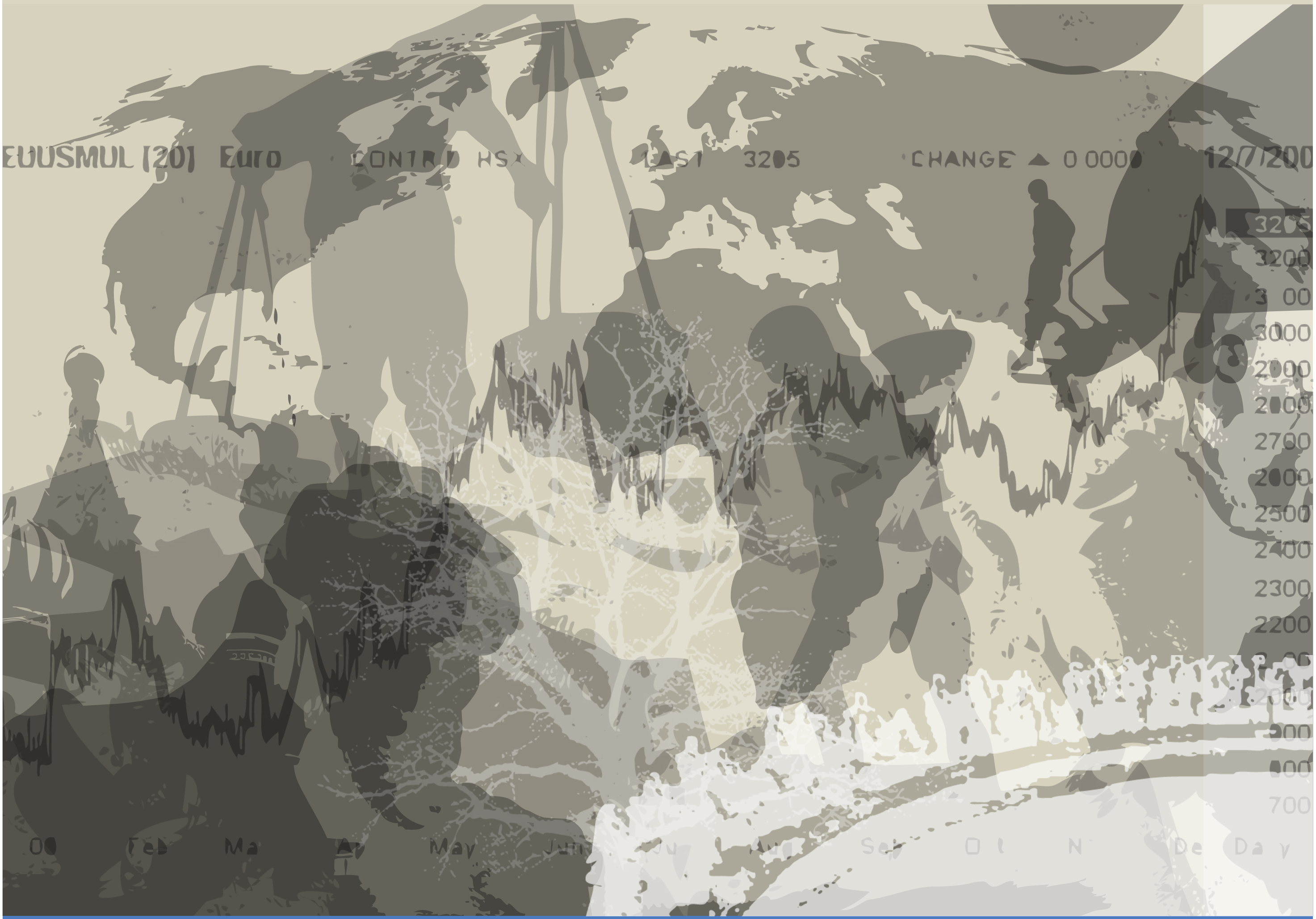
Norwegian Institute
of International
Affairs

Parabasis

Cyber-diplomacy in Stalemate

Eneken Tikk and Mika Kerttunen



NUPI Report
5 / 2018

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

Any views expressed in this publication are those of the author. They should not be interpreted as reflecting the views of the Norwegian Institute of International Affairs. The text may not be printed in part or in full without the permission of the author.

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: post@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

Parabasis

Cyber-diplomacy in Stalemate

Eneken Tikk and Mika Kerttunen*

Published by the Norwegian Institute of International Affairs

∗ Dr Eneken Tikk is in charge of the international engagement of the Cyber Policy Institute (CPI) in Jyväskylä, Finland. and is Senior Research Scientist at the Tallinn University of Technology. She has participated in three consecutive UN GGEs (2012/2013, 2014/2015 and 2016/2017) as adviser to the Estonian expert. Dr Mika Kerttunen is Director of the Cyber Policy Institute and Senior Research Scientist at the Tallinn University of Technology. He served as adviser to the Finnish expert in the 2016/2017 UN GGE. The views expressed in this paper are those of the authors, and should not be read as representing the views, positions, or attitudes of any government. If these views are read as benign subversion to some specific agendas, the authors take pride in being able to insert our constructively critical questions in the discourse. The authors thank William Boothby, Martha Finnemore, Juha Kukkola, James A. Lewis, Phil Lark and Anatoly A. Streltsov for their feedback and comments. Special thanks go to Walle Bos for early editing and research assistance, Liisi Adamson for great brainstorming sessions and Niels Nagelhus Schia for the opportunity publish this analysis in the NUPI Cyber Security Center series.

Contents

Executive Summary

Governments and industry around the world are working together to bring the next billion users online,[1] but their synergies fade when it comes to how to keep online populations safe and secure. Further, the third and fourth billion of Internet users will enter a terrain very different from that available to their predecessors. Vulnerabilities in ICTs as well as *de facto* exploitation of these vulnerabilities by state and non-state actors has been acknowledged and problematized. Evidence of malicious and hostile operations involving ICTs and the Internet abounds. Uncertain about the true potential of ICTs, governments and users have focused on rules and responsibilities for protecting against cyberattacks, espionage and data manipulation. But where is there an understanding of how to remedy and improve the situation?

Dealing with cybercrime and human rights online clearly falls within the responsibilities of the national authorities. However, not all issues of cybersecurity can be settled within national borders: they call for coordinated efforts and cooperation on the part of the international community. The most serious international issues concern international stability and security, requiring dialog and action involving all states.

The work of an expert group embedded in a UN First Committee process has received considerable attention. Working on the basis of the proposition that state use of ICTs has come to threaten international peace and security, these Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) have sought to advise on courses of action. Their dialog is characterized by two competing worldviews. One group of countries holds that the issue of cybersecurity can be resolved only by a treaty process, with clear red lines drawn up. The other group argues that any undesirable state uses of ICTs can be dealt with adequately under the UN Charter and international law. The fault lines here resemble those of the Cold War.

Still, three out of five UN GGEs have been able to table progressive reports that many capitals have sought to implement. Experts have designed an agenda of responsible state behavior in the use of ICTs, referring to obligations deriving from international law, drafting a set of recommendations on additional standards of behavior, accompanied by a menu of measures that states can employ to avoid unwanted escalation or misunderstanding in case of a cyber-incident.

[1] UN Sustainable Development Goal (SDG) 9 sets the target to “significantly increase access to information and communications technology and strive to provide universal and affordable access to the internet in least developed countries by 2020.”

Diplomats have rushed to communicate these reports to their capitals, seeking to achieve wider endorsement and national implementation of this guidance.

The inability of the most recent UN GGE (2016/2017) to deliver a consensus report has been read as indicating the failure, even collapse, of either the Group or the entire international cybersecurity dialog.[2] This study pushes back on this assessment. Like any UN Disarmament Committee process, the UN GGE is a highly politicized and accordingly contested venue, where consensus on key issues can be sought, but not always achieved. Moreover, any UN GGE is a process within a process, whereby the outcome of one Group does not necessarily render the whole agenda or series of UN GGEs obsolete. The authors argue that a no-consensus outcome can be seen as rewarding as a consensus report.

This analysis discusses implications of the no-outcome of the last round of expert negotiations. From the perspective of strategic stability, the no-consensus outcome indicates no agreement on the fundamentals of international cybersecurity, including the existence and the nature of the threat as well as the direction of international movement to address the threat. The 2017 end game underscores the lack of real urgency in fixing the tensions (and any other security issues) around ICTs in an international politico-military setting.

Despite the lack of clear guidance from the 2016/2017 Group or consensus on several fundamental issues, reports of the UN GGEs offer a roadmap for countries wishing to advance their cybersecurity. However, closer examination of this roadmap reveals very few determinate measures towards the alleged *hard* security threat embedded in ICTs. Instead, the Group has often focused on routine transparency, cooperation and coordination issues that resemble arms control in their framing but not in their content or addressees. Still, if implemented, the recommended measures would solve the majority of cybersecurity issues and insecurities.

This study concludes that dealing with acute hard-security questions has never been a real prospect in the GGE process. Consequently, the 2017 no-consensus outcome itself is no real signal of hazard. If anything is to be read as alarming, it is the carefully crafted consensus text on the

[2] See Stefan Soesanto and Fosca D'Incau, "The UNGGE is dead: Time to fall forward" August 15, 2017), http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; also Melissa Hathaway, "When Violating the Agreement Becomes Customary Practice" in Fen Osler Hampson and Michael Sulmeyer (eds.) *Getting beyond Norms New Approaches to International Cyber Security Challenges* (Waterloo, ON: Centre for Governance Innovation, 2017); Liis Vihul and Michael N. Schmitt, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; Robert McLaughlin and Michael N. Schmitt, "The need for clarity in international cyber law. International law implications of the lack of consensus" (September 18, 2017), https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/; Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" (June 29, 2017), https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what); NATO CCD COE, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html. Coming from established and aspiring thought leaders, the mainstreaming of such a claim would hinder implementation of the UN GGE guidance, and the 'universalization' of the attitudes and approaches promoted by three consecutive UN GGE reports.

allegedly hard issues, combined with soft recommendations "achieved" in the Group's reports. As neither of the camps has achieved critical mass of support for its propositions, the world is likely to witness another round of First Committee negotiation of norms, rules and principles of responsible state behavior in cyberspace. Calls for stronger institutionalization of the dialog can be expected to continue—but this is not likely to materialize in the near future.[3]

Discussion of the UN GGE process, however, is only a step towards the goal of this report. We seek to evaluate the current state of, and possible next steps for, developing consensus on, and wider understanding of, responsible behavior in uses of ICTs. The quest for international cybernorms[4] has become a distinct discourse within and around the international cybersecurity dialog. The authors inquire whether this is merely a *Glasperlenspiel* played between governments, or whether there is an acute and real need to determine and agree upon additional norms, rules and principles in the use and development of ICTs.

Any search of norms of responsible behavior in the use of ICTs must extend far beyond the UN GGE mandate and process. The authors hope that this report will open for further angles to the discussion of responsibilities that, in sum, can provide an open, free, safe and peaceful cyberspace.

The first part of this report analyzes and contextualizes the UN First Committee process. The second part offers the authors' extensions to the theme, analyzing the relative successes and failures of the leading cyberpowers in promoting the world order of their liking. In particular, we analyze how Russia, as the initiator of the First Committee process, has created momentum and gathered support for *its calls* for specific international regulation and institutionalization of the process on the one hand, and stronger governmental control of the development and use of ICTs and the flow

[3] Statement of the Deputy Secretary of the Security Council of the Russian Federation, Oleg Khramov, at the international OSCE conference on cybersecurity (3 November 2017), http://www.mid.ru/. In addition, Germany, Switzerland and Mexico have called for the establishment of a subsidiary organ of the UN General Assembly, to build common understanding and provide guidance on how existing international law, non-binding norms of responsible state behavior, confidence-building and capacity-building measures can be implemented.

[4] The term "norm" is used in two senses in the present report. Strictly, and in the context of the UN First Committee resolution on Developments in the Field of Information and Telecommunications in the Context of International Security, the scope of the term "norms" derives from the 2015 report of the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. In this report, the UN GGE calls on states to adopt, *voluntarily*, standards for responsible state behavior that in the view of Group are not established under international law, although they may derive from it See para 9-10 of the UN GGE report of 2015 (UN A/70/174). Beyond direct discussion of the UN GGE and the First Committee process, norms are understood as expectations of behavior that apply between states in the context of development and use of ICTs. The basis of such expectations could be international law, in which case the expectation becomes that each state would honor its international obligations and guarantee the rights of other states (see Stephen D. Krasner, "Structural causes and regime consequences: regimes as intervening variables," *International Organization* 36:2 (Spring 1982), fn 80); further, it is recognized that expectations of behavior could also be prescribed by social pressure applicable between states with a given identity (see Peter Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996), fn 89).

of information on the other. In conclusion, we offer some recommendations for governments wishing to pursue the goal of free and open cyberspace—indeed a rule-based world order.

Introduction

The lack of consensus in the 2016/2017 round of expert negotiations[5] conducted under the aegis of the First Committee has created momentum for reviewing the many proposals for ensuring responsible state behavior in cyberspace and mitigating the threats that state use of ICTs may pose to international peace and security.

Since 1998, Russia has sought to convince the world of the need for a new legal instrument for dealing with international information security.[6] In parallel, Moscow and Beijing have initiated a non-binding Code of Conduct together with a group of Shanghai Cooperation Organization (SCO) countries.[7]

[5] See, e.g., 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, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm. Also: Cuba at the final session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, available at http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information. Further, see 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 Dialog in This Sphere, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

[6] See, e.g., the Ministry of Foreign Affairs of the Russian Federation, Convention on International Information Security (Concept as of September 22, 2011), http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666. See also the Russian submissions in A/54/213.

[7] On September 12, 2011 the Permanent Representatives of Russia, China, Tajikistan and Uzbekistan to the United Nations sent a joint letter to the UN Secretary General requesting that the Draft International Code of Conduct for Information Security be circulated as an official document of the 66th session of the General Assembly. See annex to the letter (A/66/359), dated September12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General: "International code of conduct for information security." Another letter was sent on January 9, 2015, from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/69/723).

Meanwhile, the Western governments have backed processes and initiatives aimed at promoting practices and norms of responsible state behavior. The London Process[8], the Bildt[9] and Kaljurand[10] Commissions, the Global Forum on Cyber Expertise,[11] and the Hague Process[12] all distance themselves from intergovernmental negotiations, offering expert interpretations and recommendations instead.

The discourse of international cybersecurity abounds with the views and voices of the ICT industry as well. Microsoft has created an alliance around its *Digital Geneva Convention* calls on governments "to protect civilians on the internet in times of peace", and promotes "a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety."[13] Redmond has also initiated a public commitment among more than 40 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.[14] German Siemens, together with several other technology majors, has formulated a digital charter for the private sector.[15] Similarly, Norilsk Nickel, a leading Russian mining company, is working on a charter on information security of industrial critical infrastructure.[16] Meanwhile, Google has emphasized baseline privacy, human rights, and due

[8] The London Process refers to a series of conferences ("Global Conference on Cyberspace") held since 2011: in London (2011), Budapest (2012), Seoul (2013), The Hague (2015) and New Delhi (2017). These events convene representatives of governments, the private sector and civil society to discuss and promote practical cooperation in cyberspace, to enhance cyber-capacity building, and to discuss norms for responsible behavior in cyberspace. Statements of the conference chairs encapsulate various principles and conclusions on responsible state behavior in cyberspace.

[9] The primary objective of the Bildt Commission (formally the Global Commission on Internet Governance) "is the creation of 'One Internet' that is protected, accessible to all and trusted by everyone." The Commission was launched in January 2014. (https://www.cigionline.org/initiatives/global-commission-internet-governance)

[10] The Kaljurand Commission (formally the Global Commission on the Stability of Cyberspace) develops "proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace." The Commission was established in June 2017 (https://cyberstability.org/).

[11] The Global Forum on Cyber Expertise "is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level." The Forum was launched at the Global Conference on Cyberspace in the Hague in April 2015 (https://www.thegfce.com/).

[12] The Hague Process refers to another Dutch initiative: this one involves holding consultation meetings to stimulate discussion on international law and cyber as well as gain support and increase awareness of the *Tallinn Manual* process. https://www.thehaguesecuritydelta.com/events/event/923-the-tallinn-manual-2-0-and-the-hague-process-from-cyber-warfare-to-peacetime-regime-2016-02-03.

[13] See Brad Smith, Keynote Address at the 2017 RSA Conference "The Need for a Digital Geneva Convention," https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

[14] "Cybersecurity Tech Accord," signed by 34 global technology and security companies in April 2018, https://cybertechaccord.org/.

[15] https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

[16] See https://www.kommersant.ru/doc/3496533.

process principles in digital evidence gathering.[17] Entrepreneur Elon Musk, concerned with the "third revolution in warfare" has openly called for "morally wrong" lethal autonomous weapons systems to be banned under the 1980 UN Convention on Certain Conventional Weapons.[18]

In addition, strong voices have come from think-tanks and academia. The Global Commission on the Stability of Cyberspace has involved dozens of scholars to develop norms to protect the Internet infrastructure and the financial sector.[19] Korean academics are working on the Bright Internet Agenda, focusing on preventive measures and collaborative efforts between disjointed initiatives and agendas.[20] A UNODA 2017 publication contains an international commentary on the voluntary, non-binding norms of responsible state behavior which the UN GGE 2015 report recommended states to consider.[21] Moscow State University has initiated an international research partnership to provide a commentary to the UN GGE's 2015 recommendations. These state- or corporation-sponsored processes are complemented by numerous scholarly proposals for better international cybersecurity through norms of responsible state behavior.

Such a diversity of views in the international norms discourse has several implications. While all these parallel tracks offer valuable food for thought and discussion, there is little prospect of any one of these propositions being comprehensively pursued, let alone universally accepted. Accepted standards of responsible state behavior in cyberspace remain a distant dream, not just because of vast technical capacity divides and the acknowledged difficulties of attributing state behavior in cyberspace. Fundamental questions of the international cybersecurity discourse are far from being settled politically. The discourse appears highly fragmented, in terms of underlying assumptions as well as proposed solutions. Importantly, proposals for new binding and non-binding norms are often premised on controversial arguments and beliefs about issues of international cybersecurity, their root causes, effects and trends. Lack of shared terms and definitions across disciplines and groups further complicates mutual understanding and communication.

On the other hand, this disintegrated dialog may offer new leads during the operational pause created by the 2016/2017 UN GGE (no-report) outcome. It allows states and scholars to (re-) position themselves in the discourse and invites scholars to study critically the arguments and proposals on the table.

[17] Kent Walker, "Digital security and due process: A new legal framework for the cloud era" (2017), https://www.blog.google/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/.

[18] See https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war

[19] See https://cyberstability.org/

[20] See http://www.bigs2017.org/

[21] Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (New York: UNODA 2017). https://www.un.org/disarmament/publications/civilsociety/civil-society-and-disarmament-2017/

To determine how to move the normative agenda of international cybersecurity forward, it can be helpful to take a few steps back. Firstly, there is much to be learned from the circumstances that, directly or indirectly, may have led to the no-report result in the 2016/2017 UN GGE. Secondly, there is much to be studied about the pre-existing norms, cyber-specific and general, national and international, before making any definitive move towards replacing, renewing or expanding them. Thirdly, scholarly work in this field can offer additional insights and openings. Finally, there are many ways of achieving common understanding and mutual acceptance on these issues, and not all of them have been exhausted.

Part I: GENESIS

The UN GGE Process: Goals, Expectations, Outcomes

The International Cybersecurity Dialog in the UN First Committee

The Original Proposal and Context

The First Committee of the United Nations is tasked with disarmament and international security affairs. Among its main topics are nuclear disarmament, non-proliferation, arms race and illicit arms trade.[22] It is to this theatre that Russia has striven to bring the issue of the development and use of ICTs since the late 1990s.

The groundwork and idea for a resolution on international information security[23] came from the Kremlin. The Russian draft resolution initially emphasized the threat of *information weapons* and *information wars*. It is seems fair to conclude that at least one of Moscow's goals was to offset the US superiority in military development and deployment of ICTs demonstrated in the First Gulf War, and to restrain further operational development in this field.[24] A related and no less important objective for the Russian government has been to retain control over the information environment and eliminate "threats to information support to Russian Federation state policy" as experienced in the Chechen wars.[25] In these aspirations, Moscow originally adopted the terms of the mid-1990s US military doctrine.[26]

Recent Chinese and Russian rhetoric on the need for *traffic rules* for the *information highway*[27] also draws on the language used in the Clinton Administration's policy aimed at promoting

[22] United Nations First Committee, "List of draft proposals for the 72nd session" (as of November 2, 2017).

[23] UN General Assembly (1999) Resolution Adopted by the General Assembly, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70, January 4; the resolution was adapted without a vote. Since 2006, the resolution has been open for co-sponsorship.

[24] For further discussion of Russia's concerns beyond the Committee I initiative, see Eneken Tikk-Ringas (ed). *Evolution of the Cyber Domain: Implications on National and International Security* (Abingdon: Routledge, 2016). See also Eneken Tikk, "Cyber: Arms Control without Arms?" in Tommi Koivula and Katariina Simonen (eds.), *Arms Control in Europe: Regimes, Trends and Threats* (Helsinki: National Defence University, 2017).

[25] *Information Security Doctrine of the Russian Federation* (September 9,2000).

[26] Ambassador Andrej Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation on Information Security, remarks at the opening of the Forum on "State, Civil Society and Business Partnership on International Information Security," Garmisch-Partenkirchen (April 23, 2015). See, for example, U.S. Joint Publication 3-53 *Doctrine for Joint Psychological Operations* (July 10, 1996) and Joint Publication 3-12 *Joint Doctrine for Information Operations* (October 9, 1998).

[27] An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open and cooperative cyberspace. Remarks delivered on February 10, 2014 at UNIDIR: "Nowadays, the information "highway" has reached almost every corner of the world. It is of great concern, however, that in this virtual space

information superhighways—to share information, to connect, and to communicate as a global community:

From these connections, we will derive robust and sustainable economic progress, strong democracies, better solutions to global and local environmental challenges, improved health care, and—ultimately—a greater sense of shared stewardship of our small planet.[28]

Suspicious of this agenda, Russia has built a counter-narrative with vivid illustrations. Moscow's original proposal in the UN First Committee concerning banning *information weapons*[29] and their use, by means of a dedicated international legal regime.[30] The first Group might well have attempted to achieve just that, given the emphasis of Russia's 1999–2003 submissions to the First Committee.[31] Several countries shared the Russian view on the advisability of an international arms control regime with regard to *information weapons*, among them Belarus,[32] Mexico,[33] and Brazil.[34] Unconvinced, the USA argued that it would be "premature to formulate overarching principles pertaining to information security in all its aspects,"[35] dismissing the need for an arms-control approach. Aligning with the USA, the UK held that a multilateral instrument for restricting the

where traffic is very heavy, there is still no comprehensive "traffic rules". As a result, "traffic accidents" in information and cyber space constantly occur with ever increasing damage and impact."

[28] "… the President of the United States and I believe that an essential prerequisite to sustainable development, for all members of the human family, is the creation of this network of networks. To accomplish this purpose, legislators, regulators, and business people must do this: build and operate a Global Information Infrastructure (GII). This GII will circle the globe with information superhighways on which all people can travel." Remarks prepared for delivery by Vice President Al Gore, World Telecommunication Development Conference, Buenos Aires (March 21, 1994).

[29] A/54/213, page 10: Means and methods used with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defense, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State.

[30] See letter dated September 23, 1998, from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (A/C.1/53/3) and Russian contribution in Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213), page 8.

[31] See letter dated September 23, 1998, from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (A/C.1/53/3) and Russian contribution in Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213), Developments in the Field of Information and Telecommunications in the Context of International Security (A/55/140) and Developments in the Field of Information and Telecommunications in the Context of International Security (A/56/164/Add-1).

[32] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).

[33] UN Developments in the Field of Information and Telecommunications in the Context of International Security (A/56/164), UN Developments in the Field of Information and Telecommunications in the Context of International Security (A/60/95).

[34] Developments in the Field of Information and Telecommunications in the Context of International Security (A/60/95/Add.1).

[35] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).

development or use of certain civil and/or military technologies was unnecessary, as the law of armed conflict, in particular the principles of necessity and proportionality, already governed the use of such technologies.[36] Sweden, speaking on behalf of the EU in its written submission, held that within the context of the General Assembly, the First Committee should not be the main forum for discussing the issue of information security. The EU believed there were other committees better suited for discussion of at least some of the aspects of the issue, since in the EU this mainly concerned subjects other than disarmament and international security.[37]

The USA and UK also framed the Russian aspirations as a desire for governmental control over the free flow of information. Whitehall warned against the Kremlin's call for a multilateral instrument as an "impingement on the free flow of information as a key principle of the information society."[38] The USA argued that a treaty approach would contravene the principle of the free flow of information critical to the growth and development of all states: "The implementation of information security must not impinge upon the freedom of any individual to seek, receive and impart information and ideas through any media—including electronic—and regardless of frontiers, as set forth in article 19 of the Universal Declaration of Human Rights."[39]

The first UN GGE was convened in 2004/2005, to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on international information security concepts.[40] However, Moscow's alarming appeal did not lead to consensus during the first round of UN GGE deliberations. As the Chair noted, "even with the use of translation, the members /…/ spoke different languages with respect to essential issues related to international information security", notably because of the lack of "unified and generally accepted definitions of key terms and concepts, and differing interpretations of international law in the area of international information security."[41] With the Group operating on the basis of consensus, even one dissenting view was, and still is, enough to prevent a final report.[42]

Rising Tensions in the Mandate

The mandate of the second UN GGE that convened in a series of meetings in 2009/2010 was "to continue to study existing and potential threats in the sphere of information security and possible

[36] Developments in the Field of Information and Telecommunications in the Context of International Security (A/59/116).

[37] UN Developments in the Field of Information and Telecommunications in the Context of International Security (A/56/164).

[38] Developments in the Field of Information and Telecommunications in the Context of International Security UN (A/59/116), page 11.

[39] Developments in the Field of Information and Telecommunications in the Context of International Security UN (A/29/116/Add. 1), page 3.

[40] UNGA Resolution A/RES/58/32 (18 December 2003). The first UN GGE met in 2004/2005, the second met in 2009/2010, the third group in 2012/2013, the fourth group in 2014/2015, and the fifth group in 2016/2017.

[41] A/C.1/60/PV.13, page 7.

[42] It is essential to observe that although the UN GGE is pro forma an expert group, its members regularly occupy prominent decision- and policy-making positions in their respective governments.

cooperative measures to address them."[43] Assembling after the experience of politically motivated cyberattacks in Estonia and Georgia, the second Group was unanimous about the need to address issues of international information security in the First Committee:

> Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.[44]

The Group recommended further dialog among states to discuss norms pertaining to state use of ICTs; as well as confidence-building, stability and risk reduction measures; information exchange; and capacity-building in less developed countries. [45]

The third UN GGE, 2012/2013, continued to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. This time, the mandate included reference to norms, rules or principles of responsible behavior of states, and confidence-building measures with regard to the information space as well as concepts aimed at strengthening the security of global information and telecommunications systems.[46]

During the 2012/2013 UN GGE, the focus returned to the question of a possible new and binding agreement on international information security. Russia's national position on this matter had not changed significantly since the inception of the First Committee process. However, in the 2012/2013 UN GGE, Moscow yielded to the US–UK proposition that there was no need for a new international legal instrument and that existing international law would be sufficient to maintain peace and security in cyberspace. The 2013 report concluded: "the application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability."[47] This conclusion went further, as the Group also stated that "common understandings on how such norms shall apply to State behavior and the use of ICTs by States" required further study. Further: "given the unique attributes of ICTs,

[43] UN Resolution A/60/45 (6 January 2006) Developments in the field of information and telecommunications in the context of international security.

[44] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/65/201 (30 July 2010).

[45] Ibid.

[46] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013).

[47] Ibid, para 16.

additional norms could be developed over time."[48] With these conclusions, the 2013 report could be read as the optimal point of balance in the international cybernorms dialog, settling on little.

The mandate of the fourth Group, 2014/2015, was "to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behavior of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts."[49] An additional element in the mandate was a request to study "how international law applies to the use of information and communications technologies by States."[50]

This time, the experts were able to provide additional references to international law that they deemed applicable to state uses of ICTs. The Group was not, however, in a position to clarify how international law applied, and the section on international law became a selective enumeration of the provisions of the UN Charter. Further, in the Group's discussions it became evident that participating experts, as well as states, held differing views on the composition, interpretation and implementation of international law. This was evidenced, for example, by the listing of concepts like state responsibility and due diligence in a section of the report titled "voluntary and non-binding" norms, rules and principles.

Despite obvious difficulties in elaborating and agreeing on matters of international law in the fourth GGE, the mandate for 2016/2017 explicitly took up the question "how international law applies to the use of information and communications technologies by States."[51] Answering this question, however, proved to be a bridge too far.

[48] Ibid.

[49] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015).

[50] Ibid.

[51] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/72/327 (August 14, 2017).

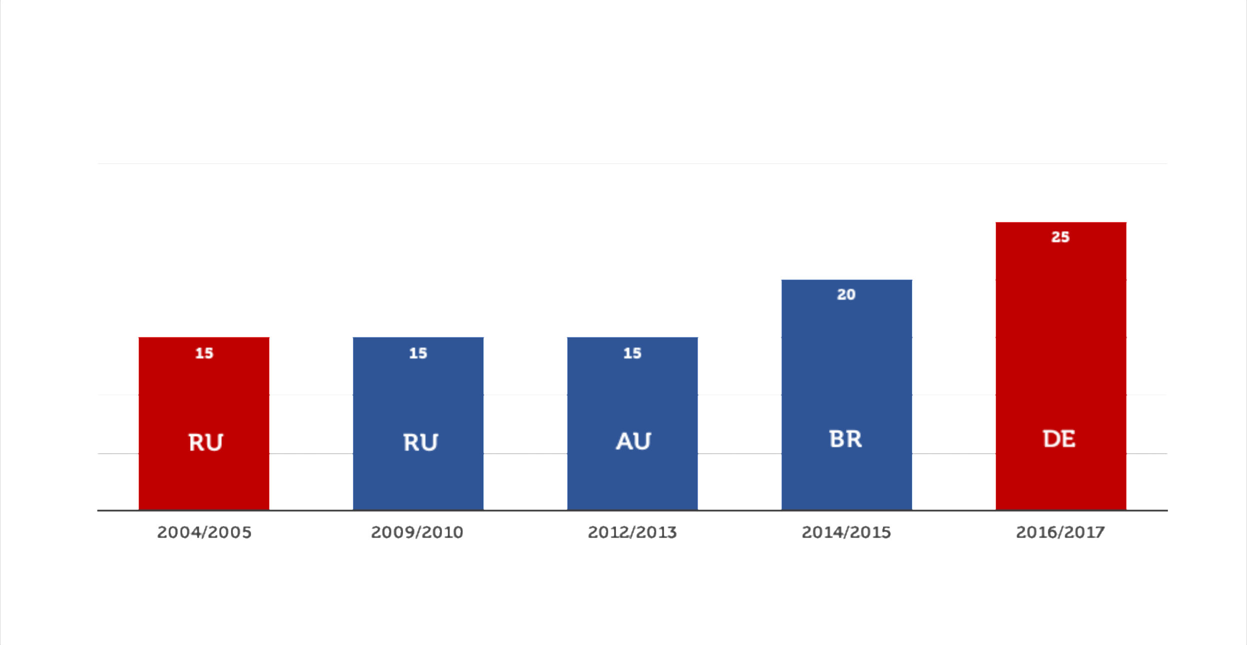


Illustration 1. The growth of the UN GGE, and the respective chairmanships. The first and the most recent one (in red) did not result in a report. The number on the top of the pillar indicates the number of Experts in the respective Group. Authors' compilation of UN data.

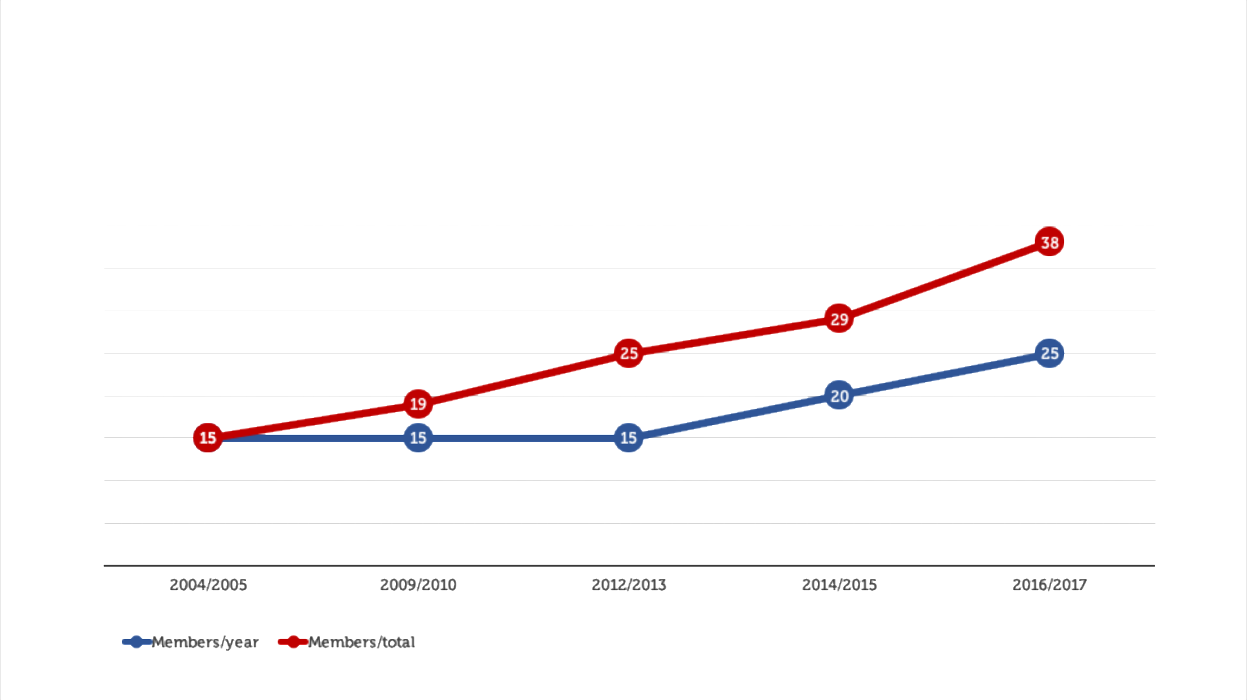


Illustration 2. Cumulative participation of states in the UN GGEs (2004–2017). Authors' compilation of UN data.

Gradual Compartmentalization of the Norms Discourse

For observers, the UN GGE process has been confusing as regards the scope and definition of "norms, rules and principles" and their relationship to international law. Despite the mandate, throughout the years of discussing and studying relevant concepts, the UN GGE has never fully clarified the use of such terms as *norms*, *rules*, or *principles*.

In this context, it is noteworthy that the 2013 report addressed the applicability of international law, as well as the potential need for new norms, under the same heading: "Recommendations on norms, rules and principles of responsible behavior by States."[52] Para 16 of the 2013 report reads:

> *The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time.*[53]

At face value, the 2013 report can be read as maintaining that, while there is agreement on the applicability of international to state use of ICTs, additional binding norms might be required over time. This balance can be detected in references made to otherwise contested issues. Paragraphs 17–20 of the 2013 report reflect the Group's views on the applicability of some earlier UN recommendations,[54] noting the SCO Code of Conduct and offering general confirmation of the applicability of international law, making particular reference to the UN Charter[55] as well as the concept of sovereignty.[56] Paragraphs 21–25 offer general guidance with regard to human rights and fundamental freedoms, cooperation, internationally wrongful acts, and supply-chain security. In other words, the 2013 report captured the different directions of leading cyberpowers' thinking in well-crafted consensus language. Furthermore, the 2013 report emphasized the application of norms derived from existing international law relevant to the use of ICTs by states.[57]

The logic of addressing norms changed considerably in the 2015 report. The application of international law to the use of ICTs (section VI of the report) was here discussed separately from norms, rules and principles for the responsible behavior of states (section III of the report). Such compartmentalization was necessary, for several reasons. Where states could not agree on specific applications of international law, this would not be framed to mean that there was a need for a new treaty. This move also provided a convenient way of disagreeing about international law, even

[52] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (June24, 2013), p. 8.

[53] Ibid.

[54] Ibid. See para 17 referring to resolutions 64/25, 65/41 and 66/24 inviting Member State views and assessments as well as to resolutions 55/63, 56/121, 57/239, 58/199 and 64/211 that contain other measures.

[55] Ibid, para 19.

[56] Ibid, para 20.

[57] Ibid, para 16.

among otherwise like-minded states.[58] It is evident that, between the 2013 and 2015 reports, the experts did not manage to agree on the status of certain concepts under public international law, such as “state responsibility” and “due diligence.”

Further, this provided an opportunity for all states to clarify what in their view required further normative guidance or reinforcement. The section on norms, rules and principles in the 2015 report emphasizes the strictly voluntary and non-binding nature of the recommendations contained therein:[59] the previously stated connection between international law and norms had disappeared.

However, despite emphasis on *voluntary norms* in paras 9 and 10 of the 2015 report, the title of section III still referred to norms, rules *and* principles, confusingly retaining the scope of discussion set by the 2013 report. The 2015 report offered recommendations for eleven voluntary norms, rules and principles that in the view of the experts were likely to improve the international cybersecurity situation.[60] These recommendations are widely regarded as the main success of the 2014/2015 GGE.[61]

In the enthusiastic climate created by the apparent success of the 2015 GGE report, the international community placed high hopes on the fifth (2016/2017) GGE. At least 60 countries competed for the 20 available seats,[62] many of them newcomers to the process—which demonstrated the growing interest in the work of the GGE and the issues discussed in the Group. In addition to the expectation of increased buy-in through the inclusion of new states in the discussion, states were also hoping for further progress and clarifications of the recommendations made in the 2015 report. Desires for a strict ban on “information weapons” and demands for new treaty negotiations seemed to have withered. Lively academic and political discussions, as well as corporate proposals,[63] were underway about how international law could be applied in and to cyberspace or further developed to promote international peace and security. New proposals for non-binding norms were made, in the hope that the next GGE would include them in the 2017 report.[64]

However, in the context of an ambitious mandate, seasoned experts soon realized that achieving further consensus during the 2016/2017 GGE would be difficult. On the one hand, differing views

[58] The phrase “like-minded States” is used to refer to states that hold views largely aligned with those of the USA.

[59] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (July 22, 2015), paras 9 and 10.

[60] Ibid, para 13.

[61] For a commentary on the 2015 recommendations, see Tikk (ed.), *A Commentary*.

[62] The five Security Council Permanent Members are automatically included in the GGE.

[63] Microsoft’s proposal for a digital Geneva Convention (Smith, *op.cit*).

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

on international law prevented the Group from crafting further consensus language on the application of the recommendations listed in para 13 of the 2015 report, or even listing further applicable concepts and rules. On the other hand, prioritization of the international law section above other topics indicated lack of progress on this topic, with other sections being held hostage.

UN GGE 2016/2017: An Autopsy of an Alleged Failure

Picking up and examining the broken pieces of the process that the UN GGE Experts have left behind has become a forensic thread in the work of international cybersecurity and international law experts. What was deliberated, who agreed and who rejected what, why, and with what outcome? Although such questions may well yield insights into the positions, policies and politics of states, the GGE cannot decide, or authoritatively conclude, that international law *is* or *is not applicable*. At most, the GGE may offer perspectives. Neither the views of individual experts, nor positions of selected countries, provide grounds for concluding that cyberspace is a "lawless space."

Indeed, the GGE is *the* discussion of responsible behavior for states in their use of ICTs. It represents *the* attempt of the cyber-superpowers to convince each other, and the international public, not only of looming threats but also of the need to take measures to mitigate them. It is *the* negotiation of how states ought to understand, interpret and implement international law, build confidence and develop their capacities.

However, the GGE has never been mandated to create, or dismiss, existing international law. It was tasked to discuss, and (literally) study, how international law can be, and is, applied to threats to international peace and security resulting from state use of ICTs. The fact that 25 experts were not able to agree on the issue, largely due to the underlying political differences, should not be read as diminishing the authority of international law. No GGE report can take away any of the rights of the states and obligations towards other states under this body of law.

Describing the 2016/2017 GGE as a failure over-emphasizes the relationship between the GGE and international law and make GGE success conditional on a tangible outcome—a report—regardless of its content. In fact, however, there is value in the 2017 no-report outcome. It demonstrates how fragile and carefully crafted any previous "agreements" on the subject have been. It highlights principal differences between the leading cyberpowers and the challenges of overcoming these. The process also provides valuable information on where nations stand and what they are ready to accept, or not.

The outcome of the most recent GGE confirms that there are significant differences of opinion between states on how to apply international law to state use of ICTs, and that there was insufficient determination among the participating experts to overcome these differences. This outcome, indeed, stands as a call for each state to come up with its own views on how to apply international law to issues of cybersecurity.

Not surprisingly, the 2017 result remains open to interpretation. Competing narratives will reflect how differently the various parties read, interpret and communicate the whole process, its value and its potential. Interestingly, they also show the differences in states' and scholars' understanding and interpretation of international law. There is hardly one single decisive point of failure in the 2016/17 GGE process. In the analysis below, we discuss possible differences, misunderstandings and challenges that may explain why the Group failed to achieve consensus.

True Differences

Perhaps the most straightforward explanation of why and how the 2016/2017 GGE did not manage to achieve consensus derives from a simple comparison of positions and perspectives, political and practical views, and preferences about the nature, development and use of ICTs. International cybersecurity discussion, where expertise is complemented by global representation, is a marketplace of sometimes diametrically opposing worldviews and belief systems, a contestation predating any ICT/ cyber-discourses.

Broadly, there are two main views regarding how international cyber security should be achieved and organized: The Western or "like-minded" approach, which focuses on promoting and explaining existing international law, and the Russo–Sino call for *lex specialis* and reinforced international political structures, mainly the UN, as the mechanism for maintaining international peace and security. There are various concepts and rules of international law that evoke contradictory reactions among participating states.

Differences on International Law

A set of differences surrounds discussion of the implications of prohibiting the use of force in the context of ICT use. Underscoring that Article 2(4) of the UN Charter constitutes a prohibition of state-on-state cyberattacks, China has argued that any reference to Article 51—the right to self-defense—as well as to the applicability of International Humanitarian Law (IHL), would send a wrong message to the international community, indicating legitimization of cyber-conflict.[65] The Chinese stand on these norms and instruments of international law is strictly textualist,[66] political and principled at the same time. Deriving from the desire to ban information weapons in the first place and building on the Western proposition that existing international law is sufficient to address concerns of international information security, the Sino–Russo interpretation is that the prohibition of use of force in Article 2(4) of the UN Charter should be read as absolute in the context of ICTs.

The like-minded, equally principled, justifiable and logical view that Article 51 and IHL are applicable to cyber-incidents in case Article 2(4) is breached contradicts the absolutist logic adhered to by China and Russia. However, the like-minded reading is tainted by the evident operational interests that the leading normative voices—the USA, the UK and the Netherlands—have

[65] Julian Ku, "Forcing China to Accept that International Law Restricts Cyber Warfare May Not Actually Benefit the U.S.," *Lawfare* (August 25, 2017); Ku, "How China's Views on the Law of *Jus ad Bellum* Will Shape Its Legal Approach to Cyberwarfare," *Aegis Series Paper* No. 1707 (2017).

[66] On the textualist reading of legal scripts see e.g. Antonin Scalia and Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* (St. Paul, MN: Thomson/West, 2012).

vested in the cyber-domain. Thus, while a technical reading of the law makes it impossible to think that reference to Article 51 in the UN Charter would legitimize, let alone incentivize, armed conflict in cyberspace, such reading of the debate disregards the more political stance that cyber-wars and weapons should never become a reality.

Another difference centers on the topic of sovereignty. According to the Sino–Russo view, sovereignty, too, is an absolute concept that only the sovereign state itself can condition. According to China, each country has the right to manage its own cyberspace in accordance with its domestic legislation.[67] Russia and China have made it clear that they deem it within their right to stop information (both incoming and outgoing) at their borders, on the grounds that each country has the right to manage its own cyberspace in accordance with its domestic legislation.[68] Such a view, again, is the principled stand of these countries, and their established reading of international law. The argument for strong, flat, sovereignty has been taken up by other countries, albeit on the basis of different considerations.[69] For most countries, ICTs tend to be of foreign origin, and as such may be seen as an opening to unforeseeable and undesired influence and interference.[70] These countries' claims for sovereignty may reflect their distrust of Western technologies and donors whose goals and interests might be contrary to theirs.

These takes on sovereignty stand in opposition to the US and "like-minded" drive for the free flow of information, as well as the operational ambitions of the major cyberpowers. A clear rule of sovereignty could also be regarded as interfering with the like-minded investment in cyber espionage and low-intensity cyber operations. In line with recent US thinking, the UK has recently taken the view that sovereignty cannot be regarded a rule, but merely a principle of international law.[71] Differences involving sovereignty are also evident in the context of content, where a reading of the US First Amendment implies high tolerance of all forms of speech, whereas the Sino–Russo view favors a much more controlled information environment. These differences predate the cybersecurity dialog, and will survive it.

Further, sovereignty and the exercise thereof are problematic as to specific rights and obligations that can be claimed in the context of ICTs. Countries differ greatly in their capacities and priorities in dealing with information/cyber-security. Cuba, for example, has concluded that the "unequal

[67] Developments in the Field of Information and Telecommunications in the Context of International Security (A/61/161).

[68] *Ibid.*

[69] 2012 WCIT vote, see https://www.ip-watch.org/2012/12/13/wcit-split-after-split-vote-on-internet-governance-resolution/.

[70] Note Cuba's view, whereby "we are talking about technologies that originate in developed countries, among which the United States of America, the world's largest hegemonic Power, particularly in the field of information and telecommunications, enjoys a pre-eminent position that enables it to impose technological standards that facilitate the use of information and telecommunications systems as a means of aggression," in Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).

[71] UK Attorney General Jeremy Wright's speech on the UK's position on applying international law to cyberspace. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

development of states, among other factors, makes it rather difficult to establish uniform international regulations that can be generally applied to all countries that share these technologies."[72] This lack of attribution capability has been emphasized and echoed repeatedly in international cyber-dialog.

On some issues there are also considerable differences among the otherwise aligned countries. The USA and the UK, for instance, do not acknowledge "due diligence" as an established obligation in international law, whereas Germany and the rest of the EU seem firmly supportive of due diligence as a binding rule under customary international law.[73] Finally, there seems to be at least some rejection of the binding nature of ILC Draft Articles of State Responsibility, as reflected in para 13 d and f of the 2015 report. Perhaps the most controversial question in the context of the Draft Articles concerns countermeasures. While some countries have held back in discussing countermeasures in the first place, others are hesitant about their potential implementation, especially by countries that have voiced objections to the customary status of restrictions in Articles in the Draft Articles.

ICTs and the free flow of information

The struggle over information and communication technologies has been on the UN agenda in various forms and venues since the world organization was established. While the technologically most developed countries seem to prioritize the free flow of information, the developing countries have tended to pursue equal access to information and information technologies. On the other hand, Russia and China have been hesitant to subscribe to a world order premised on de-centralized flows of information, and perceive certain ICTs and the free flow of information itself as a threat. These fault lines have largely remained the same throughout UNESCO's agenda of New World Information and Communication Order (NWICO),[74] the World Summit of Information Society[75] and the World Congress on International Telecommunications (WCIT).

[72] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).

[73] In the US 2011 international cyber security strategy, *cybersecurity due diligence* in the US administrative culture refers to States' duty ("should") to recognize and act "on their responsibility to protect information infrastructures and secure national systems from damage or misuse." This reference to responsibility does not, however, recognize any legal or financial liability on the part of the state. See also Department of State *International Cyberspace Policy Strategy* (March 2016).

[74] A 1978 UNESCO study concluded that the international information system demonstrated a profound imbalance between developed and developing countries, where the developed countries "dominated the information circuit from start to finish". As a result, 75 countries called for a new world order for information, mainly involving the re-organization and re-consideration of policies and regulations pertaining to the media, access to information, copyright, and spectrum management. (International Commission for the Study of Communication Problems, *The New World Information Order* (Paris: UNESCO, 1978).

[75] Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium, Document WSIS-03/GENEVA/DOC/4-E (12 December 2003).

As became clear in the First Committee process, to China the problem of information security involves not only the risks arising from the weakness of the basic information infrastructure, but also the political, economic, military, social, cultural, and numerous other types of problems created by the use, or misuse, of information technology.[76] In his statement to the General Assembly, the Russian Chair of the 2004/2005 UN GGE noted that issues of international information security are rooted in the global information revolution.[77] Not surprisingly, China and Russia have preferred to focus on "international information security."

According to the USA, however, the implementation of information security must not impinge upon the freedom of any individual to seek, receive and impart information and ideas through any media—including electronic—and regardless of frontiers, as set forth in Article 19 of the Universal Declaration of Human Rights.[78] The UK has clarified its choice of terms, shedding further light on the underlying differences: there is scope for potential confusion in the use of the term "information security," as it is used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed. The UK does not recognize the term "information security" when used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[79] In this discussion it remains to be seen whether cyberspace will be understood as a singular, global environment, or the sum of national "cyber" or "information spaces," sometimes referred to as a "Balkanized" cyberspace, or a "splinternet."[80]

The Question of Lex Specialis

Throughout the First Committee process, Russia has never given up the idea of clarifying and codifying the applicable norms and principles to govern uses of ICTs. Having argued that "contemporary international law has virtually no means of regulating the development and application of [information] weapons,"[81] Moscow has made numerous proposals as to concrete

[76] A/61/161.

[77] A/C.1/60/PV.13, p. 5. See also 2000 Information Security Doctrine of the Russian Federation, which was re-adopted in 2008 and remained in force until December 2016, when a new Doctrine on Information Security of the Russian Federation was adopted. See further the Chinese contribution in 2006, whereby the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected (Developments in the Field of Information and Telecommunications in the Context of International Security (A/61/161)).

[78] 59/116/Add.1.

[79] UK 68/156, a position shared almost verbatim by Sweden in (69/112).

[80] See, e.g. Beverley Earle and Gerald A. Madek, "International Cyberspace: From Borderless to Balkanized," *Georgia Journal of International and Comparative Law,* Vol 31:2 (2003), pp. 225ff.

[81] 59/116, Russia, 1, para 6.

issues and ways of resolving them,[82] and has continued to develop normative frameworks[83] that can be acceptable to other countries.

The Kremlin has moved, both unilaterally and in cooperation with China and Central Asian states, to build alternative platforms for its agenda. In 2009, the member-states of the Shanghai Cooperation Organization (SCO) settled on an agreement for cooperation aimed at ensuring "international information security."[84] In 2011, Russia tabled a concept *Convention on International Information Security*, which at the time was distributed mainly through Russian embassies and diplomatic representations.[85] In 2013, an agreement on cooperation was concluded among the members of the Commonwealth of Independent States to improve information security.[86] In 2011 and 2015, Russia and China were supported by other SCO countries in submitting to the UN Secretary-General another draft document aimed at facilitating international consensus on international norms and rules guiding the behavior of states in the information space.[87]

Russian national policies have confirm the commitment to a treaty process, seeing it as a high priority to "create conditions for promoting internationally the Russian initiative to develop and adopt the Convention of International Information Security by United Nations Member States."[88] This Russian objective is accommodated in the consensus language of the 2012/2013 Group's conclusion on the applicability of international law, to be read in conjunction with two other sentences in para 16: "Common understandings on how such norms shall apply to State behavior

[82] 59/116, Russia, 1, para 14.

[83] See SCO Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (June 2009), Concept Convention on International Information Security (Russian MFA, September 2011), and International code of conduct for information security (A/66/359; A/69/723).

[84] The agreement was concluded between People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on July 16, 2009.

[85] The Concept Convention was uploaded on the website of the Russian Ministry of Foreign Affairs on September 22, 2011.

[86] CIS Information Security Agreement was signed by heads of CIS states in St. Petersburg on November 20, 2013.

[87] "International code of conduct for information security," Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UNGA A/69/ 723 (13 January 2015), and UNGA A/66/359 (14 September 2011).

[88] "Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020" (September 2013) (http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russian-federation-in-the-field-of-international-information-security-to-2020.html), Chapter III Priorities of State Policy of the Russian Federation; see also Igor N. Dylevsky, et al, "Political and Military Aspects of the Russian Federation's State Policy on International Information Security," *Military Thought* 24:1 (2015).

and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time."[89]

Over the past two decades, Russia has consistently maintained and furthered the call for a binding and universal agreement on international information security, taking steps at the national, regional and international levels to socialize and promote this idea (see below).

In contrast, especially the UK and the USA have remained dismissive about negotiating a treaty. In 1999, the USA argued that "given the clear need to analyze all aspects of information security and reach a thorough understanding of how they interact, it would be premature to formulate overarching principles pertaining to information security in all its aspects" and that "it would be highly unwise for the General Assembly to formulate strategies or direct activities that might preempt or interfere with the work of the international community that is already under way."[90] One year later, it added: "with respect to military applications of information technology, an international convention is completely unnecessary. The law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies."[91] Also the UK has also dismissed the need for a multilateral instrument that would restrict the development or use of certain civil and/or military technologies: "with respect to military applications of information technologies, such an instrument is unnecessary. The law of armed conflict, in particular the principles of necessity and proportionality, governs the use of such technologies. Moreover, such an approach might impinge on the free flow of information, which was also recognized by the World Summit on the Information Society as a key principle of the information society."[92]

[89] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98), para 16.

[90] US, 59/116/Add.1.

[91] Ibid.

[92] A/59/116.

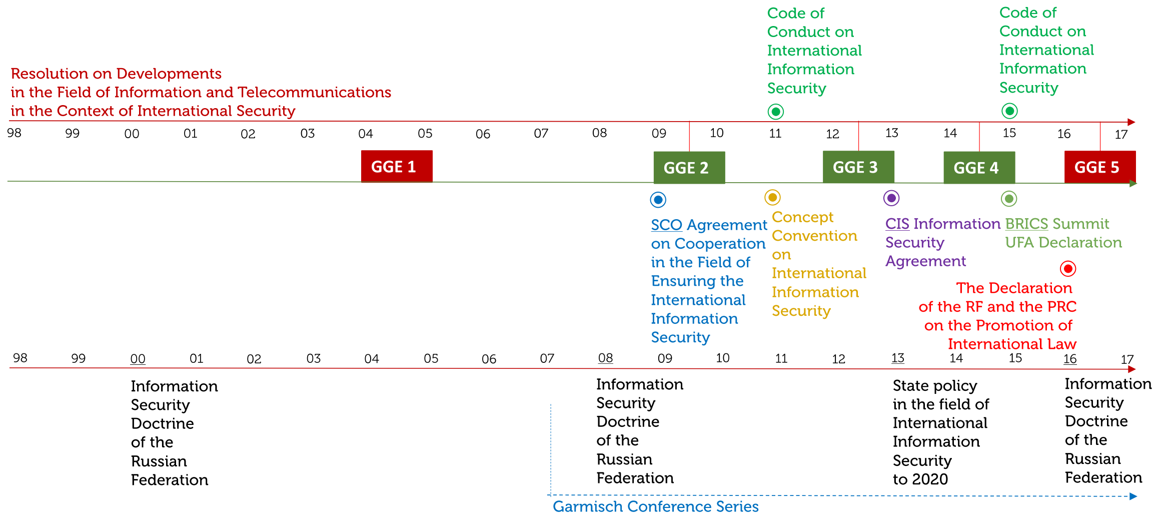

Code of Conduct on International Information Security
Code of Conduct on International Information Security
Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security
98 99 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17
GGE 1
GGE 2
GGE 3
GGE 4
GGE 5
SCO Agreement on Cooperation in the Field of Ensuring the International Information Security
Concept Convention on International Information Security
CIS Information Security Agreement
BRICS Summit UFA Declaration
The Declaration of the RF and the PRC on the Promotion of International Law
98 99 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17
Information Security Doctrine of the Russian Federation
Information Security Doctrine of the Russian Federation
State policy in the field of International Information Security to 2020
Information Security Doctrine of the Russian Federation
Garmisch Conference Series

Illustration 3. Overview of Russian International Information Security Policy. Authors' compilation and graph.

Thus, any discussions of international law are possible within very limited margins in the UN GGE. Differing interpretations of international law are not only possible, but, in the case of ICTs, clearly visible. A dialog that would consider different readings of international law and open interpretations to a more inclusive dialog might be welcomed by the international community.[93] Politically, however, a law-focused international process might well underscore that there is little recourse to be had. Different readings of international law will always be possible, and attempts to lock specific interpretations would require a new normative regime. Building such a regime in a highly contested and unequal environment, focusing on the use of ever-developing information and communication technologies, seems unlikely to result in an agreement.

[93] Margaret Mead, Rosalyn Higgins and Harold H. Koh, "From cyber norms to cyber rules: re-engaging states as law-makers, *Leiden Journal of International Law,* Vol 30:4 (2017).

Although authoritative research and analysis has been offered on issues of international law,[94] on many issues there is no consensus among scholars,[95] let alone among states. A more inclusive discussion of the applicability of international law in the context of cybersecurity could reveal grave, frequently irreconcilable, differences between states.[96] So far, 70 states have shared their views on international cybersecurity issues and normative remedies in the First Committee Process.[97] Their submissions highlight differences regarding specific concepts and rules of international law.[98] National submissions also underscore that many cybersecurity issues would need to be addressed in national legislation and policy, thus calling for a more critical and less politicized search for remedies to issues of international cybersecurity.[99]

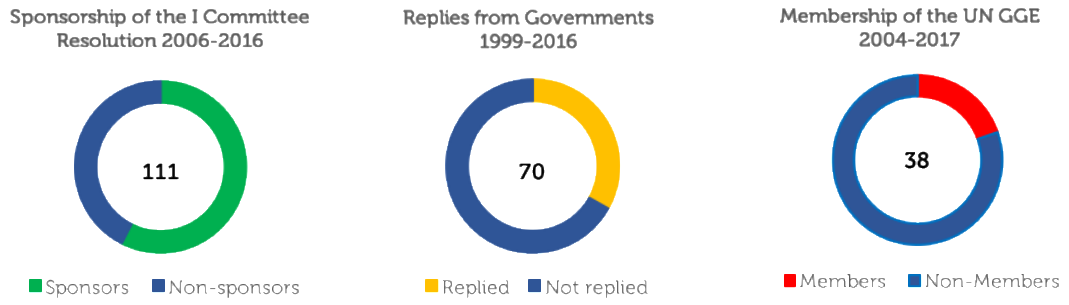


Illustration 4. Support to various elements of the First Committee process. Authors' compilation based on UN data.

[94] Notably Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. (Cambridge: CUP, 2013); and Michael N. Schmitt (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: CUP, 2017). Note not only that that the contributing authors of the Tallinn Manual differ in their views on specific concepts and rules of international law, but also that, between intervening years the two publications, views on some aspects of international law have changed.

[95] A thorough review of scholarly positions is beyond the scope of this analysis. However, Ambassador Kriangsak Kittichaisaree, one of the authors of the Tallinn Manual 2.0, published his partially dissenting views on international law and cyber security shortly after 2.0 edition was released. See Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Cham: Springer, 2017).

[96] Eneken Tikk, "Will Consequences Deepen Differences about International Law,“ *Temple International and Comparative Law Journal,* forthcoming 2019 (still forthcoming, being there for almost year now, it will be either 1 (2018) or 1(2019)..), for a 2017 intragovernmental seminar on the "Policy of consequences."

[97] See references and overview of the submissions in Annex A and sponsorship in Annex C.

[98] Analysis of national views contradicts the claim of some of the Tallinn Manual contributors that "all of us understand international law the same way," shared at 2.0 launches as well as several dedicated workshops. However, they confirm the findings of Professor Anthea Roberts in her recent book, *Is International Law International?* (Oxford: OUP, 2017)).

[99] See Annex B for an overview of national submissions in the First Committee process. Notice the Australian National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 and the Foreign Influence Transparency Scheme Bill 2017 introduced to the House of Representatives on 7 December 2017, which took a determined stand against "espionage and foreign interference activity against Australian interests."

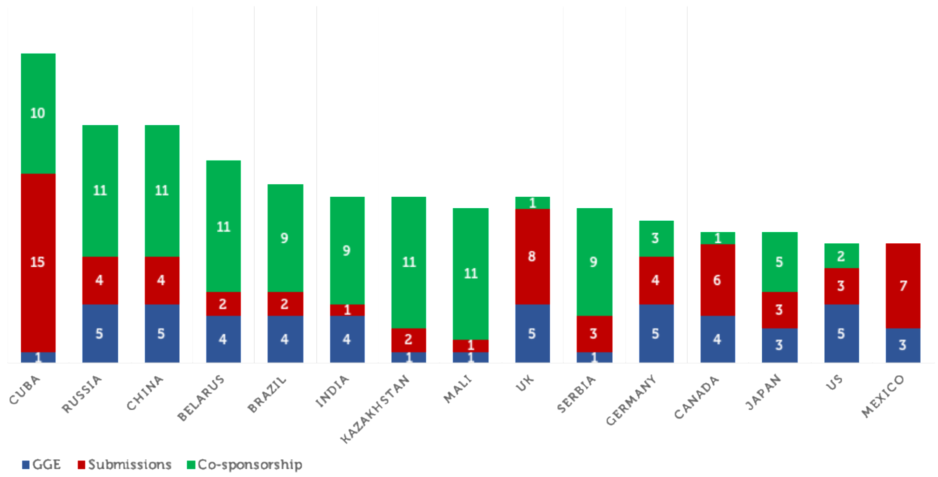


Illustration 5. The most active countries in the First Committee process, by UN GGE participation, national submissions and co-sponsoring respective resolutions. Authors' compilation, based on UN data.

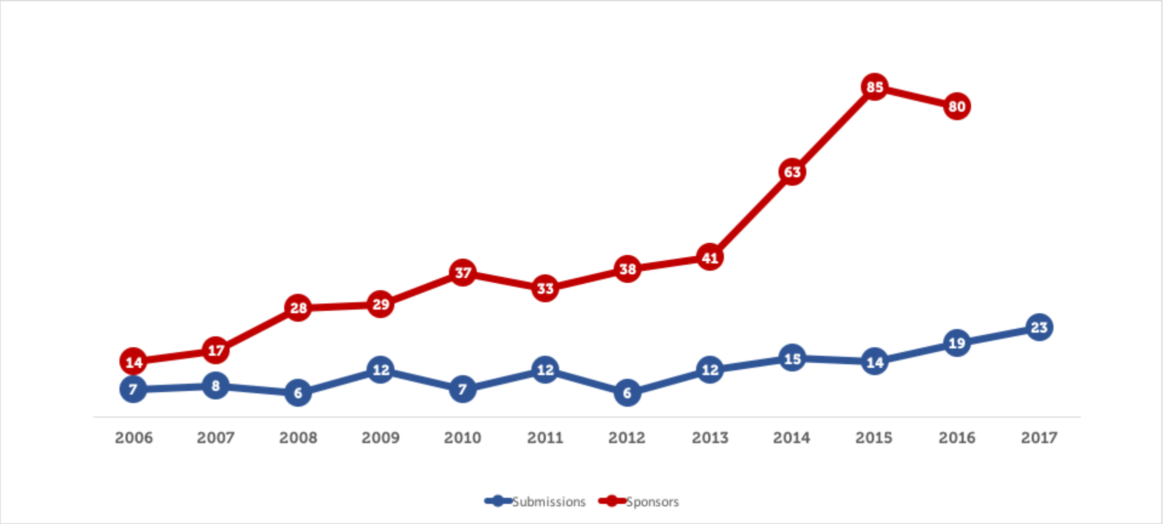


Illustration 6. Sponsorship of the resolution and the number of yearly national submissions. Authors' compilation, based on UN data.

Methodological Challenges

Attempting to edit away and mitigate the irreconcilable differences, experts within the UN GGE faced considerable methodological challenges. These have concerned the acknowledgement, and perhaps even the understanding, of underlying assumptions—in particular, the meaning and use of terms and concepts involved as well as the logic and relationship between them. Freedom in the usage of words and disregard of theoretical models may be advantageous to diplomats/negotiators seeking to promote the interests of their own capitals. In the UN GGE setting, this has led to the absence of clarity on "content of the concepts" that UNGA Resolutions had requested the UN GGEs to define.[100]

Disregard of the Hierarchy and Logic of Norms, Rules and Principles

In bundling the concepts of norms, rules and principles in the context of recommendations for voluntary and non-binding guidance for state behavior, UN GGE members created an inevitably confusing language.[101] Although directed at increasing clarity and predictability of affairs, these concepts have a logical hierarchy. Norms, rules and principles (or principles, norms and rules, to be more accurate) operate at different levels of abstraction.

According to Krasner, principles are beliefs of fact, causation and rectitude.[102] Principles refer to politically, administratively and morally anchored assumptions of the state of affairs, and provide the foundation for more explicit rules and reasoning.[103] As noted, leading actors differ in their views on fundamental questions related to the development and use of ICTs. Exploring shared principles that are not contingent on, or conditioned by, any particular group identity could help implementation of the recommendations on, and the reading of, norms. As an example, take traffic rules: Australia, Malaysia and the UK drive on the left, unless most other countries today; similarly, countries around the world practice differing standard speed limits. Nonetheless, there is fundamental and universal agreement that road traffic for the sake of safe and smooth flow needs to be regulated and that speed limits are necessary, for instance, in densely populated areas.

Norms are difficult to define and agree on unless they are properly contextualized and anchored in a set of underlying (or guiding) principles. A principle-oriented thread of the international cybersecurity discourse could serve to clarify the path. While it may as yet be premature to try to formulate an exhaustive list of overarching principles for international information security, some

[100] UNGA, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/58/32 (2003); A/RES/60/45 (2005); A/RES/66/24 (December 2011); A/RES/68/243 (December 2013); and A/RES/70/237 (December 2015).

[101] It is essential to distinguish between norms, rules and principles, as they differ in level of abstraction and normative cause. In the international cyber-security discourse, it is widely accepted that the cyber activities of states are governed by a loosely coupled set of regimes (Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities,* Global Commission on Internet Governance, Paper Series No.1 (May 2014)). Nye adopts Krasner's definition of a regime, as consisting of principles, norms, rules, and decision-making procedures around which expectations converge in a given issue area (Krasner, pp. 185–205; on regimes p. 185; on norms, rules, and principles, p. 186.). In Krasner's explanation, principles refer to beliefs of fact, causation and rectitude, whereas norms are standards of behavior defined in terms of rights and obligations. Rules, according to Krasner, are specific prescriptions or proscriptions concerning action. For a more detailed discussion of the recommendations made in the 2015 GGE report, see Tikk (ed.) (2017) *A Commentary.*

[102] See Krasner, p. 202.

[103] Charles T. Kotuby Jr. and Luke A. Sobota, *General Principles of Law and International Due Process* (Oxford: OUP, 2017), p. 19.

directions could be considered. To support their absolutist reading of the prohibition of use of force, Russia and China recently reaffirmed the *principle* that states shall refrain from the threat or use of force in violation of the UN Charter.[104] Another useful framing direction for audiences of the work of the GGE could be to re-emphasize that nothing in the Group's work should be read as undermining international law. There might be space for concluding that efforts at international cybersecurity are necessary to support a trusted and functioning ICT infrastructure. Furthermore, despite political differences, almost all states seem to recognize the value of a more predictable and stable state of international cyber- affairs, as well as the rule of law.[105]

Krasner defines norms, seen from an international law perspective, as expectations of behavior defined in terms of rights and obligations.[106] Unless agreed goals at the principle level can be resolved, such rights and obligations may be interpreted with very different assumptions and goals in mind. Shannon observes that the more parameters a norm possesses and the more abstract those parameters are, the easier will it be for the actors to interpret them favorably to their particular interests.[107] This is an essential observation with regard to accepting, and implementing, the recommendations of the UN GGE.

A superficial reading of the UN GGE 2015 report would indicate that it identifies new norms of responsible state behavior in the use of ICTs. However, the structure of paragraph 13 does not clarify which of the recommendations are construed as norms, which as rules, and which as principles. Furthermore, the 'norms' in paragraph 13 are not new, nor are they norms: they are in fact recommendations as to norms, rules or principles. Some of them derive from areas of international law that did not achieve expert consensus as being fully settled as binding obligations. Others open up themes and issues where it was felt that additional norms needed to be developed. Still others add emphasis to pre-existing norms to be followed in the context of international information security. Most importantly, these normative sentences must first be accepted as norms, in order for them to be implemented.[108]

[104] The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law, June 25, 2016.

[105] Mika Kerttunen, "National Cyber Security Strategies. A Normative Reading" (Tartu: Cyber Policy Institute, forthcoming 2018).

[106] See Krasner, p. 202.

[107] Vaughn P. Shannon, "Norms Are What States Make of Them: The Political Psychology of Norm Violation." *International Studies Quarterly* 44 (2000), pp. 293–316.

[108] It should be noted that not even the UN GGE participant states have explicitly taken up these recommendations in their national cyber or information security policies and strategies.

Questions of Application of Social Norms Theory

Mixing legal and political science readings of “norms” in the discourse on responsible state behavior is unfortunate.[109] The inconsistency in use of terms and concepts in the UN GGE mandates and reports has created profound confusion, and highly differing assumptions, among observers of the process. As a result, the impact and implications of the UN GGE reports have been interpreted in various ways and created varying expectations.

In sociology and political science, “norms” are usually seen as collective expectations as to the proper behavior of actors with a given identity.[110] However, applying the sociological norms theory to the exercise of state interests is problematic in the context of national security, as observed by Katzenstein.[111] In particular, the premise of “given identity” may have been beyond reach in the UN GGE discussions, for reasons discussed above. Wendt also notes that the international system is not a very “social” place, which in turn makes constructivism difficult.[112] Ironically, what seems to be shared among the participating states is a strong belief in their own sovereignty and the possession of contingent interests. The outcome of the 2016/2017 GGE underscores that states are much more autonomous of the social system in which they are embedded than are individuals.

Without supranational authority and clear alignment of interests, states remain, by definition, solitary actors—not incompetent to cooperate, but making any decisions to do so primarily on the basis of their own priorities and interests. The 2016/2017 GGE was unable to provide a superstructure for identifying, let alone agreeing, on such shared interests. Such a superstructure would be easier to detect, or create, in entities and organizations like the EU, NATO, SCO, or ASEAN, where states have previously agreed on agendas, structures and mechanisms, even principles, seen as supporting their interests, expectations and applicable remedies.

State behavior is not only norms-driven, at least not driven by *voluntary norms*: it is also affected by ideological, administrative and individual interests, some more durable, some petty.[113] The analogy often applied in this context, between ‘table manners’ and state behavior, escapes the aforementioned considerations. This assumption of and relationship between social pressure and international dynamics is problematic. According to the very (social) definition of norm, the social forces that cause normative change obviously operate more strongly at national and regional levels as well as within groups of similar value systems than universally.

[109] See, for instance, Michael N. Schmitt and Liis Vihul, *The Nature of International Law Cyber Norms* , Tallinn Paper No. 5 (Tallinn: CCD COE, 2015).

[110] See in particular Katzenstein 1996.

[111] Katzenstein, “Introduction,” and especially note 12. Katzenstein’s study offers a sociological perspective on the politics of national security.

[112] Alexander Wendt, *Social Theory of International Politics* (Cambridge: CUP, 1999), p. 2

[113] Cf. April Barton, "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution" *Washington University Law Review* 78 (1), 2000, where the focus on cyber norms is strictly on community-level development and convergence of cyber norms and traditional social norms.

Given the immature understanding of what cybersecurity is all about, and how it can or may affect international peace and security, it is hard to see how the necessary level of peer pressure can emerge among 193 actors with (justifiably) sovereign interests and authority. The application of social norms theory to state behavior may easily disregard the actual political processes whereby decisions and policies are formulated and implemented. As Wendt observes, "reducing norms and rules to patterned behavior makes it difficult to distinguish behavior that is norm-governed from behavior which is not, and this undermines the point of talking about norms, rules, and thus socialization in the first place."[114]

Unclear Relationship Between Norms and International Law

When norms are to be detached and kept separated from discussions of international law, this should be done in a manner that avoids confusion as to the status and definition of "norms." Although the Group has underscored the voluntary and non-binding status of the 2015 recommendations, there have been calls for their "universalization." The expectation of "universalization" through implementation could be seen as creating the potential for a treaty or a desire to clarify customary law. This reading, however, runs contrary to the current principal stands of the USA and aligned cyber- powers. A more correct reading, therefore, is that the words "non-binding" and "voluntary" express exactly the normative status that the sentences in para 13 are intended to have. The Group's inconsistency with the normative status of recommendations becomes problematic, for instance, for those who view state responsibility and due diligence obligations as legally binding.

It seems fair to conclude that the Group has either worked without clear conceptual foundations or has knowingly dismissed the need for methodological vigor and consistency in its work. The absence of commonly accepted topology, lexicon and definitions has remained an impediment and challenge to a constructive dialog ever since the first UN GGE. The Group's inconsistency in its use of the terms "norms, rules and principles" may have added to difficulty in achieving consensus. With their erratic treatment of "norms," the 2013 and 2015 GGE reports may have set overly high expectations as to further agreement and understanding. On the other hand, the facilitating language of the Group has encouraged several events and forums to pick up the theme of cybernorms, in hopes of enhancing and informing further discussion on the topic, as well as the implementation of the Experts' recommendations. [115]

[114] Wendt, p. 101. He continues: "Dogs engage in patterned behavior, but we do not call it norm-governed nor its result a society. Why do so with the patterned behavior of states?"

[115] Several of them were mentioned in the introduction. The SCO countries have since 2011 circulated an international code of conduct for information security as an annex to their letter to the Secretary-General, in their view reflecting the emerging consensus among the international community. See Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the UN Secretary-General (UN A/69/723). See also Smith, *op.cit.* See further the Global Commission on the Stability of Cyberspace, co-hosted by The Netherlands and Singapore to develop proposals for norms and policies to enhance

Procedural Complications

A GGE outcome is conditioned by several factors: the dynamics of the Group, the working methods adopted, the overall political climate, as well as the individual red lines, and diplomatic abilities, of the participants. Failures often build on misunderstanding, misperception or bad leadership. They may concern the procedure at hand or be more conceptual in nature.

The 2014/2015 GGE has been read as the most progressive and productive of the GGEs. For the public, it contributed a set of voluntary, non-binding norms, opened up a more than marginal discussion and offered the prospect of further insertions. The "like-minded" rushed to advertise this achievement, reading from it the applicability of the right to self-defense and international humanitarian law.[116] Russia, however, has interpreted the 2015 outcome as a testament of the need for additional norms, rules and principles, and thus as evidence of the inadequacy of existing international law.[117] However, as discussed, the balance in the UN GGE process was optimal in the 2013 report.

The Groups of 2014/2015 and 2016/2017 were convened with scant intervals. This might have resulted in insufficient time to coordinate and consolidate views on the matter. Also, from the original 15 experts, the 2014/2015 Group was increased to 20, and the 2016/2017 process involved 25 experts (see Annex B). This may have entailed qualitative and quantitative challenges in organizing the work. The GGEs normally conduct four week-long sessions over a period of eleven months. With 25 participating countries, discussions may easily become repetitive and prolonged.

A move to satisfy the curiosity of states, and the request for greater inclusiveness, may have also undermined the process. With 15 members, the UN GGE had provided a more controlled environment for strategic dialog among the leading cyberpowers, with marginal oversight from other countries. A group of 25 is a very different matter: much less predictable and manageable, bringing to the table expectations that the forum is unable, and unfit, to satisfy. Compromise language needs to accommodate very different worldviews, legal concerns, implementation considerations and other points raised by members of the Group. Here, the imperatives of expertise and national representation may well collide.

Although the mandate of the UN GGE is set by the UNGA, it becomes another procedural matter in and during the Group's discussions. Especially the 2015 report indicates that the Group has

international security and stability and guide responsible state and non-state behavior in cyberspace (see https://cyberstability.org/).

[116] Michele G. Markoff, "Advancing Norms of Responsible State Behavior in Cyberspace," US State Department blog (9 June 2015) Available until 2017 at http://2007-2017-blogs.state.gov/stories/2015/07/09/advancing-norms-responsible-state-behavior-cyberspace. html.

[117] See the (incomplete) translation of Ambassador Krutskikh's comments to the Russian newspaper *Kommersant*, https://www.csis.org/blogs/strategic-technologies-blog/russian-newspaper-kommersant-interviews-special-representative. See also Yelena Chernenko, "Global cybersecurity: 6 questions on the key issues as seen from Moscow," https://www.rbth.com/international/2015/08/19/global_cybersecurity_6_questions_on_the_key_issues_as_seen_from_48615.html.

interpreted its mandate quite broadly. This might have been an essential factor in the high expectations for even more normative guidance. Notably, the Group has not been able to create visible links between its perception of cyber-threats to international peace and security, and corresponding measures to be taken by the international community. The emphasized focus on “peacetime” norms since 2015 may, on the one hand, be read as yielding to the Russian and Chinese preference for peaceful settlement of disputes—or it may reflect the lack of sufficient “conflict” substance in international cyber-affairs.

Further considerations

Regardless of the fate of the UN GGE itself, the Group’s reports have provided fertile ground for contributions from industry, academia and non-participating states.

While the 2013 and 2015 GGE reports did not specify the relationship with or the role of the private sector in international cybersecurity, they acknowledged that such a relationship exists, or should be established. The 2015 report concludes: “while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.” This opening creates a good opportunity for the private sector to contribute its views and proposals to the process. It also makes clear the need to allocate responsibility and accountability for cybersecurity issues more broadly than to governments.

The relationship between the UN GGE recommendations and pre-existing norms and rules requires further clarification. Instruments that states have deemed relevant in the context of international information security include the OECD Guidelines for the Security of Information Systems,[118] the Budapest Convention[119] and ITU ITRs.[120] The ongoing EU cybersecurity reform, which combines significant developments in network and information security,[121] personal data

[118] Mentioned by Australia in 1999 08 UN Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213). Adopted in 2002, the OSCE Guidelines establish a framework of principles, applicable to all participants, to enhance the security of information systems and networks in order to foster economic prosperity and social development. In 2012, the OECD initiated the review of these Guidelines. See the November 2012 report "The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy". See http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsaculturеofsecurity.htm.

[119] Council of Europe Treaty No.185, signed November 23, 2001, entered into force July 1, 2004. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[120] International Telecommunication Regulations, Dubai, WCIT-12, Dubai (December 14, 2012). http://www.itu.int/en/wcit-12/Pages/itrs.aspx.

[121] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

protection,[122] cybersecurity[123] and cyber-diplomacy,[124] can offer valuable leads for implementing the UN GGE recommendations. Moreover, studies have identified a significant body or principles, norms and rules that are applicable to various aspects of cybersecurity, and point to the need for thorough study and implementation of pre-existing norms before turning to new normative instruments.[125]

Scholars could also provide additional leads when analyzing the recommendations as to their new contribution, expected outcomes, and the preconditions and support mechanisms for implementation.[126] Furthering the discussion on the understanding and implementation of international law, general differences in interpreting and using international law between states should not be overlooked. A comparative study of international law in the context of cybersecurity might help in dealing with some of the challenging issues that the UN GGE is expected to address.

The strategic pause created by the 2017 no-consensus outcome offers a window of opportunity to develop and enhance national capacities to narrow the digital gap, address everyday cybersecurity issues and reduce perceived insecurities; develop regional normative initiatives that build on shared threats and capabilities; study state and legal practice for a better understanding of the margins of responsible state behavior; and engage industry to develop state and industrial standards of behavior as well as practical steps to raise the level of cybersecurity.

Engagement of civil society and academia will prepare the international community for what lies ahead: a continued push for a convention that would refine state power and international security in cyberspace, creating much-sought *predictability* of affairs.[127] Whether this push will lead to actual treaty negotiations is uncertain. However, it will make it incumbent upon every state to have an informed position on the matter. States should form and express their views about the implementation of international law, as well as the potential need for *lex specialis*.

The questioned, yet prevalent, combining of social norms theory with state behavior emphasizes the leading role of national strategies, policies and regulatory approaches in identifying, comparing and promoting international norms. To date, some 80 countries are reported to have developed

[122] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[123] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.

[124] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), adopted June 7, 2017. http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

[125] See Eneken Tikk, "Future Normative Challenges," in Paul Cornish (Ed.) *Handbook on Cybersecurity* (Oxford: OUP, forthcoming 2019).

[126] Eneken Tikk offers a ten-step schema, a "norms test," for evaluating the need to expand the scope of norm proposals. See Eneken Tikk, op.cit.

[127] See Illustration 3 explaining the international cyberpolicy goals and instruments of the Russian Federation.

national cybersecurity strategies,[128] although the call for a strategy could be an emerging norm of its own.[129]

While the GGE format itself is unable to accommodate larger participation, individual experts and participating states could arrange regional discussions and contribute their points of view by written submissions in the underlying First Committee process. Close to 70 states have already shared their experience and views on ways to mitigate risks to peace and security stemming from state use of ICTs.[130] National undertakings and experiences in providing international cybersecurity and stability are questions of practical importance, and can help to promote mutual understanding and more widely accepted standards of behavior.

On the other hand, national experience might reveal what could have constituted another choking factor in the 2016/2017 dialog. Albeit costly and serious at the national, corporate and individual levels, (very) few cybersecurity problems have become direct issues of international peace and security. Some countries doubt the existentiality of threats posed by uses of ICTs that both Russia and the USA have forcefully advertised. In the UN GGE's own language, the indicated international cyber-threat leans heavily on hypotheticals. Despite extensive examination of ICTs as a threat, the Group may not have succeeded in making the case for securitizing the development and use of ICTs as a matter of international security.

Indeed, cyber-incident and risk assessments indicate more than state-on-state hostilities. More than indicating the potential of cyber-war and warfare, data breaches, website defacements, increasing cybercrime and botnet topologies, testify to a cyber-crisis surface where the risk of unwanted or unforeseen developments cannot be effectively prevented, due to low awareness or obvious capacity gaps. Therefore, the UN GGE has, without necessarily meaning to, developed at least two separate agendas of international cybersecurity: one that can be understood and explained in terms of traditional geopolitics and where the likelihood of conflict/no conflict does not depend significantly on ICTs as such. Absent ICTs, the relationships between the USA, China, Russia, Iran and North Korea remain largely the same. What geopolitics cannot exhaustively satisfactorily is the surface of *potential* cyber-crisis that has emerged with the extensive adoption of ICTs across the world, without due recognition of the accompanying risks and means of mitigation. Jumping onto the international information highway has come too fast, too soon, for countries that are not able to run sustainable information systems and services: states that have must run on Windows XP cannot be helped by any of the UN GGE recommendations.

[128] Kerttunen, "National Cyber Security Strategies" (forthcoming 2018).

[129] The need for a national cybersecurity strategy required under the African Union Convention on Cyber Security and Personal Data Protection (Article 24 (2)) and the EU NIS Directive (Article 2a).

[130] See Annex D.

Also, despite the cyberthreat mantra, the UN Security Council has not once examined cybersecurity as a threat to international peace and security. However, the UN First Committee remains the most authoritative platform for disarmament and international security issues. Without evidence of cyber-threats that constitute a threat to international peace and security, an 2019/2020 UN GGE would be unlikely to provide actionable guidance to the international community. It will fall upon the next experts to revisit their mandates critically, and convince the international community of the gravity of the threat and the actual need at hand.

Conclusions

None of the findings described in this report should be seen as tolling the death-knoll for the GGE process. Although the GGE is in critical condition, it is far from extinguished. There are strong proponents of maintaining the process, and the Group is likely to convene again in 2019. Regardless of whether another GGE emerges, the real question is what we have learned from the process so far, and from the 2016/2017 flat-line in particular.

Although the GGE cannot change or create international law, it does flag important considerations for further discussion. There exists scant established state practice with regard to the use of ICTs, let alone broad consensus on normative standards of behavior in the context of ICTs. States holding strong views on international law will try to convince the rest of the international community to side with them. Attempts to socialize undecided or uninformed states are likely to result in even stronger counter-narratives and stands. While there is an urgent need for better understanding of how international law can be applied to uses of ICTs, there is an even more pressing need for thorough and critical study of existing international law. It is clear from the reading of the views and positions expressed in and on the margins of the GGE that there are at least potential gaps in international law that could permit the development and use of ICTs in destabilizing or even hostile ways.

Where effective norms cannot be negotiated, their existence and the need for them could be traced and observed in state behavior. There are many examples of cynical exploitation, by various states, of perceived gaps or vagueness in international law. There is also evidence of calculated inability, or refusal, of victim states to invoke international law in their defense, despite scholarly enthusiasm for legal remedies. Whether is acceptable for states taking refuge in existing legal principles to be given the widest freedom of behavior is a highly pressing issue, a question that requires an answer from every sovereign nation.

The USA and the like-minded states want current international law to be endorsed and, perhaps, somewhat clarified by the GGE, and have encouraged national statements on this account. The Sino–Russo coalition is likely to push for *lex specialis*, for example by gradually strengthening the normative status of the Group's recommendations. However, both sides need to offer more convincing evidence to substantiate their arguments and propositions.

There is a potentially high price to pay for the lack of conceptual and methodical coherence in the international discourse on cybernorms. Without a structured and framed dialog between states, any guidance to the international community is made subject to competing interpretations, and may become meaningless. Failure to assign the right meaning and weight to facts, to identify the factors of causality in cybersecurity issues, and to define appropriate remedies, is likely to prolong the search for shared understanding and agreement.

It is essential that the GGE no-outcome should be interpreted, not as leaving the world in the dark, but as showing that additional light needs to be shed on how to maintain international peace and security in the context of technological development. The GGE is not the highest authority to tell states what to do and what not to do in cyberspace. There are other instances, such as existing international law and responsible state practices. The speed at which the international community can create effective remedies to international cybersecurity issues, need not be dictated by experts. Useful guidance for the way forward can be found in the 1999 US submission: the international community must do a substantial amount of systematic thinking before going further. To this end, member states should seek ideas and insights from a broad range of experts in their respective governments and societies.[131]

In accepting, for the purpose of argument, that there is a threat to international peace and security resulting from uses of ICTs, one should also note that the main actors in any such potential conflict are longstanding members of the UN GGEs. Therefore, actual implementation of the Group's guidance, even if only by states represented in the UN GGE, would significantly reduce the risk of the feared cyber-conflict. The time is indeed ripe for analysis of state behavior and leadership.

In the meantime, the Russian Federation appears to have a clear end-state and end-game in mind. Its policy documents and initiatives promote an "international information security system" where a global treaty and international agency are the focal points. To reach that end-zone, Russia is gathering the Shanghai Cooperation Organization and the BRICS countries under a reviewed *Code of Conduct*.[132]

In the light of the above, there is space in the international cybersecurity dialog for another GGE, as well as other formats and venues. What has been missing is an independent, neutral platform that could serve as a "glue" between the various initiatives and agendas, focusing on less politicized reading of views and progress, and ready to offer guidance and advice to and between these agendas and initiatives.

Epilog: The Roadmap

If we were to side with those who believe that the UN GGE is gone, never to return, it would be useful to consider where that would leave us. As the search for accepted standards of responsible state behavior in cyberspace continues, we should note one essential contribution that the UN GGE

[131] A/54/213.

[132] See Yelena Chernenko, "К кибербезопасности подошли с трех сторон," *(Cybersecurity approached from three sides),* https://www.kommersant.ru/doc/3496533.

has made, regardless of the political controversies. A pragmatic reading of the Groups' reports reveals that, in a relatively short period of time, the experts have constructed a roadmap that any country, regardless of its political system or capacity level, will find useful in developing a basic understanding and awareness of the requirements and means of international cybersecurity.

All the drama around the UN GGE aside, the GGE process, and the 2014–2015 Group in particular, has delivered highly useful and meaningful guidance. By designing a global-scale information security management program, the 2014–2015 GGE has provided good clues to achieving world peace.

For the purpose of introducing the roadmap, we may set aside the controversial classification of norms, rules, principles and confidence-building measures discussed above. As Table 1 shows, the Groups have provided clarifications and guidance on upholding the rule of law in the context of state uses of ICTs; and on exchange of national views and information, critical infrastructure protection as well as incident prevention and mitigation. These leads and recommendations are actionableand can serve as guidance for national, regional and further international engagement.

Drawing on the three GGE reports, states should be able to contextualize and prioritize the recommendations and guidelines in light of their own national cybersecurity issues and situation. Although hardly any country is in a position (or has the need) to implement the whole roadmap at once, its guidance is applicable to national cybersecurity strategy and legislation processes. Supporting it as a framework for thinking and further discussion would duly acknowledge the work of the UN GGE work and its outcomes.

There is only one "but" attached to this achievement. What the UN GGE has called states to do cannot be brought about by foreign ministries or defense organizations. The measures recommended by the GGE consistently target computer emergency-response organizations, IT and ICT ministries and government CISOs. This means it will be necessary to channel the Group's guidance not merely to the national capitals, but from the politico-military domain to the national ICT authorities.

In Table 1, the UN GGE key findings and recommendations are combined with guidance of the Organization for Security and Cooperation in Europe (OSCE). The Table is meant to provide a one-stop overview of tangible and feasible guidance that addresses security concerns in international cooperation. In these times of disputes, norm-crafting and doomsday speeches and books,[133] such an approach should be applauded and promoted.

[133] As this report was being finalized yet another such book was published: David E. Sanger's aptly titled *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Penguin Random House, 2018) on how "the rise of cyberweapons transformed geopolitics like nothing since the invention of the atomic bomb." This premise, if not totally fake – which it probably is – sings the music of doom that the Kremlin and the Western cybersecurity industry like to hear.

OSCE and GGE International Cyber Security Roadmap

	OSCE[134]	GGE[135]	2016/2017 GGE Chairman's Impressions
Upholding and developing the rule of law	Have in place modern and effective national legislation to facilitate exchange and cooperation #6	Establish/provide 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 (2015, ¶16 d i)	
		States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (2015, ¶13 c)	An official notification from one State to another State should be regarded as providing the notified State with actual knowledge of the alleged activity. The notified State should acknowledge receipt of the request via the relevant national point of contact. On becoming aware of malicious ICT activities within or transiting through ICT systems located on their territory and that are likely to affect another State adversely, States should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease. A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates. If the State knows the malicious ICT activity is transiting through its territory and is able to identify the State from which it is originating, it may choose to notify that State instead of, or in addition to, seeking assistance from other States. It is understood that notifying a State does not imply responsibility of the notified State for the incident.
		States should respect resolutions on the promotion, protection and enjoyment of	Experts underscored that States should recognize that personal data held on, transmitted through or processed by ICTs can have a profound impact on life and security. States should take appropriate

[134] Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202, 10 March 2016.

[135] UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, A/68/98 (24 June 2013,), paras 22, 24, 25 and 26); and Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, A/70/174 (22 July 2015), paras 13, 16 and 17.

		human rights on the Internet (2015, ¶13 e)	steps to protect personal data, including its confidentiality, integrity, accessibility and authenticity, while respecting relevant international, legal human rights instruments.
Cooperation and assistance		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 (2015, ¶13 a)	Managing and mitigating ICT-related incidents in an effective and timely manner requires cooperation among States and between States and other stakeholders, as well as measures to enable it.
		States should consider how to best cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats (2015, ¶13 d)	To support implementation of this norm, experts proposed that States support the work of the UN Commission on Crime Prevention and Criminal Justice and its on-going efforts to study, in a comprehensive manner, the problem of cybercrime.
		States should intensify cooperation against criminal and terrorist use of ICTs, harmonize legal approaches, and strengthen practical collaboration between law enforcement and prosecutorial agencies (2013, ¶22)	
		Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory (2015, ¶17 e)	
		Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions (2013, ¶26 f)	

	Facilitate cooperation between authorized authorities responsible for securing critical infrastructures #15	Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely on ICT-enabled industrial control systems, including guidelines and best practices among States against disruptions perpetrated by non-State actors (2013, ¶26 e)	
		States should respond to appropriate requests for assistance by another State whose Critical Infrastructure is subject to malicious ICT acts (2015, ¶13 h)	Experts discussed that a State receiving an appropriate request for assistance following an ICT incident should: acknowledge receipt of the request via the relevant national point of contact; determine, in a timely fashion, whether it has the capacity and resources to provide the assistance requested and respond; in its initial response, indicate the nature, scope and terms of the assistance that might be provided, including a timeframe for its delivery; and in the event that assistance is agreed upon, promptly provide the arranged assistance.
		Establish focal points and cooperation for the provision of assistance in investigations (2015, ¶17 b)	
Exchange of views and information	National views of national and international threats #1	Voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs (2015, ¶16 c)	
	Information in relation with security of and in the use of ICTs #2	Voluntary sharing of national views and information on vulnerabilities and identified harmful functions in ICT products (2015, ¶16 c)	Publicly communicate elements of approaches to the use of ICT capabilities.
	Measures that States have taken to ensure an open, interoperable, secure, and reliable Internet #4	Prevent practices that are acknowledged to be harmful or that may pose threats to international peace and security (2015, ¶13 a)	Experts suggested that States consider sharing information on best practices for protecting critical infrastructures, including on: baseline security requirements; Incident notification procedures; Incident handling tools and methodologies; Emergency resilience; and lessons learned from previous incidents.
	Effective responses to threats to and in	Establish focal points and cooperation for the exchange	

	the use of ICTs #5	of information on malicious ICT use (2015, ¶17 b)	
	Best practices, awareness-raising, information on capacity-building #5	Voluntary sharing of national views and information on best practices for ICT security (2015, ¶16 c)	Experts felt States should be encouraged to raise awareness among senior decisionmakers across all branches of government as well as diplomatic personnel on the recommendations of the GGEs and the importance of CBMs to the maintenance of international peace and security. Results could be achieved by involving a wide variety of national representatives in activities that enhance practical understanding of the issues.
	Information on national organization; strategies; policies and programs—including on cooperation between the public and the private sector #7	Voluntary sharing of national views and information on national organizations, strategies, policies and programs relevant to ICT security (2015, ¶16 c) (2013, ¶26 a)	Use existing mechanisms, including the UN Secretary-General's annual report on developments in the field of ICTs in the context of international security, other opportunities as well as relevant international and regional organizations and forums to report on national implementation of CBMs and to exchange information and experiences.
	Provide a list of national terminology: terms and definitions or explanations #9		
	Exchanges in different formats: workshops, seminars, roundtables at regional and sub-regional level, to investigate further areas for cooperation #12	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 (2013, ¶26 b)	
		Enhanced sharing of information on ICT security incidents, involving the more effective use of existing channels or the development of new channels and mechanisms to receive, collect, analyze and share information related to ICT	In order to facilitate notification and exchanges of information on incidents, and to support implementation of measures relating to the classification of ICT incidents, develop voluntary arrangements, such as standard incident severity schemas; encourage sharing of and participation in activities, including exercises relating to these and other voluntary incident classification

		incidents, for timely response, recovery and mitigation actions (2013, ¶26 c)	arrangements, through appropriate international, regional, sub-regional and bilateral forums.
	Consultations to reduce the risks of misperception, and possible emergence of pol-mil tension or conflict #3	The development of and support for mechanisms and processes for bilateral, regional, sub-regional and multilateral consultations to enhance inter-State confidence-building and reduce the risk of misperception, escalation and conflict that may stem from ICT incidents (2015, ¶16 b)	
Critical infrastructure	To protect critical national and international ICT infrastructures, including their integrity #3	A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages CI or otherwise impairs the use and operations of CI to provide services to the public (13 f)	Recommendations that States consider the potentially harmful effects of their ICT activities on the general functionality of global ICT systems and the essential services that rely on them.
		Voluntary provision of national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national-level laws and policies for the protection of data and ICT-enabled infrastructure (2015, ¶16 d)	
		States should seek to facilitate cross-border cooperation to address CI vulnerabilities that transcend national borders (2015, ¶16 d)	
		States should take appropriate measures to protect their CI from ICT threats (2015, ¶13 g)	Experts also suggested that States should participate in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of national and cross-border critical infrastructure against existing and emerging threats.
		The development of technical, legal and diplomatic mechanisms to address ICT-	

		related requests (2015, ¶16 d iii)	
		The adoption of 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 about incidents (2015, ¶16 d iv)	
		Consider categorizing CERT as critical infrastructure (2015, ¶17 c)	
Incident prevention and handling	Measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level #8	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 (2015, ¶13b)	States should give consideration to establishing the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of serious ICT incidents and to determine appropriate responses. Once those structures and processes are in place, States should develop JCT incident assessment or severity templates to evaluate and assess ICT incidents. Wherever possible, the templates should be in line with existing practices and avoid duplication.
		Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents (2015, ¶17 a)	
	Nominating contact points to facilitate communications and dialog #8	States should 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 (2015, ¶13 h)	Given the varied and distributed nature of critical infrastructure ownership, experts felt that States should promote, in consultation with the relevant stakeholders, minimum standards for the security of critical infrastructures and promote cooperation with the private sector, academia and the technical community in critical infrastructure protection efforts.
		The development of mechanisms and processes for consultations on the protection of ICT-enabled CI (2015, ¶16 d ii)	
Computer Emergency Response		Establish a national computer emergency response team and/or cybersecurity incident response team or officially	

		designate an organization to fulfil this role (2015, ¶17 c)	
		Identify appropriate points of contact at the policy and technical levels to address serious ICT incidents (2015, ¶16 a)	Implement the measure relating to the identification of appropriate points of contact (2015 GGE report ¶16(a)) at both the policy and technical levels to address serious ICT incidents and create a directory of such contacts that can be shared bilaterally, regionally or at the global level. Systematize and exercise the use of such points of contact at both the policy and technical levels, and develop guidance on the expected roles and responsibilities of points of contact.
		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 (2013, ¶26 c)	
	Provide and update contact data of national structures that manage ICT-related incidents and coordinate responses #8	Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, 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 (2015, ¶17 d)	
		States should not conduct or knowingly support activity to harm the information systems of authorized emergency response teams of another State. A State should not use authorized emergency response teams to engage in malicious international activity (2015, ¶13 k)	
		Exchanges of information and communication between national CERTs bilaterally, within CERT communities, and	

		other forums, to support dialog at political and policy levels (2013, ¶26 d)	
Integrity of the supply chain		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 (2015, ¶13 i)	Take steps, including through existing forums, to prevent the proliferation of malicious ICT tools and techniques. In doing so, States should encourage the legitimate activities of research communities, academia, industry, law enforcement, CERTs/ CSIRRTs and other ICT protection agencies in ensuring the security of their ICT systems. Take steps to prevent non-State actors, including the private sector, from conducting malicious ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory. Take steps to prevent non-state actors, including the private sector, from using harmful hidden functions for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory.
		States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (2015, ¶13 i 2)	Identify trust-building measures that can help allay concerns about harmful hidden functions in ICT products, encouraging the private sector and civil society to play an appropriate role to this end.
Reporting of vulnerabilities	Responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and sharing available measures, also with ICT business and industry #16	States should encourage responsible reporting of ICT vulnerabilities (2015, ¶13 j)	Establish national structures that enable a responsible reporting and handling of ICT vulnerabilities; Establish appropriate coordination mechanisms amongst public and private sector entities; Engage in targeted capacity-building to support effective and responsible sharing of ICT vulnerabilities.
		States should share information about available remedies to vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure (2015, ¶13 j 2)	In addition, and to avoid misunderstandings or misinterpretations, including those stemming from non-disclosure of information about potentially harmful ICT vulnerabilities, experts encouraged States to share, to the widest possible extent, technical information on serious JCT incidents. This information could include the indicators of attribution and compromise, the malware and method used and associated

			remedies. Experts felt that States should ensure that such information is handled responsibly and in coordination with other stakeholders, as appropriate.
Role of the private sector, civil society and academia	Promote PPPs #14	States should encourage the private sector and civil society to play and appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services (24)	Encourage research on ICTs in the context of international peace and security, including on methodologies to enhance the technical attribution of ICT incidents.
		State should consider how to best cooperate in implementing the above norms and principles, including the role that may be played by the private sector and civil society organizations (25)	Support policy-relevant and technical research on emerging JCT-related risks and threats.

Table 1. OSCE and GGE International Cyber Security Roadmap, authors' compilation.

PART II: REVELATION

Кто кого ?[136]

Introduction

With all eyes turned towards the USA and China as the powerhouses of economic and technological development, Russia is often regarded as a lesser force in international cybersecurity. Dealings with Russia have alternated between almost-uncritical engagement and highly aggressive reactionary behavior. Especially since the annexation of Crimea, the West has rejected any openings coming from Moscow. Exchanges with Russian scholars and professionals have been deliberately limited.[137] Critical analysis of Russian strategy is scarce.[138]

In treating Russia as the usual suspect, it is easy to miss how, twenty years after first alarming the international community of the threat that ICTs could pose to international peace and security, Russia can demonstrate considerable sympathy to their basic plea examined in the first part of this report. Russia has built a solid partnership with China, gained support from BRICS, the Collective Security Treaty Organization (CSTO), and the Shanghai Cooperation Organization (SCO) as well as considerable attention from the developing countries.[139] The Moscow-

[136] Lenin's question, "The whole question is — who will overtake whom?" (Весь вопрос — кто кого опередит?) at the All-Russian Congress of Political Education Departments, in October 1921, pointing to the class struggle but also to the raging civil war between the Bolsheviks and White Russians (V.I. Lenin in *Lenin Collected Works*, Vol. 33 (1966)). Both Trotsky and Stalin later used the shortened version of the question.

[137] Georgetown University's annual International Conference on Cyber Engagement is a notable exception among Western cybersecurity conferences and workshops. Western governments have abstained from attending the Russian flagship information security conference in Garmisch-Partenkirchen, Germany. In 2015, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) rejected the participation of Russian nationals at its annual conference, referring to the fact that CCD COE had been refused participation at their annual conference for Russian nationals; see NATO Foreign Ministers' Statement of April 1, 2014 (https://www.nato.int/cps/ua/natohq/news_108501.htm).

[138] Notable exceptions include Andrei Soldatov, "Why We Should Care About Russia's Stance on the Internet," *Cyber Dialog 2014,* MUNK School of Global Affairs, University of Toronto; Andrei Soldatov & Irina Borogan, "How Putin Tried to Control the Internet," https://motherboard.vice.com; and Juha Kukkola, Mari Ristolainen & Juha-Pekka Nikkarila, *Game Changer: Structural transformation of cyberspace*, Finnish Defence Research Agency Publication 10 (2017).

[139] For example, the VII BRICS Summit Ufa Declaration (July 9, 2015) concluded that "the use and development of ICTs through international cooperation and

initiated resolution[140] in the UN First Committee has been sponsored by almost 120 states, and has triggered an exchange, involving more than 70 countries, of national views and positions on international cybersecurity.[141] Russian sentiments can be read in Western scholarship and corporate initiatives.[142] Moreover, the once-clear line that the USA had drawn between Internet Governance and international cybersecurity has become blurred with the emergence of the cybersecurity governance sub-discourse.[143] For many, the appeal of a convention is not a matter of control over information: increasingly, it is the necessary predictability and certainty that only rules can provide.

The Kremlin's information-security policy is tailored to national interests and long-term strategy. The Russian configuration of technological independence, political controls and normative guarantees represents an ideal of national strategy and international policy coherence that many states have not been able to achieve. President Putin, Minister Lavrov and Ambassador-at-Large Krutskikh have achieved an impressive alignment of Russia's security aspirations regarding internal and foreign information.

Moreover, while Russian international information-security policy targets Western cyber-capabilities, Moscow has continued to develop and employ advanced electronic warfare capabilities outside of international attention and normative considerations.[144] In other words,

universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and open digital and Internet space." On December 23, 2014, the CSTO member states signed "The protocol of cooperation between CSTO members on countering criminal activity in the information sphere." On June 16, 2009, the SCO members signed "The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security."

[140] UN General Assembly Resolution (1999), Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70.

[141] Eneken Tikk & Mika Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy," Cyber Policy Institute (2017).

[142] See in particular Microsoft's plea, "The need for a Digital Geneva Convention" (Smith, *op.cit*).

[143] On the cybersecurity–internet governance nexus, see the commentary and summaries of IGF 2017; and Georgia Tech School of Public Policy Internet Governance Project, "What is Internet Governance," www.internetgovernance.org..

[144] On Russian EW capacity, see R.N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum" (Tallinn: International Center for Defense and Security, 2017)

the Kremlin has been able to question and compromise the one aspect in the use of ICTs that the West promotes, and that Russia is least interested in developing.

Where the West has had difficulties in advancing, Moscow, together with Beijing, has captured new terrain. This is significant, as the Western-led "cybernorms" campaign can be seen as catering to an even broader community of the treaty-minded. The Kremlin has steered the governing discourse from resilience to international peace and security and has also successfully challenged the Western narrative of the rule of law. While the like-minded are re-framing the international cybersecurity dialog to protect international stability,[145] Moscow and Beijing are already advancing to the next plane.

In sum, Russia has not just maintained, but developed and strengthened, its call for an *international information security system*.[146] Moscow has been persistent and successful in soliciting support for its main demand and proposed measures. The recruitment of CIS, SCO and BRICS all testify to an ever-solidifying move towards technical, legal and political autonomy in cyberspace.[147]

Meanwhile, the West has not managed to convince or engage states beyond its own perimeters.[148] Most importantly, it has been unable to demonstrate the authority of existing international law. Western scholarship, especially within the international cybersecurity discourse, has remained short on methodology, evidence and clear argumentation.

[145] The authors are of the view that focus on stability, although it allows the UN First Committee discourse to better accommodate the "peacetime" dimension of international cybersecurity, presumes the use of ICTs as threat to international peace and security. Moreover, although "stability" refers to the desired outcome of international order and stable and peaceful international life, it also can be used as shorthand for the status quo and domestic repression.

[146] Igor N. Dylevsky, Sergei A. Komov and Sergei V. Korotkov., "The Military Policy of the Russian Federation in the Field of the International Information Security: Regional Aspect," *Voennaia mysl'*, No. 2 (2007); Ministry of Foreign Affairs of the Russian Federation (RU MFA). "Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020" (2013); I.N. Dylevsky *et al.*, "Political and Military Aspects of the Russian Federation's State Policy on International Information Security," *Military Thought*, Volume 24:1 (2015); RU MFA (2017) "Statement of the Deputy Secretary of the Security Council of the Russian Federation Oleg Khramov at the international OSCE conference on cybersecurity."

[147] Kukkola, Ristolainen & Nikkarila, *Game Changer* (2017).

[148] Although the 2017 Global Conference on Cyberspace (The London Process) was hosted in New Delhi, both India and Pakistan joined the Shanghai Cooperation Organization in 2016, thereby linking regional economic and security aspirations with those of Russia and China.

Instead, it has created a plethora of ideas and mini-agendas that outsiders find hard to follow or relate to.

Whereas Moscow and Beijing are largely immune to Western accusations of cyberattacks and espionage, the normative authority of the like-minded has been affected by leaks of foreign espionage, mass surveillance and especially government expectations of corporate assistance in their efforts. Especially the continuing trend of securitizing ICTs has prevented the Western democracies from achieving full coherence of national approaches.

The Clinton–Gore promise of the free and open world on the shoulders of ICT giants is fading into an illusion. As cyberspace becomes painted with a forbidding palette of threats, liberal democracies engage in wide-scale securitization of ICT affairs. Proliferation of military cyber-capabilities and conduct of below-the-threshold cyber operations is accompanied by deafening silence on the part of international law, enabled by the lack of national cyber-resilience. Strategic contestation over and around ICTs is corroding the world order and making it increasingly difficult to maintain a credible narrative of ICTs as representing a technology of freedom and prosperity.

Obviously, the West needs to anticipate further pressure towards a treaty. The question becomes how to answer to these calls. To effectively counterbalance the Russian moves, the like-minded will need to create credible and actionable support for their rhetoric of a free, open and secure cyberspace.[149] The next logical move for Russia would be to push the contestation to the landscape of freedoms and economic benefits where the end-game is not just the Western world order but also economic significance. The fact that Moscow has both the opportunity and confidence to do so should alert Western thinkers to the importance of reviewing their strategy and upping their game to take the "oxygen input" from the Russian surge.

In order to escape this largely self-inflicted cybersecurity trap, the West needs to play (or appear to be playing) the high cyber-game on terms that fit its own values and objectives. The West seems to have lost the high ground in information-society development it held from the 1990s up until 2007. In particular, the securitization of ICTs at national

[149] While highlighting the endurance and coherence of Russian information-security policy and also being critical to and skeptical of the maneuvers undertaken by the like-minded, our argumentation and conclusions are *not* intended to endorse the direction or content of the Russian policy.

and international levels has become the antithesis of a true information society, not a means to achieve it.[150] Defending and promoting the Western way of life will require making use of the ideals and rationale of the information society. Here the end- game must focus on three fronts: restoring the credibility of the original promise, lifting up international law in more than words, and balancing the governing discourse on peace and security.

The Age of Alignment: From Telecommunications to the Global Culture of Cybersecurity

In 1994, US Vice-President Gore inaugurated the First World Telecommunication Development Conference in Buenos Aires. His opening speech described international telecommunications as the topography on which to build the international information highway. That highway, the USA promised, would bring all the communities of the world together. It would become a metaphor for democracy itself.[151] Not only did this event mark the extraordinary alignment of the USA and ITU, it also sent a clear and logical message: telecommunications are the arteries of the information society. Embracing these technologies would make the world a better place.

In 1994, only 25 million people were online. By 2002, the world online population had risen to 660 million and was growing fast. Concerned with attacks against critical information networks, the USA championed the next logical and sound plea, this time in the UN Second Committee, to provide confidence to users and consumers that the systems and services they use are reliable.[152] For any country to prevent potentially damaging attacks, cybersecurity was to be seen as a global problem, not a solely domestic one, Behind this invitation was a clear and compelling rationale to all states: ICTs were being harnessed as an engine of economic development, growth and social advancement, and, for that potential to materialize, confidence of users and consumers in the security and integrity of the systems was essential. As all countries depended on information technology for the provision of essential goods

[150] Especially since 2010, the Western states have employed an approach whereby international and national cybersecurity are to guarantee free and open cyberspace. On how broad security discretion poses the risk of undermining or even destroying democracy on the grounds of defending it, see, e.g., Klass and others v. Germany, Application no. 5029/71, ECtHR (1978) and Leander v. Sweden, Application no. 9248/81, ECtHR (1987).

[151] "Remarks prepared for delivery by Mr Al Gore," International Telecommunication Union (21 March 1994).

[152] Second Committee, Summary Record A/C.2/57/SR.17 (7 November 2002).

and services, business and financial transactions and government services, all nations bore responsibility for cybersecurity.[153]

Ignoring the Russian call for *international securitization*[154], the George W. Bush administration invoked the responsibility of governments, businesses, organizations and individuals to protect ICT infrastructure and develop a shared, global culture of cybersecurity.[155] In this early chapter of international cybersecurity, there appeared to be a near-perfect division of national and international, state and corporate efforts to provide security in and to an increasingly populated cyberspace. The next ten years, however, would see an entirely new and different approach to cybersecurity emerging.

The Ascent of the First Committee

The Kremlin's unease at the rapid proliferation of ICTs and the freedoms these technologies promised was more a matter of than suspicion and distrust. It was an acknowledgment that it was in Moscow's interest to retain a multi-polar world order with the UN playing the central role in dealing with global challenges and threats.[156] In this Kremlin-projected world order, the development and proliferation of ICTs would not be spontaneous and individualistic, but centralized and governed.

It took time for the rest of the world to comprehend the Russian threat picture. However, after years of relatively fruitless efforts, Moscow suddenly found dozens of countries subscribing to its basic plea that the development and use of ICTs constitute a threat to international peace and security.

One small European state became instrumental to this paradigm shift. Estonia takes pride in having taken the issue of cybersecurity to the awareness of its NATO allies and the international community. Faced with cyberattacks in 2007, Estonian politicians wildly compared such attacks to nuclear explosions, blockades and other military-grade

[153] Ibid.

[154] International securitization refers to a process where state actors a) present and transform issues into questions of security and b) position often originally domestic security concerns as international ones. Securitization usually entails calls for extrajudicial mandates, extraterritorial rights as well as extraordinary measures and resources.

[155] Second Committee, Summary Record A/C.2/57/SR.17 (November 7, 2002).

[156] "Joint Statement of the BRIC Countries' Leaders," Yekaterinburg (June 16, 2009).

vocabulary—rhetoric that also supported Estonia's efforts to launch the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn and helped to establish a much-desired NATO footprint on the southern shore of the Gulf of Finland. Since then, Estonia has taken the floor in the UN, warning other countries against the cyber-threat and promoting the UN First Committee as the appropriate venue for dealing with the issue. Estonia is also among the countries that has begun developing offensive cyber-capabilities.

Paradoxically, a poster child for how ICTs can aid societal and economic development, Estonia has played all the tunes that Moscow wants everyone to hear: ICTs as a weaponized technology, a new way of warfare and a new type of arms race that should be controlled and subjected to a whole new regime and order. More and more countries chose to securitize the development and use of ICTs.[157] Accordingly, it became impossible for Washington to insulate the USA against the First Committee dialog and the UN Group of Governmental Experts on International Information Security (UN GGE) as one of its working formats.

For both the Russian Federation and the USA, the duel in the First Committee and the UN GGE has concerned strategic stability. As Moscow has found a strategic partner in Beijing, the three superpowers cannot afford to disengage from the First Committee discourse. However, the emphasis on ICTs in the context of international peace and security is not the only option, nor is it the natural one for most other countries. No matter how weapon-like ICTs may appear when presented in daily reports of cyberattacks, terms like "information war" and "cyber-terrorism" are misnomers for the frameworks in which to deal with such incidents.

The cyber-threat narrative with reference to state actors and military cyber-capabilities ignores the essence of the vulnerabilities inherent in the information-society model. It downplays the root factors and causes of the current situation. In elevating the issue of cybersecurity to the highest international and political level, such narratives erode the role of domestic and societal resilience.

On closer examination, the national cyber-threat assessments of the leading cyberpowers do not align with international cyber-policy posture. Even the UK National Cyber Security Centre (NCSC) has concluded that the vast majority of people in the British Isles will not be

[157] This can be seen in the development of national cybersecurity strategies as well as the increasing sponsorship of the First Committee process. .

directly harmed by [nation-state] actors: “They are much more likely to fall victim to cybercrime, whether directly by being targeted or indirectly through one of their service providers being compromised.”[158]

However, the same indicators and metrics that measure cybercrime and the lack of national resilience serve as examples of the threat of ICTs to international peace and security. As a result, the cyber-threat becomes something that cannot be verified or falsified.

A Patched but Rocky Road

The West has put enormous efforts into arguing that there is no need for new international law. The USA, UK, Canada and Australia—all have been unyielding in their national positions.[159] Other like-minded states have put forward strong arguments for the international rule of law.[160] As noted, the *London Process* has offered several: proposals for principles governing behavior in cyberspace,[161] a call for applying offline laws and norms online,[162] reiteration of the UN GGE findings,[163] discussion of legitimate responses available when breaches of international law occur, as well as a strong agenda for taking norm development forward.[164] *The Hague Process* has undertaken to export a Western reading of international law. A further Dutch initiative aims at continuing the norms discourse, a diversion to the international law negotiations made during the 2014/15 GGE. Rather than strengthening the main message, however, these many efforts appear to be fragmenting it.

[158] UK National Cyber Security Centre, “Active Cyber Defence – One Year On” (February 2018), p. 8.

[159] See national annual submissions on information security to the UNGA (UNODA, “Developments in the field of information and telecommunications in the context of international security“) as well as national cybersecurity strategies (CIPedia, National Cyber Security Strategy).

[160] These include Germany, The Netherlands, Estonia, Switzerland, Finland, South Korea.

[161] London Conference on Cyberspace (2011). “Summary by the Chairman” (November 1–2).

[162] Budapest Conference on Cyberspace (2012). “Summary by the Chairman” (October 4–5).

[163] Seoul Conference on Cyberspace (2013). “Seoul Framework for and Commitment to Open and Secure Cyberspace” (October 17–18).

[164] The Hague Global Conference on Cyberspace (2015). “Chair’s Statement” (April 16–17).

Doubts about the applicability of existing international law, in the context of cyber-threats, have been expressed by Western scholars and major companies in the West. For example, D.B. Hollis's "duty to hack," e-SOS and the concept of International Law of Information Operations all highlight the lack of legal certainty and underscore the potential of international law.[165] Despite being advertised as doing the contrary, the *Tallinn Manual* points out inconsistencies in law and legal scholarship.[166] This scholarship confirms that alternative readings of international law are possible; and A. Roberts's analysis has shown that different approaches to international law are not only possible but also real.[167] Although this provides convenient ambiguity for cynical operators and policymakers, it also underscores the lack of certainty, predictability and stability.

The "norms" turn, initially seen as a successful Western counter-demand to the treaty proposition, has drawn additional attention to the perceived gaps in international law.[168] On the one hand, the norms discourse directly points to inconsistencies in and regarding international law.[169] On the other hand, the artificial and insufficiently clarified separation between "norms" and international law has alerted scholars in both IL and IR to review, and examine in detail, the letter of the law as against the practice of it.[170]

[165] Duncan. B. Hollis, "Why States Need an International Law for Information Operations," *Temple University Legal Studies Research Paper No. 2008-43* (2008); "An e-SOS for Cyberspace," *Harvard International Law Journal,* 52: 2 (2011); "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?," *Temple University Legal Studies Research Paper* No. 2014-16. (2014)

[166] These include the question of data as an object or not, the threshold of armed attack, the interpretation of the plea of necessity, and foreign espionage as coercive or non-coercive practice.

[167] Anthea. Roberts, *Is International Law International?* (Oxford: OUP, 2017).

[168] Tikk (ed.) (2017), *A Commentary*,

[169] Whereas in the UN GGE some countries were not willing to accept the applicability of the right of self-defense and IHL in the context of state use of ICTs, others were unable to accept, without reservations, the binding nature of due diligence, and the law of state responsibility.

[170] A rich discussion has emerged around the UN GGE 2015 recommendations on voluntary, non-binding norms, rules and principles. See, for example, Anna-Maria Osula, and Henri Rõigas (eds.), *International Cyber Norms Legal, Policy & Industry Perspectives* (Tallinn*:* NATO CCD COE Publications, 2016); Dennis Broeders. *The Public Core of the Internet, An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press 2016); S. Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms.* Microsoft Corporation; H. Farrell, "Promoting Norms for Cyberspace," *Cyber Brief, Digital and Cyberspace Policy Program* (New York: Council on Foreign Relations, 2016); Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global

Absent the norms discourse, gaps in international law could be left to the legal community to debate, which would involve a slower and controllable pace and remaining realistic as to international law as a discipline. The norms dialog has come to target and involve stakeholders across the spectrum.[171] The unclear relationship that has come to exist between international law and norms, because of the UN GGE framing, creates unrealistic expectations towards international law—and fuels claims that international law is impotent. As Mead, Higgins and Koh put it: "the reluctance of states to engage in international law-making has left a power vacuum, lending credence to claims that international law

Cybersecurity," *American Journal of International Law*, 110:3 (2016); Elaine Korzak, 'The Quest for Cyber Norms," *Bulletin of the Atomic Scientists*, 72:5 (2016): 348–350; Kubo Mačák, "Is the International Law of Cyber Security in Crisis?'" in N. Pissanidis., H. Rõigas and M. A. Veenendaal (eds.) *2016 8th International Conference on Cyber Conflict Cyber Power,* Tallinn: NATO CCD COE Publications; Tim Maurer, 'The New Norms: Global Cyber-Security Protocols Face Challenges', *IHS Jane's Intelligence Review,* (March 2016): 52–53; Brian M. Mazanec, "Why International Order in Cyberspace is Not Inevitable," *Strategic Studies Quarterly* (Summer 2015): 78–98; Eneken Tikk-Ringas, "International Cyber Norms Dialog as an Exercise of Normative Power," *Georgetown Journal of International Affairs*, *International Engagement on Cyber VI*, Vol. 17:3 (2017). See also Stefan Soesanto and Fosca D'Incau, "The UNGGE is dead: Time to fall forward" (August 15, 2017), http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; also Melissa Hathaway, "When Violating the Agreement Becomes Customary Practice," in Fen Osler Hampson and Michael Sulmeyer (eds.) *Getting Beyond Norms: New Approaches to International Cyber Security Challenges* (Waterloo, ON: Centre for Governance Innovation, 2017); Liis Vihul and Michael N. Schmitt, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; Robert McLaughlin and Michael N. Schmitt, "The need for clarity in international cyber law. International law implications of the lack of consensus" (September 18, 2017), https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/; Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" (June 29, 2017), https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what); NATO CCDCOE, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

[171] A notable example is the Global Commission on the Stability of Cyberspace (GCSC), co-partnered by the governments of The Netherlands, Singapore and France, Microsoft Corporation and the Internet Society, and sponsored by the government of Estonia. GCSC seeks to "link the dialogs on international security with the new communities created by cyberspace" in its goal to support "policy and norms coherence related to the security and stability in and of cyberspace." See cyberstability.org.

fails in addressing modern challenges posed by rapid technological development."[172]

An important obstacle to the like-minded plea for existing international law as a platform of international cybersecurity is the developing countries' hesitance to accept this—not due to differences of opinion about the law itself, but because of the lack of capacity and the perceived high costs of implementation. For those audiences, it is essential to distinguish and maintain a clear separation between cybersecurity and issues of international peace and security. Here the West needs to attend another emerging merger: that of Internet governance with international security. This is essential if the like-minded want to keep the issue of international cybersecurity out of ITU and avoid a return to the WCIT 2012 situation where a vote split the international community about the role of governments in internet governance. It is also crucial because Internet governance is a topic that might serve to isolate the USA.

What is to Be Done?[173]

To push back on the Russian initiative effectively, the West will need to undermine at least one of the three pillars in the Kremlin's strategy: the general distrust towards ICTs, the insufficiency of existing international law, or the existential threat narrative. On the first account, deeply rooted suspicions cannot be argued away. On the second, Russia has been able to strengthen general perceptions of legal insecurity, thereby solidifying its claim. On the third, the like-minded still possess a strong advantage: their experience of transparency, openness, growth and resilience.

It is in the interests of the West to shift the leading narrative from threats to opportunities and emphasize national accountability. The fact that the UN GGE has not been able to establish a real linkage between state use of ICTs and threats to international peace and security, or verify any existential threat linked to ICTs, should encourage a more critical and analytical look at the types of threat that the proliferation and convergence of ICTs actually bring. The GGE should examine the impact that the development and use of military cyber-capabilities and ICTs by rogue and hostile states and their proxies have or may have on international peace and security. If ICTs cannot be found to constitute an existential threat, any dialog in the arms control realm should be

[172] Mead, Higgins and Koh, "From cyber norms to cyber rules" (2017).

[173] *Что делать?* (Chto delat?), V.I. Lenin (1902). "What Is To Be Done? Burning Questions of Our Movement" in *Lenin Collected Works*, Volume 5 (1961).

strictly limited to the development and employment of particular capabilities.

The West should avoid trying to counter the Russian narrative as a whole. The discourse needs to mature beyond either/or approaches that toy with the idea of one camp surrendering to the other. The West will need more than merely a friendly or adversarial policy option if it is to succeed in countering the Russian informational, cyber and normative power projection. The policy of undermining can be envisaged as a non-confrontational approach and principle aimed at organizing various otherwise individual proactive and reactive measures according to a single, coherent intention and a shared long-term objective. Essentially, such undermining would seek to deny, diminish, nullify, turn, change or overwhelm Russian activities, the effects and the support of them. It would aim at raising the cost of such activities through cyber-specific and other means.

The West is uniquely placed to counterbalance Russia's threat narrative with a progressive initiative. A *Cyber Marshall Plan,* building robust national capacities and unprecedented transfers of ICTs, could effectively undermine the Kremlin agenda and agitation of fear, insecurity and xenophobia. A determined program launched in the spirit of the original Marshall Plan would honor the ingenious ideal of creating a climate of wealth, health and security. It would also undermine the Russian project of showing, through its own active operations, the vulnerability of cyberspace.[174]

The like-minded countries cannot afford the fragmentation and soloing that goes against their acknowledged shared concerns and priorities. For instance, mingling Internet governance concepts in the context of international cybersecurity helps to import governance into the agenda of First Committee. It could also pin Internet governance to further pressure of state-centric control.[175] In this context, any differences within the like-minded concerning Internet governance could easily become diverging factors in the international cyber-dialog. Moving forward, the like-minded will need to be cognizant of the

[174] The authors thank Juha Kukkola for this clear remark in his commentary to the draft of this paper.

[175] Entering the UN GGE discussion in 2015, the Netherlands proposed further work and specific measures for establishing special normative protection for certain systems and networks, including certain critical components of the global Internet. See UN A/70/172, p. 8.

differences and non-alignments in their midst and learn to put these aside in negotiations.

Further, the like-minded must become more mindful of the potential disadvantages of any long-term securitization of ICT matters. Where civil society, academia and the people's representatives are excluded from the dialog, the exercise of executive power on the margins of legitimacy is likely to result in strong pleas for transparency and accountability.

If the dialog has been diluted to the point of no return, there are options to avoid overwhelming vote counts that go in an undesired policy direction. One approach would be to bucket together the three core interests of security, human rights, and technological development. These buckets could be negotiated separately, and partially within true expert communities, but they would not be agreed or implemented in segregation. Another way to increase the "shades of grey" in cyber-discourse could be to identify shared national interests and objectives across camps and continents. This would help to build new thematic coalitions aimed at solving problems outside the stagnated blocks and opined arguments.

Too much foreign and security policy emphasis on ICTs is counterproductive to the transparent and democratic development of information societies. Securitization reverses the fundamental principle of democracy where the public sphere is transparent and the people are protected. Foreign policy emphasis distances the development of the information society from the society itself. Alongside an overwhelming threat narrative that they support, the Western governments keep pressing for deployment of ICT infrastructure and e-services. For example, the Estonian 2017 identity card vulnerability has given rise to questions of the accountability, and potentially liability, of governments to their own constituencies.[176]

[176] For the incident and associated questions, see Tallinn University of Technology (2018) Lessons of the ID Card Case (in Estonian), https://www.ria.ee/public/PKI/ID-kaardi_oppetunnid.pdf. See also Kalev Aasmäe, "Estonia's ID card crisis: How e-state's poster child got into and out of trouble," http://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble, and Bruce Schneier, https://www.schneier.com/blog/archives/2017/09/security_flaw_i.html. Curiously, since the blocking of 750 000 ID cards, 441 000 were renewed during the following six months, which gives rise to questions about the statistics whereby the number of issued ID cards reflects the inclusion of the Estonian population in the information society and e-state: of a total population of 1.3 million, roughly only one third considered it worth the effort to renew the e-

Moreover, the appetite of Western governments for military cyber-capabilities constrains their argument about the authority of international law.[177] Being tuned to the governing international peace and security paradigm, especially the US–UK discourse of international law and cybersecurity favors self-defense, countermeasures and International Humanitarian Law. Operational interests inevitably condition a narrow reading of Human Rights Law and the principles of sovereignty and non-intervention. The desire to maintain operational freedom of maneuver causes tensions with the otherwise like-minded rule-of-law champions, while also leaving Russian and Chinese questions and doubts about international law unanswered. More importantly, the use of ICTs to punish the Estonian government, discredit and subvert democracy in Georgia and Ukraine as well as to conduct extensive foreign influence operations challenges international stability and undermines Western assertions that international law provides adequate protection against malicious and hostile uses of ICTs.

As a result, the West is self-eroding its political leadership and normative-moral authority. The USA has accused Russia and China of stepped-up efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.[178] Unfortunately, so have some of the like-minded. Furthermore, attacks against Western information systems and services have demonstrated the inadequacy of their own cybersecurity practices. Despite decades of acknowledgment of inherent vulnerabilities in ICTs, little demonstrable progress has been made in securing critical and essential, let alone routine, functions that depend on ICTs. Inadequate national resilience leaves societies open to manipulation and bullying, to the point where questions emerge from within these democracies, about the sustainability of core democratic processes and functions.[179]

The recent US policy of consequences as an expansion of the discourse of deterrence and the discussion of legitimate responses under international law runs the additional risk of revealing real differences in the national understanding, interpretation and implementation of

functionality of their national identity cards (the not-renewed cards remained valid as 'normal' id-cards: authors' experience).

[177] From authors' observations of Western-sponsored teaching of international law in the context of ICTs, which almost without exception begins and ends with operational and "cyber military" law.

[178] DoD (2018).

[179] https://warontherocks.com/2016/07/open-letter-congress-must-investigate-russian-interference-in-the-presidential-election/.

international law.[180] Despite tailored, calculative, comprehensive and engaging international partners, the implementation of such measures might run against the rule of law narrative when implemented at a time of heightened tensions. [181]

Lack of national resilience combined with the securitization approach further puts pressure on freedoms and liberties. Western pleas to their populations about the need to accept the burden of security in their online activities is the very antithesis of the world order that the USA and the like-minded countries have been constructing. Whatever China and Russia have done to subvert and undermine the Western pleas for an information society has been matched by what the West itself has failed to achieve as regards protecting it. Accordingly, the proponents of a different world order may well question the viability of the information society as an economic and societal model. Penetration of and dependence on ICTs has allowed China and Russia to undermine the international order from within the system.

Russia has recently demonstrated significant interest in the foundations and parameters of a digital economy.[182] Moscow has supported Nornickel's initiative for a code of information security conduct to further the agenda of the Information Security Charter for Critical Industrial Facilities.[183] Since 2007, Moscow State University, in cooperation with the Russian Ministry of Foreign Affairs, has organized the International Forum on International Information Security where Moscow both develops and presents its leads on international information security. In 2018, the agenda has come to include the issues of information security in the context of developing a digital economy. Should a digital economy model with Russian characteristics emerge, this could be highly appealing to states that do not subscribe to Western values of transparency and accountability.

[180] Department of State, "Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats Through International Engagement" (May 31, 2018).

[181] See Eneken Tikk, "Will Consequences Deepen Differences about International Law?" *Temple International and Comparative Law Journal,* 2019 (forthcoming), for a 2017 intragovernmental seminar on the "policy of consequences."

[182] "Building Foundations of the Digital Economy: Lessons from the Global Experience," World Bank Country Office, Moscow (February 1, 2017).

[183] See Nornickel, "Code of Conduct for Information Security," https://www.nornickel.com/news-and-media/press-releases-and-news/code-of-conduct-for-information-security/?dateStart=46800&dateEnd=1520114399&type=news.

The Russian game has always involved bringing more voices into the conversation. Keeping the talks up in the UN GGE is just one avenue for Russia to address the General Assembly and all governments, with the message that the information society and digital economy as the latest incarnations of the Western way of life do not represent a sustainable world order. Arguing otherwise may have been manageable behind the closed doors of the UN GGE—but it could trigger entirely different sentiments in open venues like the Internet Governance Forum.

Can We Go Forward if We Fear to Advance?[184]

Further pressure towards a treaty is inevitable. As parity with the USA is the Russian condition of strategic stability, the Kremlin will not abandon the treaty argument to reduce its insecurity. In this effort China and Russia remain aligned. Russia has, or will shortly have, the confidence and collaboration to push for formal negotiations. The Western rejection, as well as the argument of sufficiency of existing international law, can be seen as an attempt to avoid restraint. Accordingly, the West will have difficulties in convincing the international community of its stand.

An outright rejection on the part of the West would not necessarily prevent negotiations. For instance, drafting and the voting of a UN resolution to negotiate a legally binding instrument to prohibit nuclear weapons split the West, the BRICS, the SCO and the developing countries.[185] A convention may result from further corporate or civil society initiatives. For example, the 1997 Anti-Personnel Mine Ban

[184] Paraphrasing Lenin's "Can We Go Forward If We Fear to Advance Towards Socialism" (V.I. Lenin. "The Impending Catastrophe and How to Combat It." *Lenin's Collected Works*, Vol 25 (1961)).

[185] UNGA (2016). "General and complete disarmament: taking forward multilateral nuclear disarmament negotiations," A/C.1/71/L.41 (14 October). The resolution was sponsored by Austria, Brazil, Chile, Costa Rica, Democratic Republic of the Congo, Ecuador, El Salvador, Guatemala, Honduras, Indonesia, Ireland, Jamaica, Kenya, Liechtenstein, Malawi, Malta, Mexico, Namibia, Nauru, New Zealand, Nigeria, Palau, Panama, Paraguay, Peru, Philippines, Samoa, South Africa, Sri Lanka, Swaziland, Thailand, Uruguay, Venezuela and Zambia.

In the December 2016 UNGA voting, Albania, Andorra, Australia, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Micronesia, Monaco, Montenegro, Norway, Poland, Portugal, Republic of Korea, Romania, the Russian Federation, Serbia, Slovakia, Slovenia, Spain, Turkey, the United Kingdom, and the United States voted against the resolution. Armenia, Belarus, China, Finland, Guyana, India, Kyrgyzstan, Mali, Morocco, the Netherlands, Nicaragua, Pakistan, Sudan, Switzerland, Uzbekistan and Vanuatu abstained.

Treaty (the Ottawa Convention) was borne out of civic engagement and NGO movement.[186] It is not unprecedented for a group of countries or a regional organization to become the platform for a global instrument. The 2001 Convention of Cybercrime (the Budapest Convention) is by origin a European instrument that has gradually gained support from countries around the world. [187] Furthermore, a treaty may result from spillovers from a related area or set of questions. For instance, differences about space issues may give rise to the question of similar themes in the context of ICTs, absent *lex specialis*. If Western concerns over Chinese and Russian advances in quantum computing, artificial intelligence, electronic warfare and lethal autonomous capabilities prove well-founded, then it would eventually be in the Western interest to establish a strong treaty-based regime to limit such development and employment.[188]

The US conclusion that China and Russia want to shape a world order consistent with their authoritarian model[189] leads to the question of whether the West is ready and able to shape the world according to its own model. Beijing and Moscow have emerged as a battle pair, ready to fight against the ICT expansionism that they both have long accused the USA of exercising. Washington, on the other hand, has been finding it hard to create a solid “like-minded” front.

With competition between regimes occurring across all dimensions of power, a solid and credible playbook is needed to halt the advance of the Sino–Russo version of the world. To restore a free, open and rules-based world order, the West needs a three-pronged game plan that can counter and undermine Russia’s three basic claims: (a) that the use of ICTs threatens international peace and security, (b) that international law is

[186] UNOG (1997). *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction*. China, the USA and Russia did not sign the convention. The USA, however, announced in 2014 that it would abide by the terms of the Treaty, with the exception for anti-personnel mines employed on the Korean Peninsula.

[187] Council of Europe (2001).

[188] For recent Western statements on Chinese and Russian capabilities see, e.g., Curtis M. Scaparrotti, “Military Assessment of Russian Activities and Security Challenges in Europe,” Committee on Armed Services, United States House of Representatives (March 28, 2017); DOD, “Military and Security Developments Involving the People’s Republic of China 2017” (2017); DIA, “Russia Military Power” (2017); and William Carter, “Chinese Advances in Emerging Technologies and their Implications for U.S. National Security,” Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities (January 9, 2018).

[189] DoD (2018).

not sufficient to provide safeguards, and (c) that ICTs do not provide economic prosperity but in fact erode societal stability.

Firstly, the West needs to defend its base—without the promise of social benefits and economic development the narrative of ICTs will collapse. This goal, however, cannot be achieved by means of narratives or *opinio juris*. Carefully crafted indexes and metrics will not suffice without upgrades of national resiliency. Credible and visible examples of functioning information societies are needed to convince the developing countries of the benefits. This will entail demonstrating responsible state behavior, not just talking about it. Emphasizing national-level responsibility for the development of the information society and use of ICTs would benefit from international coordination of relevant experience, practices and examples. Here the UN Second Committee offers a more suitable platform than the First Committee as it allows a far wider choice of vocabulary, measures and forms of engagement.

It is essential for the like-minded governments to channel the cybersecurity discourse towards greater national accountability and resilience as prerequisites for maintaining international peace, security and stability in the use of ICTs. Here, the emerging concept of cybersecurity governance[190] offers an opportunity. The UN GGE 2015 recommendations and the further work done by the OSCE provide a solid foundation for improving levels of cybersecurity and defusing national insecurities. The West need not subscribe to Russo–Sino claims of cyberwar—but it will have to offer its own positive agenda of ICTs as the sources of future development and social empowerment.

Cybersecurity through governance offers an alternative to cybersecurity through securitization: it calls on governments to employ new approaches to governance with a view to the changes, and challenges, that come with ICTs. Building on terms adopted in the IT industry to describe new approaches to the changes pushed by major technological, intellectual and behavioral transformations, cybersecurity governance emphasizes government-level accountability, with systemic contributions from all stakeholders.

Secondly, the West must add authority to its own "rules of the road." It must be very cautious of framing voluntary and non-binding norms, to avoid signaling that little or no protections exist for the private sector

[190] See, for example, Paul Rosenzweig, "The International Governance Framework for Cybersecurity," *Canada-United States Law Journal*, 37:2 (2010).

and public services short of International Humanitarian Law. Here, state practice analysis could offer additional opportunities for showing how some countries are managing to achieve cybersecurity without the need to bend, amend or create international law. On the one hand, this could offer additional ways to interpret and apply the UN Charter and other relevant sources of law. On the other hand, it could contour the rule of law more broadly, emphasizing the interrelationship of national and international law in providing a framework for national and international contributions to cybersecurity.

Finally, the West will need to distance itself at least partially from the "governing threat" narrative and from the First Committee as the leading venue. The UN GGE would be an appropriate platform for capping the development or certain uses of military cyber-capabilities. Otherwise, continuing discussions in the UN GGE format will only emphasize the threats undermining, or even embedded in, the Western way of life. As noted by the EU, the First Committee is not the most appropriate venue for discussing issues so intrinsically linked to economic prosperity, social development and technological innovation.

To advance, the West needs to prepare for treaty negotiations as one possible future, albeit likely to materialize only if the UN GGE negotiations break down. Here it is essential to recognize the value and potential of independent and constructive national views on matters of international law and its development. The 2016/17 GGE featured countries like Switzerland, Finland and South Korea, all of which are regarded as champions of the rule of law and are potentially accepted as honest brokers in international cyber-affairs. Furthermore, Singapore seems to be emerging as advocate of developing and implementing cyber- norms in accordance with ASEAN values. Preparing for the worst-case scenario offers new openings to avoid it.

Meanwhile, there are speed humps on the way to legal certainty and binding commitments when it comes to development and use of ICTs. Putin's Russia and Trump's USA find common ground on that there is no hurry with an actual solution to cybersecurity issues other than their own. For the rest of the world, however, this slow-motion may not be the preferred pace.

Beware of Voluntarism

The contemporary rapport between Presidents Putin and Trump excludes the concerns of the broader international community and even of their own allies. While this contingent stand does not remove the fundamental differences between two world views, it effectively postpones any sustainable solutions.

It appears that, in the upcoming round of the dialogue, Moscow and Washington put strong emphasis on voluntarism instead of any binding commitments. The next UN GGE, therefore, is to be distanced from direct international law discussions and leave it to a next, perhaps another, venue and format. This means another two years spent on crafting voluntary and non-binding measures.[191]

A dialogue on norms, rules and principles is very difficult to reject by an international community in dire need for increased predictability and certainty in state use of ICTs. For Washington and Moscow, however, norms provide an escape route from the very difficult conversation about international law and the boundaries of their own cyber operations as well as the consequences thereof under international law. Conveniently for the main architects of the cybernorms discourse, any discussion of actual guarantees to civilians and civilian objects in military use of cyber capabilities is blocked out by China, and increasingly Russia, claiming that there is no need for such exchange as any military use of these capabilities is precluded under the UN Charter.

The USA has recently pledged to ensure that adversaries understand the consequences of their malicious cyber behavior. The White House plans to leverage a range of tools, including prosecutions and economic sanctions, as part of a broader unilateral deterrence strategy.[192] Some European countries are following the suit, while others hesitate. The divide between the EU countries on sanctions is similar to what NATO will be inevitably facing over cyber operations – not all countries are interested in beefing up offensive and hostile cyber attitudes. Not everyone, therefore, is happy to follow the UK and the Netherlands.

There are, however, complex and powerful relationships between the USA and some EU cyber star countries. The United States has worked

[191] On September 28, 2018, Deputy Secretary of State John J. Sullivan hosted a ministerial meeting on advancing responsible state behavior and deterring malicious activity in cyberspace. The Deputy Secretary raised re-starting expert-led international talks on responsible state behaviour at the United Nations, emphasizing that “responsible state behavior in cyberspace should be guided by international law, adherence during peacetime to non-binding norms of state behavior, and implementation of practical confidence building measures”. https://www.state.gov/r/pa/prs/ps/2018/09/286318.htm.

[192] The White House, *National Cyber Strategy of the United States* (September 2018). p. 2-3, 8, 10, 21.

with like-minded states in coordinating and supporting each other's responses to significant malicious cyber incidents. Such cooperation and support comprise intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.[193]

The Department of Defense has recently announced accelerating the development of cyber capabilities for both warfighting and countering malicious cyber actors. The US is preparing to employ cyberspace operations throughout the spectrum of conflict, from day-to-day operations to wartime, in order to advance US interests.[194] Time is an essential factor for further developing cyber capabilities, be they called defensive, active defensive, intelligence or outright offensive.

For Moscow, there is no issue with the voluntary norms framing, either. Pragmatically, it is progress elevating the 2015 UN GGE recommendations to a higher normative status. Although, and because, there is no real effect to such move, it keeps alive and relevant the process Moscow incepted twenty years ago to make the world aware and wary of the US ambitions in cyber operations. As of today, holding the *status quo* also supports Russian cyber operations that undermine the prospect of ICTs as a delivery mechanism of democracy, societal empowerment and economic prosperity.

If the USA and Russia both settle on devoting the next round of the 2019/2020 UN GGE talks to wordsmithing voluntary and non-binding norms, the rest of the international community is simply on the waiting list. Neither Moscow nor Washington want any binding commitments – if they do, it is only to twist their main competitor's arm. Between the Kremlin and the White House, the game is strictly one of world order, national ambitions and strategic stability. International cybersecurity proper is but a pawn in their hands. As long as these two remain on the same page, the world is back to early space age, but with even less legal certainty. Back then the US and the Soviet Union shared the interest in explicit bilateral commitments and in reining in the rest of the world. Similar strategic elitism constitutes the logic of the nuclear non-proliferation treaty splitting the world to haves and have-nots.

The era of political attribution and targeted consequences may seem like progress towards international cybersecurity. Yet all the names named, and the numbers counted support the narrative that the two

[193] The White House, *National Cyber Strategy of the United States* (September 2018), p. 21.

[194] *Department of Defense Cyber Strategy* (September 2018), Summary, p. 4.

superpowers need the world to believe: that in securing our systems and services, we need to focus, first and foremost, on the hard security threat that stems from potential politico-military use of ICTs. By default, the outcome of the norms talk is no commitment. Norms cannot increase predictability especially in times of superpower competition and contestation and obvious differences about international law. As discussed above, norms do not address actual questions of international peace and security. Conveniently for operators, they also have little impact on national cyber resiliency, capacity and prowess as factors to severe routine cyber attacks. The climate of sub-security is ideal for the Athenians and the Spartans but not for the Melians.

The upside of the cybernorms conversation is that it enables all states to insert their concerns and solutions in the dialogue. At the time of writing, a compromise solution seems to be to request the UN Office for Disarmament Affairs (UNODA) to collaborate with regional organizations, such as the AU, the OAS, the OSCE, and the ASEAN Regional Forum to convene a series of consultations for UN member states to share views on the issues within the Group's mandate in advance of the next UN GGE sessions.

If countries make use of this opportunity, their input will clarify acute issues of cybersecurity, highlight workable solutions and indicate where disagreements exist about international law or the utility of current practices.

At the receiving end of cyber geopolitics, diverting from talks on international law is alarming. States with strong cyber operational interests keep arguing that everything is clear on this account.[195] Their point of reference, misleadingly, is the Tallinn Manual. According to the Dutch Minister of Foreign Affairs, Tallinn Manual is "our set of instructions for state behaviour in cyberspace". Mr. Blok identifies Tallinn Manual as guidance to defending supermarkets, parking garages, the port of Rotterdam, power plants and public services. The important pretext is that the Tallinn Manual only addresses cyber operations conducted by or on behalf of States. It does not say much about the prevention of such operations and it remains inconclusive about the guarantees that, in case such operations are conducted by States, apply to the supermarkets, ports and public services mentioned by His Excellency.

[195] HE Mr. Stef Blok MA, Minister of Foreign Affairs, *Militair Rechtelijk Tijdschrift* Jaargang 111:3 (2018).

The Dutch bring up a very important angle in this discussion. Cyber operations have proven useful during peacetime rather than in an acute military conflict.[196] Any voluntary or non-binding agreement in this context only indicates the extent States with robust operational capabilities are actually free to pursue their political ambitions and contingent objectives. It also emphasizes that little, if anything, is clear in international law. Short of conflict, states have demonstrated that there is little effective remedy against cyber attacks under international law. The USA has qualified her cyber confrontations with Russia and China under national legislation, staying away from international law terms and concepts. Moreover, the UK and the USA have recently promoted a view whereby national sovereignty, which their own cyber operations are most likely to infringe, is not a legally guaranteed right at all.[197]

Accordingly, where states talk about norms, it is essential to pay close attention to their exact words and framing. Where norms are claimed to derive from international law, they tend to offer restrictive interpretations of international law. Where, however, reference is made to norms drawn from state practice and empirical approaches, such constructions are a testament of the lack of solid normative guarantees.

Russia and the USA cannot be expected to lead the next UN GGE process in the interests of anyone but themselves. The question is whether the rest of the international community recognizes, and is willing to step up for, their own concerns. Several communities of interests can be identified.

The status quo offers an opportunity for countries promoting the rule of law to steer the conversation more firmly towards the guarantees to international peace and security stemming from international law. The focus of this community would be on proposals for norms that refer to some obligations and concepts in international law as voluntary or non-

[196] On the lack of battlefield cyber employment, see Martin Libicki, "Cyber War that Wasn't" in Geers, Kenneth (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015), pp. 49-54.

[197] On 23 May 2018, the Attorney General Jeremy Wright QC MP set out the UK's position on applying international law to cyberspace. He says: "Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law." *Cyber and International Law in the 21st Century, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.*

binding. The questions of this community would target the claims that the current international social contract somehow allows attacks against critical infrastructure or justifies cyber espionage. This group would stand behind the rule of law as an indispensable element for the prevention of armed conflict.[198]

Another important community is comprised of states who refuse to believe the governing threat narrative and the resulting choice of 'remedies'. Countries convening around actual and evidenced cybersecurity issues would equally find the UN GGE a format that, both by its mandate and composition, cannot adequately address neither the real issue or practical remedies. This community would stress that the lack of politico-normative predictability, combined with vulnerabilities and dysfunctional technical systems, all increase national insecurity and may lead to escalation. It would also recall that the eagerness of governments to adhere to self-help and cyber responses of various kind goes against the 2012 UN General Assembly resolution on the rule of law strongly urging States "to refrain from promulgating and applying any unilateral economic, financial or trade measures not in accordance with international law and the Charter of the United Nations". The contrast between the spirit of the resolution and the climate of the day is revealing and alarming.[199]

Finally, there is a community of interest to return to already established practical measures and mechanisms, while recognizing the political road blocks on the way to involving, for instance, the work done in the International Telecommunications Union or the World Trade Organization as parts of the solution. Actual ability to install the latest operating system updates is a factor of international peace and security more than any non-binding norm. This community may want to push back on discussing issues of cybersecurity in a closed venue with an arms control mandate by referring to the Charter of Digital Trust, the acknowledged role of incident responders in implementing the recommendations of the UN GGE, or, for instance, the work of the Transporting Assets Protection Association (TAPA)[200]. This community

[198] It is the view of the UN Security Council that the rule of law is "an indispensable element for peaceful coexistence and the prevention of armed conflict". United Nations Security Council, Statement by the President of the Security Council, S/PRST/2014/5 (21 February 2014).

[199] UNGA, Declaration of the High-level Meeting of the General Assembly on the Rule of Law at the National and International Levels, 67/1 (30 November 2012).

[200] TAPA's mission is to minimize cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards,

can point out that actual cybersecurity starts, and is resolved, at national and individual, rather than international or regional level.

The game of international cyber diplomacy contains elements of immediacy and elements of distance. Paraphrasing the renown samurai Miyamoto Musashi (c. 1584-1645), in both playing and analyzing this strategic game, it is essential to take a distanced view of things close-by and to see remote thing as if they were close. The early years of UN level talks produced very little but were kept alive by the Russian optimism. Few years ago, the West became too euphoric of its own success. Now, it seems that apologetic pragmatism is the driving force. Pragmatism, however, does not always turn into progress.

recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats. Transported Asset Protection Association, "Mission, vision, values". Available from https://www.tapaonline.org/our-mission-vision-values.

Annex A

Developments in the Field of Information and Telecommunications in the Context of International Security: Replies from Governments 1999–2017

	99[201]	00[202]	01[203]	02[204]	03[205]	04[206]	05[207]	06[208]	07[209]	08[210]	09[211]	10[212]	11[213]	12[214]	13[215]	14[216]	15[217]	16[218]	17[219]
Afghanistan																			X
Albania																		X	
Argentina						X													
Armenia															X				X
Australia	X												X			X		X	
Austria																X			
Bangladesh									X										
Belarus	X																		X

[201] A/54/213
[202] A/55/140 and A/55/140/Add.1
[203] A/56/164 and A/56/164/Add.1
[204] A/57/166 and A/57/166/Add.1
[205] A/58/373
[206] A/59/116 and A/59/116/Add.1
[207] A/60/95 and A/60/59/Add.1
[208] A/61/161 and A/61/161/Add.1
[209] A/62/98 and A/62/98/Add.1
[210] A/63/139
[211] A/64/129 and A/64/129/Add.1
[212] A/65/154
[213] A/66/152 and A/66/152/Add.1
[214] A/67/167
[215] A/68/156 and A/68/156/Add.1
[216] A/69/112 and A/69/112/Add.1
[217] A/70/172 and A/70/172/Add.1
[218] A/71/172
[219] A/72/315

	99[201]	00[202]	01[203]	02[204]	03[205]	04[206]	05[207]	06[208]	07[209]	08[210]	09[211]	10[212]	11[213]	12[214]	13[215]	14[216]	15[217]	16[218]	17[219]
Bolivia			X		X			X											
Brazil							X				X								
Brunei	X								X										X
Burkina Faso									X										
Canada							X								X	X	X	X	X
Chile							X		X										
China						X		X	X	X									
Colombia														X		X		X	
Costa Rica						X													
Cuba	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
El Salvador					X											X	X	X	X
Equador													X						X
Estonia																			X
Finland																		X	X
France																X			
Georgia					X	X							X			X	X		
Germany													X		X		X		X
Greece												X	X						X
Guatemala				X															
Guyana													X						
India																		X	
Iran															X				
Japan															X			X	X
Jordan		X						X		X								X	X
Kazakhstan											X		X						
Lebanon						X		X	X	X	X							X	
Lithuania											X								
Madagascar																			X
Mali											X								
Mexico			X			X	X	X	X		X	X							
Mozambique																	X		
Netherlands													X		X		X		X
Niger										X									
Norway																			X
Oman	X														X				
Panama				X								X		X			X		

	99[201]	00[202]	01[203]	02[204]	03[205]	04[206]	05[207]	06[208]	07[209]	08[210]	09[211]	10[212]	11[213]	12[214]	13[215]	14[216]	15[217]	16[218]	17[219]
Paraguay																			X
Peru																	X		
Philippines			X																
Poland		X																X	
Portugal													X			X	X	X	X
Qatar	X	X						X		X		X		X			X		X
Russia	X	X	X		X														
Saudi Arabia	X																		
Senegal					X														
Serbia											X					X		X	
Singapore																			X
South Korea																X	X		
Spain											X				X	X	X	X	
Sweden			X[220]													X			
Switzerland																X		X	
Syria				X															
Tajikistan											X								
Thailand											X								
Togo																		X	
Turkey														X	X				X
Turkmenistan													X					X	
Ukraine					X						X	X		X	X				
UK	X					X						X			X	X	X	X	X
UAE								X											
US	X					X							X						
Venezuela						X													

[220] On behalf of the States members of the European Union that are Members of the United Nations.

Annex B

Membership of the UN Group of Government Experts (UN GGE) 2004-2017

	2004–2005	2009–2010	2012–2013	2014–2015	2016–2017
Argentina			X		
Australia			X		X
Belarus	X	X	X	X	
Botswana					X
Brazil	X	X		X	X
Canada			X	X	X
China	X	X	X	X	X
Colombia				X	
Cuba					X
Egypt			X	X	X
Estonia		X	X	X	X
Finland					X
France	X	X	X	X	X
Germany	X	X	X	X	X
Ghana				X	
India	X	X	X		X
Indonesia			X		X
Israel		X		X	
Italy		X			
Japan			X	X	X
Jordan	X				
Kazakhstan					X
Kenya				X	X
Malaysia	X			X	
Mali	X				
Mexico	X			X	X
Netherlands					X
Pakistan				X	
Qatar		X			
Russia	X	X	X	X	X

Senegal					X
Serbia					X
South Africa	X	X			
Spain				X	
South Korea					X
Switzerland					X
UK	X	X	X	X	X
US	X	X	X	X	X

Annex C

Sponsors of the UN Information-Security Resolution 2006-2016*

In 2017, no resolution was adopted. The item was included in the agenda of the General Assembly for 2018.

	2006 [221]	2007 [222]	2008 [223]	2009 [224]	2010 [225]	2011 [226]	2012 [227]	2013 [228]	2014 [229]	2015 [230]	2016 [231]
Algeria									X	X	X
Angola							X	X	X	X	X
Argentina						X	X	X	X	X	X
Armenia	X	X	X	X	X	X	X	X	X	X	
Azerbaijan			X	X	X	X					X
Australia					X					X	
Bangladesh											X
Belarus	X	X	X	X	X	X	X	X	X	X	X
Belgium										X	X
Benin									X		X
Bolivia				X					X	X	X
Brazil			X	X	X	X	X	X	X	X	X
Burkina Faso									X	X	X
Burundi									X	X	X
Cabo Verde											X
Canada					X						
Central African Republic									X		
Chad									X		X

[221] A/61/389
[222] A/62/386
[223] A/63/385
[224] A/64/386
[225] A/65/405
[226] A/66/407
[227] A/67/404
[228] A/68/406
[229] A/69/435
[230] A/70/455
[231] A/71/28

	2006[221]	2007[222]	2008[223]	2009[224]	2010[225]	2011[226]	2012[227]	2013[228]	2014[229]	2015[230]	2016[231]
Chile	X	X	X	X						X	X
China	X	X	X	X	X	X	X	X	X	X	X
Colombia						X	X	X		X	
Congo									X	X	
Costa Rica					X	X	X	X			
Côte d’Ivoire									X	X	X
Cuba		X	X	X	X	X	X	X	X	X	X
Cyprus					X	X				X	X
DPR of Korea			X		X	X	X	X	X	X	X
DR of the Congo					X	X	X	X		X	X
Djibouti									X	X	
Ecuador								X	X	X	X
Egypt							X	X	X	X	X
El Salvador						X	X		X	X	X
Equatorial Guinea									X		
Eritrea								X	X	X	X
Estonia										X	X
Ethiopia	X	X	X	X	X	X	X	X	X	X	
Fiji			X								
Finland											X
France										X	
Gabon									X		
Gambia							X	X	X		
Germany					X					X	X
Ghana									X	X	X
Greece										X	X
Guatemala					X	X	X	X	X		
Guinea									X	X	
Guinea-Bissau									X	X	X
Haiti			X	X							X
Hungary										X	X

	2006[221]	2007[222]	2008[223]	2009[224]	2010[225]	2011[226]	2012[227]	2013[228]	2014[229]	2015[230]	2016[231]
India			X	X	X	X	X	X	X	X	X
Indonesia					X	X	X	X	X	X	X
Israel										X	
Japan		X	X	X	X					X	
Kazakhstan	X	X	X	X	X	X	X	X	X	X	X
Kenya									X	X	X
Kyrgyzstan	X	X	X	X	X	X	X	X	X	X	X
Lao People's DR							X	X	X	X	X
Latvia											X
Lesotho									X	X	
Madagascar	X	X	X	X			X	X	X	X	X
Malawi									X	X	X
Malaysia										X	X
Mali	X	X	X	X	X	X	X	X	X	X	X
Malta										X	X
Mongolia										X	X
Montenegro										X	X
Morocco								X	X	X	X
Myanmar	X	X	X	X	X	X	X	X	X	X	X
Namibia									X	X	X
Nepal										X	X
Netherlands										X	X
Nicaragua		X	X	X	X	X	X	X	X	X	X
Niger											X
Nigeria									X	X	X
Oman									X	X	
Pakistan								X	X	X	X
Panama										X	
Poland											X
Portugal										X	X
Republic of Korea										X	X
Russian Federation	X	X	X	X	X	X	X	X	X	X	X
Rwanda				X					X		
Saint Lucia				X							
Samoa											X
Senegal									X	X	X

	2006[221]	2007[222]	2008[223]	2009[224]	2010[225]	2011[226]	2012[227]	2013[228]	2014[229]	2015[230]	2016[231]
Serbia			X	X	X	X	X	X	X	X	X
Seychelles			X								
Sierra Leone					X	X	X	X			X
Slovakia										X	X
Slovenia					X						
Spain										X	X
Sri Lanka								X	X	X	X
Sudan			X	X			X	X	X	X	X
Syrian Arab Republic				X	X	X	X	X	X	X	X
Swaziland									X	X	
Switzerland										X	X
Tajikistan	X	X	X	X	X	X	X	X	X	X	X
Thailand									X	X	X
Tunesia											X
Turkey					X	X	X				X
Turkmenistan	X	X	X	X	X	X	X	X	X	X	X
Uganda					X	X	X	X	X	X	
Ukraine					X	X	X	X			
United Arab Emirates									X	X	
UK of GB and N-Ireland										X	
United States of America					X					X	
Uzbekistan	X	X	X	X	X	X	X	X		X	X
Venezuela										X	X
Viet Nam			X	X	X	X	X	X	X	X	X
Zimbabwe			X	X			X	X	X	X	X
Yemen									X	X	X

Norwegian Institute of International Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | post@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

Eneken Tikk is lead of strategy and power studies at the Cyber Policy Institute (CPI) in Jyväskylä, Finland, and Senior Adviser to the board of the ICT for Peace Foundation in Geneva, Switzerland.

Mika Kerttunen is Adjunct Professor in military strategy at the Finnish Natioanl Defense University and visiting faculty member at University of Tartu Law School. He is also Senior Research Scientist at Cyber Policy Institute (Estonia).

This report was financed by NUPI’s Centre for Cyber Security Studies.