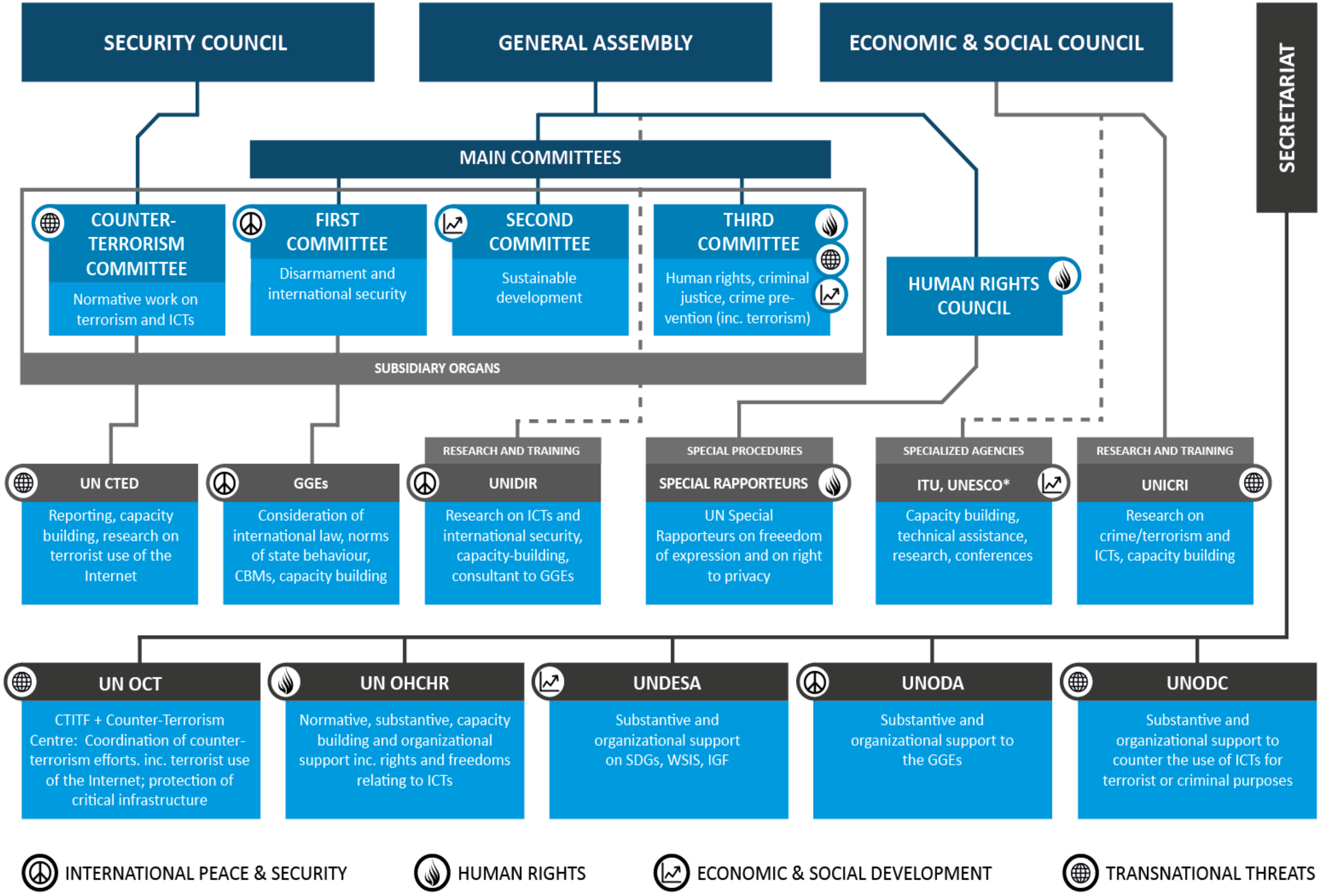
Beyond the United Nations, efforts to shape norms and build confidence among States in response to ICT-related insecurities have become central to other international and regional bodies. These include efforts aimed at reducing the risk of conflict stemming from the use of ICTs; defining what the response should be in the event of an ICT incident (both above and below the threshold of armed conflict); strengthening critical infrastructure or the resilience of global financial services; managing digital risk; and enhancing cooperation to respond to terrorist and criminal use of the Internet. They include the African Union, the ASEAN Regional Forum (ARF), the Brazil, Russian Federation, India, China and South Africa (BRICS) grouping, the Council of Europe, the European Union, the Group of Seven (G7), the Group of 20 (G20), the Organization of American States (OAS), the Organization for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE) and the Shanghai Cooperation Organization (SCO). A growing number of actors are also providing capacity-building support and technical assistance to support States' efforts to implement these and related measures at the regional and national levels.

These normative processes and related confidence-building, capacity-building, and cooperative efforts combine with existing regimes—in the fields of international law, law enforcement, telecommunications, cable infrastructure, finance, trade, and intellectual property—to constitute a variegated “regime complex for managing global [ICT] activities”.[33] Importantly, this means that the effectiveness of any norm-development process (for instance, the GGE) will depend on how States interact with other regimes and the norm-shaping and implementation processes emerging therein. A glaring example of this is how persisting differences between States on key rules and principles of international law or on the role of the United Nations in managing crisis continue to spill over into the ICT realm.

While this “regime complex” may appear fragmented or even “cacophonous”,[34] important progress has nonetheless been made on several fronts. For instance, on the political–military front and until recently, the work of the GGEs had evolved from a highly conceptual discussion on controlling “information weapons” towards the confirmation of international law and the identification and articulation of specific norms of State behaviour in the use of ICTs that has spread to other organizations.[35] This work has also influenced confidence-building efforts at the regional level (e.g. via the OSCE, ARF, and OAS) and has provided an important framework for the identification of capacity-building needs within States. Similar assumptions can be made with regard to the normative base emerging in relation to the ICT-related human rights norms articulated in recent years, and in response to the criminal and terrorist use of the Internet and ICTs.

These initial frameworks can serve as important guidance for States as they shape their own national strategies, which in turn can contribute to greater international stability and security. Yet, as evidenced by the failure of the 2017 GGE to reach a consensus report, important divisions among States persist, some of them legal or technical, many more of them political. Indeed, some of the emerging norms only appear to be spreading or cascading within certain subgroups—at times with set-backs within these same groups—and remain contested elsewhere. Similar observations can be made about other normative processes. Reaching a point whereby norms spread, cascade, and are internalized at the national level, and on-going disagreements are bridged, will remain the principle test moving forward, requiring important investment in diplomatic action and capacity-building. In this regard, sustained effort in trust- and capacity-building, dialogue, and engagement among States, between States and other key actors, and across regimes are imperative.

Figure 2. ICTs, international peace and security, and the principal organs of the United Nations


SECURITY COUNCIL
GENERAL ASSEMBLY
ECONOMIC & SOCIAL COUNCIL
SECRETARIAT
MAIN COMMITTEES
COUNTER-TERRORISM COMMITTEE
Normative work on terrorism and ICTs
FIRST COMMITTEE
Disarmament and international security
SECOND COMMITTEE
Sustainable development
THIRD COMMITTEE
Human rights, criminal justice, crime prevention (inc. terrorism)
HUMAN RIGHTS COUNCIL
SUBSIDIARY ORGANS
UN CTED
Reporting, capacity building, research on terrorist use of the Internet
GGEs
Consideration of international law, norms of state behaviour, CBMs, capacity building
RESEARCH AND TRAINING
UNIDIR
Research on ICTs and international security, capacity-building, consultant to GGEs
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS
UN Special Rapporteurs on freeedom of expression and on right to privacy
SPECIALIZED AGENCIES
ITU, UNESCO*
Capacity building, technical assistance, research, conferences
RESEARCH AND TRAINING
UNICRI
Research on crime/terrorism and ICTs, capacity building
UN OCT
CTITF + Counter-Terrorism Centre: Coordination of counter-terrorism efforts. inc. terrorist use of the Internet; protection of critical infrastructure
UN OHCHR
Normative, substantive, capacity building and organizational support inc. rights and freedoms relating to ICTs
UNDESA
Substantive and organizational support on SDGs, WSIS, IGF
UNODA
Substantive and organizational support to the GGEs
UNODC
Substantive and organizational support to counter the use of ICTs for terrorist or criminal purposes
INTERNATIONAL PEACE & SECURITY
HUMAN RIGHTS
ECONOMIC & SOCIAL DEVELOPMENT
TRANSNATIONAL THREATS

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

2. The United Nations, ICTs, and International Peace and Security

2.1 The normative work of the General Assembly's First Committee

Until recently there was a general view that despite the complexity of ICTs and an increase in their malicious use, including by States, good progress had been made in reaching agreement on the norms—both binding and non-binding—applicable to State use of ICTs and in developing a framework for ensuring a stable and secure ICT environment. Most of these discussions have taken place within the General Assembly's First Committee on disarmament and international security and its GGEs, the resulting framework then picked up, endorsed, or operationalized by different regional, subregional, plurilateral, and specialized bodies or in bilateral arrangements between States. This section of the report discusses this progress as well as important fault lines that have emerged around how to apply existing legal rules and principles to the use of ICTs by States and around the most appropriate forum and format for bringing these discussions forward within the United Nations.

The genesis of ICT-related norm-shaping efforts in the context of international peace and security

The General Assembly has served for decades as the centre of gravity for diplomatic negotiations over information technologies and their perceived and real effects, notably as they relate to the concept of sovereignty. Hence, it was only natural that cyberspace and related ICTs, including the Internet, would end up on its agenda.[36]

To date, most discussions in the United Nations relating to ICTs in the context of international peace and security have taken place within the General Assembly's First Committee on disarmament and international security spurred by a draft resolution tabled by the Russian Federation in 1998. Following closely on the heels of that first resolution, in 2000 Russia proposed a series of "Principles of International Information Security" that would form the basis of a new legal instrument or a code of conduct to regulate State uses of ICT with the objective of protecting the "information environment" and outlawing so-called "information weapons".[37] The initiative emerged against a background of Russian concerns over the perceived Western dominance of the information technology (IT) sector.[38] More specifically, it also related to concerns over United States military superiority resulting from its advances in military IT that had become apparent during the 1991 Gulf War as well as growing emphasis in Western military strategy on information warfare, information operations, and information dominance.[39]

The Russian Federations' efforts to shape an international legal regime in international information security were supported by a growing number of States, yet were met with distrust by Western States.[40] This was reportedly in large part due to the draft resolution's emphasis on information *per se,* the potential human rights implications of such emphasis, and the central role the proposed regime afforded governments and multilateral organizations in managing ICT insecurities and risk, with no mention of the role non-State actors such as private companies and technical organizations play in their management and resolution.[41]

Some States were reticent to discuss the issue of information security within a disarmament context. It risked launching the international community "on a complex enterprise encompassing many interrelated factors that the First Committee did not ordinarily address: technical aspects relating to global communications, as well as nontechnical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, antiterrorist cooperation, and other issues considered in the Second or Sixth Committee".[42] Other States argued that the focus on information rather than cybersecurity placed content rather than infrastructure at the centre of the debate.[43] The resolution would also have tabled discussion on—and invited public scrutiny of—advanced ICT capabilities, a step no State with a technologically sophisticated military was willing to take at that time.[44] Several attempts to segment the topic—pushing it out of the First and into the Second and Third Committees—failed.[45] As a means to move the discussion forward, the Russian Federation proposed the establishment of a GGE to study the matter.[46]

The United Nations Groups of Governmental Experts

The General Assembly regularly establishes GGEs to study or investigate emerging international security concerns and make recommendations.[47] In the ICT arena, mounting challenges posed by growing "cyber insecurities" involving State and non-State actors eventually convinced other States to engage on the matter within the First Committee and via a series of such groups.[48] Working towards an "open, secure, stable, accessible and peaceful ICT environment", negotiations within the GGEs (five to date) have generated some important normative achievements. Indeed, the process unwittingly channelled a debate originally (and divisively) focused on "preventing an arms race in information weapons" towards a more productive and much-needed discussion on norms governing State behaviour in cyberspace and the use of ICTs. It has resulted in an important agreement among the experts that existing international law including the Charter of the United Nations applies to the use of ICTs by States. It also resulted in a number of non-binding political norms of State behaviour, and confidence- and capacity-building measures. The increase in the GGE's membership—from 15 to 25 experts (see figure 3)—also demonstrates the growing weight afforded to them.

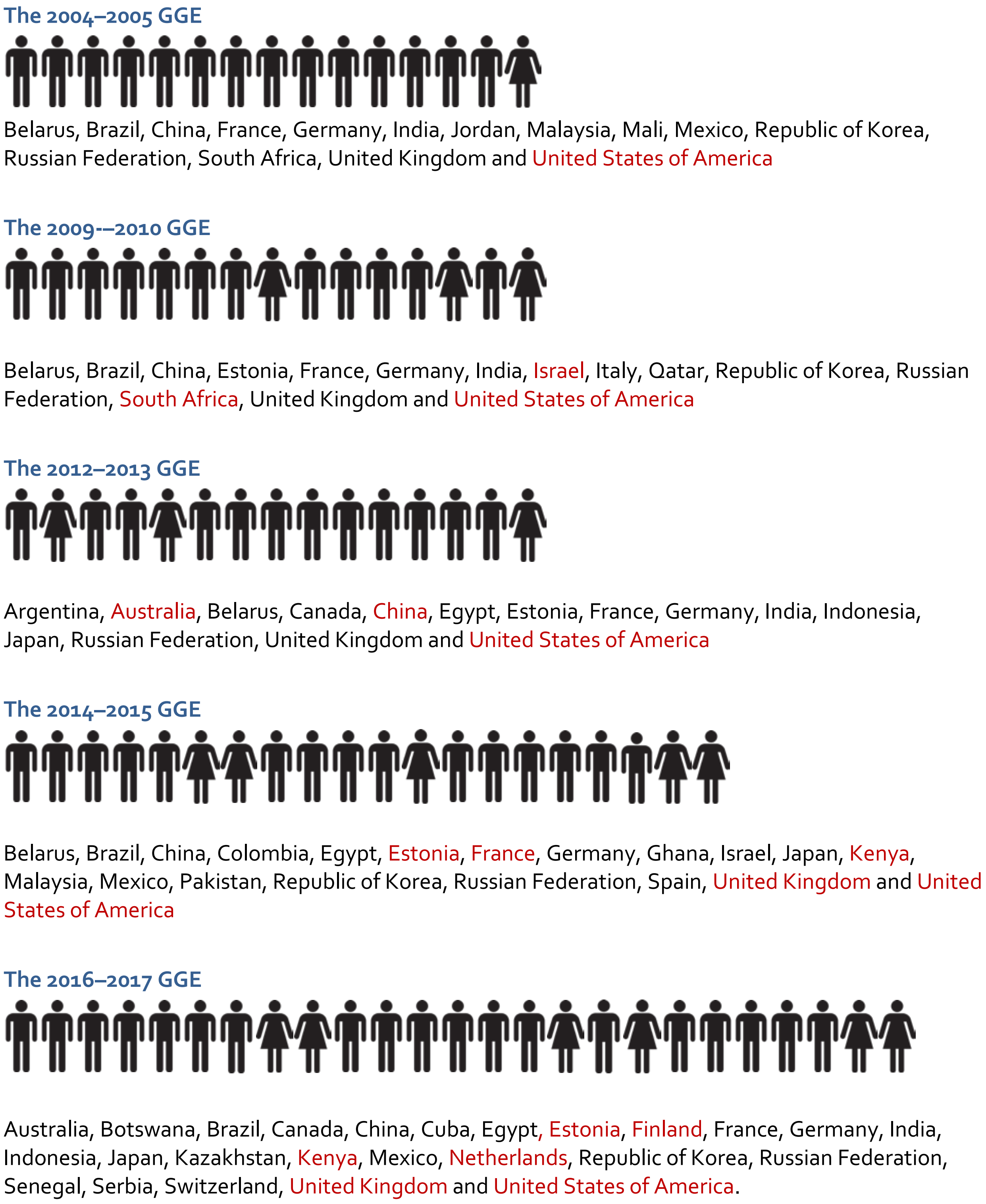
Despite their non-binding character, the GGE reports have been viewed as important building blocks towards greater stability in cyberspace. They have also spawned several complimentary initiatives at the global and regional levels aimed at building awareness of, and consensus around, the norms agreed upon by the GGEs, building trust and confidence among States and between States and other stakeholders, and increasing efforts to build capacity in developing countries. At the same time, and as the most recent GGE has demonstrated, they also have important limitations.

The 2009–2010 GGE

The Russian Federation's proposal to establish a GGE to study developments in the field of information security was adopted in 2001 and met between 2004 and 2005. Yet, given differing views and positions, the group of 15 States failed to produce a report.[49] However, in 2006, the General Assembly adopted resolution 60/45, agreeing to convene a new GGE in 2009. The establishment of this new GGE in 2009 thus coincided with a change in government in the United States and the new administration's "reset" strategy vis-à-vis the Russian Federation, as well as the disruptive ICT incidents in Estonia (2007) and Georgia (2009) which had, by then, captured global attention. [50]

Adopted in July 2010, this first consensus GGE report was succinct, yet it marked an important step forward in terms of acknowledging the ICT threats and vulnerabilities affecting the global community. It noted that States and not just criminals and terrorists were possible vectors of ICT-related threats, and that a lack of shared understanding regarding norms governing State use of ICTs was creating a growing risk of misperception, with the potential to "affect crisis management in the event of major incidents".[51] The report suggested a number of cooperative measures to meet these challenges, stressing the important role of the private sector and civil society in any steps taken to achieve "a secure and resilient digital environment".[52] The 2009–2010 GGE was followed by two more, producing consensus reports in 2013 and 2015 respectively, each more detailed on the nature of the threats and responses required, influenced in no small part by growing State use of cyberspace and ICTs for non-peaceful purposes.

Figure 3. GGE Membership since 2004



The 2004–2005 GGE

Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, Republic of Korea, Russian Federation, South Africa, United Kingdom and United States of America

The 2009-–2010 GGE

Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, Republic of Korea, Russian Federation, South Africa, United Kingdom and United States of America

The 2012–2013 GGE

Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russian Federation, United Kingdom and United States of America

The 2014–2015 GGE

Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russian Federation, Spain, United Kingdom and United States of America

The 2016–2017 GGE

Australia, Botswana, Brazil, Canada, China, Cuba, Egypt, Estonia, Finland, France, Germany, India, Indonesia, Japan, Kazakhstan, Kenya, Mexico, Netherlands, Republic of Korea, Russian Federation, Senegal, Serbia, Switzerland, United Kingdom and United States of America.

The 2012–2013 GGE

Despite its difficult trajectory and the very different positions and interests of participating experts, the 2012–2013 GGE reached consensus on a number of important issues (see figure 4).[53] It confirmed that existing international law applies to cyberspace, notably that the Charter of the United Nations is "essential to maintaining peace and stability" and for "promoting an open, secure and accessible ICT environment".[54] Moreover, the Group confirmed that the international norms and principles constituting State sovereignty (understood as both rights and responsibilities) apply "to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory", and that States should "meet their international obligations regarding internationally wrongful acts attributable to them", refrain from using proxies, prevent their territories from being used by non-State actors for unlawful use of ICT, and respect fundamental human rights and freedoms.[55]

The 2013 Group also emphasized the need to intensify cooperation to respond to criminal or terrorist use of ICTs, including harmonization of legislation and collaboration between law enforcement and prosecutorial services (elements of which have since been picked up in Security Council resolutions and in projects managed by the UN Office on Drugs and Crime and the UN Counter-Terrorism Executive Directorate). Mirroring developments at the regional level, notably within the OSCE, the Group recommended a range of confidence- and capacity-building measures to "promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception".[56] It was hoped that progress in making ICTs secure, including through capacity- building, would also contribute to "developing a global partnership for development", as described in former Millennium Development Goal 8. The document also echoed the 2009 GGE's call to engage the private sector, academia, and civil society in implementing the Group's recommendations.[57]

Overall, the report was a significant achievement, particularly since the period was punctuated by further revelations and accusations of State-sponsored disruptive ICT-related incidents, State-sponsored industrial and political espionage, and whistle-blower revelations of intrusive State surveillance and monitoring practices, sending ripples of unease throughout the international community and leading to calls for more responsible State behaviour.

The 2014–2015 GGE

Immediately following the presentation of the 2013 report, the Russian Federation successfully pushed for the establishment of a fourth GGE, tasked with studying how the norms, rules, and principles agreed on in 2013 should be operationalized.[58] It was also asked to examine "relevant international concepts aimed at strengthening the security of global information and communications systems" and advance discussions on possible cooperative, confidence-building, and capacity-building measures. The membership of the GGE was expanded from 15 to 20 in response to the growing interest of States beyond the P-5 to participate in the discussions.

The 2014–2015 GGE concluded its work in June 2015.[59] It worked, once again, against a background of mistrust driven in large part by the growing frequency of significant ICT incidents implicating States, including the Security Council's permanent five members. Nonetheless, the group produced a report largely confirming the 2012–2013 consensus that international law, in particular the Charter of the United Nations, applies to State uses of ICTs (see figure 4). It also identified as of central importance the commitments of States to the "principles of the Charter and of other international law", including:

> sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.[60]

Contrary to what many were hoping, the Group did not advance the discussion on what constitutes an armed attack or related thresholds in the ICT context. It did include in its report, however, "the inherent right of States to take measures consistent with international law and as recognized in the Charter" in response to an ICT incident, an indirect reference to the self-defence provisions under article 51 of the Charter. Some progress was made on international humanitarian law in that a paragraph was inserted broadly noting established principles of international law, including humanity, necessity, proportionality, and distinction.[61] The international law section of the report also included reference to important United Nations Human Rights Council resolutions.[62]

Another important achievement was the Group's inclusion of a set of non-binding political norms relating to State behaviour in peacetime, all of which have important implications for international peace and security (see figure 4). Although some of the norms restate principles of existing international law, likely reflecting difficult negotiations, the 11 proposed norms offer an important framework for States to work towards greater stability. They include recommendations relating to the protection of critical infrastructure, the protection of national computer emergency response teams (CERTs) and their systems from malicious activity, preventing the use of a State's territory for the commission of internationally wrongful acts, linking attribution of internationally wrongful acts to standards of proof, ensuring the integrity of the supply chain, protecting human rights online, and enhancing cooperation to share information, particularly with regard to prosecuting terrorist and criminal use of ICT.[63] As discussed later in this section, a number of confidence- and capacity-building measures were also recommended.

The 2016–2017 GGE

Many observers had been sceptical that any new GGE could break new ground, arguing that the GGE process had likely exhausted its normative potential. Rather than lose themselves in yet more process, States needed to get beyond discussing potential norms and instead focus on implementing existing normative recommendations and use alternative mechanisms to iron out persisting disagreements. Nonetheless, another GGE started work in August 2016 with a similar mandate, this time with the participation of 25 experts. It concluded its work in July 2017 having failed to produce a consensus report.

As publicly discussed by some experts and in several post-GGE analyses,[64] most disagreement in the 2016–2017 GGE emerged around the international law section and on the future format of these discussions. In accordance with its mandate, the Group attempted to advance discussion on *how* international law applies to State uses of ICT as per the recommendations of the 2015 report, including on the peaceful resolution of disputes (corresponding to paragraph 26), sovereignty and jurisdiction (corresponding to paragraphs 28a and b); self-defence (corresponding to paragraph 28c), international humanitarian law (corresponding to paragraph 28d), and internationally wrongful acts (corresponding to paragraphs 28e and f). These efforts—notably those relating to the latter three areas of law—were reportedly rejected by several States for a

Figure 4. GGE recommendations on international law and non-binding norms of State behaviour

The 2004–2005 GGE

No consensus for a report

The 2009–2010 GGE

International Law

- Existing agreements include norms relevant to the use of ICTs by States.

The 2012–2013 GGE

International Law

- International law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and promoting an open, secure, peaceful and accessible ICT environment;
- State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory;
- State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments;
- States must meet their international obligations arising from internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts and ensure their territory is not used for unlawful uses of ICTs.

Voluntary norms

- States should cooperate against criminal and terrorist use of ICT including through harmonizing legal approaches and strengthening collaboration between law enforcement and prosecutorial agencies;
- States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.

The 2014–2015 GGE

International Law

- The Group identified as of central importance the commitments of States to the following principles of the Charter of the United Nations and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States;
- State sovereignty and international norms and related international norms and principles apply to state conduct of ICT-related activities;
- States have jurisdiction over the ICT infrastructure located within their territory;
- In their use of ICTs, States must observe among other principles of international law, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the affair of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect human rights and fundamental freedoms;
- States have an inherent right to take measures consistent with international law and as recognized in the UN Charter. The Group recognized the need for further study on this matter;
- The Group noted the established legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;
- States must not use proxies to commit internationally wrongful acts and ensure their territory is not used by non-state actors to commit such acts;

- States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, an indication that an activity was launched or originates from the territory or the ICT infrastructure of a state may be insufficient to attribute the activity to that State. Accusations of organizing and implementing internationally wrongful acts should be substantiated;
- Common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment.

Voluntary norms

- Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
- In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;
- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;
- States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;
- States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
- The Group observed that, while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity.
- Given the unique attributes of ICTs, additional norms could be developed over time.

The 2016–2017 GGE

No consensus for a report

Figure 5. GGE recommendations on confidence building and cooperative measures

The 2004–2005 GGE

No consensus for a report

The 2009–2010 GGE

To reduce the risk of misperception stemming from ICT disruptions, the Group recommended that States:

- Implement confidence building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
- Exchange information on national legislation and national information and communications security strategies and technologies, policies and best practices.

The 2012–2013 GGE

To increase transparency, predictability and cooperation, the Group recommended that States consider:

- The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation. The extent of such information will be determined by the providing States. This information could be shared bilaterally, in regional groups or in other international forums;
- The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed;
- Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms;
- Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels;
- Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors;
- Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security.

Additional recommendations

- Enhance common understandings and intensify practical cooperation through regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums, and other international organizations.

The 2014–2015 GGE

To enhance trust and cooperation, and reduce the risk of conflict, the GGE recommended:

- The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;
- The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

- Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;
- The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:
  - i. A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
  - ii. The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
  - iii. The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests; and
  - iv. The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.

Additional recommendations

- Consider additional confidence-building measures to strengthen cooperation on a bilateral, subregional, regional and multilateral basis, including through agreements to:
  - o Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;
  - o Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;
  - o Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;
  - o Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector- based cooperation; and
  - o Cooperate, in a manner consistent with national and international law, with requests to investigate ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

The 2016–2017 GGE

No consensus for a report

number of reasons (some legal, some technical, and others more political)—leaving little doubt of the significant differences in positions and interests between States or groups of States on how the rules and principles governing State behaviour in the use of ICTs should be applied. Some argue that one of the core problems of the Group vis-à-vis the international law discussion was the over-emphasis by some experts on detailed legal technicalities, while others suggest that it was likely the wrong forum for government experts to be discussing matters of international law.[65] Regardless, the exercise likely served the important purpose of allowing States to signal red lines to each other on what they view as acceptable behaviour and how they will likely react in the event of a serious ICT incident, part of the "gradual process of establishing shared expectations".[66]

Confidence-building measures in the work of the GGEs

The UN GGEs themselves have demonstrated how trust among highly competitive actors is difficult to build. It is particularly challenging in an environment where anonymity is perceived as advantageous to only some States and where other geopolitical interests and concerns are framing State action. Nonetheless, over the past few years, a range of international and regional organizations—often supported by independent experts, universities, think tanks, and non-governmental organizations—have established processes aimed at identifying measures that can best help respond to the growing mistrust among States on their uses of ICTs and enable broader adherence to norms. While at times slow to take root, these processes have served as a form of pressure valve, allowing for more direct discussion on key issues, which can help create an environment more conducive to implementing the binding and non-binding norms relating to State uses of ICT discussed in the previous section.

Both the 2013 and 2015 GGE reports included several recommendations on confidence-building and cooperative measures (figure 5). The wide range of measures addressed is aimed at those ICT-related activities that risk leading to conflict between States. Their wide-ranging focus also addresses the priorities of States not affected by the broader strategic concerns of the major powers.

Importantly, as outlined in the following section, regional forums such as the OSCE, ARF, and OAS have since taken up many of these confidence-building measures (CBMs).[67] Regional and subregional CBM processes are helping to strengthen the framework resulting from the work of the GGEs. They have opened new channels for dialogue and experience-sharing and for identifying obstacles to implementation, not only of the CBMs emerging within each regional and subregional setting, but also the non-binding political norms of State behaviour recommended by the GGEs. Providing greater guidance on and support to implementing the CBMs at the national level will be key moving forward.

Whither the norm-shaping work of the First Committee GGEs?

The fact that the latest GGE could not reach consensus on a report does not necessarily impede further discussion of ICT and international security. What future format such discussions would take within the United Nations remains to be seen however. Another GGE at this stage is unlikely, unless there is agreement that the core focus be the more difficult matters around which consensus could not be reached in the 2016–2017 GGE. Before the current GGE had commenced its work, some had suggested the adoption of a General Assembly resolution that would open the discussions to a broader group of Member States through an open-ended working group of the General Assembly's First Committee.[68] While this option would address the criticism that the GGE format has been insufficiently inclusive, what it would focus on and how agreement would be reached among the entire General Assembly membership (i.e. 193 States) remains unclear. And while others have in the past suggested the Geneva-based Conference on Disarmament (CD) as a possible alternative venue for these deliberations, the limited membership of the CD, as well as its character as a negotiating body, might undermine its role as an effective alternative.[69] For some, an arrangement similar to the Committee on the Peaceful Uses of Outer Space (COPUOS) or its more narrowly focused Legal Sub-Committee could be the way forward.[70] For yet others, moving the discussion outside the UN—or supporting non-UN or parallel initiatives to develop new or additional norms—could be a better option for the near to middle term, although the question of how to best channel the results of these initiatives back into the multilateral space and thereby ensure their legitimacy vis-à-vis the broader international community again arises.[71] Possibly a hybrid option which considers principles of transparency and inclusivity, while also advancing more technical/substantive work, might be an option.[72] Whatever the choice, both creativity and openness on the part of all stakeholders to new alternatives will be necessary. In the meantime, further efforts can be made to implement the recommendations on non-binding norms and confidence- and capacity-building of earlier GGE reports.

2.2 The work of the Security Council

In addition to the different General Assembly bodies that have focused on ICTs in the context of international peace and security, several UN Member States are keen to see the Security Council play a stronger role on cybersecurity-related matters beyond the terrorism-related resolutions in which ICTs are increasingly mentioned.

For instance, in November 2016, the Security Council was briefed for the first time, via an open Arria-formula meeting chaired by the governments of Senegal and Spain, on cybersecurity. The objective of the meeting, which involved the participation of representatives from governments, regional organizations, the private sector, and civil society, was to broaden discussion beyond terrorist use of the Internet to cover the potential of State use of ICTs in fuelling political or military tensions and the importance of the protection of ICT-dependent critical infrastructure in such cases.[73]

As a sign of growing concern, another Arria-formula meeting organized in April 2017 on the topic of “hybrid wars as a threat to international peace and security” and chaired by Ukraine, focused on the changing character of warfare propelled by the “increasing use of new technologies and strategies”.[74] The concept note circulated ahead of the meeting discussed the theoretical underpinnings of so-called hybrid warfare, citing “cyber technologies, interference with political processes, and systematic dissemination of propaganda domestically and internationally, among the means to achieve political objectives”, drawing attention to their use by States in recent conflicts and their impact on international peace and security. Whether a more formal discussion on State use of ICTs in the context of international peace and security will emerge on the Security Council agenda in the future remains to be seen.

2.3 Select norm-shaping and confidence-building initiatives outside the UN framework

Several other initiatives relating to ICTs and international security have emerged alongside the work of the GGEs. Some are proposing normative solutions that are perceived as contradicting the recommendations of the GGEs. Others stem from the work of the GGE and involve follow-on work beyond the UN to cascade the recommended norms across different groupings, including collective security organizations such as the North Atlantic Treaty Organization (NATO), or those focused on financial stability, trade, and economic development, for which a stable and secure ICT environment is also viewed as key. Yet others are intended to study or propose additional norms while bringing other actors such as the private sector, academia, and civil society into the discussion. And in some cases, it is these other actors themselves who are proposing norms and making suggestions on how to move their implementation forward.

The Shanghai Cooperation Organization

In 2011, some of the members of the SCO (China, the Russian Federation, Tajikistan, and Uzbekistan) presented an "International Code of Conduct for Information Security" to the General Assembly.[75] The proposed code of conduct included voluntary provisions banning the use of the Internet for military purposes, notably for the conduct of hostile activities or acts of aggression via the proliferation of "information weapons" or related technologies. It also called for the respect of existing norms such as sovereignty, territorial integrity, and political independence and guaranteeing the supply chain integrity.[76] Although it strongly emphasizes the importance of countering terrorist and criminal use of ICTs, it is silent on the question of cross-border cooperation, likely since the latter would require access to data and digital evidence located within individual State jurisdictions. In addition, the document has been criticized by some on the basis that human rights provisions in the document are linked to caveats making them contingent on national security, without providing for the relevant protections.[77]

In January 2015, China and the Russian Federation presented a revised draft of the Code of Conduct to the General Assembly on behalf of the SCO, signalling their sustained interest in a new binding instrument. While the revised draft no longer refers to the term "information weapons", it continues to reflect Russian and Chinese concerns regarding technological dependence and the threat of sabotage.[78] It includes a new section recognizing, in accordance with a 2014 United Nations Human Rights Council resolution, that human rights apply online as they do offline, although it conditions this recognition on national security prerogatives. Western commentators argue the draft Code reflects a vision of cybersecurity crisis management incompatible with the recommendations of the 2013 and 2015 GGE reports.[79] It is unclear whether the Russian Federation will continue to pursue the Code of Conduct within the General Assembly, although its continued attachment to the proposal was confirmed by the Russian expert to the GGE in a recent interview.[80]

The OSCE

As discussed in the previous section, several regional organizations and fora have developed working agendas on cybersecurity and ICTs in the context of international and regional security, particularly through the lens of confidence-building and cooperative measures. The OSCE, for example, commenced its work in this area in 2011, resulting in the establishment, by the OSCE Permanent Council, of an open-ended informal working group (IWG) on CBMs under the auspices of the OSCE Security Committee in 2012. The IWG was tasked with elaborating and building consensus around CBMs that can enhance interstate cooperation, transparency, predictability and stability, and reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs, and to report on progress made.[81] Since then, some sixteen CBMs have been negotiated and adopted.[82] Aimed principally at enhancing cooperation and transparency between

OSCE participating States, the relevant Permanent Council and Ministerial Decisions stressed that these efforts be "consistent with international law, inter alia, the [Charter of the United Nations] and the International Covenant on Civil and Political Rights; the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms"[83] and should complement efforts by the United Nations, international and regional fora. Their importance confirmed at a December 2016 OSCE Ministerial meeting, the IWG has since stepped up its deliberations on how best to implement CBMs across the region. Indeed, a number of OSCE participating State proposals on how to implement some of the CBMs are currently on the IWG agenda, while broader CBM-related activities tend to feature in the annual OSCE Chairmanship conferences.[84] In addition, and following an initial, informal assessment of implementation of the CBMs, the Secretariat has requested an academic steering group to submit proposals that can support OSCE efforts to implement the CBMs.

The ASEAN Regional Forum

In 2015, the ASEAN Regional Forum developed a "Work Plan on Security of and in the Use of ICTs".[85] It sets out several measures aimed at "promot[ing] a peaceful, secure, open and cooperative ICT environment and prevent[ing] conflict and crises by developing trust and confidence between States in the ARF region, and by capacity building".[86] Similar to the OSCE process, it established an open-ended "Study Group" responsible for developing the processes and procedures necessary for implementing the CBMs and for conducting workshops and seminars on a number of topics aimed at enhancing cooperation and transparency and deepening understanding of related issues such as norms of State behaviour. The actual work plan is focused on developing measures that can promote transparency and build confidence to deepen understanding of the ARF participating States as a means to reduce the risk of misperception, miscalculation, and escalation of tension leading to conflict; enhancing practical cooperation between ARF participating States to protect ICT-enabled critical infrastructure with the view to also developing resilient government ICT environments; and improving cooperation including by developing regional capacity to respond to criminal and terrorist use of ICTs. Renewed efforts are underway to move the ARF process forward.

The OAS

More recently, the Organization of American States moved in a similar direction as the OSCE and the ARF. Building on an earlier commitment to generate confidence-building measures that enhance international peace and security and that increase cooperation, transparency, predictability, and stability among States in the use of cyberspace, in May 2017 the OAS adopted a resolution establishing a "Working Group on Cooperation and Confidence-Building Measures in Cyberspace". The task of the Group is to prepare a set of draft CBMs, based on the consensus reports of the GGE to enhance interstate cooperation, transparency, predictability, and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.[87] Meanwhile, the OAS is implementing a programme aimed at supporting OAS member states in cyber security strategy development, awareness raising and capacity building.

NATO

ICTs in the context of armed conflict were first included on NATO's political agenda during the Prague Summit in 2002. This focus was ratcheted up in 2007 following the disruptive ICT incidents affecting Estonia, and this lead to the adoption of the organization's first cyber defence policy in 2008. Cyber defence has received ever-greater attention since. Indeed, between the Lisbon Summit in 2010 and the Wales Summit in 2014, cyber defence was included in NATO's Strategic Concept (i.e., linking it to collective defence, crisis management, and cooperative security) and eventually was assigned its own policy slot via the NATO Policy on Cyber Defence. The latter recognized the application of Article 5 of the Washington Treaty to "a major digital attack on a Member State", while also providing for improved information-sharing and mutual assistance arrangements between NATO allies, as well as training, exercises, and relations with industry actors. The 2016 Warsaw Summit saw NATO take up the recommendations of the 2015 GGE, notably the commitment "to act in accordance with international law, including the [Charter of the United Nations], international humanitarian law, and human rights law, as applicable" and "follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace". It also welcomed the work that had been achieved on voluntary international norms of responsible State behaviour and confidence-building measures regarding cyberspace. At the same time, NATO recognized cyberspace as an operational domain, committing additional resources to defence capabilities and pledging to "further develop NATO–[European Union] cyber defence cooperation".[88] Conversely, many non-NATO States view this posturing as acting contrary to goals and recommendations of the GGE, including the use of ICTs for peaceful purposes and the peaceful resolution of disputes that might emerge around ICTs.

The European Union

The European Union (EU) has played an important role in shaping norms for behaviour in cyberspace. Over the past few years and driven by the increased ability of State and non-State actors to conduct malicious ICT activity, the European Union has adopted a "Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" (referred to as the "EU Cyber Diplomacy Toolbox"), which builds on the EU Cybersecurity Strategy and EU Cyber Diplomacy and reads as a form of deterrent vis-à-vis malicious ICT activity.[89]

Adopted in June 2017, the Cyber Diplomacy Toolbox endorsed the recommendations of the 2010, 2013 and 2015 GGEs, encouraging the 29 members of the EU to "strongly uphold the consensus that international law is applicable to cyberspace" and that they "be guided by the UN GGE reports' recommendations in their use of ICTs". The Council's Draft Conclusions also take up the GGE consensus that "malicious cyber activities might constitute wrongful acts under international law" and that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs" (paragraphs 28e and f of the 2015 GGE report). On the thorny issue of attribution, the Council notes that attribution is ultimately a "sovereign decision" based on all-source intelligence and that any effort to attribute an incident should be established in accordance with the international law of State responsibility.[90]

Key elements of the "toolbox" include continued diplomatic engagement and dialogue as well as support for filling capacity-building needs in third countries. In addition, it highlights the role that signalling the likely consequences of a joint EU diplomatic response could have on influencing the behaviour of potential aggressors in cyberspace. To this end, it concluded that leaning on existing measures within the Common Foreign and Security Policy, including, if necessary, "restrictive measures" (i.e. sanctions), in response to the malicious use of ICTs "would be suitable for a framework of a joint EU diplomatic response to malicious ICT activity", and encourage cooperation and facilitating mitigation of immediate and long-term threats.[91]

Another significant development within the EU was the adoption, in August 2016, of the Network and Information System (NIS) Directive, "the first EU-wide legislation on cybersecurity [to] support and facilitate strategic cooperation between Member States as well as the exchange of information".[92] The Directive provides legal measures to boost the overall level of cybersecurity in the EU through a number of obligations relating to preparedness (establishment of cybersecurity incident response team (CSIRTs) and a competent national NIS authority), national and regional cooperative measures (national cooperation groups and a regional CSIRT network), promotion at the member State-level of a culture of security across sectors, and compliance, by digital service providers, of security and notification requirements. Importantly, it also includes a paragraph requiring States to respect existing human rights obligations when implementing the Directive, notably on privacy and data protection. While important challenges remain on this front, the EU can establish effective mechanisms to monitor implementation of the instrument. Such monitoring mechanisms can draw important lessons from EU member States' implementation efforts, which can in turn be shared more broadly.

The BRICS Grouping

For the BRICS countries—Brazil, Russia, India, China and South Africa—the UN and the principles of the UN Charter remain pivotal to any normative action relating to the use of ICTs. BRICS leaders commenced discussions on ICTs and norms of behaviour in 2013, its eThekwini Declaration and Action Plan noting the importance of "contributing to and participat[ing] in a peaceful, secure, and open cyberspace", and emphasizing the "paramount importance" of "universally accepted norms, standards and practices" for security in the use of ICT.[93] Successive statements have captured these issues, recommending, in addition to a number of practical cooperative measures, that the grouping should also "focus its efforts on confidence-building measures, capacity-building, the non-use of force, and the prevention of conflicts in the use of ICTs."[94] The more recent Xiamen Statement re-emphasized the "central role of the UN in developing universally accepted norms of responsible state behaviour in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment". In addition, it stressed "the paramount importance of the principles of international law enshrined in the Charter of the United Nations", and "the need to enhance international cooperation against terrorist and criminal misuse of ICTs". Additionally, the Declaration promotes cooperation in accordance with "the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs or any other mutually agreed mechanism" and acknowledged an [yet-to-be-unveiled] initiative of the Russian Federation on "a BRICS intergovernmental agreement on cooperation in ensuring security in the use of ICTs".[95]

The Group of 20

In November 2015, the G20, comprising the leaders of the twenty largest economies in the world, issued an important communiqué, affirming that existing international law, including the Charter of the United Nations, applies to State behaviour in cyberspace and called on all States to "abide by the norms of responsible state behaviour" recommended in the 2015 GGE report.[96] The G20 leaders affirmed the norm that no State should conduct or support the ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. The communiqué also called on all States to "respect and protect the principles of freedom from unlawful and arbitrary interference of privacy", including in the context of digital communications. The G20 communiqué and its endorsement of the 2015 GGE report in general, represent an important step toward socializing and internalizing its recommendations.

More recently, in March 2017, G20 finance ministers and central bank governors committed to strengthening the resilience of the global financial system against malicious uses of ICTs that could “disrupt financial services crucial to national and international financial systems, undermine security and confidence and endanger financial stability”.[97] The related communiqué requested the Financial Stability Board to perform a stocktaking exercise of existing regulations and supervisory practices in G20 jurisdictions, and of existing international guidance, including on effective practices. The results of this initial stocktaking exercise will be presented before the end of 2017. Some observers view this as an important step towards a new norm aimed at protecting the integrity of financial data, suggesting that G20 efforts in this area build on the recommendations of the 2015 GGE report on norms to prevent attacks on critical infrastructure in peacetime and the work of other organizations such as the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI–IOSCO), which released a “Guidance on Cyber Resilience for Financial Market Infrastructures” in 2016.[98]

The Group of Seven

The Group of Seven (G7), too, has focused significant attention on cybersecurity. While these efforts commenced several years ago, the April 2017 Lucca Declaration on Responsible State Behaviour in Cyberspace, builds on the “Principles and Actions on Cyber[space]” the grouping had endorsed in Ise-Shima, Japan, in May 2016.[99] Following from the recommendations of the 2013 and 2015 GGE reports, the Ise-Shima Principles had included recognition by the G7 of the inherent right of individual or collective self-defence as recognized in article 51 of the Charter of the United Nations as well as international humanitarian law, “in response to an armed attack through cyberspace”. The 2017 Lucca Declaration specifically takes up a number of international law questions that reportedly impeded consensus in the most recent GGE, notably the use of non-forcible countermeasures, including measures conducted via ICTs, in response to an internationally wrongful act—in this case malicious ICT activities that do not amount to an armed attack—committed by another State directly or via proxies. The Declaration also endorses and promotes the 11 voluntary, non-binding norms of responsible State behaviour in cyberspace recommended by the 2015 GGE, listing them alongside the norm endorsed by the G20 relating to ICT-enabled theft of intellectual property.

State-led initiatives

As leading global powers, China, Russia and the United States play an important role in shaping and adhering to norms. Smaller States, too, are increasingly engaging on these issues.

For its part, and mirroring its growing normative engagement on other issues, **China** is increasingly involved in norm-shaping and trust-building initiatives relating to cyberspace and international security. It is doing this through several forums including the SCO, the GGE, the G20, the BRIC grouping, the Asian–African Legal Consultative Organization (AALCO), through its hosting of international conferences relating to the Internet or cybersecurity and through a number of Track 1 and 1.5 initiatives.[100] China’s recently launched “International Strategy of Cooperation on Cyberspace” is a first attempt to articulate an official policy on cyberspace and cybersecurity for a global audience. The principle of sovereignty is the normative cornerstone of the policy and related activities, which maintains that each State has the right to regulate cyber infrastructure and activities within its territory.[101] The new strategy also presents an alternative to the Western preference for multi-stakeholder governance of the Internet and ICT systems in general, proposing instead principles of “shared governance” and “shared benefits” and alternative approaches to international rules and cooperation.[102] China’s promotion of—and participation and investment in—international organizations such as the United Nations, including in the area of international peace and security, has also grown significantly at a time when the United States is divesting in the Organization, and will likely increase in tandem with China’s efforts to shape global norms as they apply to ICTs and in other, related areas.[103]

As discussed in section 2.1, the **Russian Federation** has been working via the First Committee of the UN General Assembly to achieve its normative goals since the late 1990s and remains steadfast on ensuring that any agreement pertaining to norms and ICTs is reached under the auspices of the United Nations. It also works via the Shanghai Cooperation Organization and other sub-regional fora, as well as the BRICS grouping to develop cooperative measures to respond to information security threats.

For many years, the **United States** was steadfast in its position that existing global norms should be the starting point for any discussion on ICTs in the context of international security and for ensuring stability of the ICT environment. The Obama administration’s 2011 International Strategy for Cyberspace was the first major outward-looking US cyberspace initiative in this regard, laying out its vision of how the international community might proceed.[104] Centred on the need to prevent States from “exerting traditional power in cyberspace” and the importance of international consensus on “norms for responsible state behaviour”, the Strategy emphasized the links between national and global cybersecurity, an approach that had already been embraced by many EU States and that is largely influencing capacity-building efforts in this area.[105]

As part of its longer-term approach, US government officials see value in building on the current normative work on ICTs and international security via a mechanism similar to the Proliferation Security Initiative (PSI).[106] The emphasis on a PSI-like initiative stems from assessments of its track record as a useful instrument for spurring rapid international cooperation on critical global security challenges. In this regard, one commentator notes how it has “mobilized co-operative nuclear non-proliferation activities, led to international legal developments, and has been adopted to promote new non-proliferation initiatives” with initial resistance replaced by “acceptance (albeit, in some cases, grudging) among governments and independent analysts, out of recognition that its informal and flexible nature makes it a valuable complement to formal mechanisms”.[107] In the ICT area, it would involve working with groups of “like-minded States” that would “observe international norms of appropriate state behaviour, cooperate seamlessly against common cyber-threats, refrain from destabilising activity, and join together in the future to sanction bad actors and to aid each other in mitigation and remediation”.[108] According to former US State Department Cyber Coordinator Christopher Painter, the PSI is a useful analogy since “this is a long term process where we’re trying to get countries around the world to adopt norms and every country has [its own] self-interests”. Efforts, he suggested, will need to focus on socializing work underway and building support “with an increasingly big tent of countries over time”.[109]

There are some indications that the Trump administration will continue the previous administration’s policy of normative engagement. It will do so, however, not within the United Nations, which it is placing “on the backburner”, but with “smaller groups of allied countries” and will focus on “call[ing] out bad behaviour and impos[ing] costs on adversaries”.[110] Without significant investment in diplomatic action, however, including via the UN and beyond the “like-minded”, it is unclear how the administration will attain its longer-term, “bigger-tent” objectives.[111] Some have suggested a two-prong approach, leaning on both multilateral engagement and working with like-minded partners.[112]

The **Netherlands** has invested significantly in influencing the normative environment, launching initiatives ranging from the Internet Freedom Coalition to the Global Forum on Cyber Expertise (GFCE) and supporting efforts such as the Tallinn Manual (discussed below), which is aimed at deepening understanding of how international law applies to the use of ICTs in conflict and in times of peace. More recently it launched the Global Commission on the Stability of Cyberspace (GCSC), a body comprised of representatives from governments, the technology sector, civil society, and academia drawn from different geographical regions. Focusing primarily on "developing additional proposals for norms and policies to enhance international security and stability and guide the responsible behaviour of state and non-state actors", the initiative also aims to identify linkages with other ICT-related regimes and promote a greater degree of regime coherence.[113] The composition of the Commission (key to its legitimacy), its work plan (particularly in terms of setting priorities that can help bridge some of the significant gaps between the positions and interests of different groups on norms of State behaviour), and how it channels the outcome of its work back into the multilateral process will likely be the key things to watch out for as the Commission gets underway.

The so-called "London Process" of Global Conferences on Cyberspace has also served as a platform for governments to propose norms, principles, and measures. The **United Kingdom** launched the initiative in 2011 with the aim of bringing a broader group of stakeholders into the policy discussions and debates around cyberspace. For instance, the United Kingdom availed of the opportunity to table a set of Principles for Cyberspace, confirming some of the principles emerging in other forums.[114] Since then, the Conference has been hosted by the governments of Hungary (2012), the Republic of Korea (2013), which presented a "Framework for an Open and Secure Cyberspace", and the Netherlands (2015), which used its conference to launch the GFCE (discussed in more detail below). India is set to host a follow-on conference in 2017. It will be important to determine the real contribution of the Global Conferences to broader stability and security, beyond raising awareness and bringing together different stakeholders.

Bilateral processes

Bilateral processes of engagement have played an important role in shaping or promoting norms of State behaviour as they apply to ICTs, or for building confidence and strengthening cooperation between States, and their number continues to grow.[115]

Russia and the United States have shared a fitful relationship on ICT and cybersecurity-related matters, a first agreement on these matters signed between the two back in 1999 and leading to initial confidence-building work—including the establishment of a crisis communications line—between the two powers.[116] While the current context does not, however, appear to provide a strong basis upon which the two countries can effectively cooperate,[117] these first steps to build trust between them had an important influence on norms and confidence-building processes at the regional and international levels. In addition, more recently Russia has signed cooperative agreements with China, India and countries in Central Asia.

From a normative perspective, likely the most important development to date is the agreement reached between the heads of state of the United States and China in September 2015. Against a background of growing tensions on ICT-enabled intellectual property and trade secret theft, bilateral talks between the two States let to an agreement whereby neither State would knowingly support or conduct such activity, including as it relates to trade secrets or confidential business information. In addition to the intellectual property theft provisions, the two States also committed to furthering the norms of State behaviour and a number of the cooperative measures reflected in the 2015 GGE report relating to a duty to respond to reports of malicious activity in cyberspace and cooperate in responding to cybercrime.[118] Importantly, the two States also agreed to a process of high-level, regular ministerial meetings that have helped to ensure follow-on dialogues that can include discussions of conformance to these measures.

While some remain sceptical, the agreement has been viewed as an important step and a useful example of how norms begin to spread.[119] In this regard, it may be viewed as a limited "cascade" in the sense that while the US–China agreement was immediately followed by similar agreements between the United Kingdom and China, Germany and China, and shortly thereafter by the G20 communiqué discussed above, it has yet to be adopted universally by all States.

The research community

The United Nations Institute for Disarmament Research (UNIDIR) has focused significant energy on broadening access to, and deepening understanding of, ongoing discussions relating to ICTs in the context of international peace and security. To this end, it has conducted several studies on the topic of international cybersecurity, including the *Cyber Index* report. Since 2012 UNIDIR has hosted an annual conference on International Cyber Stability, which carries a strong normative focus and brings together government representatives, academia, and industry actors.[120] In 2016 it launched an "Expert Workshop Series on International Cyber Security Issues" in collaboration with the Center for Strategic and International Studies (CSIS). The initiative includes a series of roundtables aimed at identifying areas of common understanding and divergence on issues relating to cyberspace and international security, notably norm development, legal measures, and possible approaches to the malicious use of cyber tools. The aim of the project, now in its second phase, is to provide Member States with the opportunity to engage with technical, academic, and industry experts from across regions on a range of policy, legal, normative, and technical issues relating to cyberspace and international security and stability.[121]

Beyond the United Nations, several leading academic institutions have invested significant resources in deepening understanding of norms and ICTs. For instance, since 2011, a Harvard–Massachusetts Institute of Technology–University of Toronto consortium has hosted an annual conference on norms, ICTs, and international stability and security covering a broad range of normative issues spanning defence, diplomacy, trade, and human rights, resulting in policy-relevant publications.[122] Other annual events on issues relating to norms and international security and stability include the one organized by the International Information Security Research Consortium (IISRC) in Garmisch-Partenkirchen, Germany.[123]

Organizations such as the East-West Institute have embarked on research initiatives on universalizing the norms recommended by the 2015 GGE,[124] while more recently Leiden University's "Programme on the Development and Implementation of Cyber Norms" together with the ICT4Peace Foundation has put out a call for "an open consultation on how to implement the GGE recommendations on responsible State behaviour in cyberspace".[125]

More targeted initiatives include the *Tallinn Manual on the International Law Applicable to Cyber Warfare*—developed by a group of independent legal scholars and coordinated by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). The first edition of the Manual, published in 2013, explored the applicability of jus ad bellum and jus in bello principles to cyber operations. It also considered the applicability of related bodies of international law, such as the law of State responsibility, and offered a range of definitions, including the definition of the muchdisputed term "cyberattack". The Tallinn Manual was nonetheless dismissed by a number of States and scholars on the basis that it was developed by a group of largely Western legal experts and thus was not considered representative of the views of experts from other regions. To allay some of these concerns, a process leading to the publication of a so-called "Tallinn Manual 2.0" was launched in The Hague in February 2016, with much broader participation of legal experts from across Europe, North and South America, Africa, and Asia and the Pacific, and the technology sector. The process also engaged governments. The focus of this second edition of the Tallinn Manual is "peacetime cyber operations"—those operations that fall below the threshold of armed conflict—which may generate countermeasures or violate the principle of non-intervention.[126] While this version of the Manual also includes some revisions to the original, some non-Western legal experts still view the effort with scepticism.[127]

Beyond the CCDCOE initiative, other norm-related proposals have gained some traction in international circles. One such proposal stems from a report by a Dutch academic entitled "The Public Core of the Internet: An International Agenda for Internet Governance", which argues for committing States to protecting the core infrastructure of the Internet.[128] Such an approach would identify the "the legitimate domain of … states, where they can stake a claim and take up their role without harming the infrastructure of the Internet itself".[129] It would similarly identify which core functions of the Internet—the public core, so to speak—should be protected from State action.[130] To this end, the proposed norm would involve States committing to refraining from interfering with the "public core" of the Internet, declaring it a neutral space.

Other infrastructure-related research efforts include those by the Carnegie Endowment for International Peace (CEIP), within the framework of its broader work on norms. CEIP experts have been working with global financial actors to develop a "Global Norm Against Manipulating the Integrity of Financial Data", which would build on some of the actions taken or recommended by the G20 and the GGE noted above.[131]

Another proposal to gain some traction relates to the thorny question of attribution. In 2013, experts at the Atlantic Council suggested the establishment of a "Multilateral Attribution and Adjudication Council" as an example of an international mechanism that could help to reach consensus on the attribution of illegal cyber campaigns by States and a formal process for adjudicating associated interstate disputes.[132] Since there is growing consensus that attributing an attack will ultimately be a political or sovereign decision based on intelligence and forensics, it is unlikely that States would agree to such a mechanism. Further study on the viability of establishing an attribution body has since been conducted by experts at RAND Corporation, who suggest that to be trusted, any such arrangement would need to focus on establishing standards for reaching an attribution finding, on how to credibly communicate an attribution finding, and on conducting effective attribution investigations. However, they do not believe that States should play a role in such an arrangement. Instead, "to avoid an appearance of bias and to protect transparency", the proposed "Global Cyber Attribution Consortium" should be made up of industry and academic experts.

Undoubtedly, standardization of and transparency in reaching attribution findings would find many supporters, including among States, particularly if the geographical representation of its experts is considered. It is, nonetheless, difficult in the current geo-political context to see how such an arrangement would rally broad endorsement in the short-term. At the same time, making practical progress in testing it would likely be an important contribution, as would using such arrangements to build capacity and confidence so that existing imbalances in technical attribution knowledge and capabilities can be gradually ironed out. In the longer term, some of the tested working modalities might even be considered by States—including how they might be applied to the standing up of a panel of experts—in the event that an ICT incident is ever brought to the attention of the Security Council under chapter VII of the Charter. Either way, the question of attribution will likely figure strongly on the agenda of the UN and other bodies in the years to come.

The private sector

Technology companies are becoming increasingly influential on the international stage and have a vested interest in shaping norms of behaviour relating to the use of their products and services. This interest is partly propelled by revelations of close collaboration by some companies with law enforcement agencies in mass data collection and surveillance and by the growing realization that ICT products and services are being used by States (or their proxies) to conduct or support offensive activity against other States, with significant implications for users.

Efforts by technology companies include a range of voluntary measures. For instance, companies such as Google and Facebook have adopted an approach whereby they notify users if their account has been targeted or compromised by a State or a State-sponsored party in the hope that these efforts will also help shape State behaviour.[133] Approaching vulnerabilities from a prevention perspective, a growing number of (largely US-based) companies are offering so-called "bug-bounties", rewarding friendly hackers who uncover critical security vulnerabilities in some of the most important software supporting the Internet.[134] Managed by a panel of volunteers selected from the security community, the programme is an interesting insight into how "distributed resourcing approaches" may help both small and large companies, while also preventing malicious actors from benefitting from vulnerabilities.[135] Also from a preventive perspective, numerous technology companies are using their terms or conditions of service to establish acceptable user behaviour on their platforms or products. This use of terms of service tends to be aimed at content- or illicit funding-related issues, and underpinned by existing principles and norms. Yet, important lessons can likely be garnered from these efforts for broader international security purposes.

Other companies are linking their own experiences to current State-led norm-shaping processes. For instance, in December 2014 Microsoft launched a report, *International Cybersecurity Norms—Reducing Conflict in an Internet-dependent World*, proposing a set of six norms aimed at limiting malicious activity below the threshold of armed conflict.[136] The suggested norms include i) improving defences and reducing risk by developing national cybersecurity capacity, and domestic, regional, and international organizational structures and approaches that increase understanding among States; and ii) limiting conflict or offensive operations, with the aim of avoiding escalation and limiting the potential for damaging impacts in or through cyberspace. The Microsoft proposal suggests that implementation of these norms should be accompanied by efforts to include cybersecurity issues in the United Nations draft articles on the Responsibility of States for Internationally Wrongful Acts with the expectation that such an approach could eventually help move emerging norms from politically to legally binding.[137]

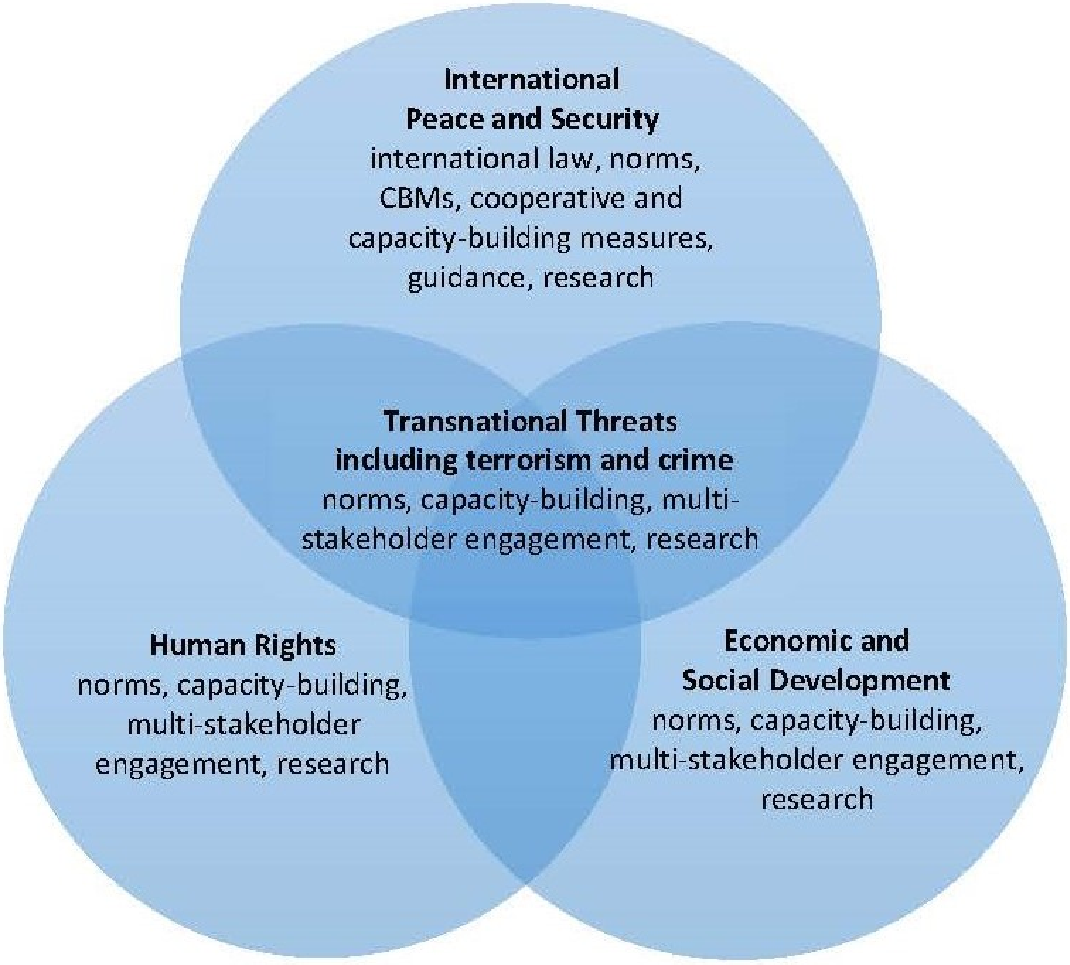
Building on its earlier report, in June 2016 Microsoft launched a new publication recommending additional norms relating to offensive and defensive practices in cyberspace. Importantly it also included norms for global industry actors, notably supporting defence and refraining from offence, with the overall aim of protecting users and enhancing their trust in technology.[138]

The company has since become more ambitious in its normative objectives, even calling for the passing of a "Digital Geneva Convention" to protect civilians on the Internet.[139] The call emphasizes the progress to date within the GGE, the G20, and other international, regional, and bilateral forums on setting the foundations for new and international norms. It suggests that the time is ripe for renewed bilateral action between the Russian Federation and the United States, with the aim of protecting both economic and political institutions from malicious State activity, while also calling for a broader multilateral agreement affirming recent cybersecurity norms as global rules; and for companies themselves—the "first responders" when it comes to cyber incidents—to take responsibility and operate "as a neutral Digital Switzerland". This "neutral digital Switzerland" would "assist and protect customers everywhere; not aid in attacking customers anywhere; and make efforts to retain the world's trust", not least because "every government, regardless of its policies or politics, needs a national and global IT infrastructure that it can trust".[140] Critics have noted that the core principles of the proposed 'Geneva Convention' resemble a mix of existing public and private international law.[141] Hence, it is unclear whether States or companies will openly embrace the idea of the proposed "Convention". Nonetheless, the initiative, which Microsoft continues to adapt to evolving circumstances, remains important in terms of advancing the debate on norms and shaping a role for—and responsibilities of—key industry actors in the debate.

3. Linkages and Lacunae: Other ICT-Related Norm-Shaping Processes within the United Nations

Most of the normative discussions on ICTs and international security have taken place within the General Assembly's First Committee and its GGEs. There are, however, a number of other ICT-related issues on the UN agenda with direct or indirect international security implications. UN human rights bodies are working on the rights implications of the malicious use of ICTs by different actors, while UN development bodies view cybersecurity preparedness at the national level as key to economic growth and poverty alleviation. The Security Council and several other UN entities are engaging on transnational threats such as the use of the Internet and ICTs for terrorist and criminal purposes. The UN also remains involved in the highly charged debates over Internet governance, which increasingly intertwine with those relating to international peace and security (see figure 6). This section highlights progress on some of these inter-related normative discussions, highlighting where progress has been made and where challenges remain.

Figure 6. Linkages between the international peace and security pillar and other pillars of the United Nations' work



International Peace and Security
international law, norms, CBMs, cooperative and capacity-building measures, guidance, research

Transnational Threats including terrorism and crime
norms, capacity-building, multi-stakeholder engagement, research

Human Rights
norms, capacity-building, multi-stakeholder engagement, research

Economic and Social Development
norms, capacity-building, multi-stakeholder engagement, research

3.1 Transnational threats

3.1.1 Terrorism, ICTs, and international peace and security[142]

Several international and regional organizations are focusing attention on the use of the Internet for terrorism and violent extremism, viewing the issue as a threat to international and regional security. These include the normative work of the European Union, the Council of Europe, the OSCE, the SCO, the Global Counterterrorism Forum (GCTF) as well as the more operational focus of the EUROPOL Internet Referral Unit (IRU) and INTERPOL's capacity-building efforts, most of them involving private sector and civil society actors to some extent or other.[143] Non State-led initiatives are also shaping the normative environment on these issues.[144]

Within the UN, terrorism has long featured on the international peace and security agenda. Recent developments, notably involving the Islamic State, have accelerated such attention. The issue is not a traditional cybersecurity problem, since it is not concerned with protecting ICTs from intentional interference, but rather with how ICTs, notably the Internet and social media platforms, are used for propaganda purposes—to groom, radicalize, and recruit supporters, raise funds, obtain embargoed items, and incite hatred and violence. Still, as evidenced in national strategies, many States still view terrorist use of the Internet as a national and international security threat with links—direct or otherwise—to cybersecurity.

As a result, international discussions on terrorist use of the Internet are often mired by tensions on where the relevant policy discussions should take place and where responsibilities should lie. This situation is compounded by problems that continue to hamper UN counter-terrorism efforts, including long-standing disagreements between States on how to define terrorism,[145] on how to safeguard human rights and fundamental freedoms online while also ensuring public safety and national security, and on the most appropriate global mechanism to respond to cybercrime, which itself is key to investigating and prosecuting online terrorist activity.

Nonetheless, the following section highlights that despite this situation, significant work is underway at the UN to respond to the use of the Internet for terrorist purposes, some of it directly or indirectly linked to traditional cyber- or digital security efforts, particularly those related to protecting rights and privacy, ensuring a safe ICT environment, and protecting critical infrastructure. Moreover, it demonstrates that there is a normative framework emerging to respond to such activity, even if the spreading or cascading of such norms at the global level remains a significant challenge.

The Security Council, ICTs, and terrorism

The United Nations has adopted 19 binding instruments on the topic of terrorism. None mention cyberspace, ICTs, or the Internet, even if several are indirectly relevant to ICTs.[146] The growing importance of the issue to international security is nonetheless evident in the extent to which the United Nations counter-terrorism bodies have engaged on the matter. Security Council resolutions 1267 (1999) and 1373 (2001) provide the framework for the Council's wider counter-terrorism regime that has since been refined through a series of follow-up resolutions, some of which explicitly address terrorist use of ICTs.

ICTs and resolution 1267

The Security Council's most active phase on counter-terrorism began in 1998 with a resolution responding to the 1998 bombings of the US embassies in Nairobi and Dar es Salaam, imposing sanctions on the Taliban government of Afghanistan upon their refusal to hand over Osama bin Laden who was held responsible for the attacks.[147] The scope of the resolution was expanded following the September 2001 terrorist attacks on the United States to freeze the assets of, impose a travel ban on, and penalize financial or material support to "Usama bin Laden, members of the Al-Qaida organization and the Taliban and other individuals, groups, undertakings and entities associated with them".[148] After 2001, the "Consolidated List" and the financial sanctions were explicitly broadened to cover the provision of Internet hosting or related services.[149] By the end of 2015, concerns regarding the Islamic State in Iraq and the Levant (ISIL) had grown to the extent that the Security Council expanded its sanctions framework to include it (now called the ISIL and Al-Qaida Sanctions list).[150] More specifically, it re-emphasized concerns relating to the increased use of ICTs and the Internet by terrorists and their supporters, and the need to report on and recommend measures to prevent the criminal use of the Internet by ISIL, Al-Qaida, and associated individuals as it pertains to existing sanctions, issues currently being studied by the 1267 Sanctions Monitoring team.[151]

An inter-governmental High-Level Review of United Nations Sanctions—established in 2013 "to consider ways of updating and strengthening the implementation of sanctions"—captured some of these developments (see Table 1).[152] With regard to ICTs, the group highlighted how the Internet, digital technologies, and mobile communications systems provide platforms for "inciting hatred, raising funds, obtaining embargoed or otherwise restricted items, recruiting supports and combatants into causes that contravene international norms and are targeted by sanctions".[153] Expected to infuse a new dynamic into UN sanctions implementation, the work of the High-Level Review reportedly fell victim to "deteriorating P5 relations in the wake of the 2014 Crimea crisis" and its recommendations did not receive much institutional backing.[154] Nonetheless, the rather ambitious recommendations merit attention in light of the growing interest in applying sanctions to individuals and entities providing material support to terrorists over the Internet or through certain ICT products and services. In short, consideration of the application of such sanctions would require a serious risk assessment to identify and address potential negative impacts on other stakeholder activities and national economic and social prosperity.

ICTs and resolution 1373

Adopted in 2001, Security Council imposed a set of binding obligations on all Member States to criminalize the financing of terrorism, freeze the assets of known terrorists and supporters, refrain from providing "active or passive" support to entities or persons involved in terrorist acts, prevent the movement and travel of known terrorists, and intensify law enforcement cooperation to counter terrorism.[155] A follow-up resolution called upon States "to take measures … to prohibit by law incitement to commit terrorist acts and to prevent such conduct."[156] While neither resolution explicitly refers to the Internet or ICTs, an agenda-setting counter-terrorism report by the Secretary-General published in 2006 suggested they provide a basis for criminalizing incitement through the Internet.[157] A more recent resolution noted the evolving nexus between terrorism and ICTs, in particular the Internet, and the use of such technologies to incite, recruit, fund, or plan terrorist acts[158] and directed the Counter-Terrorism Committee Executive Directorate (CTED) to address the issue in consultation with Member States, international, regional, and subregional organizations; the private sector, and civil society, and to advise the Counter-Terrorism Committee (CTC) on further approaches.[159]

Table 1. ICT-related recommendations of the High-Level Review on UN Sanctions

i.	Member States should address transnational threats and new technologies, including the use of the Internet for illicit activities, within existing frameworks, including under Security Council resolutions 2161 and 2178. Other stakeholders, including Internet users and the IT industry, should be engaged to address such threats in the implementation of sanctions. (rec. 146)
ii.	The Security Council should enhance investigative capacities and strengthen international cooperation to determine which countries and/or individuals or entities are responsible for abuses of cyberspace affecting international peace and security, facilitating the imposition of UN sanctions. (rec. 147)
iii.	The Security Council should encourage adoption of relevant national legislation criminalizing the use of the Internet for terrorist purposes (e.g. for recruitment, fundraising, etc.) and encourage international cooperation between Member States as well as with intergovernmental bodies in this regard. (rec. 148)
iv.	The Security Council should expand and extend to other sanctions regimes the prohibition in the Al-Qaida and Taliban sanctions related to the provision of financial or economic resources for Internet hosting or related services for the purposes of promoting terrorism or other norm-breaking activities, as a violation of the asset freeze. (rec. 149)
v.	The Security Council should ensure the provision of additional resources to meet the technical and substantive skills needed to strengthen the Secretariat's capacity to assist sanctions actors, including expert groups, and for the groups themselves to have the requisite resources and technical expertise to carry out the increasing demands of their mandates. (rec. 150)

As the Council became increasingly sensitive to the challenges posed by ISIL's success in online-based propaganda and recruitment,[160] in 2014 Member States were urged to act cooperatively when taking national measures to prevent terrorists—particularly foreign fighters—from exploiting technology, communications, and resources to incite support for terrorist acts.[161] With respect to groups operating in Libya, resolution 2214 included any support provided to such groups via "information and communications technologies, such as the Internet, social media, or any other means".[162] In 2015, the Security Council adopted another resolution[163] linked not just to existing counter-terrorism resolutions but also to resolutions on Women, Peace and Security and on the Protection of Civilians in Armed Conflict.[164] It focused on the need to protect youth from terrorist groups intent on using the Internet to groom, recruit, and incite young people to violence, including in post-conflict contexts, and called on Member States and United Nations entities such as the Peacebuilding Support Office to pay special attention to the protection of this vulnerable group and the engagement of young people in shaping solutions, including online.

At a more practical level, the Security Council's subsidiary bodies have increased efforts to support implementation of the aforementioned resolutions. For instance, CTED has engaged key technology and social media companies and other stakeholders in the work of the CTC. This has included working with the ICT4Peace Foundation on a project relating to "Private Sector Engagement in Responding to Terrorist Use of ICT", aimed at deepening understanding of the role of technology and social media companies in responding to terrorist and extremist use of their products and services.[165] The results of the initial phase of this project—presented to the CTC in February 2017—shed light on the norms and principles that a growing number of global technology companies are using to frame their activity in this area. This emerging framework recognizes the importance of enhancing public safety with actions that remain anchored in the rule of law, protecting and respecting human rights and fundamental freedoms consistent with international law, including international human rights law, and upholding core principles such as transparency, accountability, predictability, and remedy. It also points to some progress in the area of self-regulation by industry actors, notably with regard to using their terms or conditions of service to shape user behaviour and in protecting privacy and core human rights principles.[166]

At the same time, the project highlighted several normative and technical challenges requiring urgent attention, particularly trends of increasingly restrictive cybersecurity and counter-terrorism legislation across different jurisdictions, suggesting the limited possibility of these norms cascading and being internalized on a global scale, at least in the near future.[167] A second phase of the project, Tech Against Terrorism, focuses on working with technology start-ups and developing an online knowledge-sharing platform through which support and guidance can be sought by those companies struggling to deal with terrorist use of their products and services.[168]

In response to growing pressure from governments across the globe to regulate global companies for failing to block violent extremist activity and propaganda on their platforms, Facebook (including YouTube), Microsoft, and Twitter have created the Global Internet Forum to Counter Terrorism, bringing together under one umbrella a series of initiatives including the EU Internet Forum, the Shared Industry Hash Database, discussions with the United Kingdom, and the conclusions of the recent G7 and European Council meetings.[169] The objective of the Forum is to "formalise and structure existing and future areas of collaboration between our companies and foster cooperation with smaller tech companies, civil society groups and academics, governments and supra-national bodies such as the EU and the [United Nations]".[170] This it intends to do through enhanced work on technological solutions, research, and knowledge-sharing (including through the CTED–Tech Against Terrorism initiative mentioned above). Whether this will stop the calls for government regulation is thus far unclear and it is hard to see how existing ethical concerns will be reconciled.[171] In this regard, perhaps some form of independent oversight mechanism could eventually be put in place to address the concerns of governments and citizens alike.

Regarding other measures taken by the Security Council to counter terrorist use of ICTs, in May 2016 the Security Council held an open debate focused on countering the narratives and ideologies of terrorism. At that meeting, it adopted a presidential statement (S/PRST/2016/6) requesting the CTC to present a proposal to the Council by 30 April 2017 for a "comprehensive international framework" to counter the use of narratives by ISIL, Al-Qaida, and other terrorist groups that encourage, motivate, and recruit members to commit terrorist acts.[172] The proposal will consist of three core elements: legal and law enforcement measures in accordance with obligations under international law, including international human rights law, and relevant Security Council resolutions and in furtherance of General Assembly resolutions; public private partnerships; and the development of counter-narratives.[173]

Needless to say, developing a "comprehensive international framework" for countering terrorist narratives will be no easy task unless current challenges relating to existing counter-narrative efforts are acknowledged and addressed, and the framework is underpinned by existing principles.[174] In this regard, a potential model to follow could be that developed by the United Nations Office on Genocide Prevention and the Responsibility to Protect aimed at preventing incitement of atrocity crimes and the conditions that can lead to violence. Following from a series of expert consultation meetings, it produced a consensus list of some 40 policy options, laying the basis for a comprehensive framework for States, civil society, media producers, and other stakeholders, and placing an awareness of central issues such as identity, division, hate speech, and incitement to violence at its heart. Evidently, such an approach would need to be adapted to additional actors involved in the counter-narrative area, but can serve to underscore some of the core norms and principles that should underpin this work.[175]

The General Assembly, the Internet, and terrorism

Countering terrorism

In 2006, the General Assembly adopted a Global Counter-Terrorism Strategy and accompanying Action Plan. The Strategy addressed countering the use of the Internet for terrorist purposes and using the Internet as a tool to counter the spread of terrorism.[176] The establishment of a dedicated working group on terrorist use of the Internet within the Counter Terrorism Integrated Task Force (CTITF)[177]—a United Nations interagency mechanism created by the Secretary-General to promote the implementation of the Strategy—led to modest steps aimed at deepening understanding of the issues and supporting States in their efforts to respond to terrorist-related threats, including through the use of ICTs.[178] The working group has since developed a "Compendium on Legal and Technical Aspects of Countering the Use of the Internet for Terrorist Purposes",[179] highlighting the instruments (laws and conventions), programmes, resources, and technical means used by States to counter the use of the Internet for terrorist purposes and identifying areas where future engagement may be necessary.

Building on Member State responses to an extensive survey, the Compendium confirmed that States are responding to terrorist uses of the Internet by applying existing cybercrime and counter-terrorism legislation to Internet-related acts or enacting specific legislation on terrorist use of the Internet.[180] States identified challenges related to balancing protection of fundamental rights, such as freedom of expression, opinion, and privacy, with efforts to criminalize certain conduct or improve access to the tools needed to carry out investigations and prevent terrorist activity online.[181] They also highlighted issues stemming from the absence of a global instrument to respond to cybercrime (discussed below) such as exchange of information and cross-border collaboration, as well as sovereignty and jurisdictional conflicts surrounding access to data and digital evidence located in the territory of another State.

Preventing violent extremism online

In response to the growing trend in violent extremism and the minimal focus that was being afforded to preventive efforts in the Counter-Terrorism Strategy, in January 2016 the United Nations Secretary-General presented a Plan of Action to Prevent Violent Extremism to the General Assembly.[182] In the Plan, the Secretary-General calls for a comprehensive approach encompassing not only essential security-based counter-terrorism measures but also systematic preventive steps to address the underlying conditions that drive individuals to radicalize and join violent extremist groups. The Plan is an appeal for concerted action by the international community, providing some 70 recommendations to Member States and the United Nations system to prevent the further spread of violent extremism, and includes an entire section on "Strategic communications, the Internet and social media".[183] A first conference was organized in Geneva in April 2016 for the international community to share experiences and good practices on how to prevent violent extremism. However, while there was certain emphasis on the need to engage with the online dimension of violent extremism and link it to off-line efforts, there was limited participation of relevant technology and social media companies in the conference deliberations.

The newly established United Nations Office of Counter-Terrorism, which brings together the existing CTITF and the United Nations Counter-Terrorism Centre under one Under-Secretary-General, is expected to strengthen on-going work and drive more coherence in this area, including in on-going work relating to preventing violent extremism.[184]

Terrorism and critical infrastructure protection

Scepticism still abounds as to whether terrorist groups will develop the capacity to conduct ICT-enabled attacks against critical infrastructure providing essential services to citizens. Nonetheless, several international and regional organizations have highlighted growing concern that such attacks might eventually take place.[185] While not specifically referenced in the report, some of the proposed norms in the 2015 GGE report have some relevance to State responsibilities in dealing with the issue, since they fall into the general understanding of cybersecurity as the protection of ICTs from unauthorized access or attempted access. These include the norms compelling States not to conduct or knowingly support actions that intentionally damage critical infrastructure (CI), a State's responsibility to secure its own infrastructure, the expectation that States support other States that have fallen victim to attacks on their CI, and the expectation of responsible reporting of vulnerabilities and information sharing that could prevent or mitigate cyber-enabled attacks on CI.[186]

Many of the efforts already being implemented by States to protect critical infrastructure from malicious State activity are equally applicable to attacks perpetrated by terrorist groups. For instance, the EU Network and Information Systems (NIS) Directive adopted in 2016 and discussed above, can serve to bolster the preparedness of States against such threats, as can other cooperative and capacity building measures being promoted by the International Atomic Energy Agency (IAEA) or the Meridian Process within the GFCE. Furthermore, in February 2017, Ukraine—victim of an attack against its electric grids—successfully tabled a resolution at the Security Council on the "Protection of Critical Infrastructure Against Terrorist Attacks". While it does not specifically reference cyber- or ICT-enabled attacks against critical infrastructure or essential services, the resolution does refer to the threats and vulnerabilities posed by growing inter-connectivity and the new security concerns they raise. It also mentions cybersecurity among the range of domestic measures required to protect critical infrastructure.[187] It will be important to monitor implementation of this resolution, notably the inter-linkages with other developments relating to cybersecurity and critical infrastructure protection such as the ones mentioned above, as well as the growing number of capacity-building initiatives aimed at strengthening government preparedness in light of cyber-enabled critical infrastructure threats and vulnerabilities, some of which are being tied to development assistance cooperation. It will be equally important to encourage United Nations legal and counter-terrorism structures and Member States to consider work underway outside the United Nations—for instance, by the International Law Association—to understand how existing international law applies to such terrorist activity, and where potential gaps in existing instruments might lie.[188]

3.1.2 Crime, ICTs, and international peace and security[189]

Ever since the invention of the optical telegraph at the end of the eighteenth century, those with illicit intent have been quick to take advantage of information technology.[190] Over time, and as crime has become more organized, ICTs and cyberspace have provided criminal groups with important advantages, enabling the shift of their operations from the purely local to the national and global. Over the past two decades, cybercrime—which refers to offences against and by means of computer systems—has become an increasing source of concern considering the huge financial costs and social harm associated with activities such as computer-related fraud, forgery, and copyright offences, illegal access to or interference with computer systems or data, sale of illicit goods, online distribution of child pornography, and violations of network security. Today, effectively responding to online criminal activity is a major challenge for States. Yet, shaping or implementing norms to mitigate illicit online behaviour is complicated by attribution challenges and requires significant cross-jurisdictional law enforcement cooperation and collaboration, which is not always forthcoming.

In addition, States are availing of some of these same illicit capabilities, creating important tensions and undermining trust since, in many instances, victims (whether States, private sector actors, civil society, or other) do not know whether they are a victim of crime or a State-sponsored operation. Indeed, concerns have mounted that hackers with sophisticated ICT skills are being used by States to meet broader political and military goals. While State use of proxy actors to carry out covert activity is hardly new, the nature of more recent shifts has sounded alarm bells, largely because the tools and techniques originally the preserve of States "are starting to make their way into the broader communities of criminals" who are shifting from large-scale financial theft to providing services ranging from sabotage and intelligence-gathering to data breaches and data manipulation.[191] Moreover, the use of criminal "cyber proxies" has been identified as an important advantage in armed conflict, not least because of the additional element of plausible deniability that using such criminal actors provides, and in terms of bolstering the capabilities of the State.[192] Outside the realm of conflict, States are increasingly relying on these modern-day "privateers" for a range of objectives such as power balancing and cutting costs, providing them with lists of targets and the resources to carry out their operations.[193] The main concern is that these actions can potentially lead to miscalculations in terms of attribution and scale of response, thereby increasing risk for all States and posing a threat to international peace and security.[194]

The United Nations response to criminal use of cyberspace and ICT

Since the early 2000s, the criminal use of ICTs has been on the agenda of the General Assembly, first within the Second Committee and later the Third Committee, where discussions have focused predominantly on establishing a normative base to respond to computer and cybercrime.[195] The United Nations First Committee GGEs have also stressed the need for enhanced cooperation for exchanging information, mutual assistance, the prosecution of terrorist and criminal use of ICTs, and other cooperative measures to address such threats, and has also made recommendations on the normative basis for responding to State use of proxies to conduct internationally wrongful acts.[196]

Undoubtedly, measures to respond to criminal use of ICTs require significant cross-border cooperation, including exchanges of information and intelligence. The question of a global convention to enable such cooperation and exchanges of information to tackle cybercrime was centrally discussed at the twelfth United Nations Congress of the Commission on Crime Prevention and Criminal Justice (CCPCJ) in 2010.[197] However, the Congress revealed limited consensus among

States regarding the most appropriate way forward. A number of States advocated for "globalizing" the existing Council of Europe Convention on Cyber Crime (also known as the Budapest Convention), which criminalizes (that is, delineates as improper) certain forms of human behaviour for individuals and includes norms for law enforcement cooperation.[198] The Convention is seen as the most comprehensive instrument in place, has the highest number of State Parties (53 to date), and is open for signature to non-members of the Council of Europe. Some analysts have noted the difficulty of scaling up to the global level the procedural and cooperation commitments as well as the comparatively high standards agreed upon in a European context.[199] Moreover, several States and groupings, including the Russian Federation, the BRICS and many developing countries, object to signing a convention in the drafting of which they had not been involved, and to some provisions relating to cross-border access to data to which they object on procedural and substantive grounds. Emerging at the same time as a strong re-emphasis on questions of sovereignty, these States continue to call for the negotiation of a new mechanism under the auspices of the United Nations.[200]

The likelihood of agreement on a new *global* mechanism remains low for the foreseeable future. The 2010 CCPCJ nonetheless resulted in a General Assembly resolution that called for an open-ended intergovernmental expert group to study the problem of cybercrime and international responses to it.[201] Three sessions of the open-ended working group have been held to date—in 2011, 2013 and 2017—the first resulting in a draft "Comprehensive Study on Cybercrime" produced by the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU), which provides an important reference framework for Member States on a number of issues relating to trends, legislation, law enforcement and investigations, electronic evidence and criminal justice, international cooperation, and the role of the private sector.[202] The "Comprehensive Study" has also served as a framework for UNODC's Global Programme on Cybercrime, established in 2013 to support Member States in "prevent[ing] and combat[ting] cybercrime through crime prevention and criminal justice technical support" implemented with key partners, and through the development of a growing Cybercrime Repository which hosts case law, legislation, best practices, and lessons learned from Member States.[203]

Nonetheless, the reports from the second and third sessions of the CCPCJ expert group suggest that persistent disagreements among States on some of the normative issues underpinning the response to cybercrime, including cooperation between States, cross-border access to data, and differing capacities between States, will continue to hamper efforts in the coming period.[204] Moreover, while the number of States that have ratified the Budapest Convention has increased, the deliberations from the latest meeting of the CCPCJ expert group on cybercrime note how some experts continue pushing for "a strengthened international legal framework for combating cybercrime", while others "expressed the view that the Budapest Convention was becoming outdated".[205]

The absence of a global mechanism has not prevented the emergence of regional instruments aimed at tackling cybercrime. For instance, over the past decade and a half, several regional organizations—including the African Union, the Arab League, and the SCO—have adopted legal instruments promoting international cooperation and harmonization of national legislation to combat cybercrime. Yet, these instruments do not always have the backing needed to support implementation at the national level. For instance, the African Union instrument was finally adopted in 2014 after a lengthy drafting process, yet it has only nine signatories and one ratification, potentially "diminish[ing] its prospects for spurring national cyber policy development and the subsequent harmonization of regional policy".[206] This is problematic for a region where

Internet growth is highest and where online criminal activity is increasing, with repercussions for both public and private sectors and, of course, users—not just in Africa but across the globe.

Elsewhere, regional organizations have established practical mechanisms to support member States in their response to cybercrime. For instance, since 1999, member States of the OAS have participated in a dedicated working group on cybercrime, principally focused on strengthening judicial and law enforcement cooperation within the region and with other organizations and mechanisms.[207] Specialized State-led agencies such as EUROPOL and INTERPOL have dedicated significant resources to establishing in-house capacity to support member States' efforts in investigating online criminal activity, while other organizations such as the EU, the Council of Europe, and the OSCE have established normative frameworks or support capacity-building efforts in this area. Recent years have seen an increase in collaborative efforts between law enforcement agencies, leading to a renewed, yet still obstacle-ridden, focus on mutual legal assistance treaties (MLATs).[208]

Important collaborative efforts have also emerged between law enforcement agencies, technology and social media companies, and specialized technical groupings such as computer emergency response teams (CERTs) and cybersecurity incident response team (CSIRTs) in both understanding and responding to existing and emerging methods of online criminal activity.[209] This underlines the importance of continuing engagement of non-State actors—particularly IT product and service providers and public interest groups—in seeking solutions to cybercrime at the normative level, and in supporting efforts aimed at law enforcement cooperation and capacity-building at the operational level.[210]

A highly complex area of online criminal activity is the growing State use of proxies for political and military purposes. The 2015 GGE report called attention to this concern, recommending in its section on how international law applies to State uses of ICTs, that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts".[211] Implementing this recommendation is difficult, not least because of the attribution challenge, i.e. difficulties inherent in determining whether a given individual or entity is working at the behest of a State. While the increasing use of circumstantial evidence in the forensics process may help temper some of these challenges, as discussed earlier, attributing an incident to an individual or entity acting on behalf of State will ultimately be a political decision.[212]

Moving forward, and in the absence of a global cybercrime mechanism, the United Nations Secretary-General could further encourage sustained dialogue on the measures required to enhance law enforcement and prosecutorial cooperation and collaboration on cybercrime. On some of those issues that evidently have clear implications for international security and on-going normative processes, efforts can be made to encourage, at minimum, General Assembly cross-committee engagement and targeted research. At a more practical level, the Secretary-General and the relevant United Nations leadership can encourage Member States to support UNODC's Global Programme on Cybercrime, make more use of its "Comprehensive Study" and its growing cybercrime repository, which includes databases on cybercrime case law, legislation, and practical lessons. These are useful initiatives which are being used to exchange experiences and deepen understanding on how States can overcome some of the legal and technical challenges in responding to online criminal activity.[213] Similarly, lessons from the support of the ITU to governments in harmonizing cybercrime policies and legislation and in the area of capacity-building might be reported on more regularly and disseminated more broadly, as might research by institutes such as the United Nations Interregional Crime and Justice Research Institute (UNICRI).[214]

3.2. Cross-cutting issues

3.2.1 Human rights, ICTs, and international peace and security[215]

Since the end of the Second World War, protecting fundamental rights from State abuses of ICTs has been a priority for many actors, influencing efforts to include basic principles such as freedom of expression and opinion in the core human rights instruments.[216] During the 1970s, the emergence of the first networked computers and unprecedented transnational data transfers, coupled with the commercialization of new capabilities enabling remote processing and storage of citizens' private information, led to fierce debates within the General Assembly on questions of individual privacy and data protection, in turn related to some of the first discussions on data sovereignty.[217]

Today it is impossible to ignore the human rights issues that have developed alongside, or as a result of, the malicious use of ICTs by both State and non-State actors. The misuse of ICTs by terrorists and criminals has served in a number of States—including well-established democracies—as justification for mass surveillance, censorship, curbs to freedom of opinion and expression, even the legitimization of crackdowns on internal opposition, undoing decades of work by rights and pro-democracy groups around the globe. Revelations of US surveillance practices, as well as lingering perceptions of technological and informational/knowledge economy imbalances, have also led to the re-emergence of a data sovereignty debate that first emerged in the 1970s, with a number of States determining how to ensure that the personal data of their citizens can be stored within State borders.[218] The lack of transparency regarding much State action on ICT-related capabilities and their uses has also meant that legitimate tensions between human rights and national security concerns are harder to resolve.

Within the United Nations, principal norm setters on these issues are the Third Committee of the General Assembly, and its subsidiary body, the Human Rights Council and its Special Procedures—specifically, the Special Rapporteurs on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Protection of Privacy. Indeed, these and other bodies have produced a number of important resolutions, declarations, sets of principles, and reports over the past five years.[219] The most recent United Nations resolutions include the Human Rights Council resolution on the Promotion, Protection, and Enjoyment of Human Rights on the Internet,[220] and the General Assembly resolution on the Right to Privacy in the Digital Age,[221] the latter propelled by the reactions of the governments of Brazil and Germany to the Snowden revelations of mass data collection and surveillance practices in the United States.[222] This resolution pitted traditional allies against each other while also reawakening Cold War-era concerns regarding State surveillance practices and over-dependency on US IT products and services, and highlighting important differences in how States approach and interpret questions relating to data protection and privacy.

Beyond the United Nations, regional organizations have taken strong normative stances on the implications of restrictive government techniques applied in response to public safety and national security concerns. For instance, in 2014, the Council of Europe's Commissioner for Human Rights, Nils Muižnieks, released a paper on "The Rule of Law on the Internet and in the Wider Digital World" urging member States to:

> Ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and affording the guarantee of judicial oversight to prevent possible abuses. In addition, domestic courts must examine whether any blocking measure is necessary, effective and proportionate, and, in particular, whether it is

> targeted enough so as to impact only on the specific content that requires blocking. Member states should not rely on or encourage private actors who control the Internet and the wider digital environment to carry out blocking outside a framework meeting the criteria described above.[223]

The report was followed by an in-depth report on the "State of Democracy, Human Rights and the Rule of Law", and a comparative study on "Filtering, Blocking and Take-Down of Illegal Content on the Internet". This latter study compares policy and practice across the organization's 47 member States, describing and assessing both the legal framework and the relevant case law and practice in the field and the impact of those measures on freedom of expression.[224]

Major technology companies have also taken strong normative stances on the question of encryption in communications technology, pushing back against calls by law enforcement agencies for access to encrypted devices and arguing that government efforts to bypass or disallow encryption through legislative means would render communications more vulnerable and place citizens and ICT systems at risk.[225] Furthermore, influential reports, such as that published by leading encryption experts in 2015 criticizing the viability of government efforts to legitimize backdoors to encrypted communication, have helped bolster the case of privacy advocates, notably the assertion that "such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend".[226] Another useful contribution to the debate includes a report by the Berkman Center, which explores the significance of encrypted communications technologies and their impact on legitimate government interests. The report found that it is unlikely that encrypted technologies will become the norm, noting instead that a combination of market forces and commercial interests "will likely limit the circumstances in which companies offer encryption that obscures user data from the companies themselves". It also noted that trends in technological development suggests "a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will 'go dark' and beyond reach".[227] Nonetheless, draft legislation on this issue is currently under consideration in a range of jurisdictions, strongly influenced by the surge in terrorist-related incidents across the globe.[228]

In light of some of the human rights challenges such legislation might pose, the most recent report of the Special Rapporteur on the Freedom of Expression, "The Use of Encryption and Anonymity in Digital Communications", attempts to reconcile tensions between States' obligations to ensure privacy and freedom of expression and opinion on the one hand, and national security and public safety prerogatives on the other.[229] It suggests that restrictions for the purpose of guaranteeing public safety and national security should be guided and limited by existing norms and core principles such as legitimate aim, necessity, and proportionality,[230] as well as principles of State responsibility such as transparency and accountability. The recently launched "13 Principles on the Application of Human Rights to Communication Surveillance"—a civil society initiative—can also be considered as a normative guide for State action.[231]

Private companies themselves have increasingly been called to task by United Nations human rights bodies (as well as non-United Nations groups) for the role they play in exacerbating human rights and privacy concerns, particularly during moments of political instability and crisis. These concerns have multiplied as companies are increasingly compelled to take action, particularly against terrorist use of their online products and services, through proactive content removal policy and practice or by acquiescing to government demands to remove or block certain applications that permit users to circumvent government censorship. Apple's recent decision to remove virtual private network (VPN) software from its App Store in China is a case in point.[232]

Such actions have led to the emergence of a rich debate regarding the roles and responsibilities of the private sector and the emergence of new standards and principles aimed at shaping private sector behaviour in the use of ICTs. In particular, the Guiding Principles on Business and Human Rights endorsed by the Human Rights Council in 2011 provide "a global standard for preventing and addressing adverse effects on human rights linked to business activity".[233] Beyond the United Nations, the European Commission has developed an "ICT Sector Guide on Implementing the UN Business Principles".[234] Other self-regulating efforts or efforts to shape behaviour in this area include the Telecommunications Industry Dialogue's "Guiding Principles on Freedom of Expression and Privacy", also based on the Business and Human Rights Principles.[235] Many of these initiatives are captured by the broader work of the Global Network Initiative, a multi-stakeholder body established to provide informed guidance to ICT companies in view of increasing pressure from governments "to act in ways that may impact the fundamental human rights of privacy and freedom of expression".[236]

Other measures informed by human rights concerns include those introduced by the United Kingdom and France to the Wassenaar Arrangement—the multilateral arms export control regime—aimed at restricting exports of network intrusion and IP surveillance products to authoritarian regimes. Some members of the Arrangement are already implementing the controls. In other States, such as the United States, technology and telecommunications companies, human rights groups, and technology researchers have voiced important concerns relating to the manner in which the controls might be interpreted and implemented and are working to shape a more informed approach to their application.[237] These and other concerns are shared beyond the US. Viewing the Wassenaar Arrangement as an outgrowth of the Cold War expert controls regime, some observers believe that such controls today will further impact the "digital divide" and the much needed transfer of knowledge and technology, and are calling for caution with regard to their implementation.[238]

The emergence of these new norms, principles and standards relating to ICTs and human rights are important in themselves, but equally important for the maintenance of international peace and security and, as discussed in the next section, sustainable development. The United Nations Secretary-General could play an important role in promoting the socialization and implementation of these norms within the UN, by ensuring they are streamlined across the capacity-building and technical assistance work of the Organization, as well as encouraging engagement with other organizations and initiatives. Moreover, the United Nations could also help to ensure that human rights groups are part of the discussions and encourage globally recognized technology companies and ICT service and product providers to lead by example by standing by the principles and standards they publicly claim to defend.

3.2.2 Development, ICTs, and international peace and security

Few States today would dispute the links between development and security. A recent report noted how "economic development is the area where the UN has come the farthest in integrating new technologies into its discussions and work".[239] This work, which commenced with the 2000 Millennium Declaration, now covers a range of policy areas including sustainable development, disaster risk reduction, climate change, financing for development and the work of the World Summit on the Information Society. While most of this work emphasizes the opportunities of ICTs, it just as often signals the risks posed by vulnerable ICT systems to realizing such opportunities.

The last two GGE reports on ICTs in the context of international peace and security emphasized these links, as have efforts by other groups such as the G20 and G7. This emphasis reflects a broad acknowledgement that attaining stability in this area will be difficult if there are notable imbalances in capacity and system security across the globe, and affirms that security and stability remain at risk if vastly different levels of capacity for ICT security among States persist.[240] The OECD has also emphasized the links between ICT security and development, initially in its 2002 Security Guidelines which, following review, have resulted in the 2015 OECD Recommendation on "Digital Security Risk Management for Economic and Social Prosperity".[241] The 2030 Sustainable Development Goals (SDGs) re-emphasize these links. Indeed, Goal 16 of the SDGs, which is centred on peaceful and inclusive societies, clearly articulates that peace, development, and human rights are indivisible and interrelated, a point since picked up by several United Nations development programmes and specialized agencies in efforts to frame ICT-related capacity support and technical assistance to Member States.

Certainly today, cybersecurity capacity-building and technical assistance support is on the agenda of every international ICT security-related regime within and beyond the United Nations and is becoming increasingly difficult to delink from international security and global development debates. Indeed, both emerging and developing economies have long insisted that a persisting "digital divide" prevents major progress in governing cybersecurity risk at the global level.

Within the United Nations' economic and social development pillar, ECOSOC has engaged on ICT-related issues for more than a decade,[242] as have the General Assembly's development-oriented Second and Third Committees. Specific US-backed resolutions were adopted in 2002, 2004, and 2009, each referring to cybersecurity-related resolutions adopted in the First and Third Committees and the links between them. The first of these resolutions was broad in scope and included references to the importance of fostering "a global culture of cyber security in the application and use of information technologies".[243] It emphasized factors such as awareness, responsibility, response, ethics, democracy, risk assessments, security design and implementation, security management, and international cooperation; and called for technology transfers and capacity-building efforts to bridge the emerging digital divide. The second resolution, for which the United States was joined by 69 co-sponsors, including China (but not the Russian Federation), highlighted key elements needed for effective cybersecurity, proposed specific steps to protect critical infrastructures, and emphasized the role of the private sector.[244] The third resolution, adopted in 2009, did not receive the backing of either China or the Russian Federation, but proposed a voluntary and useful self-assessment tool to help States take stock of i) cybersecurity needs and strategies, ii) stakeholder roles and responsibilities, iii) policy processes and participation, iv) public-private cooperation, v) incident management and recovery, vi) legal frameworks, and vii) the means to develop a global culture of cybersecurity.[245] Today, this guidance serves as a basis for States as they move to develop national strategies. Indeed, the 2015 GGE (which included both China and the Russian Federation) recommended that efforts by States to enhance cooperation and build capacity should stem from the provisions of this resolution.[246]

Strategy development and capacity-building

A growing body of different tools and methodologies are being developed to support national cybersecurity policy and strategy formulation and implementation at the national level. Within the United Nations system, UNIDIR has played an important role in building the capacity of States to engage with the high policy and strategic issues under discussion within the First Committee, including its GGEs, on issues relating to international peace and security. On the development side, several United Nations agencies and programmes, including the ITU, have long realized the importance of capacity-building and technical assistance.[247]

Beyond the United Nations, and as policy and practice in this area have matured, a growing number of actors have sought to realign their actions in this area, strengthening the links between security in the ICT environment and social and economic development, and anchoring the response to risk management. For instance, at the inter-governmental level, the OECD Recommendation on Digital Security Risk Management makes an interesting departure from traditional approaches to cybersecurity, placing economic prosperity and not just stability and security as its end goal. This is key as many States are more concerned about the economic and social development challenges posed by ICT threats than the strategic issues on the agenda of some of the major powers.

Building on some three decades of experience in developing policies and instruments for innovation and trust in the digital economy, including the 2002 Council Recommendation "Guidelines on Security of Information Systems and Networks" which influenced the aforementioned United Nations resolutions on a Culture of Cyber Security, the 2015 Recommendation is centred around some eight inter-dependent principles (general, operational, and security specific) that should form the basis of national strategy development for digital risk management.[248] The justification for shifting to a digital security risk management approach are manifold, including the fact that the term "cybersecurity" tends to convey a sense of specificity which is often misleading, and can have important implications for policy and related measures. Furthermore, the OECD argues, the term does not necessarily convey the dynamic nature of digital risk nor the economic and social dimensions of the risk.[249] In contrast, a risk-management approach implies a rational and proportioned analysis of the subject matter, and helps identify the use of the right tools for managing risk, and the incorporation not only of "a preventive notion in relation to … incidents, but also a 'resilience' or recovery capacity in response to them".[250] The guidance provided by the OECD redirects earlier thinking by its member States to a more holistic and cyclical public policy approach to managing digital security risk involving strategic and economic decision-making; this ensures that related "security measures" fully support the economic and social activities at stake and do not undermine them, and that digital risk management is an integral part of the State's overall risk management framework, rather than a separated, isolated silo. A review of the OECD Recommendation will be carried out in 2018 and will likely turn up some interesting lessons and good practices.

Other efforts in this area include those supported by the Oxford Martin School's Global Centre for Cyber Security and the Potomac Institute for Policy Studies. Both have worked in partnership with governments and international or regional bodies, including the ITU, to develop methodologies that assess or support self-assessment of national cybersecurity "maturity" or "readiness". They are developed on the basis of set criteria and also anchored in the concept of risk management. [251]

Developing and implementing national cybersecurity or digital risk management strategies requires significant capacity. To this end, capacity-building efforts have mushroomed over the past five years implemented through a number of international and regional organizations,[252] international financial institutions (e.g. the World Bank), technical bodies,[253] government agencies, universities and research bodies, dedicated institutions (for example, EUROPOL's Cybercrime Centre, INTERPOL's Centre of Excellence in Singapore, NATO's Cooperative Cyber Defence Centre of Excellence, the Marshall Centre's Program on Cyber Security Studies), or via a growing number of dialogue processes, supported intellectually by think tanks and non-governmental organizations, technically by experts in the public and private sectors, and financially by international or regional organizations, governments, industry actors, or a mix of these.[254]

More recently, the Netherlands launched the Global Forum for Cyber Expertise (GFCE), grouping together under one umbrella a number of existing capacity-building initiatives.[255] The general idea behind the initiative is that States with limited capacity (policy or technical) will be able to draw from a pool of expertise (public and private). Its launch was accompanied by a political declaration emphasizing the need for more capacity-building, exchange of good practice, and enhanced international cooperation on cybersecurity matters.[256]

Several of these capacity-building efforts clearly push certain interests and values, but just as many are policy neutral.[257] Over time, capacity-building can contribute to international peace and security while also enabling economic growth. Moving forward, the United Nations can help raise awareness among Member States and within and beyond the United Nations system of the growing need to streamline, structure, and bring coherence to these efforts and encourage effective monitoring and assessment of results.[258]

3.2.3 Internet governance and international peace and security

Questions relating to the Internet and how the functions and resources it is comprised of are governed or managed have become enmeshed with some States' strategic interests and, to some extent, some of the normative discussions relating to cyberspace or ICTs and international peace and security.[259] A number of States, including China, the Russian Federation and many developing countries, openly insist that States should play a key role in governing Internet policy and the Internet's critical resources, i.e. "the globally unique virtual identifiers—including domain names, Internet Protocol (IP) addresses, and autonomous system numbers—necessary for the day-to-day operation of the Internet, as well as the Domain Name System (DNS), a distributed set of servers that translates domain names into associated IP addresses for routing information to its destination".[260]

Other States, including the United States, EU members and others, believe that efforts should be made to maintain what is generally referred to as the "multi-stakeholder model" of Internet governance, defined often as "a form of participatory and diverse form of governance", and try to keep discussions on Internet governance separate from discussions on international peace and security.[261] These very different stances on Internet governance and where it should sit on the international policy agenda reflect important power struggles that followed from the commercialization of the Internet in the late 1990s. They might also be viewed as an extension of age-old tensions that have tended to emerge whenever new information technologies have threatened traditional notions of sovereignty.[262]

States, sovereignty, and Internet governance

Policymakers and scholars have often approached Internet governance as a monolithic system. Yet, the Internet does not represent one single, unitary function or resource meaning, first, that it cannot be easily regulated and, second, that its governance is distributed across actors responsible for certain functional areas and associated tasks. More accurately its management involves a complex matrix, which Raymond and deNardis have very helpfully broken down into six core functional areas:

- control of "critical internet resources";

- setting Internet standards;
- access and interconnection coordination;
- cybersecurity governance;
- information intermediation; and
- architecture-based intellectual property rights enforcement.[263]

In each functional area they have defined administrative tasks and identified the primary institutional actor responsible for each task. While acknowledging that their taxonomy might be incomplete, they demonstrate how the functions are not only performed by different types of actors, but also involve "a variety of distinct governance activities such as contracting, deliberating, legislating, standard setting, regulating, adjudicating and enforcing".[264] The actors involved range from the private sector owners and operators of products, services, platforms, and infrastructure, to voluntary technical and standard-setting bodies, to governments, inter-governmental bodies, and civil society groups. Moreover, not all the arrangements meet the criteria of multi-stakeholder governance, in that many of the specific functions of Internet governance are not (and should likely not be) multi-stakeholder at all in that they "only involve one actor or a single class of actor".[265]

Despite the layered and distributed character of the Internet, over the past decade some States have developed a vested interest in playing a greater role than they already play in Internet governance. The justifications are manifold, although of late they tend to be increasingly linked to geopolitical and economic interests and concerns. They also stem from a perceived imbalance in the control of decision-making and critical Internet resources.

The fact that the office of National Telecommunications and Information Administration in the US Department of Commerce maintained, until recently, an oversight role over a small number of key Internet functions—including the Internet domain name system root zone, which "definitively tracks the list of names and IP addresses of all the authoritative servers for top-level domains (for example, .com, .edu., .uk etc.) and other core Internet infrastructure registries"—gave rise to significant international tension, with many States arguing that the Internet was "controlled" by the United States. Since the Internet Corporation of Assigned Names and Numbers (ICANN) was, again, until recently, contracted by the US government (via the Internet Assigned Numbers Authority—(IANA)) to administer the Internet's root and is also responsible for allocating IP address blocks to the five regional IP address registries and managing the database for Internet protocol numbers for the Internet Engineering Task Force (IETF), it too became the source of tension. So, too, did the domination by US companies of the privately owned digital networks, technology, and social media platforms that underpin the Internet and, by extension, economic, social, and political life across the globe and that are playing a greater role in some of the decisions relating to public safety, and national and international security discussed in previous sections.[266]

In addition, and as discussed earlier in this report, while the low-barrier access to the Internet and the capacity to communicate and transfer information and ideas across borders has brought significant economic benefits, it has also enabled a seemingly unprecedented dispersion of power—much to the alarm of many States. Certainly, this dispersion of power has combined with a range of other non-technological factors to dilute, to some extent, the influence of the State and its role in exercising authority (or in some contexts, control) over social, political, and economic life within its territory.[267] At times it has also hindered the State's capacity to guarantee public safety and national security, particularly with regard to online criminal activity and terrorist use of the Internet and, more recently, State-backed efforts to influence the domestic political process of other States. These and other related issues have propelled several States to reassert sovereignty and control, including by seeking a more prominent or equal role in Internet governance-related policy—particularly with regard to the management of critical Internet resources—using different forums, including within the United Nations, to this end.

The United Nations and Internet governance

Within the United Nations, the initial push for a greater role for States in Internet governance emerged via the ITU at the end of the 1990s.[268] The ITU organized the first World Summit on the Information Society (WSIS) in Geneva in 2003 and a second in Tunis in 2005, attended by thousands of participants and scores of Heads of State.[269] The Geneva and Tunis Summits represented the first steps in what would become years of diplomatic wrangling over the aim of some States to "mak[e] State actors pre-eminent in the formulation of global internet policy", particularly with regard to critical Internet resources.[270] Russian experts, for example, argue that a core objective of the Russian Federation's national information security strategy was achieved with the "adoption of the provision recognizing the lead role of governments in the WSIS process", and "the confirmation of the importance of international law, national legislation and sovereignty in developing the international information society".[271] Notwithstanding, the WSIS process also opened the door for greater participation of non-governmental actors in multilateral policy discussions relating to the "information society". This greater participation included public interest advocacy groups that brought technical and normative concerns to the table for the first time, including the fact that the Internet was being used for malicious purposes by a growing number of actors, including States.[272] In addition, the multi-stakeholder dimension of the WSIS was formalized through the establishment of the Internet Governance Forum (IGF), an annual multi-stakeholder event during which key Internet governance issues are discussed.[273]

Recent WSIS developments reveal continuing tensions. In 2014, the General Assembly requested ECOSOC to conduct a 10-year review of the implementation of WSIS outcomes and report on its findings at its seventieth session.[274] The process was complicated by some States' refusal to include any reference to multi-stakeholder governance that would involve the participation of industry, civil society, or academia. For instance, some countries suggested the report was an "unbalanced view of perspectives on WSIS implementation",[275] and their intransigence on this point (and others) reportedly led to lengthy discussions on both content and process, including tense discussions on the annexed report on enhanced cooperation entitled "Mapping of International Internet Public Policy Issues".[276]

Notwithstanding, a WSIS review Outcome Document was finally approved by the General Assembly in December 2015. While the reference to the multi-stakeholder model was maintained and efforts to include strong references to multilateralism were unsuccessful, the report nonetheless stressed that any future efforts "should continue to follow the provisions set forth in the outcomes of the summits held in Tunis and Geneva" and extended both the WSIS and the IGF for another 10 years.[277] While many welcomed this outcome, others interpreted it as a prominent role for States in Internet governance moving forward, not least because the Tunis agenda, while recognizing a role for non-State actors in Internet governance, had also placed strong emphasis on States and the multilateral process.[278]

Beyond WSIS, the ITU itself has become the focus of some States' interest in playing a greater role in shaping Internet governance policy, leading to suggestions that the United Nations was "taking over the internet".[279] While this claim is largely exaggerated, not least since, as discussed, the Internet is not a monolithic system and the ITU is just one small specialized agency of the United

Nations, the positioning of ITU member States has given rise to concern. Already in 2003, a number of States unsuccessfully called for the Internet—by then described as a public resource—to be governed by States at the national level and the ITU at the international level.[280] The proposal would have restricted the role of the private sector, technical organizations, and civil society to technical and business development of the Internet.[281] While many governments' positions on Internet governance has since shifted significantly, differences between governments on the ITU's role in Internet governance were again pushed to the fore at the ITU World Conference on International Telecommunications (WCIT) in Dubai in December 2012. The aim of the conference was to update existing regulations, yet it was used by a group of States—emerging and developing economies in particular—to push a vote on a role for the ITU in Internet governance.[282] Indeed, while the number of ITU member States that signed the treaty was significant, the refusal by an equally significant group of States led by the United States to sign the new International Telecommunication Regulations agreement rendered the effort moot.[283] Nonetheless, it is obvious that the rift remains and that efforts to shape the future of Internet governance continue. China, for one, has confirmed its position on Internet governance with its insistence on shaping a norm of "Internet sovereignty" during the World Internet Conferences (WIC) it has hosted in Wuzhen and in other forums.[284] This concept maintains that each State should have the right to regulate cyber infrastructure and activities in its territory, interpreted as "including the ability to control the content and flow of information within and across its borders".[285] The increase in recent years in the use of the Internet to promote terrorism or violent extremism and the use of the Internet by States or State proxies to propagate false news and information has only served to bolster such arguments.

Some steps are being taken to build confidence among various actors moving forward and to ensure that any changes to the current modes of Internet governance do not overly affect the overall functionality of the Internet and its associated benefits and freedoms. A first step included the Global Multistakeholder Meeting on the Future of Internet Governance Conference (NETMundial) hosted by Brazil in 2014 at which some 1,500 representatives from civil society, academia, technical communities, governments, and international and regional organizations participated. Its concluding statement contained a shared set of principles and a roadmap to guide the evolution of Internet cooperation and governance.[286] However, while a "NETmundial Initiative" involving several parties was established to carry forward the outcome of the conference, it too has been criticized on several fronts, including for a lack of transparency and accountability, duplicating the work of existing multi-stakeholder forums such as the IGF, and perceived hidden agendas and interests.[287]

Separating the governance of core Internet coordinating functions from a US government oversight role has also been perceived an important step in allaying some of the persisting (and more strategic) concerns voiced by States relating to perceived US control of core Internet functions. Indeed, in March 2014 the US Commerce Department's National Telecommunications and Information Administration announced it would hand over oversight of the Internet domain name system root zone and other core Internet infrastructure registries under IANA to ICANN, whose governance structure includes governments. A broad range of actors from across the Internet's core operational communities worked to develop consensus proposals regarding the nature of the transition, "to ensure that ICANN remains accountable and the internet remains stable, secure, and resilient absent US oversight".[288] Despite much domestic pressure in the United States, the IANA transition was completed on 1 October 2016, its services transferred to Public Technical Identifiers (PTI) "a purpose-built organization affiliated to ICANN, responsible for providing the IANA functions to the community".[289] As a nod to those States pushing for a greater role in Internet governance, under the revised ICANN governance mechanisms the Government

Advisory Committee will have more power, yet it will only able to exercise that power through consensus.

How the IANA transition will influence the positions of those States still calling for a greater role in Internet governance matters remains to be seen. At least for now, it does not seem to have dispelled earlier concerns. Looking forward, it remains unclear whether the debate on Internet governance will be resolved by normative considerations, technological innovation, weighted national interests, the subtleties of international politics, market dynamics, or business concerns. Most likely, it will be a combination these, informed by ongoing and emerging initiatives underway both within and beyond the United Nations aimed at producing legitimate solutions to ongoing Internet governance dilemmas, including, but not limited to, how they relate to international peace and security.[290]

4. Concluding Remarks

State and non-State uses of cyberspace and ICTs for malicious purpose are considered among the top threats facing States in recent years. Failure to respond to these "cyber insecurities" are expected to carry important implications for international peace and security. At the national level, formulating policy and strategy to shape a coherent response is already complex. Scaling this up to regional and international levels is doubly so, not least because of different State positions and interests. Exacerbating this situation is a shifting geopolitical environment, which makes consensus on normative issues difficult, though not impossible, to reach.

As discussed in this report, the current normative framework for dealing with our common "cyber insecurities" is very broad, with responsibilities and interests spanning different policy areas as well as different regimes, many of which fall under the purview of the United Nations and which have direct or indirect implications for international peace and security. These include:

- The discussions on how international law—including the Charter of the United Nations, customary international law, human rights, and international humanitarian law—applies to cyberspace and ICTs;
- The character of voluntary non-binding political norms aimed at shaping State behaviour in the use of ICTs;
- The growing number of initiatives aimed at building confidence and trust among States to reduce the risks of conflict stemming from the use of ICTs;
- The even broader number of capacity-building initiatives on both policy and technical issues pertaining to the security of ICTs and cyberspace at all levels;
- Multilateral and multi-stakeholder efforts to respond to terrorist use of the Internet;
- International discussions regarding the most effective global policy framework for combating cybercrime and measures to provide legislative and capacity-building support to States;
- International efforts implemented via voluntary bodies such as the Wassenaar Arrangement to apply export restrictions to designated dual-use technologies and software; and
- International efforts to protect user privacy and human rights, including the protection of basic rights such as freedom of opinion and expression, when responding to threats to public safety and national security.

Combined, these different processes, measures, and initiatives are helping advance the discussion on norms of responsible behaviour. As discussed, a key question moving forward is how to best leverage the progress already achieved and ensure a shift from the mere articulation of norms to their implementation, while also keeping existing channels open for dialogue on those normative issues giving rise to tensions and where there continues to be limited consent. An equally important challenge is ensuring the coherence and legitimacy of follow-on normative work within and beyond the United Nations. This in turn, requires significant levels of collaboration, cooperation, and trust-building within and among States and, importantly, the engagement of a broad range of actors.

What role for the United Nations?

The United Nations can play a significant role in supporting many of the on-going normative, confidence-building, and capacity-building processes—however, in order to do so, the United Nations' leadership will need to scale up the attention required to drive the different processes forward. The following recommendations identify several areas on which that attention can be focused.

- **Internal arrangements:** Within the United Nations, the Secretary-General can play an important role preparing the Organization for the likelihood that matters relating to cyberspace and ICTs will increasingly figure on the United Nations peace and security agenda, with important overlaps with human rights and development issues. Shaping coherent responses will require an important degree of awareness-raising and capacity-building within the Organization. It will also require mechanisms to determine the United Nations' comparative advantages, as well as the roles and responsibilities of United Nations departments, programmes, funds, and agencies on cybersecurity matters. The establishment of an internal arrangement within the Office of the Secretary-General tasked with advising the Secretary-General on these issues would be a useful first step in this regard, as would strengthening on-going work of the CEB.

- **International peace and security:** As noted in the 2015 GGE report, and bearing in mind efforts underway in other international and regional organizations and forums, the United Nations should play a leading role "promoting dialogue on the security of ICT in their use by States and developing common understandings on the application of norms, rules and principles for responsible state behaviour".[291]

  The organization can use existing forums to support continued dialogue, coordination, and cooperation at the high policy level and serve as a platform for exchanges of information and experience involving the work of the GGE and related processes.

  Since norms themselves do not create a stable and secure environment, significant effort will be required to foster a conducive environment for their acceptance and implementation. The United Nations can leverage existing mechanisms to help resolve tensions and conflict provoked or exacerbated by State use of ICTs. Given current geopolitical tensions, this will likely be the most challenging aspect of the United Nations' work in contributing to international peace, stability, and security in the coming years. Hence, promoting confidence, trust-building efforts, and enhancing political and technical cooperation among States and between States and other actors will remain crucial moving forward.

  Efforts can also be made to determine how to better integrate ICTs into its broader conflict management toolbox.

- **Human rights and development:** The emergence of new norms and principles, and debates and proposals relating to the use of information technologies by States and non-State actors, and the human rights implications are important. The United Nations can play a crucial role in ensuring the dissemination and socialization of these norms and principles by working with other organizations and initiatives to ensure they are streamlined across their capacity-building and technical assistance work. Moreover, it can strengthen efforts to ensure that core human rights groups are actively engaged in on-going normative discussions, while also encouraging globally recognized technology companies and ICT service and product providers to lead by example and adopt and implement the principles and standards that can best protect user rights.

  Efforts can also be made to strengthen on-going initiatives to integrate ICTs and emerging technologies into the UN's work on economic and social development, while also highlighting the benefits of these efforts for broader peace and security and the protection of human rights. In this regard, encouraging the effectiveness and coherence of UN capacity-building efforts, while also identifying complementarity between UN efforts and those of non-UN entities, will be key moving forward.

Similarly, the Secretary-General might also consider how to best diffuse tensions on Internet governance related issues, notably by supporting efforts aimed at ensuring the engagement of all relevant actors in UN-centred Internet governance-related discussions.

Finally, achieving an “open, secure, stable, accessible and peaceful ICT environment” requires the engagement of actors with different capacities and capabilities from across different sectors at all levels of the global ICT chain. This is a highly complex endeavour, often exacerbated by different levels of economic development across the globe and requiring a significant injection of capacity building and technical assistance resources. The United Nations (and its Member States) can do much more to help ensure coherence of efforts among the range of United Nations entities engaging in cyber/ICT security or digital risk management capacity-building, while also tying these efforts to the Organization’s broader goals.

Notes

[1] See, for example, http://www.unidir.org/programmes/emerging-security-issues/annual-cyber-stability-conference and http://www.unidir.org/programmes/emerging-security-issues/international-security-cyber-issues-workshop-series; see also UNIDIR and CSIS (2016), “Report of the International Security Cyber Issues Workshop Series”, p. 9, http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

[2] For example, ICTs provide important possibilities for data collection for situation analysis, early warning and response, crisis mapping and management, in support of peacekeeping operations and peacebuilding. See Expert Panel on Technology and Innovation in UN Peacekeeping, “Performance Peacekeeping,” 22 December 2014; UN Secretary-General, “Report of the High-Level Independent Panel on Peace Operations”, UN document A/70/95 - S/2015/446, 17 June 2015. See also Einseidel, S. et al. (2017), “Civil War Trends and the Changing Nature of Armed Conflict”, United Nations University Centre for Policy Research, Occasional Paper No. 10, http://www.ditchley.co.uk/assets/media/OC_10%20CivilWarTrendsandChangingNatureofArmedConflict%20-%2003-2017_FINAL2.pdf; see also the conference background note: “Non-state actors and the changing nature of conflict”, http://www.ditchley.co.uk/assets/media/Conference%20description%20Non-state%20actors.pdf.

[3] Gleick, J. (2012), *The Information: A History, A Theory, A Flood*, Vintage; Chandler, D. and Munday, R. (2011), *A Dictionary of Media and Communication*, Oxford University Press.

[4] Gray, C.S. (1996), “The Continued Primacy of Geography”, *Orbis*, 40(2), pp. 247–259; Libicki, M.C. (2007), *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press; Dombrowski, P. and Demchak, C.C. (2014), “Cyber War, Cybered Conflict, and the Maritime Domain”, *Naval War College Review*, 67(2).

[5] Nye, J.S. (2014), “The Regime Complex for Managing Global Cyber Activities”, Global Commission on Internet Governance.

[6] Kuehl, D. cited in Kramer, F.D. et al. (2009), *Cyberpower and National Security*. National Defense University Press.

[7] Raymond, M. and DeNardis, L, “Multistakeholderism: Anatomy of an Inchoate Global Institution”, *International Theory*, 7(3), pp. 572–616; see the “Disaggregated Internet governance taxonomy” table on pp. 590–592 which very usefully disaggregates Internet governance into six functional areas and then further into 43 specific tasks of administrative responsibility and the corresponding primary institutional actor. See also ‘Internet Live Stats’, http://www.internetlivestats.com/. According to the website, around 40 per cent of the world population has an internet connection today. In 1995, it was less than one per cent.

[8] Definition drawn from Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), pp. 425–447.

[9] See New America, *Global Cyber Definitions Database*, http://cyberdefinitions.newamerica.org/.

[10] On “cyber insecurities” see Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), pp. 425–447; on “cyber uncertainties” see OECD (2015), “Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document”.

[11] The five different forms of vulnerability access exploitation discussed by Finnemore and Hollis include remote access (or hacking), supply chain access (via back doors or hidden functions), denial of access (such as distributed denial of service attacks), proximity access (e.g. whereby physical proximity to machinery or wireless signals allow adversaries to connect to the same network); and insider access (provided willingly à la Snowden, or through spear phishing); Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), pp. 432–433; see also OECD (2015), “Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document”, p. 32.

[12] Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), p. 433; see also Carr, M. (2015), “Power Plays in Internet Governance”, *Millennium Journal of International Studies*, 43(2), pp. 640–659.

[13] Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), p. 433.

[14] Maurer, T., and Morgus, R. (2014), ‘Compilation of Existing Cybersecurity and Information Security Related Definitions’. New America Foundation, p. 32.

[15] Kavanagh, C. (forthcoming 2018), “IT and Cyber Capabilities as a Force Multiplier for Transnational Crime’ in Comolli, V. (ed.), *Organized Crime and Illicit Trade. How to Respond to This Strategic Challenge in Old and New Domains*, Palgrave Macmillan.; see also Warner, M. (2012), “Cybersecurity: a Pre-History”, Intelligence and National Security, 27(5).

[16] CSIS list of Significant Cyber Incidents, https://www.csis.org/programs/technology-policy-program/cybersecurity/significant-cyber-incidents.

[17] Ibid. More recent reports of politically motivated incidents, including the Office of Personnel Management (OPM) breach which involved big data theft and aggregation, compromising the personnel records and security clearance files of the entire US federal bureaucracy, will likely have important ramifications. For a discussion on the OPM breach, see Figueroa, Z. (2016), "Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure", *Catholic University Journal of Law and Technology*, 24(2).

[18] Other States have been implicated in some of these political espionage practices, cooperating and reportedly facilitating spying on their own populations and on private companies. And while many may argue that political espionage is a traditional state practice tacitly accepted by all, the sheer scope and lack of transparency and oversight is unprecedented.

[19] Dyn, "Dyn Analysis Summary of Friday October 21 Attack", http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/; see also *Security Intelligence*, "Lessons from the Dyn DDoS attack", 1 November 2016, https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/; and *Welivesecurity*, "10 things to know about the October 21 IoT DDoS attacks", 24 October 2016, https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks.

[20] For example, the hacking of three power distribution centres in Western Ukraine's Ivano-Frankivsk region in December 2015 took nearly 60 substations offline while also disabling backup power supplies, leaving more than 230,000 residents without electricity. See US ICS-CERT, Alert -H-16-056-01, "Cyber-Attack Against Ukrainian Critical Infrastructure", 16 February 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01; see also *Wired*, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", 3 March 2016, http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[21] This has reportedly been the case in recent elections in a number of countries, for example, in the United States, France and Russia. A number of tactics are used to influence electoral outcomes or undermine the opposition, including propaganda campaigns, DDOS attacks, spoofing results, targeted leaks and infrastructure hacking.

[22] According to a joint UNIDIR–CSIS report, only three or four such incidents to date would qualify as a use of force or armed attack, in that they involved physical destruction. In this regard, the report notes that "there is an implicit threshold generally held among states that a cyber incident that produces physical destruction, casualties or death, would qualify as the use of force." UNIDIR and CSIS (2016), *Report of the International Security Cyber Issues Workshop Series*, p. 7, http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf. At the same time, numerous governments and non-governmental organizations are developing means to classify ICT-related incidents in terms of their severity and the nature of the response required, the details of which are being shared between States as part of confidence-building and transparency exercises, or shared publicly (see, for example, CSIS' list of "Significant Cyber Events", https://www.csis.org/programs/technology-policy-program/cybersecurity/significant-cyber-incidents.

[23] UNIDIR and CSIS (2016), *Report of the International Security Cyber Issues Workshop Series*, p. 9, http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

[24] OECD (2015), *Companion Document to the OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, p. 19, http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[25] See Hathaway, M. et al. (2015), "Cyber Readiness Index 2.0: A Plan for Cyber Readiness—A Baseline and Index", Potomac Institute for Policy Studies, http://www.belfercenter.org/publication/cyber-readiness-index-20; or the UNIDIR "Cyber Index" developed in conjunction with CSIS, available at http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

[26] World Economic Forum, "The Global Risks Report 2017", 12th ed., http://www3.weforum.org/docs/GRR17_Report_web.pdf.

[27] Finnemore, M. and Hollis, D. (2016), "Constructing Cyber Norms for Global Cyber Security", *The American Journal of International Law*, 110(3), p. 426.

[28] See ibid., pp. 438–445 for a discussion on the four attributes of a norm. See also Finnemore, M. and Sikkink, K. (1998), "International Norm Dynamics and Political Change", *International Organization*, 52(4), pp. 887–917; and Erskine, T. and Carr, M. (2016), "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace", in Osula, A.M and Rõigas, H. (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, 2016.

[29] Ibid.

[30] General Assembly, “Report of the 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, para. 10.
[31] Finnemore, M. and Hollis, D. (2016), “Constructing Cyber Norms for Global Cyber Security”, *The American Journal of International Law*, 110(3), p. 445.
[32] “The ‘Arria-formula meeting’ are very informal, confidential gatherings which enable Security Council members to have a frank and private exchange of views, within a flexible procedural framework, with persons whom the inviting member or members of the Council (who also act as the facilitators or conveners) believe it would be beneficial to hear and/or to whom they may wish to convey a message.” See http://www.un.org/en/sc/about/methods/bgarriaformula.shtml.
[33] As discussed by Nye, there is no single regime for the governance of cyberspace. Rather, there is “a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages”; see Nye, J.S. (2014) “The Regime Complex for Managing Global Cyber Activities”, Global Commission on Internet Governance, p. 7.
[34] Hollis, D. (2014), “Cacophony or Concert? Minor Notes on Metanorms for Cyberspace”, https://prezi.com/l2rzahogaatm/neither-cacophony-nor-concert-minor-notes-on-metanorms-for-cyberspace/?utm_source=prezi-view&utm_medium=ending-bar&utm_content=Title-link&utm_campaign=ending-bar-tryout.
[35] Kavanagh, C. and Stauffacher, D. (2014), “A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security”, ICT4Peace Foundation; see also Hurwitz, R. (2015), “A Call to Cyber Norms: Discussions at the Harvard–MIT–University of Toronto Cyber Norms Workshops, 2011 and 2012”, American Bar Association.
[36] Kavanagh, C. (forthcoming 2018), “IT and Cyber Capabilities as a Force Multiplier for Transnational Crime’ in Comolli, V. (ed.), *Organized Crime and Illicit Trade. How to Respond to This Strategic Challenge in Old and New Domains*, Palgrave Macmillan.
[37] General Assembly, “Developments in the Field of Information and Telecommunications in the Context of International Security”, UN document A/54/213, 10 August 1999.
[38] Franda, M. (2001), *Launching into Cyberspace: Internet Development and Politics in Five World Regions*, Lynne Reider; Komov, S.A., Korotov, S.V. and Dylevsky, I.N. (2009), “About the Evolution of the Modern American ‘Information Operations Doctrine’”, in Komov, S.A., *International Information Security: The Diplomacy of Peace*, Moscow.
[39] Ibid.
[40] Prof. A. Krutskikh (2003), *International Information Security and Negotiations*, as described in sub-chapter 8.
[41] Tikk-Ringas, E (2012), *Policy Brief: Developments in the Field of Information Communications Technology in the Context of International Security—Work of the First Committee 1998–2012*, ICT4Peace Foundation.
[42] Maurer, T. (2011), “Norm Emergence at the UN: An Analysis of the Activities at the UN Regarding Cyber-Security”, Harvard Kenney School/Belfer Center for Science and Technology; Tikk-Ringas, E. (2012), “Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the First Committee 1998–2012”, ICT4Peace Foundation. This push-back against the merging of different ICT-related policy challenges with the GGE mandate has remained steadfast.
[43] Ibid.
[44] Many of these discussions were taking place in tandem with developments surrounding the so-called “Revolution in Military Affairs” (RMA). Centred on information dominance, information weapons, and information warfare, the RMA provoked a reaction in less technologically sophisticated States not dissimilar to that provoked by the advent of atomic and nuclear weapons.
[45] Tsagourias, N. and Buchan, R. (2015) *Research Handbook on International Law and Cyberspace*, Edward Elgar.
[46] Since 1960, more than 70 Groups of Governmental Experts comprising between 10 and 30 individuals have been established by First Committee to generate advice for the Secretary-General. Recent examples include confidence-building measures in outer space activities, steps to enhance cooperation with regard to the issue of conventional ammunition stockpiles in surplus, and verification in all its aspects, including the role of the United Nations in this field. The objective of this specific GGE was to consider existing and potential threats in the sphere of information security, potential cooperative measures, and the conduct of a study on international information security issues.
[47] For an overview of the establishment and functioning of GGEs, see UNIDIR and CSIS (2016), “Report of the International Security Cyber Issues Workshop Series”, pp. 4–7, http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

[48] Kavanagh, C, Maurer, T., and Tikk-Ringas E. (2013), "Baseline Review of International ICT-Related Processes & Events: Implications for International and Regional Security (2011–2013)", ICT4Peace Foundation.

[49] Tsagourias, N. and Buchan, R. (2015) *Research Handbook on International Law and Cyberspace*, Edward Elgar; see also Boyok, S. (2016), "UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Looking from the Past into the Future", *International Affairs, A Russian Journal of World Politics, Diplomacy and International Relations*, 62(5), p. 244.

[50] See, for example, Tsagourias, N. and Buchan, R. (2015) *Research Handbook on International Law and Cyberspace*, Edward Elgar.

[51] General Assembly, "Report on Developments in the Field of Information and Telecommunications in the Context of International Security", UN document A/65/201, 30 July 2010.

[52] The cooperative measures included enhanced dialogue on norms relating to state uses of ICT, particularly with the aim of protecting critical infrastructure; confidence, stability, and risk-reduction measures to address the implications of state use of ICT; information exchanges on national ICT security strategies and technologies, policies and practices; identification of measures to support capacity-building in less-developed countries; and efforts to develop common terms and definitions; see ibid., para. 18.

[53] General Assembly, "Report of the 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.

[54] Ibid.; see in particular para. 19.

[55] Ibid., paras. 20 and 23.

[56] This would include "improv[ing] the security of critical ICT infrastructure; develop[ing] technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridg[ing] the divide in the security of ICTs and their use"; ibid.

[57] Kavanagh, C., and Stauffacher, D. (2014), "A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security", ICT4Peace Foundation. A number of official documents, including the resolution for cybersecurity (A/RES/58/199), the Russian Federation's Draft Convention on International Information Security, and a growing number of national security strategies expect the private sector to play a significant role in protecting cyberspace.

[58] This point refers to complex issues such as what would constitute an armed attack in cyberspace as well as issues pertaining to neutrality, perfidy, and attribution.

[59] General Assembly, "Report of the 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.

[60] General Assembly, "Report of the 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, para. 26.

[61] General Assembly, "Report of the 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.

[62] Ibid., Section VI.

[63] Ibid., Section III, para. 13.

[64] For formal statements or interviews with experts on the 2016–2017 GGE see, in particular, US Department of State, "Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security", 23 June 2017; Russian Federation Ministry of Foreign Affairs, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere", 29 June 2017. For expert or observer analysis, see Geneva Digital Watch newsletter, "UN GGE: Quo Vadis?", no. 22, 30 June 2017, which includes an interview with the GGE Chair Karsten Geier of Germany; and Schmitt, M. "International Cyber Law Politicized: The GGE's Failure to Advance Cyber Norms", 30 June 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/, which provides a legal assessment of the points of disagreement on international law.

[65] See Lewis. J.A. (2017), "The Devil was in the Details: The Failure of UN Efforts in Cyberspace", https://www.thecipherbrief.com/article/tech/devil-was-details-failure-un-efforts-cyberspace-1092; and Lotrionte, C. (2017), "Geopolitics Eclipses International Law at UN", https://www.thecipherbrief.com/geopolitics-eclipses-international-law-un-1092.

[66] Ibid.; see also Finnemore, M. and Hollis, D. (2016), "Constructing Cyber Norms for Global Cyber Security", *The American Journal of International Law*, 110(3), pp. 425–447.

[67] For more details on these processes see Kavanagh, C. and Stauffacher, D. (2013), "Confidence Building Measures and International Security", ICT4Peace Foundation.

[68] Korzak, E. (2015), "The 2015 GGE Report: What Next for Norms in Cyberspace?", https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

[69] Per its mandate, the Conference on Disarmament is "the single multilateral disarmament negotiating forum of the international community", resulting from the first Special Session on disarmament of the United Nations General Assembly held in 1978. It is the successor to other Geneva-based negotiating forums, which include the Ten-Nation Committee on Disarmament (1960), the Eighteen-Nation Committee on Disarmament (1962–1968), and the Conference of the Committee on Disarmament (1969–1978).

[70] See Lotrionte, C. (2017), "Geopolitics Eclipses International Law at UN", https://www.thecipherbrief.com/geopolitics-eclipses-international-law-un-1092; and Korzak, E. (2015), "The 2015 GGE Report: What Next for Norms in Cyberspace?", https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

[71] See General Assembly, "Report of the 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, para. 35.

[72] A recent example of a hybrid model includes that provided by the Fissile Material Cut-off Treaty (FMCT) Preparatory Group mandate (A/RES/71/259). The mandate provides for the establishment of a 25-member high-level expert group, but also includes a provision whereby the Chair of the preparatory group must organize open-ended consultative meetings so that "all Member States can engage in interactive discussions and share their views", and then convey these back to the preparatory group for consideration. Although the GGE on ICTs is not working explicitly towards a treaty arrangement as is the case here, the principles of transparency and openness in this model might be useful to consider; see General Assembly, "Treaty Banning the Production of Fissile Material for Nuclear Weapons or Other Nuclear Explosive Devices", UN document A/RES/71/259, 27 December 2016.

[73] *What's in Blue*, "Open Arria-Formula Meeting on Cyber Security", 28 November 2016, http://www.whatsinblue.org/2016/11/open-arria-formula-meeting-on-cybersecurity.php.

[74] What's in Blue, "Arria-formula Meeting on Hybrid Wars", 30 March 2017, http://www.whatsinblue.org/2017/03/arria-formula-meeting-on-hybrid-wars.php.

[75] General Assembly, "International Code of Conduct for Information Security", UN document A/66/359, 14 September 2011. Also in 2011, the Russian Federation tabled a "Concept for a Convention on International Information Security" at the second International Meeting of High-Ranking Officials Responsible for Security Matters in Yekaterinburg, engaging in high-level meetings with a range of States on the merits of the proposal.

[76] Ibid.

[77] The SCO's earlier 2009 Agreement on Information Security features similar provisions, as do several of the agreements shaping high-level ICT strategy and policy in the States of the Commonwealth of Independent States. McKune, S. (2015), "An Analysis of the International Code of Conduct for Information Security", CitizenLab; Meyer, P (2015), "Seizing the Diplomatic Initiative", *The Washington Quarterly,* 38(2), pp. 47–61, p. 51; Grigsby, A. (2015), "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?", Council on Foreign Relations.

[78] See the letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan addressed to the Secretary-General, "International Code of Conduct for Information Security", A/69/723, 22 January 2015.

[79] See, for example, McKune, S. (2015), "An Analysis of the International Code of Conduct for Information Security", CitizenLab; Meyer, P (2015), "Seizing the Diplomatic Initiative", *The Washington Quarterly,* 38(2), pp. 47–61, p. 51; Grigsby, A. (2015), "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?", Council on Foreign Relations.

[80] Russian Federation Ministry of Foreign Affairs, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere", 29 June 2017.

[81] OSCE Permanent Council, "Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1039, 26 April 2012.

[82] OSCE Permanent Council, "Initial set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1106, 3 December 2013; and OSCE Permanent Council, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No. 1202, 10 March 2016.

[83] OSCE Permanent Council Decision No. 1039 of 26 April 2012 established the OSCE framework for the development of CBMs, which were designed to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that might stem from the use of information and communication technologies.

[84] See OSCE Permanent Council, "OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies", Decision No.5/16, 9 December 2016.

[85] The initiative stems from the recommendations of the ARF Foreign Ministers' Statement on Cooperation in Ensuring Cybersecurity resulting from the 2012 ARF ministerial meeting in Cambodia.

[86] ARF (2015), *ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies,* 7 May, p. 1, http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf.

[87] CICTE Resolution to Establish a Working Group on Cooperation and Confidence-Building Measures in Cyberspace, document OEA/Ser.L/X.2.17/ CICTE/RES. 1/17, 7 April, 2017.

[88] NATO CCDCOE, Cyber Defense Library, https://ccdcoe.org/publication-library.html.

[89] The former noted the regional body's determination to "keep cyberspace open, free, stable and secure", recognizing that "fundamental rights and the rule of law fully apply", the latter how "a common and comprehensive EU approach for cyber diplomacy could contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations".

[90] Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), document 9916/17, 7 June 2017. On how and when the EU adopts restrictive measures, see http://www.consilium.europa.eu/en/policies/sanctions/.

[91] Draft Council Conclusions, para. 5, p. 7.

[92] Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity, Brussels, 2016, http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm.

[93] 5th BRICS Summit, eThekwini Statement and Action Plan, March 27 2013, para. 34, http://www.brics.utoronto.ca/docs/130327-statement.html.

[94] 7th BRICS Summit, Ufa Declaration, September 2015, para. 34, http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html.

[95] 9th BRICS Summit, Xiamen Declaration, September 2017, para. 56, http://www.brics.utoronto.ca/docs/170904-xiamen.html.

[96] G20 Leaders' Communiqué, Antalya Summit, 15–16 November 2015, http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

[97] G20 Communiqué, Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17–18 March 2017, http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/G20-2016/g20-communique.pdf?__blob=publicationFile&v=7.

[98] Maurer, T., Levite, A., and Perkovich, G. (2017), "Toward a Global Norm Against Manipulating the Integrity of Financial Data", CEIP, http://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403; see also IOSCO, "CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures", 29 June 2016, https://www.iosco.org/news/pdf/IOSCONEWS433.pdf.

[99] "G7 Principles and Actions on Cyber", http://www.mofa.go.jp/files/000160279.pdf.

[100] For recent news on the BRIC grouping and cybersecurity, see *Xinhua,* "China, India vow to advance cooperation among BRICS nations", 15 September 2016, http://news.xinhuanet.com/english/2016-09/15/c_135689868.htm. For AALCO discussions on cybersecurity and international peace and security, including China's hardening stance on questions relating to international law, specifically jus in bello and jus ad bello, see http://www.aalco.int/Verbatim%20Record%20of%2054th%20Annual%20Session%202015.pdf; and Asian-African Legal Consultative Organization, http://www.aalco.int/Final%20Verbatim%20Record%202016.pdf. Recent conferences where China has made evident the centrality of sovereignty to the Internet and cyberspace include the annual Internet conference it organizes in Wuzhen. See for example *Xinhua*, "Chinese President underscores cyber sovereignty, rejects Internet hegemony", 16 December 2015, http://news.xinhuanet.com/english/2015-12/16/c_134922689.htm; and repeated at the third Wuzhen conference in 2016: *Xinhua*, "WIC in Wuzhen: Cyber Security is the Challenge", 16 November 2016, http://www.china.org.cn/opinion/2016-11/16/content_39717496.htm.

[101] This is interpreted as "including the ability to control the content and flow of information within and across its borders"; *New York Times*, "At U.N., China Tries to Influence Fight Over Internet Control", 16 December 2016, http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html.

[102] *Xinhua*, "International Strategy of Cooperation on Cyberspace", 1 March 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_3.htm.

[103] On the occasion of the United Nations' seventieth anniversary summit, President Xi Jinping announced that China will establish a $1 billion China–UN peace and development fund to support the United Nations' work, advance multilateral cooperation, and contribute more to world peace and development. China and the United Nations agreed that $200 million of the total amount would be hosted by the United Nations and would finance relative activities in the form of the United Nations Peace and Development Trust Fund, according to China's permanent mission to the United Nations. See *Xinhua*, "China signs agreement with UN to finance peace, security activities", 7 May 2016, http://english.gov.cn/news/top_news/2016/05/07/content_281475343697664.htm; see also *The Financial Times*, "China Expands UN Peacekeeping Role as US influence Wanes", 23 November 2016, https://www.ft.com/content/e8091efa-ad5f-11e6-9cb3-bb8207902122.

[104] Meyer, P (2015), 'Seizing the Diplomatic Initiative", *The Washington Quarterly,* 38(2), pp. 47-61, p. 51.

[105] US International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[106] For information on the PSI, see https://www.state.gov/t/isn/c10390.htm.

[107] See Belcher, E. (2011), "The Proliferation Security Initiative: Lessons for Using Non-Binding Agreements", Council on Foreign Relations*,* p. 1.

[108] See *Politico* (2015), "Officials Promote a Proliferation Security Initiative for Cyber", https://www.politicopro.com/cybersecurity/story/2015/01/us-wants-global-cyber-standards-042922; see also Kavanagh, C. (2015), "Cyber Security, Sovereignty, and U.S. Foreign Policy: Summary of a Roundtable", *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, 37(2).

[109] *Politico* (2015), 'Officials Promote a Proliferation Security Initiative for Cyber', https://www.politicopro.com/cybersecurity/story/2015/01/us-wants-global-cyber-standards-042922.

[110] See Waterman, S., "White House cyber czar says push for norms will move to small group of allies", 11 July 2017, https://www.cyberscoop.com/rob-joyce-white-house-cyber-norms/; see also a 24 March 2017 *Politico* report citing White House Homeland Security Advisor, Tom Bossert. Speaking at a security conference at the University of Texas at Austin on 23 March 2017, Bossert stressed that "The Trump administration does not plan to abandon former President Barack Obama's focus on developing international cyber rules", and that "norms [are] an important component of cyber deterrence, along with offensive capabilities … establishing norms is a two-way street, … if we establish those norms and hold our enemies to account, we have to also be prepared to live by those rules." He also added that "Senior Trump officials were committed to doing that" and that he had "not yet met somebody on this president's Cabinet that's not prepared to put their money where their mouth is and behave within the norms that we're expecting our enemies and our allies to behave and live by."*,* http://www.politico.com/tipsheets/morning-cybersecurity/2017/03/nunes-apologizes-but-calls-mount-for-independent-probe-219406.

[111] *Foreign Policy,* "Trump Administration Eyes $1 Billion in Cuts to U.N. Peacekeeping (and other programs)", 23 March 2017, http://foreignpolicy.com/2017/03/23/trump-administration-eyes-1-billion-in-cuts-to-u-n-peacekeeping/.

[112] See for example Lewis. J.A. (2017), "The Devil was in the Details: The Failure of UN Efforts in Cyberspace", https://www.thecipherbrief.com/article/tech/devil-was-details-failure-un-efforts-cyberspace-1092.

[113] See Global Commission on the Stability of Cyberspace, http://cyberstability.org.

[114] For the seven principles tabled by the UK government, see https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace. A broader list of principles is available in the annex of Kavanagh, C, Maurer, T., and Tikk-Ringas E. (2013), "Baseline Review of International ICT-Related Processes & Events: Implications for International and Regional Security (2011–2013)", ICT4Peace Foundation.

[115] Ibid.

[116] Krukskikh, A.V. (2009), "Advancement of Russian Initiative to Ensure International Information Security: Chronicles of the Decade", in Komov, S.A. (ed.), *International Information Security: The Diplomacy of Peace*, Moscow State University.

[117] *PRI,* "Senate Approves New Sanctions Over Russia's Meddling in US Elections", June 14 2017, https://www.pri.org/stories/2017-06-14/senate-approves-new-sanctions-over-russias-meddling-us-election; *RT,* "Sanctions retaliation: Russia Tells US to cut Embassy Staff; Stop Using Storage Facilities". 28 July 2017, https://www.rt.com/news/397809-russia-us-diplomats-sanctions/.

[118] Ibid.

[119] See White House, "President Xi Jinping's State Visit to the United States", September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[120] For access to the reports of UNIDIR's Cyber Stability Conference Series, see: http://www.unidir.org/programmes/emerging-security-threats/cyber-stability-conference-series.

[121] For details on the first conference in this series, see "International Security Cyber Issues Workshop Series: The Future of Norms to Preserve and Enhance International Cyber Stability",

http://www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series/international-security-cyber-issues-workshop-series-the-future-of-norms-to-preserve-and-enhance-international-cyber-stability.

[122] H Hurwitz, R. (2015), "A Call to Cyber Norms: Discussions at the Harvard–MIT–University of Toronto Cyber Norms Workshops, 2011 and 2012", American Bar Association; see also Finnemore, M. and Hollis, D. (2016), "Constructing Cyber Norms for Global Cyber Security", *The American Journal of International Law*, 110(3), pp. 425–447.

[123] See http://iisrc.net/about_eng.php.

[124] See https://www.eastwest.ngo/info/about.

[125] See https://www.universiteitleiden.nl/en/research/research-projects/campus-the-hague/public-consultation-on-un-gge-2015-norm-proposals#tab-1.

[126] Schmitt, M. (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

[127] For example, see Ku, J.G. (2017), "How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare", *Aegis Series Paper no. 1707*, Hoover Institution.

[128] Broeders, D. (2016), *The Public Core of the Internet: An International Agenda for Internet Governance*, Amsterdam University Press.

[129] Broeders, D. (2016), *The Public Core of the Internet: An International Agenda for Internet Governance*, Amsterdam University Press, p. 90.

[130] Broeders presents the "public core" as being made up of the TCP/IP Protocol Suite, numerous standards, the Domain Name Suite (DNS), and Routing Protocols. A recent meeting hosted by UNIDIR as part of its 2016 cyber experts workshop series in Geneva, however, laid bare that there is no common agreement among the technical community on what actually constitutes the public core, but that consensus could be reached with further discussion and dialogue.

[131] See CEIP, "Cyber Norms Index", http://carnegieendowment.org/publications/interactive/cybernorms. On the proposal for a global norm against manipulating the integrity of financial data, see http://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

[132] "Confidence Building Measures in Cyberspace: A Multi-Stakeholder Approach for Stability and Security", http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

[133] Charney, S., "Additional steps to help keep your personal information secure", Microsoft, 30 December 2015, http://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure/#sm.001tkwkfh13oze2atww13frnoul3b; see also Nichols, P., "Cybersecurity norms: From concept to implementation", Microsoft Secure Blog, 8 February 2016, https://blogs.microsoft.com/microsoftsecure/2016/02/08/cybersecurity-norms-from-concept-to-implementation/.

[134] Internet Bug Bounty, https://internetbugbounty.org/.

[135] See Bugcrowd's 2016 annual "State of Bug Bounty report", https://pages.bugcrowd.com/2016-state-of-bug-bounty-report?hsCtaTracking=5a517262-0946-41e5-bc39-92e570fbded8%7Cf8e0ea11-7a6d-49d5-91a1-bbe06c138919.

[136] Charney, S. et al. (2014), "International Security Norms: Reducing Conflict in an Inter-Dependent World", Microsoft.

[137] International Law Commission (2008). The draft articles seek to formulate, by way of codification and progressive development, the basic rules of international law concerning the responsibility of States for their internationally wrongful acts. The emphasis is on the secondary rules of state responsibility: that is to say, the general conditions under international law for the State to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom. See http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

[138] Charney, S. et al. (2016), "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms", Microsoft, https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf.

[139] Smith, B. (2017), "The Need for A Digital Geneva Convention", Microsoft, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0003jytv01cj9en7zwk2r5q96kwix.

[140] Smith, B. (2017), "The Need for A Digital Geneva Convention", Microsoft, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0003jytv01cj9en7zwk2r5q96kwix.

[141] For an analysis of the initiative, see Gurova, M. (2017), "The Proposed 'Digital Geneva' Convention: Towards an Inclusive Public-Private Agreement on Cyberspace?", GCSP, Strategic Security Analysis, no. 4, http://www.gcsp.ch/News-Knowledge/Publications/The-Proposed-Digital-Geneva-Convention-Towards-an-Inclusive-Public-Private-Agreement-on-Cyberspace.

[142] The 2015 UNGGE report references terrorism in paragraphs 6, 7, 13(d), 16(c), 17(e), 21(h), and 33.

[143] See Kavanagh et al. (2017), "Terrorist Use of the Internet and Cyberspace: Issues and Response", in Conway, M., Jarvis, L., Lehane, O., Macdonald, S. and Nouri, L. (eds) (2017) *Terrorists' Use of the Internet: Assessment and Response*, NATO Science for Peace and Security Series, vol. 136, Amsterdam: IOS Press.

[144] See, for example. The Global Network Initiative (2016), "Extremist Content and the ICT Sector: A GNI Policy Brief", https://www.globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf.

[145] For a discussion on the issues blocking consensus on a global counter-terrorism treaty, see Chowdury Fink, N. (2012), "Meeting the Challenge: A Guide to United Nations Counterterrorism Activities", International Peace Institute, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf. Regarding freedom of expression and opinion and privacy concerns, the issues are manifold ranging from different legal traditions regarding freedom of speech, to challenges posed by the unbounded surveillance practices of some States in response to the terrorist threat, or the risk that some responses will pose restrictions on all forms of content, and not just that relating to incitement to violence and other terrorist uses.

[146] Centre of Excellence Defence Against Terrorism (2008), *Legal Aspects of Combating Terrorism*, IOS Press.

[147] See lists created pursuant to Security Council resolutions 1267 (1999) and 1333 (2000).

[148] Security Council resolution 1390 (2002).

[149] Security Council resolution 1735 (2006). Specifically, the resolution notes in para. 20 that "the measures imposed by paragraph 1(a) of this resolution apply to all forms of financial resources, including but not limited to those used for the provision of Internet hosting or related services".

[150] Security Council resolution 2253 (2015).

[151] Specifically, the resolution noted the "Al-Qaida Sanctions Committee shall henceforth be known as the '1267/1989/2253 ISIL (Da'esh) and Al-Qaida Sanctions Committee' and the Al-Qaida Sanctions List shall henceforth be known as the 'ISIL (Da'esh) and Al-Qaida Sanctions List"; ibid., para. 1.

[152] Compendium of the High-Level Review of United Nations Sanctions, June 2015.

[153] Compendium of the High-Level Review of United Nations Sanctions, June 2015.

[154] Einsiedel, S., Malone, D. and Stagno Ugarte, B. (2015), "The UN Security Council in an Age of Great Power Rivalry", United Nations University, working paper, series 4. p.16.

[155] As discussed by Chowdury Fink, Security Council resolution 1373 might be considered "the keystone of the UN's response to global terrorism. It was passed soon after Resolution 1368, condemning the terrorist attacks which took place on 11 September 2001 in New York, Washington, DC, and Pennsylvania", and defined them as a threat to international peace and security; see Chowdury Fink, N. (2012), "Meeting the Challenge: A Guide to United Nations Counterterrorism Activities", International Peace Institute, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf.

[156] Security Council resolution 1624 (2005).

[157] General Assembly, "Uniting Against Terrorism: Recommendations for a Global Counter-Terrorism Strategy", UN document A/60/825, 27 April 2006.

[158] Security Council resolution 2129 (2013).

[159] CTED was established via Security Council resolution 1525 to support the Counter Terrorism Committee in implementing its mandated tasks of monitoring and facilitating the implementation of resolution 1373.

[160] Security Council resolution 2133 (2014).

[161] Security Council resolution 2178 (2014).

[162] Security Council resolution 2214 (2015), para. 5.

[163] Security Council resolution 2250 (2015).

[164] Security Council resolutions 1325 (2000), 1265 (1999), 1894 (2009).

[165] See Kavanagh, C. (2016), "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust", ICT4Peace Foundation, http://ict4peace.org/?p=4382.

[166] Ibid.

[167] See Kavanagh et al. (2017), "Terrorist Use of the Internet and Cyberspace: Issues and Response", in Conway, M., Jarvis, L., Lehane, O., Macdonald, S. and Nouri, L. (eds) (2017) *Terrorists' Use of the Internet: Assessment and Response*, NATO Science for Peace and Security Series, vol. 136, Amsterdam: IOS Press.

[168] See http://www.techagainstterrorism.org/.

[169] See "Global Internet Forum to Counter Terrorism", https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html.

[170] See "Global Internet Forum to Counter Terrorism", https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html.

[171] On the ethical concerns relating to corporate action in this area, see https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism.

[172] See “Security Council requests UN panel to propose global framework on countering terrorist propaganda”, http://www.un.org/apps/news/story.asp?NewsID=53909#.V-q7zjKPDdQ.

[173] For details see Security Council, UN document S/2017/375, 28 April 2017.

[174] See, in particular, Ferguson, K. (2016), “Countering Violent Extremism Through Media and Communication Strategies: A Review of the Evidence”, Cambridge: Partnership for Conflict, Crime and Security Research.

[175] Ibid., p. 23.

[176] See General Assembly, “The United Nations Global Counter-Terrorism Strategy”, UN document A/RES/60/288, 20 September 2006, Section II, para. 12(a), (b).

[177] The CTITF Office was established within the Department of Political Affairs (DPA), following the second review of the Global Strategy in 2008. It was tasked with coordinating the activities of its member entities’ six observers and facilitating greater cooperation and information-sharing among them regarding their counterterrorism-related activities. Moreover, the CTITF Office also became a focal point for States requesting assistance for strategy implementation. See Chowdury Fink, N. (2012), “Meeting the Challenge: A Guide to United Nations Counterterrorism Activities”, International Peace Institute, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf.

[178] Members of the working group include a range of entities, including the 1267 Monitoring Team, CTED, INTERPOL, and UNODC.

[179] CTITF (2009), “Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects”.

[180] These approaches focused predominantly on responding to internet-related attacks, illegal content, communication, and terrorist financing.

[181] See explanatory report of the Council of Europe protocol to the cybercrime convention for an insight into the tensions between core freedoms such as freedom of speech, and efforts to criminalize acts of a racist and xenophobic nature committed through computer systems; see Council of Europe, “Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”, document ETS no. 189, http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm.

[182] General Assembly, “Plan of Action to Prevent Violent Extremism”, UN document A/70/674, 24 December 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674.

[183] General Assembly, “Plan of Action to Prevent Violent Extremism”, UN document A/70/674, 24 December 2015, Section B., para. 55, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674.

[184] The new Office of Counter Terrorism was established through General Assembly resolution 71/291 on 15 June 2017. Mr. Vladimir Ivanovich Voronkov of the Russian Federation was appointed as Under-Secretary-General of the Office on 21 June 2017; see http://www.un.org/en/counterterrorism/. For an assessment of the United Nations system capabilities in this area, see General Assembly, “Capability of the United Nations System to Assist Member States in Implementing the United Nations Global Counter-Terrorism Strategy”, UN document A/71/858, 3 April 2017.

[185] See Kavanagh, C. et al. (2017), “Terrorist Use of the Internet and Cyberspace: Issues and Response”, in Conway, M., Jarvis, L., Lehane, O., Macdonald, S. and Nouri, L. (eds), *Terrorists’ Use of the Internet: Assessment and Response*, NATO Science for Peace and Security Series, vol. 136, Amsterdam, IOS Press.

[186] See Kavanagh, C. et al. (2017), “Terrorist Use of the Internet and Cyberspace: Issues and Response”, in Conway, M., Jarvis, L., Lehane, O., Macdonald, S. and Nouri, L. (eds), *Terrorists’ Use of the Internet: Assessment and Response*, NATO Science for Peace and Security Series, vol. 136, Amsterdam, IOS Press. See also General Assembly, “Report of the 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, Sections III, IV and VI.

[187] See Security Council resolution 2341 (2017).

[188] See Fidler, D. (2015), “Overview of International Legal Issues and Cyber Terrorism”, International Law Association, Study Group on Cybersecurity, Terrorism and international Law.

[189] The 2015 UNGGE report references crime in paragraphs 7, 13d, 16c, 17a and e; 21h, and 28e.

[190] Kavanagh, C. (forthcoming 2018), “IT and Cyber Capabilities as a Force Multiplier for Transnational Crime’ in Comolli, V. (ed.), *Organized Crime and Illicit Trade. How to Respond to This Strategic Challenge in Old and New Domains*, Palgrave Macmillan.

[191] *Financial Times*, “Cyber Crime: States Use Hackers to Do Digital Dirty Work”, 4 September 2015, https://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14. Cases alleged to have involved proxy actors include the Sony Pictures attack and the attacks against JP Morgan and other large banks in the United States committed in 2014.

[192] Maurer, T. (2015), “Cyber Proxies and the Crisis in Ukraine”, in Geers, K. (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf.

[193] Ibid.

[194] General Assembly, "Report of the 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, Section III.

[195] The first of these resolutions was introduced in 2000 in draft form by the United States on behalf of 38 other States and co-sponsored by the Russian Federation entitled Combating the Criminal Misuse of Information Technologies. Coinciding with the adoption of the Budapest Convention, the resolution was adopted without a vote in January 2001 (A/RES/55/63 and A/C.3/56/L.15/Rev.1). Earlier that year, Member States issued the Vienna Declaration on Crime and Justice (A/CONF.187/4/Rev.3) and an accompanying Plan of Action (A/RES/56/261) highlighting the challenges posed by criminal use of information technologies. A second draft resolution was adopted without a vote in January 2002 (A/RES/56/121) yet deferred for further consideration pending work by the Commission on Crime Prevention and Criminal Justice within the scope of its "plan of action against high-technology and computer-related crime". Cybercrime has also figured on the agenda of the UN Economic and Social Council.

[196] General Assembly, "Report of the 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, para. 28(e).

[197] The United Nations Congress on Crime Prevention and Criminal Justice (CCPCJ) takes place every five years and plays a major role in international standard-setting and policy-making in crime prevention and criminal justice.

[198] Finnemore, M. and Hollis, D. (2016), "Constructing Cyber Norms for Global Cyber Security", *The American Journal of International Law*, 110(3), p. 439.

[199] See Harley, B. (2010), "A Global Convention on Cybercrime?", http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.

[200] For example, Brazil voiced reservations about provisions relating to the criminalization of intellectual property infringements and the Russian Federation rejected a portion of the Convention on the grounds that it "violates [its] Constitution by permitting foreign law enforcement agencies to conduct internet searches inside Russian borders." See Gorman (2010) cited in Maurer, T., "Norm Emergence at the UN: An Analysis of the Activities at the UN Regarding Cyber-Security", Harvard Kenney School/Belfer Center for Science and Technology, p. 17.

[201] General Assembly, "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in Particular its Technical Cooperation Capacity", UN document A/RES/65/232, 23 March 2011.

[202] See UNODC (2013), *Comprehensive Study on Cybercrime*, draft, https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[203] Information on the Implementation of Crime Commission resolution 22/8, document UNODC/CCPCJ/EG.4/2017/CRP.1, 3 April 2017, https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/UNODC_CCPCJ_EG_4_2017_CRP_1_E.pdf.

[204] Deliberations at the second meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 25 to 28 February 2013, document UNODC/CCPJ/EG.4/2017/3.

[205] Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017, document UNODC/CCPCJ/EG.4/2017/4.

[206] Terebey, S. (2016), "African Union Cybersecurity Profile: Seeking a Common Continental Policy", The Henry M. Jackson School of International Studies, https://jsis.washington.edu/news/african-union-cybersecurity-profile-seeking-common-continental-policy/. Only Mauritius and Senegal have signed and ratified the Budapest Convention.

[207] See Inter-American Portal on Cyber Crime, http://www.oas.org/juridico/english/cyber.htm.

[208] See for example Chertoff, M. and Rozenweig, P. (2015), "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations", Global Commission on Internet Governance, paper series, no. 10.

[209] See for example the collaboration that has emerged between EUROPOL's cybercrime centre (EC3) and technology companies, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3; see also the Microsoft Digital Crimes Unit, https://news.microsoft.com/stories/cybercrime/.

[210] For instance, in 2013 Microsoft established a Cybercrime Centre in Redmond, Virginia. Since then, it has established five cybercrime satellite centers in Singapore, Beijing, Berlin, Tokyo, and Washington. The work of these centres involves tight collaboration with law enforcement agencies across the globe.

[211] General Assembly, "Report of the 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, Section VI. How international law applies to the use of ICTs, para. 28(e).

[212] Collier, J. (2015), "State Proxies & Plausible Deniability: Challenging Conventional Wisdom", https://www.cybersecurityintelligence.com/blog/state-proxies-and-plausible-deniability-challenging-conventional-wisdom-644.html.

[213] See UNODC Cybercrime Repository at https://www.unodc.org/cld/index-cybrepo.jspx.

[214] See for instance http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx.

[215] The 2015 UNGGE report references human rights in paragraphs 5, 13e, 26, and 28b.

[216] Penney, J. W. (2011), "Internet Access Rights: A Brief History and Intellectual Origins", *William Mitchell Law Review*, 38(1).

[217] Kavanagh, C. (forthcoming 2018), "IT and Cyber Capabilities as a Force Multiplier for Transnational Crime' in Comolli, V. (ed.), *Organized Crime and Illicit Trade. How to Respond to This Strategic Challenge in Old and New Domains*, Palgrave Macmillan.

[218] Maurer T., Morgus R. et al. (2014), "Technological Sovereignty: Missing the Point. An Analysis of European Proposals after June 5, 2013", Transatlantic Dialogues on Security and Freedom in the Digital Age, https://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf.

[219] For an insight to the wide array of resolutions, declarations, principles, standards, and reports adopted by numerous international and regional organizations, see Kavanagh, C, Maurer, T., and Tikk-Ringas E. (2013), "Baseline Review of International ICT-Related Processes & Events: Implications for International and Regional Security (2011–2013)", ICT4Peace Foundation; table 3 in Annex: Internet Governance, Human Rights and Development: Relevant Resolutions, Declarations, Agreements, Decisions and Reports.

[220] General Assembly, "The Promotion, Protection and Enjoyment of Human Rights on the Internet", UN document A/HRC/RES/20/8, 16 July 2012.

[221] General Assembly, "The Right to Privacy in the Digital Age", UN document A/RES/68/167, 25 August 2013.

[222] The report built on the report of the United Nations High Commissioner for Human Rights on "The Protection and Promotion of the Right to Privacy in the Context of Domestic and Extraterritorial Surveillance and/or the Interception of Digital Communications and the Collection of Personal Data, including on a Mass Scale".

[223] Council of Europe (2014), "The Rule of Law on the Internet and the Digital World", Issue paper published by the Council of Europe Commissioner for Human Rights, https://rm.coe.int/16806da51c.

[224] Council of Europe (2016), "State of democracy, human rights and the rule of law in Europe: Report by the Secretary-General of the Council of Europe", https://rm.coe.int/1680646af8 and Swiss Institute of Comparative Law (2015), "Comparative Study on Filtering, Blocking and Take-Down of Illegal Content on the Internet", https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806575b5.

[225] See *Wired*, "Tech Giants Agree: The FBI's Case Against Apple is a Joke", 3 March 2016, http://www.wired.com/2016/03/apple-fbi-tech-industry-support-amicus-brief/?mbid=nl_3316; or *The New York Times*, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone", 17 February 2016.

[226] See Perlroth, N., "Security Experts Oppose Government Access to Encrypted Communication", *The New York Times,* 7 July 2015; see also Abelson, H. et al. (2015)," Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", MIT-CSAIL, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

[227] Berkman Center (2016), "Don't Panic: Making Progress on the 'Going Dark' debate", p. 2 https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[228] See Perlroth, N. 'Security Experts Oppose Government Access to Encrypted Communication', *The New York Times,* 7 July 2015. The report: Abelson, Harold et al (2015), Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, MIT-CSAIL, 6 July 2015. Available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8; see also Berkman Center's 2016 Report "Don't Panic: Making Progress on the 'Going Dark' debate", which attempts to provide a more balanced discussion. Available at https://cyber.harvard.edu/pubrelease/dontpanic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[229] General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye", UN document A/HRC/29/32, 22 May 2015.

[230] See https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance.

[231] The 13 Principles include legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, and safeguards against illegitimate access; see https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance.

[232] *TechCrunch*, "Apple Removes VPN Apps from the App Store in China". 29 July 2017, https://techcrunch.com/2017/07/29/apple-removes-vpn-apps-from-the-app-store-in-china/.

[233] "UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy Framework'", http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[234] European Commission ICT Sector Guide on Implementing the UN Business Principles (no date), https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf.

[235] Telecommunications Industry Dialogue's "Guiding Principles on Freedom of Expression and Privacy", http://www.telecomindustrydialogue.org/about/guiding-principles/.

[236] See https://www.globalnetworkinitiative.org.

[237] See *Politico*, "Wassenaar Comments Pile on Before the Deadline", July 2015, http://www.politico.com/tipsheets/morning-cybersecurity/2015/07/wassenaar-comments-pile-on-before-deadline-dhs-officials-accessed-personal-email-from-work-computers-212543.

[238] *The Hindu Times, "*Wassenaar's Web: A Threat to Technology Transfer", August 2015, updated March 2016, http://www.thehindu.com/opinion/columns/wassenaars-web-a-threat-to-technology-transfer/article7499748.ece; Pyetranker, I. (2015), "An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement, *Northwestern Journal of Technology and Intellectual Property,* 13(2).

[239] The Independent Commission on Multilateralism and the International Peace Institute (2016), "The Impact of New Technologies on Peace, Security and Development", p. 4, https://www.icm2016.org/IMG/pdf/new_tech_paper.pdf.

[240] See General Assembly, "Report of the 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, paras. 30-33; and General Assembly, "Report of the 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, paras. 19-23.

[241] OECD (2015), "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document".

[242] For example, cybersecurity and its implications for development were central focuses of High-Level Segments of annual ECOSOC meetings in 2000 and 2010 respectively; ECOSOC (2011), "Cybersecurity: A Global Issue Demanding a Global Approach", http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

[243] General Assembly, "Creation of a Global Culture of Cyber Security", UN document A/RES/57/239, 31 January 2003.

[244] General Assembly, "Creation of a Global Culture of Cyber Security", UN document A/RES/58/199, 30 January 2004.

[245] General Assembly, "Creation of a Global Culture of Cyber Security", UN document A/RES/64/211, 30 June 2011.

[246] General Assembly, "Report of the 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; see in particular para. 21.

[247] See "UN-wide strategy on cyber security, cybercrime and policies on information" adopted in November 2014; and "UN Draft Compendium on UN Mandates on Cyber Security and Cyber Crime", http://www.unsystem.org/content/action-cybersecuritycybercrime-and-policies-information. These initiatives, however, only appear to cover work underway by those programmes, agencies and funds that fall under the UNs' economic and social development pillar. More specifically see the ITU and the Global Cybersecurity Index, a multi-stakeholder initiative to measure the commitment of States to cybersecurity whereby each country's level of development is analysed according to five categories: legal measures, technical measures, organizational measures, capacity-building, and cooperation. See http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[248] OECD (2015), "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document", pp. 9–12, 20.

[249] Ibid.

[250] Alvarez Valenzuela, D. and Vera Hott, F. (n.d.), "Cybersecurity and Human rights in Latin America', in del Campo, A. (ed.), *Towards an Internet Free of Censorship II: Perspectives in Latin America*, Universidad de Palermo and CELE, http://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf.

[251] The Oxford Centre has developed a comprehensive cybersecurity capacity-building programme which is currently being implemented in a number of countries. See: http://www.oxfordmartin.ox.ac.uk/cybersecurity. The Potomac Institute has developed a "Cyber Readiness Index", which examines 125 countries that have embraced, or are starting to embrace, ICT and the Internet and evaluates each country's maturity and commitment to cybersecurity across seven essential elements; http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

[252] For example, the European Commission, OSCE, ASEAN Regional Forum, OAS, African Union, and the Economic Community of West African States.

[253] For example, Computer Emergency Responses Teams (CERTs) and Computer Security Incident Responses Teams (CSIRTs) and FIRST, the leading organization in incident response, with more than 300 members.

[254] For example, the ICT4Peace Foundation implemented a capacity-building programme for diplomats on international cybersecurity negotiations in Latin America in conjunction with the OAS, as well as in Africa and in Asia.

[255] The initiative was launched as a core outcome of the 2015 Global Conference on Cyberspace.

[256] See https://www.thegfce.com/about/contents/gccs.

[257] Kavanagh, C. (2015), "The UN GGE on Cybersecurity: The Important Drudgery of Capacity Building", Council on Foreign Relations.

[258] Ibid.

[259] Carr, M. (2015), "Power Plays in Internet Governance", *Millennium Journal of International Studies*, 43(2), pp. 640–659.

[260] Raymond, M. and DeNardis, L. (2013), "Thinking Clearly about Multistakeholder Internet Governance", Paper presented at the 8th Annual GigaNet Symposium, Bali, Indonesia, p. 4.

[261] Ibid.; see also Raymond, M. and DeNardis, L. (2015), "Multistakeholderism: Anatomy of an Inchoate Global Institution", *International Theory*, 7(3), pp. 586–588.

[262] Kavanagh, C. (forthcoming 2018), "IT and Cyber Capabilities as a Force Multiplier for Transnational Crime' in Comolli, V. (ed.), *Organized Crime and Illicit Trade. How to Respond to This Strategic Challenge in Old and New Domains*, Palgrave Macmillan.

[263] Raymond, M. and DeNardis, L. (2015), "Multistakeholderism: Anatomy of an Inchoate Global Institution", *International Theory*, 7(3), pp. 590–592.

[264] Ibid.

[265] Raymond, M. and DeNardis, L. (2013), "Thinking Clearly about Multistakeholder Internet Governance", Paper presented at the 8th Annual GigaNet Symposium, Bali, Indonesia, p. 6.

[266] Carr, M. (2015), "Power Plays in Internet Governance", *Millennium Journal of International Studies*, 43(2), pp. 640–659. Regarding the size of US technology companies, see *Bloomberg*, "The Year in Technology: 2016 in Charts", 30 December 2016, https://cdn.ampproject.org/c/s/www.bloomberg.com/gadfly/amp/articles/2016-12-30/charting-the-good-and-the-bad-for-the-year-in-technology.

[267] Dunn-Cavelty, M. and Kavanagh, C., (forthcoming 2017), "Cybersecurity and Human Rights", in Wagner, B., Kettemann, M.C., and Vieth, K. (eds), *Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations,* Edward Elgar Publishing.

[268] Mueller, M.L. (2010), *Networks and States: The Global Politics of Internet Governance*, MIT Press, pp. 55–80.

[269] See http://www.itu.int/wsis/index.html.

[270] See Mueller, L.L. (2013), "Revisiting Roles: On the Agenda for Brazil", http://www.internetgovernance.org/2013/12/18/revisiting-roles-on-the-agenda-for-brazil/.

[271] Krukskikh, A.V. (2009), "Advancement of Russian Initiative to Ensure International Information Security: Chronicles of the Decade", in Komov, S.A. (ed.), *International Information Security: The Diplomacy of Peace*, Moscow State University, p.132.

[272] Ibid.; see also Kavanagh, C, Maurer, T., and Tikk-Ringas E. (2013), "Baseline Review of International ICT-Related Processes & Events: Implications for International and Regional Security (2011–2013)", ICT4Peace Foundation.

[273] See http://www.intgovforum.org/multilingual/.

[274] The annex includes a "security cluster" covering cybersecurity, cybercrime, Internet as part of critical information infrastructure, cyber conflict, child safety online, encryption, and spam, highlighting where cooperation has been achieved as well as "areas of ambiguity, unresolved issues and possible gaps". Moreover, based on external assessments, some Member States were concerned that the identified gaps could be used to support proposals in the General Assembly process to develop some form of formal mechanism to "fully implement enhanced cooperation" on these and other issues between governments (and governments alone) with evident implications for the future of Internet governance.

[275] Dickinson, S. (2016), "CSTD 18th Session: one step closer to deciding what WSIS will look like for the next 10 years", https://www.centr.org/news/blog/cstd-18th-session-one-step-closer-to-deciding-what-wsis-will-look-like-for-the-next-10-years-cstd-18th-session-one-step-closer-to-deciding-what-wsis-will-look-like-for-the-next-10-years.html.

[276] *New York Times*, "At U.N., China Tries to Influence Fight Over Internet Control", 16 December 2016, http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html.

[277] See General Assembly, "Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society", UN document A/70/L.33, 13 December 2015, para. 8.

[278] Komov, S.A., Korotov, S.V. and Dylevsky, I.N. (2009), "About the Evolution of the Modern American 'Information Operations Doctrine'", in Komov, S.A., *International Information Security: The Diplomacy of Peace*, Moscow.

[279] See, for example, *Forbes,* "Why is the UN trying to take over the Internet", 9 August 2012, https://www.forbes.com/sites/larrydownes/2012/08/09/why-the-un-is-trying-to-take-over-the-internet/#1a3d58e26df7. News articles such as this one proliferated in 2011 and 2012.

[280] See Geneva Declaration of Principles, para. 49.

[281] See Geneva Declaration of Principles para. 49(b) and (c).

[282] Maurer, T. and Morgus, R. (2014), "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate", GIGI Internet Governance Papers, no. 7.

[283] See *TechDirt*, "Who Signed The ITU WCIT Treaty ... And Who Didn't", 14 December 2012, https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml.

[284] See Geneva Declaration of Principles para. 49(b) and (c).

[285] *New York Times*, "At U.N., China Tries to Influence Fight Over Internet Control", 16 December 2016, http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html.

[286] Net Mundial Multistakeholder Statement, http://netmundial.br/netmundial-multistakeholder-statement/.

[287] See, for example, "Multistakeholderism Unmasked: How the NetMundial Initiative Shifts Battlegrounds in Internet Governance", London School of Economics Media Policy Project Blog, 5 January 2015, http://www.globalpolicyjournal.com/blog/05/01/2015/multistakeholderism-unmasked-how-netmundial-initiative-shifts-battlegrounds-internet.

[288] For a detailed discussion on the details of the transition, see "Status of the Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community by the IANA Stewardship Coordination Group", https://www.ianacg.org/icg-files/documents/IANA-transition-proposal-v9.pdf.

[289] "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends", https://www.icann.org/news/announcement-2016-10-01-en.

[290] Non-United Nations initiatives include "NetMundial" and the follow-on work of the Global Commission on Internet Governance, the final report of which succinctly noted that the future of Internet governance "needs to be based on both formal mechanisms and evolving norms to capitalize on its tremendous power to provide economic opportunity and security, while also providing resilience and privacy for all Internet users." See Global Commission on Internet Governance (2016), "One Internet", CIGI and Chatham House (p. iv), http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CIGI%20%20Final%20Report%20of%20the%20Global%20Commission%20on%20Internet%20Governance%20One%20Internet.pdf.

[291] General Assembly, "Report of the 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, para. 33.

UNIDIR

The United Nations, Cyberspace and International Peace and Security

Responding to Complexity in the 21st Century

ICT-related issues have been on the agenda of the United Nations for almost two decades, driven by both the positive benefits and the malicious purposes they can be leveraged for. This report is concerned with the UN's response to the latter in the context of international peace and security. It focuses principally on the norm-setting work currently underway within the General Assembly. It outlines where progress has been made in developing a normative framework to shape behaviour in the use of ICTs and ensure stability of the ICT environment, highlighting where challenges and on-going sources of disagreement lie.

The report also discusses linkages and complementarities with other non-UN processes, as well as linkages and complementarities with other items on the UN agenda, directly or indirectly linked to international peace and security. Finally, it identifies how the UN, particularly the UN Secretary-General, might play a role in raising awareness of, supporting and strengthening this on-going work.