The Alleged Demise of the UN GGE: An Autopsy and Eulogy

Eneken Tikk and Mika Kerttunen

New York
The Hague
Tartu
Jyväskylä

2017

We want to thank
Martha Finnemore, Anatoly Streltsov, James A. Lewis, Phil Lark and William Boothby
for their feedback and comments.

Special thanks go to Walle Bos for editing and research assistance.

We are indebted to the Estonian and Finnish Experts in the UN GGE for the opportunity to advise and observe the dialogue.

We want to express our deepest gratitude to
Michele Markoff and Andrey Krutskikh
for their contribution to our professional growth in this field.

The Alleged Demise of the UN GGE: An Autopsy and Eulogy

Eneken Tikk and Mika Kerttunen

The Alleged Demise of the UN GGE: An Autopsy and Eulogy

Eneken Tikk and Mika Kerttunen[°]

1. Introduction

The lack of consensus in the 2017 round of UN expert negotiations[1] has resulted in a renewed impetus for the many propositions on how to ensure responsible State behavior in cyberspace. Among those are: the call for a treaty that Moscow has promoted since 1998 in- and outside the UN[2]; the Code of Conduct submitted by Russia and China together with a group of Shanghai Cooperation Organization (SCO) countries in 2011[3] and 2015[4]; possibly another round of UN level negotiations of norms, rules and principles of responsible State behavior in cyberspace; a reinvigorated London Process [5] and ideas for stronger institutionalization of the dialogue[6].

[°] Dr Eneken Tikk is Senior Fellow of The Hague Program for Cyber Norms at Leiden University (The Netherlands). She has participated in three consecutive UN GGE's (2012/2013, 2014/2015 and 2016/2017) as adviser to the Estonian expert. Dr Mika Kerttunen is Director of Studies, Cyber Policy Institute (Tartu, Estonia). He served as adviser to the Finnish expert in the GGE 2016/2017. The views expressed in this paper are those of the authors. They should not be read as views, positions, or attitudes of the UN GGEs or any members of the GGE. Neither should they be interpreted as positions or thinking of any government.

[1] 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. See also Cuba at the final session of 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. See further, Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere, available at http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

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

[3] On September 12, 2011 the Permanent representatives of Russia, China, Tajikistan and Uzbekistan to the United Nations jointly sent a letter to the UN Secretary General asking to circulate the Draft International Code of Conduct for Information Security as an official document of the 66th UN General Assembly session. See annex to the Letter (A/66/359) dated 12 September 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".

[4] 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 (A/69/723).

[5] The London Process refers to a series of conferences ("Global Conference on Cyberspace") held biannually since 2011, so far in London (2011), Budapest (2012), Seoul (2013), The Hague (2015) and India (2017). These events convene governments, private sector and civil society gather 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 capture a number of principles and conclusions on responsible State behavior in cyberspace.

[6] See Statement of the Deputy Secretary of the Security Council of the Russian Federation, Oleg Khramov, at the international OSCE conference on cybersecurity, Vienna, 3 November 2017. Available at http://www.mid.ru/

Partially disappointed to the lukewarm international progress, partially encouraged by governments, major private sector companies have become active in forwarding proposals for greater public order in cyberspace. Entrepreneur Elon Musk worried of the "third revolution in warfare" has openly called for "morally wrong" lethal autonomous weapons systems to be banned under the UN's convention on certain conventional weapons.[7] Microsoft's *Digital Geneva Convention* calls on governments "to protect civilians on the internet in times of peace", and specifically "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".[8] German Siemens is formulating a digital charter for the private sector, which will be launched in the 2018 Munich Security Conference. Russian Nornickel, better known as Norilsk Nickel, a leading mining company, is similarly preparing a charter on information security of industrial critical infrastructure.[9] Google has put emphasis on baseline privacy, human rights, and due process principles in digital evidence gathering.[10]

In addition, strong voices have come forward from think tanks and academia. The Global Commission on the Stability of Cyberspace with their focus on the Internet infrastructure and the financial sector.[11] The Korean scholars have tabled the Bright Internet Agenda with focus on preventive measures and collaborative efforts between disjointed initiatives and agendas.[12] These State- or corporation-sponsored processes are complemented by numerous scholarly proposals for improving the landscape of international cyber security through norms of responsible state behavior.[13]

Such fragmentation of the international norms discourse has several implications. While all these parallel tracks potentially offer valuable food for thought and discussion, there is little prospect in any one of these propositions becoming comprehensively pursued, let alone universally accepted. Authoritative guidance for responsible State behavior in cyberspace remains far-fetched, not just because of yawning technical capacity divides and the known difficulties of attribution of state behavior in cyberspace, but also because the principal questions of the international cyber security discourse are far from being settled politically. Importantly, different proposals for new binding and non-binding norms are often premised on controversial arguments and beliefs about issues of international cyber security, their causes and trends.

This disintegrated dialogue may, on the other hand, indicate new leads during the operational pause that the 2016/2017 UN GGE outcome provides. It allows States and

---

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

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

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

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

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

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

[13] See Eneken Tikk and Liisi Adamson, list of literature on international cyber norms, available at www.univleiden.nl

scholars to (re-)position themselves in the discourse and invites scholars to critically study the proposals and arguments on the table.

To decide how to move the normative agenda of international cyber security forward, it is helpful to take a couple of steps back. Firstly, there is plenty 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 a lot to study about the pre-existing norms, cyber-specific or general, national or international, before making any definitive move towards replacing, renewing or expanding them. Thirdly, there are several ways of achieving common understanding and mutual acceptance on these issues, and not all of them have been exhausted.

The underlying interest behind this analysis is investigating and evaluating the current state of, and possible next steps for, developing international cyber norms.[14] *International cyber norms* constitutes a distinct discourse within the international cyber security dialogue, a *Glasperlenspiel* so far primarily played between governments, to determine and agree upon norms, rules or principles of responsible State behavior in the use and development of ICTs.

It has been widely concluded that the inability of the 2016/2017 UN GGE to deliver a consensus report is to be read as a failure.[15] This study pushes back on this assessment. Concluding that, like any UN Disarmament Committee process, the UN GGE is a highly politicized and accordingly contested venue, where consensus on key issues can be probed, yet not always achieved. This study further emphasizes that the UN GGE is a process within a process, whereby the outcome of one Group does not necessarily render the whole process and series of UN GGE's obsolete. The authors argue that from a political perspective, a no-consensus outcome can be as rewarding as a consensus report.

[14] The term 'norm' is used in two meanings throughout this paper. Strictly 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 has called States to adopt, *voluntarily*, standards for responsible State behavior that in the view of Group are not established under, although they may derive from international law. 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 their international obligations and guarantee the rights of other States (see Krasner, fn 80); furthermore, it has become accepted that expectations of behavior could also be prescribed by social pressure applicable between States with a given identity (see Katzenstein, fn 92).

[15] See Soesanto and D'Incau (http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance), also Melissa Hathaway (https://www.cigionline.org/sites/default/files/documents/Getting%20Beyond%20Norms.pdf), Liis Vihul and Michael N. Schmitt (https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/), Robert McLaughlin and Michael N. Schmitt (https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/), Adam Segal (https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what); CCD COE: 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 impair the implementation of the UN GGE guidance, and the 'universalization' of the attitudes and approaches that three consecutive UN GGE reports have promoted.

As the UN GGE has been a leading platform for the discussion, this analysis treats the UN GGE and further thinking of responsible State behavior as linked subjects, acknowledging that the discourse on responsible behavior is, and must remain, much broader.

2. The UN GGE Process: Goals, Expectations, Outcomes

2.1. The Original Proposal and its Context

Five GGEs have met within the framework of the UN First Committee Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security.[16]

The groundwork and idea for a resolution on information security came from the Russian Federation. The resolution initially emphasized the threat of *information weapons* and *information wars*, a choice of terms adopted from the mid-1990s aggressive rhetoric used in US military doctrine.[17] It is therefore fair to conclude that at least a partial goal of the Kremlin was to set back the US superiority in military development and deployment of ICTs that was demonstrated in the First Gulf war, and to restrain further operational development in this field.[18] In a similar pattern, current Chinese and Russian rhetoric on the need for *traffic rules* for the *information highway*[19] draws from the language used in the Clinton administration's policy aimed at the promotion of *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.[20]

---

[16] 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, 4 January; The resolution was adapted without a vote. Since 2006, the resolution has been open for co-sponsorship. 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.

[17] Ambassador Andrey 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" in Garmisch-Partenkirchen, 23 April 2015. See, for example U.S. Joint Publication 3-53 *Doctrine for Joint Psychological Operations* (10 July 1996) and Joint Publication 3-12 *Joint Doctrine for Information Operations* (9 October 1998).

[18] For further discussion of Russia's concerns beyond the I Committee initiative, see Tikk-Ringas (ed). *Evolution of the Cyber Domain: Implications on National and International Security* (2016). See also 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).

[19] 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 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.

[20] "… 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.

Moscow's original proposal in the UN First Committee was to ban *information weapons*[21] and their use by way of a dedicated international legal regime.[22] The first GGE might have been an attempt to achieve just that, given the emphasis of the Russian 1999-2003 submissions to the First Committee.[23] Several countries shared the Russian view on the advisability of an international arms control regime with regard to *information weapons*, among them Belarus[24], Mexico[25], and Brazil.[26] Unconvinced, the US argued that it would be "premature to formulate overarching principles pertaining to information security in all its aspects",[27] dismissing the need for an arms control approach. Aligning with the US, the UK suggested that a multilateral instrument that would restrict the 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.[28] The UK further took the view that a multilateral instrument approach might impinge on the free flow of information as a key principle of the information society.[29] Sweden, speaking on behalf of the EU in their 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 their view it mainly encompassed subjects other than disarmament and international security.[30]

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.[31] The Kremlin's alarming appeal during the first round of UN GGE deliberations did not attract sufficient sympathy to agree on a report. With the Group operating on the basis of consensus, one dissenting view would have been enough to prevent a report.[32] However, as the Chair noted, "even with the use of translation, the members […] spoke different languages with respect to essential issues

---

[21] 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 defence, 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.
[22] See letter dated 23 September 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.
[23] See letter dated 23 September 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).
[24] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).
[25] 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).
[26] Developments in the Field of Information and Telecommunications in the Context of International Security (A/60/95/Add.1).
[27] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).
[28] Developments in the Field of Information and Telecommunications in the Context of International Security (A-59-116).
[29] Developments in the Field of Information and Telecommunications in the Context of International Security (A-59-116).
[30] UN Developments in the Field of Information and Telecommunications in the Context of International Security (A-56-164).
[31] UNGA Resolution A/RES/58/32 (18 December 2003).
[32] 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.

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".[33]

2.2. Increasing Tension in the Mandate

The mandate for 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 cooperative measures to address them".[34] Assembling after the experience of politically motivated cyber-attacks in Estonia and Georgia, the second UN GGE 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.[35]

The Group recommended further dialogue 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.[36]

The third UN GGE in 2012/2013 continued to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. 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 the concepts aimed at strengthening the security of global information and telecommunications systems.[37]

During the 2012/2013 UN GGE, focus returned to the question of a possible new binding agreement on international information security. Russia's national position on this matter had not significantly changed since the inception of the First Committee process. However, during the 2012/2013 UN GGE, Moscow yielded to the US-UK proposition that there is no need for a new international legal instrument and that existing international law will be

[33] A/C.1/60/PV.13, page 7.
[34] UN Resolution A/60/45 (January 6, 2006) Developments in the field of information and telecommunications in the context of international security.
[35] Report of the 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.
[36] Report of the 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.
[37] 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).

sufficient to maintain peace and security in cyberspace. The 2013 UN GGE report concluded that "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".[38] However, it is less widely appreciated that this conclusion had more to it. 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". It further maintained that "given the unique attributes of ICTs, additional norms could be developed over time".[39] With these conclusions, the 2013 report could be read as the optimal point of balance in the international cyber norms dialogue, settling on little.

The mandate for the fourth GGE in 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".[40] 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".[41]

The fourth GGE was able to provide some additional references to international law that Experts deemed applicable to State uses of ICTs. The Group was not, however, able to clarify how international law applied, and the section on International Law became limited to an enumeration of selected provisions of the UN Charter. In the Group's discussions, furthermore, it became evident that participating Experts, as well as States, have rather different views on the legal status, interpretation and implementation of international law. This is evidenced by the listing of concepts like State responsibility and due diligence in a section of the report called "voluntary and non-binding" norms, rules and principles.

Despite obvious difficulties to elaborate and agree on matters of international law, the 2016/2017 mandate explicitly outlined the question "how international law applies to the use of information and communications technologies by States".[42] Answering this question became a bridge too far.

---

[38]Ibid, para 16.
[39]Ibid.
[40]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).
[41]Ibid.
[42]United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/72/327 (14 August 2017).

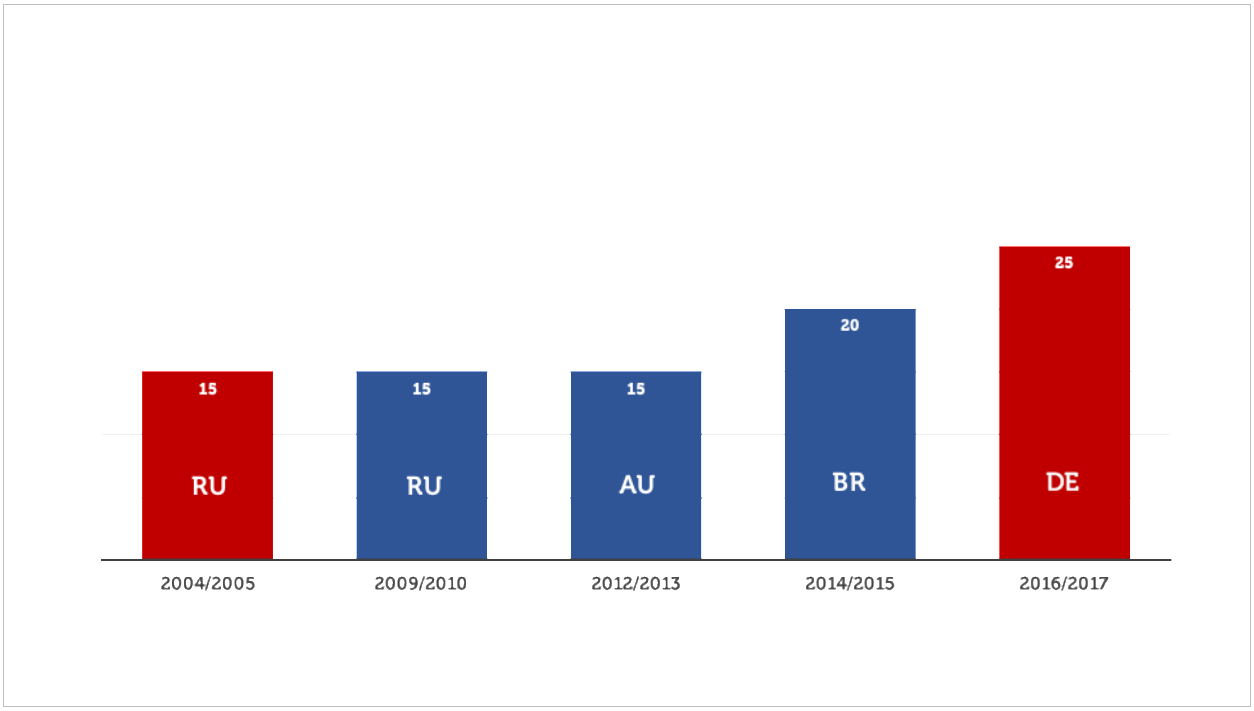

Illustration 1. The first three GGEs comprised experts of 15 States. The fourth GGE had 20 members and the most recent one 25 members. Russia, Australia, Brazil and Germany have chaired the GGEs. The first and the fifth GGE have resulted in no-consensus outcome.

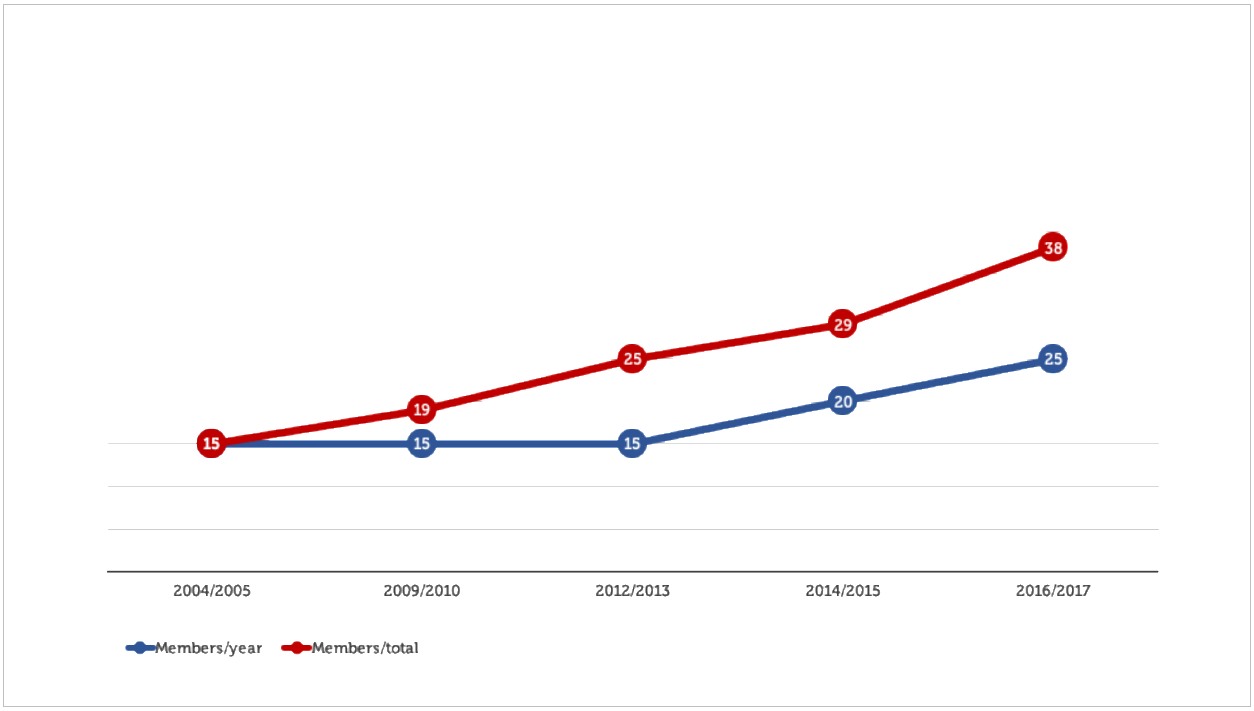

Illustration 2. The GGEs have been attended by experts of 38 States in the period of 2004-2017.

2.3. Gradual Compartmentalization of the Norms Discourse

For observers, the UN GGE process has been most confusing on the scope and definition of "norms, rules and principles" and their relationship to international law. Despite the mandate, throughout the years, requiring discussion and study of relevant concepts, the UN GGE has never fully clarified the use of terms such as *norms*, *rules*, and *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".[43] 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.[44]

On face value, the 2013 report can be read to maintain 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 is also reflected in the references that the Group made to otherwise contested leads. Paragraphs 17-20 of the 2013 report reflect the Group's views on the applicability of some of the earlier UN recommendations,[45] noting the SCO Code of Conduct and offering a general confirmation on the applicability of international law, making particular reference to the Charter of the United Nations [46] as well as the concept of sovereignty.[47] 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 cyber powers' thinking in well-crafted consensus language.

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) came to be 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. Even where States could not agree on specific applications of international law, this would not be framed to mean that there is a need for a new treaty. This move also provided a convenient way to disagree about international law, even among the otherwise like-minded States.[48]

---

[43] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN A/68/98, page 8.
[44] Ibid.
[45] 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.
[46] Ibid, para 19.
[47] Ibid, para 20.
[48] The phrase 'like-minded States' is used to refer to States that have views that largely align with those of the US.

Between the 2013 and 2015 reports it becomes visible how Experts have not been able to agree on the status of certain concepts under public international law, such as State responsibility and due diligence. Furthermore, it 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.[49] In other words, the previously stated connection between international law and norms disappeared.

At the same time, despite emphasis on *voluntary norms* in paras 9 and 10 of the 2015 report, the title of section III still refers to norms, rules *and* principles, confusingly retaining the scope of discussion set by the 2013 report. The 2015 report offered recommendations of eleven voluntary norms, rules and principles that in the view of Experts were likely to improve the international cybersecurity situation.[50] Many regarded these recommendations as the main success of the 2014/2015 GGE.

In the enthusiastic climate that the seeming success of the 2015 GGE report created, the international community placed high hopes on the fifth GGE. More than 40 countries competed for the available 25 seats, many of them newcomers to the process, demonstrating an increased interest in the work of the GGE and the issues discussed in the Group. In addition to the expectation of increased buy in through inclusion of new States in the discussion, States were also hoping for further progress and clarifications of the recommendations made in the 2015 report. After all, 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,[51] were underway about how international law can be applied in and to cyberspace or further developed for the purposes of international peace and security. New proposals for non-binding norms had been suggested in the hope that the next GGE would include them in the 2017 report.[52]

However, in the context of a gradually more ambitious mandate, it was visible to seasoned experts that achieving further consensus during the 2016/2017 GGE would be difficult. On the one hand, differences on international law prevented crafting further consensus language on the application of the recommendations listed in para 13 of the 2015 report, or to possibly even list further applicable concepts and rules. On the other hand, prioritization of the international law section above other topics indicated a lack of progress on this account, whereby other sections will remain hostage to this lack of progress.

[49]Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/172), paras 9 and 10.
[50]Ibid, para 13.
[51]Microsoft's proposal for a Digital Geneva Convention. Brad Smith (2017) The Need for a Digital Geneva Convention. Available at https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/
[52]See, for instance, Dennis Broeders (2016) The Public Core of the Internet: An international Agenda for Internet Governance, available http://en.aup.nl/books/9789462981959-the-public-core-of-the-internet.html

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

Describing the 2016/2017 GGE as a failure over-emphasizes the relationship between the GGE and international law and conditions the GGE's success to a tangible outcome, a report almost regardless of its content. However, the value of the no-report outcome in 2017 is that it clearly shows just how fragile and carefully crafted any previous 'agreements' on the same subject were. It indicates principal differences between the leading cyber powers and the challenges of overcoming these. The process also provided valuable information where nations stand and what they are ready to accept-or not.

Indeed, the GGE is *the* discussion of State responsible behavior in their use of ICTs. It is *the* attempt of the cyber super powers to convince each other, and the international public, of not just looming threats but 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 capacity.

Picking up and examining the broken pieces of the process that the Experts involved in the UN GGE have left behind, has become a forensic thread in the work of international cyber security and international law experts. What was deliberated, who agreed and who rejected what, why, and with what outcome? Though such questions, no doubt, yield insights in the positions, policies and politics of states, the GGE cannot decide, or even authoritatively conclude, that international law *is* or is not *applicable*. At most, the GGE has offered a perspective. Neither the views of individual experts, nor positions of selected countries, provide ground to conclude that cyberspace is a lawless space.

Yet the GGE has never been mandated to create, or dismiss, existing international law. The Group was tasked to discuss, and literally, study, how international law can be, and is in fact, applied to threats to international peace and security resulting from State use of ICTs. The fact that 25 experts were not able to be conclusive on the issue, largely due to the underlying political differences, should not be read to diminish 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.

The outcome of the most recent GGE simply 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 not enough determination among the participating experts to overcome them. This outcome can therefore be seen as a call for each State to come up with their own views about how to apply international law to issues of cybersecurity.

Still, the 2017 result remains wide open to interpretations. These narratives will reflect how differently various parties read, interpret and communicate the whole process, its value and its potential. Curiously, they also make visible the different extents to which States and scholars understand and interpret international law. There is hardly a single decisive point of failure in the 2016/17 GGE process. The analysis below discusses possible differences, misunderstandings and challenges that can explain why the Group did not achieve consensus.

3.1. True Differences

The perhaps easiest explanation of why and how the 2016/2017 GGE did not manage to achieve consensus, derives from a comparison of positions and perspectives involved. That is to mean the political and practical views, and preferences, about the development and use of ICTs among the super powers and other groups of countries. International cyber security discussion, where expertise is complemented by global representation, becomes a marketplace of sometimes diametrically opposing world views and belief systems. This is understandably and justifiably the case, as thus contestation predates any ICT and cyber discourses.

Contestation is most visible and sensitive in relation to the question of state sovereignty *versus* international obligations, and the relationship between the State and the individual. Broadly, there are two main views regarding how international cyber security should be achieved and organized: The Western or 'like-minded' approach, that focuses on promoting and explaining the existing international law, and the Russo-Sino call for *lex specialis* and reinforced international political structures, mainly the UN, as the mechanism to maintain international peace and security. There is also a range of concepts and rules of international law that invoke contradictory reactions among participating States.

Differences on International Law

A prominent fundamental difference attaches to discussion of the implications of the prohibition of use of force in the context of use of ICTs. In concluding that Article 2(4) of the UN Charter is a ground for banning State-on-State attacks in cyberspace, especially 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 that suggests legitimization of cyber warfare. The Chinese stand on these norms and instruments of international law is strictly textualist,[53] political and principled at the same time. Deriving from the proposition 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 reading 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, while at the same time it cannot eliminate the opposing viewpoint. In other words, while a technical reading of law makes it impossible to think that reference to Article 51 in the UN Charter would legitimize, let alone incentivize, armed

[53] 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: West, 2012).

conflict in cyberspace, such reading of the debate disregards the more political stand 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 nobody but 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.[54] Russia and China have made it clear that they deem it well within their right to stop (both incoming and outgoing) information at their borders, stating that each country has the right to manage its own cyberspace in accordance with its domestic legislation.[55] Such a view, again, is a principled stand and their long-time reading of international law. The argument for strong, flat, sovereignty is also taken by other countries, albeit on the basis of different considerations.[56] For most countries, ICTs are often of foreign origin and as such seen as an opening to unforeseeable and undesired influence and interference. [57] Their claim for sovereignty may reflect their distrust towards technologies and donors, whose goals and interests might be contrary to theirs. These takes on sovereignty go against the US and the like-minded drive for free flow of information.[58] Differences on the matter are most visible in the context of content, where the US First Amendment reading implies high tolerance to all forms of speech, whereas the Sino-Russo view prefers a much more controlled information environment. These differences, however, predate the cyber security dialogue, and are likely survive it.

Sovereignty, and the exercise thereof, is further problematic as to specific rights and obligations in the context of ICTs. Countries possess very different capacities and priorities in dealing with information/cyber security. Cuba, for example, has concluded that the "unequal 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".[59] Lack of attribution capability has been emphasized and echoed over and over in international cyber dialogue.

On some issues, there are also considerable differences among the otherwise aligned countries. The US and the UK, for instance, do not acknowledge due diligence as an established obligation in international law.[60] Also, there seems to be a broader rejection of

---

[54] Developments in the Field of Information and Telecommunications in the Context of International Security (A/61/161).
[55] (61/161)
[56] 2012 WCIT vote, see https://www.ip-watch.org/2012/12/13/wcit-split-after-split-vote-on-internet-governance-resolution/
[57] 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).
[58] See US submissions on the subject.
[59] Developments in the Field of Information and Telecommunications in the Context of International Security (A/54/213).
[60] 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 State legal or financial liability. See also Department of State *International Cyberspace Policy Strategy* (March 2016).

the binding nature of ILC Draft Articles of State Responsibility, as reflected in para 13 d and f of the 2015 report. The doctrine of countermeasures is similarly contested.

The question of ICTs and free flow of information

The struggle over information and communication technologies has been on the UN agenda in various forms and venues since its inception. While the technologically most developed countries prioritize the free flow of information, the developing countries pursue equal access to information and information technologies. On the other hand, the East Bloc has been hesitant to subscribe to a world order premised on de-centralized flows of information and perceives certain ICTs and 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),[61] the World Summit of Information Society[62] and the World Congress on International Telecommunications (WCIT).

As China has clarified in the First Committee process, the problem of information security to them not only involves 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.[63] In his statement to the General Assembly, the Russian Chair of the 2004/2005 GGE noted that issues of international information security are rooted in the global information revolution. [64] Accordingly, China and Russia prefer to focus on 'international information security'.

According to the US, however, 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.[65] The UK has clarified their choice of terms, shedding further light to the underlying differences: there is scope for potential confusion in the use of the term "information security" in that 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 validity of the term "information security" when used in this context, since it could be employed in attempts to

[61] A UNESCO study of 1978 concluded that the international information system showed 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 requesting re-organization and re-consideration of policies and regulations pertaining to media, access to information, copyright, and spectrum management. International Commission for the study of communication problems: the new world information order (1978), available at http://unesdoc.unesco.org/images/0003/000340/034010EB.pdf.
[62] Declaration of Principles Building the Information Society: a global challenge in the new Millennium, Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003.
[63] A/61/161.
[64] A/C.1/60/PV.13, page 5. See also 2000 Information Security Doctrine of the Russian Federation that 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)).
[65] 59/116/Add.1

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.[66] 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'.[67]

The Question of *Lex Specialis*

During 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",[68] Russia has made numerous proposals as to concrete issues and ways of their resolution,[69] and has continued to develop normative frameworks[70] that other countries can accept and adhere to.

Moscow has moved regionally and unilaterally to build alternative platforms for their agenda. In 2009, States of the Shanghai Cooperation Organization (SCO) settled on an agreement for cooperation aimed at ensuring "international information security".[71] In 2011, Russia tabled a concept *Convention on International Information Security*, which at the time was mainly distributed through Russian embassies and diplomatic representations.[72] In 2013, an agreement on cooperation was concluded among the Commonwealth of Independent States to improve information security.[73] In 2011 and 2015, Russia and China were supported by other SCO countries in their submission to the UN Secretary-General of another draft document to facilitate international consensus on international norms and rules guiding the behavior of States in the information space.[74]

Russian national policies confirm their commitment to a treaty process, considering it 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".[75] This Russian objective is accommodated in the consensus language of the

---

[66] (UK 68/156), a position shared almost word by word by Sweden in (69/112).
[67] See, e.g. Earle, Beverley; Madek, Gerald A. International Cyberspace: From Borderless to Balkanized, in Georgia Journal of International and Comparative Law, Vol 31, 2003, No. 2, page 225ff.
[68] 59/116, Russia, 1, para 6.
[69] 59/116, Russia, 1, para 14.
[70] See SCO Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (June 2009), Concept Convention on International Information Security (Russian MFA, September 2011), International code of conduct for information security (A/66/359; A/69/723).
[71] The agreement was concluded between People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on July 16, 2009.
[72] The Concept Convention was uploaded on the website of the Russian Ministry of Foreign Affairs on September 22, 2011.
[73] CIS Information Security Agreement was signed by heads of CIS states in St. Petersburg on November 20, 2013.
[74] "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).
[75] "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

2012/2013 Group's conclusion on the applicability of international law, which must be read in conjunction with two other sentences in para 16: "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."[76]

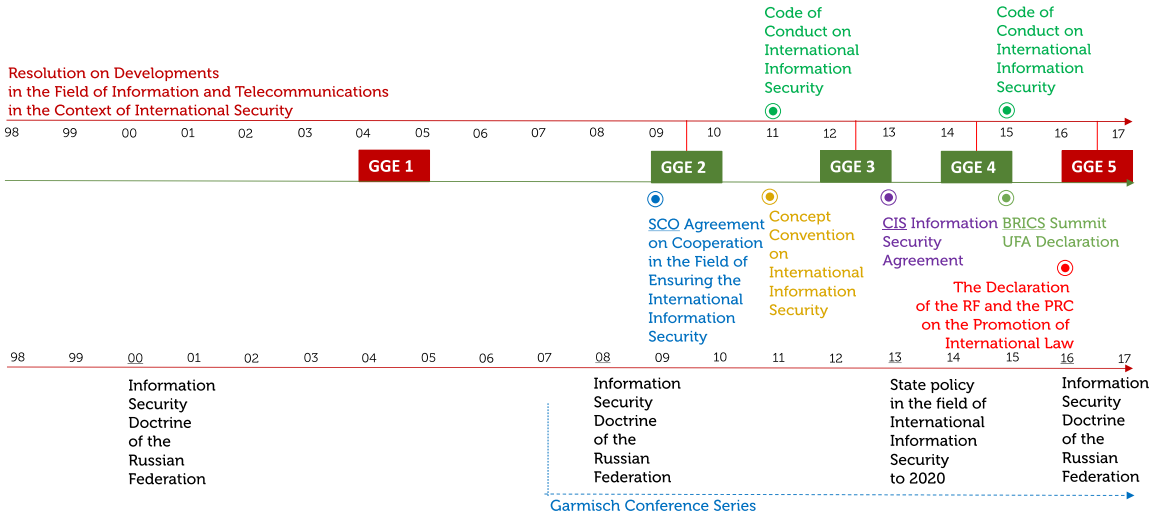

Illustration 3. Overview of Russian International Information Security Policy: In the past two decades, Russia has consistently maintained and furthered the call for a binding and universal agreement on international information security. It has taken steps at national, regional and international levels to socialize and promote this idea.

In contrast, especially the UK and the US have been nothing but dismissive about a treaty negotiation. In 1999, the US 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 pre-empt or interfere with the work of the international community that is already under way".[77] The US added, a year later, that "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".[78] 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

Russian Federation; see also Dylevsky, I.N. et al, "Political and Military Aspects of the Russian Federation's State Policy on International Information Security" Military Thought 24:1 (2015).

[76] 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.

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

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

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".[79]

Considering the above, GGE discussions of international law are possible within very limited margins. The 2014/2015 Group was able to make reference to some norms or rules of international law but not others. Some of the proposed voluntary, non-binding norms read like established international law to many observers.

Different interpretations of international law are not only possible, but in the case of ICTs, visible. A dialogue that would consider different readings of international law and open possible interpretations to a more inclusive dialogue, might be welcomed by the international community. Politically, however, a law-focused international process might underscore that there is little recourse to the situation. Different readings of international law will forever be possible, and attempts to lock specific interpretations would require a new normative regime. Calling for such a regime in a highly contested and unequal environment, focusing on use of certain technologies, would likely not result in an agreement.

Although authoritative research and analysis has been offered on issues of international law[80], it does not seem to enjoy consensus by all scholars[81], let alone States. It can be anticipated that a more inclusive discussion of the applicability of international law in the context of cyber security is to reveal grave, and in many occasions irreconcilable differences, between States. So far, 70 States have shared their views on international cyber security issues and respective normative remedies in the First Committee Process. Their submissions highlight differences on specific concepts and rules of international law.[82] National submissions also underscore that many cyber security issues would need to be addressed in national legislation and policy, thus calling for a more critical and less politicized search for remedies to international cyber security issues.[83]

---

[79] A/59/116.

[80] Notably Michael N. Schmitt (Ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press and Michael N. Schmitt (Ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. It is important to observe that the authors of the Tallinn Manual have not just different views on specific concepts and rules of international law, but also that between the two projects, views on some aspects of international law have changed.

[81] 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, published his, partially dissenting, views on International law and cyber security shortly after TM2 was released. See Kriangsak Kittichaisaree (2017) Public International Law of Cyberspace. Springer.

[82] Analysis of national views contradicts the claim of some of the Tallinn Manual authors that "all of us understand International law the same way", shared at TM2 launches as well as several dedicated workshops. At the same time, they confirm the findings of Professor Anthea Roberts in her recent book. See Anthea Roberts (2017) Is International Law International? Oxford University Press.

[83] See Annex B for an overview of national submissions in the First Committee process.

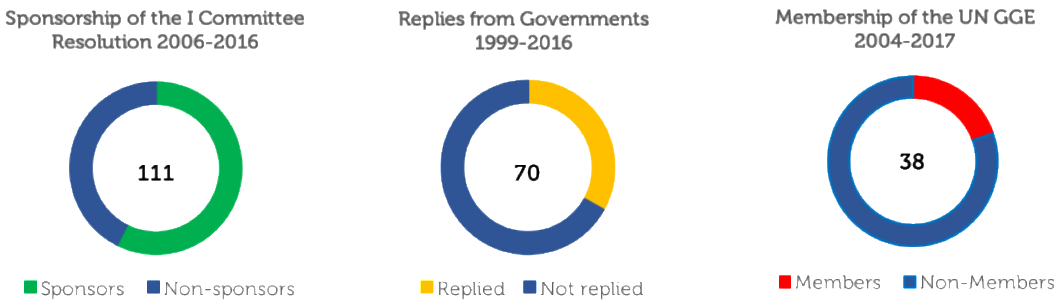

Illustration 4. Over the past decades, Russia has been able to gather considerable involvement of States in the First Committee process. Despite the relatively small number of States in the GGE, 70 States have shared their views on the issue and 111 States have sponsored the Resolution since 2006.

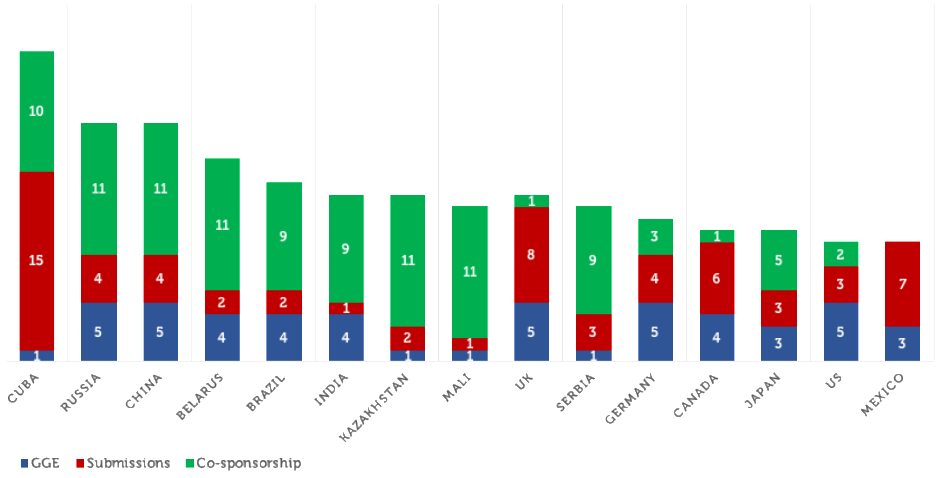

Illustration 5. The UN GGE process has been more actively shaped by the States supporting, or not completely dismissing, the Russian propositions.

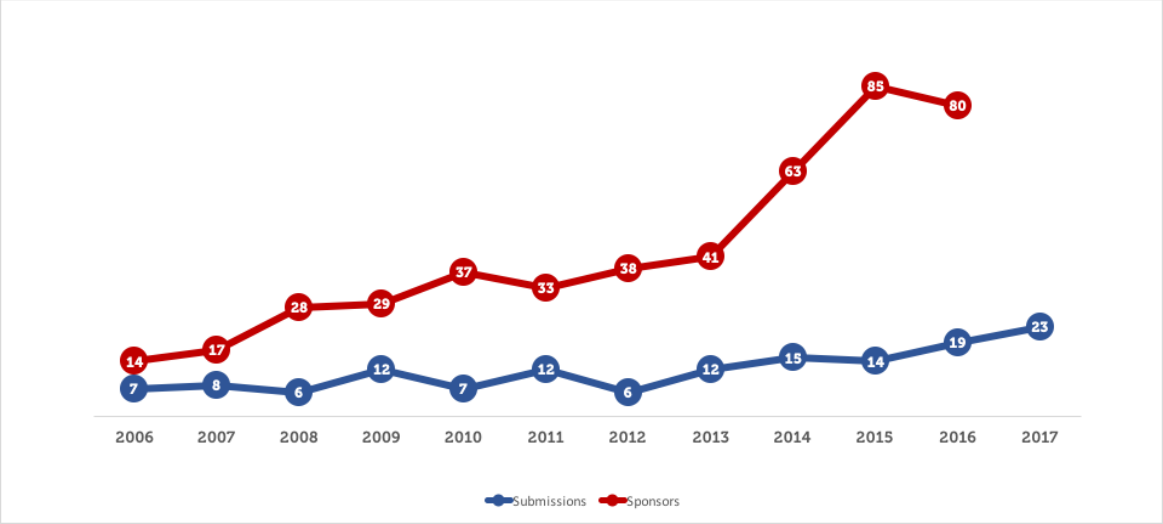

Illustration 6. Sponsorship of the resolution and the number of yearly national submissions has steadily increased.

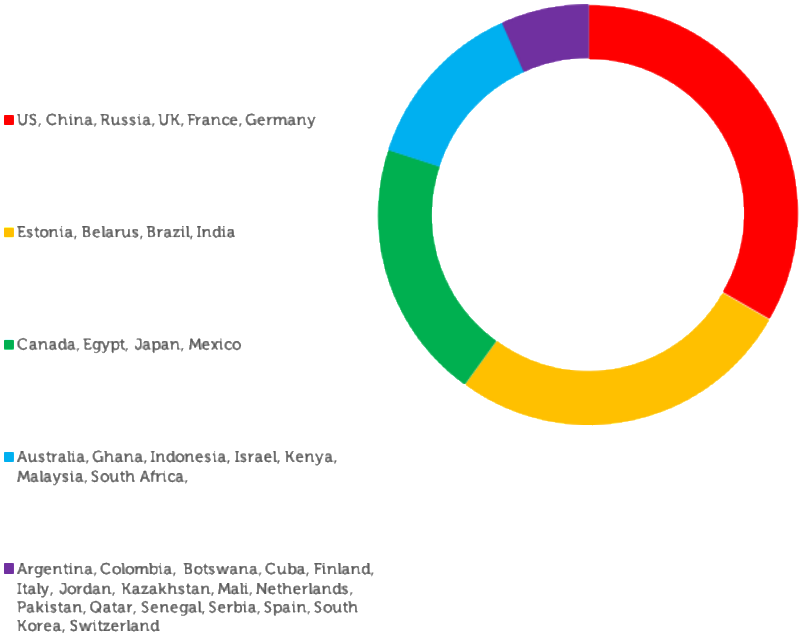

Illustration 7. The Permanent Five and Germany have been part of all UN GGEs. Estonia, Belarus, Brazil and India score 4 points. Most States, however, have participated in only one or two UN GGEs.

3.2. Methodical Challenges

Attempting to edit away and mitigate the irreconcilable differences discussed, Experts within the GGE were faced with considerable methodical challenges.

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

When combining the concepts of norms, rules and principles in the context of recommendations for voluntary and non-binding guidance for State behavior, Experts created an inevitably confusing language.[84] Although all 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) also operate at different levels of abstraction.

Following Krasner, principles are beliefs of fact, causation and rectitude.[85] Principles refer to politically, administratively and morally anchored assumptions of state of affairs and provide foundation for more explicit rules and reasoning.[86] As discussed, leading actors have different views on the very fundamental questions related to the development and use of ICTs. Exploring shared principles that are not contingent to, or conditioned by, any particular group identity, could help implementation of the recommendations on, and reading of, norms. An illustration of this can be found in the existence of traffic rules: Australia, Malaysia and the UK all have left-sided traffic, and countries around the world practice rather different standard speed limits, nonetheless there is a fundamental and universal agreement that automobile traffic needs to be regulated and that speed limits are necessary, for instance, in densely populated areas.

Norms are difficult to define and agree upon without their due contextualization and anchoring in the underlying (or guiding) principles. A principle-oriented thread of the international cyber security discourse would have the benefit of clarifying the path. While it might still be premature to try to formulate an exhaustive list of overarching principles for international information security, some directions could be considered. To support their

[84] The distinction between norms, rules and principles is essential as they differ in level of abstraction and normative cause. It is widely accepted in the international cyber security discourse that State's cyber activities 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, whereby a regime is comprised of principles, norms, rules, and decision-making procedures around which expectations converge in a given issue area (Stephen D. Krasner, "Structural causes and regime consequences: regimes as intervening variables". International Organization 36:2 (Spring 1982), 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, whereby norms are standards of behavior defined in terms of rights and obligations. Rules, according to Krasner, are specific prescriptions or proscriptions for action. For a more detailed discussion of the recommendations made in the 2015 GGE report, see [UNODA publication, forthcoming 2018].

[85] See Stephen D. Krasner (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables, page 202.

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

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 United Nations Charter.[87] A useful framing direction for the audiences of the GGE work would be re-emphasizing that nothing in the report should be read as undermining international law. There might be space to conclude that efforts of international cyber security are necessary to support a trusted and functioning ICT infrastructure. Furthermore, despite political differences, almost all States seem to see value in a more predictable and stable state of international cyber affairs.

Krasner defines norms, seen from an international law perspective, as expectations of behavior defined in terms of rights and obligations.[88] Without resolution of agreed goals at principal level, such rights and obligations would be easily interpreted with different assumptions and goals in mind. Shannon observes that the more parameters a norm possesses and the more abstract those parameters are, the easier it will be for the actors to interpret them favorably to their particular interests.[89] This will be an essential observation in the phase of accepting, and implementing, the UN GGE recommendations.

A superficial reading of the UN GGE 2015 report is that it identifies new norms of responsible State behavior in their 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 neither new, or norms. They are literally recommendations on norms, rules or principles. Some of them derive from areas of international law that did not enjoy the consensus of experts on being fully settled as binding obligations. Others open up themes and issues where it was thought 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 have yet to be accepted as norms, in order to then be implemented.[90]

Mixing of legal and political science reading of 'norms' in the international cyber norms discourse is unfortunate.[91] While noticeable in the GGE mandates and reports, inconsistency in use of terms and concepts has created profound confusion, and very different assumptions, among observers of the process. As a result, the impact and implications of the UN GGE reports have been interpreted in very different ways and raised different expectations.

Questions of Application of Social Norms Theory

In sociology and political science norms usually are referred to as collective expectations for proper behavior of actors with a given identity.[92] Applying the sociological norms theory to

---

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

[88] See Krasner (1982) Structural Causes and Regime Consequences: Regimes as Intervening Variables, page 202.

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

[90] See the Programme for Cyber Norms at Leiden University.

[91] See, for instance, Michael N. Schmitt and Liis Vihul, The Nature of International Law Cyber Norms (2015).

[92] Peter Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (New York, NY: Columbia University Press, 1996).

the exercise of state interests in the context of national security, once observed by Katzenstein[93], and especially the premise of 'given identity' may have been beyond reach in the UN GGE discussions for the reasons discussed above. Wendt goes to note that the international system is not a very "social" place, making it a hard case for constructivism on both the social and construction counts.[94] Conversely, what seems to be shared among participating States is a strong belief in sovereignty and the possession of contingent interests. The outcome of the 2016/2017 GGE underscores that states are much more autonomous than individuals from the social system in which they are embedded.

Without supranational authority and clear alignment of interests, States remain, by definition, solitary actors, not incompetent to cooperate, but only making decisions to do so based on their own premises. 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 upon agendas, structures and mechanisms perceived to support their interests, expectations and applicable remedies.

State behavior is not only norms-driven, at least not *voluntary norms* driven; it is also affected by ideological, administrative and individual interests, some perhaps more durable, some petty.[95] 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. Following the very (social) definition of norm the social force to cause normative change obviously operates stronger at national and regional levels as well as within groups of similar value systems than universally.

Given the premature understanding what cyber security is 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 manifest between 193 actors with (justifiably) sovereign interests and authority. Application of social norms theory to State behavior may easily disregard actual political processes by which decisions and policies are formulated and implemented. Wendt observes that "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."[96]

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

[93] Katzenstein (1996), see Introduction, and especially note 12. Katzenstein's book offers a sociological perspective on the politics of national security,
[94] Alexander Wendt, Social Theory of International Politics (Cambridge: Cambridge University Press, 1999, p. 2
[95] Cf. April Mara Barton (2000) where the focus on cyber norms is strictly on community-level development and convergence of cyber norms and traditional social norms.
[96] 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?"

'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 principal stands of the US and aligned cyber powers. A more likely reading, therefore, is that the words 'non-binding' and 'voluntary' are most characteristic of what the status of the normative sentences in para 13 are intended to have. Here, the inconsistency in normative status of the recommendations becomes problematic for those who view State responsibility and due diligence obligations as legally binding. In any case, a thorough reading of the GGE work so far highlights that States question whether all rights and obligations relevant to international cyber security are, in fact, found, or even grounded, in international law.

To conclude on methodical challenges, absence of commonly accepted topology, lexicon and definitions has remained a consistent impediment and challenge to a constructive dialogue since the first GGE. The Group's inconsistency in its use of the terms 'norms, rules and principles' might have added to difficulty in achieving consensus. With their inconsistent treatment of 'norms', the 2013 and 2015 GGE reports may have set overly high expectations to further agreement and understanding. On the other hand, the facilitating language of the Group has encouraged several events and fora to pick up the theme of cyber norms, in a hope to enhance and inform further conversations on the topic, as well as the implementation of the Experts' recommendations. [97]

The fact that there are many questions that remain open, and the inability to identify definitive answers or directions in the GGE work so far, indicates that either the Group has worked without clear conceptual foundations, or that it has knowingly dismissed the need for methodological vigor and consistency in its work.

3.3. Procedural Complications

A GGE's 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 easily build on misunderstanding, misperception or bad leadership. They can attach to the procedure at hand or be more conceptual in nature.

[97] Several of them are mentioned in the introduction to this article. 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 United Nations addressed to the Secretary-General (UN A/69/723). See also Brad Smith, President of the Microsoft Corporation, calling for a Digital Geneva Convention in his address of the RSA Conference 2017 (available …). 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 international security and stability and guide responsible state and non-state behavior in cyberspace (see https://cyberstability.org/).

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.[98] Russia, however, has interpreted the 2015 outcome as a testament of the need for additional norms, rules and principles and thus, evidence of the inadequacy of existing international law.[99] However, as discussed, the balance in the GGE process was best in and right after the 2013 report.

Since 2013, however, the GGEs were convened with little to no intervals. This might have resulted in too little time to coordinate and consolidate views on the matter. Also, from the originally 15 Experts, the 2014/2015 Group was sized up to 20 and the 2016/2017 process involved 25 Experts (see Annex B). This might have resulted in both qualitative and quantitative challenges in organizing the work. The GGE's normally conduct four week-long sessions over a period of eleven months. With 25 participating countries, discussion gets easily repetitive and prolonged.

A move to satisfy the curiosity of States, and the request for more inclusiveness, may have compromised the usefulness of the process. With 15 Experts, the GGE had provided a controlled environment for the leading cyber powers' strategic dialogue with marginal oversight from other countries. A GGE of 25 is a very different process, bringing to the table expectations that the format is unable, and unfit, to satisfy: the quality of compromise language would have to accommodate all the world views, legal concerns, implementation considerations and other points raised by members of the Group.

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 interpreted its mandate to be quite broad. This might have been an essential factor in the great 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 the corresponding measures to be taken by the international community. The emphasized focus on 'peace-time' norms since 2015 may, on the one hand, be read as supporting the Russian and Chinese preference for peaceful settlement of disputes. At the same time, it may be reflective of the lack of sufficient 'conflict' substance in international cyber affairs.

[98] http://2007-2017-blogs.state.gov/stories/2015/07/09/advancing-norms-responsible-state-behavior-cyberspace.html.

[99] See the (incomplete) translation of Ambassador Krutskikh's comments to the Russian newspaper "Kommersant" at https://www.csis.org/blogs/strategic-technologies-blog/russian-newspaper-kommersant-interviews-special-representative. See also https://www.rbth.com/international/2015/08/19/global_cybersecurity_6_questions_on_the_key_issues_as_seen_from_48615.html

4. Further considerations

Regardless of the fate of the GGE itself, the Group's reports have cultivated a fertile ground for contributions from industry, academia and non-participating States.

While the 2013 and 2015 GGE reports have not specified the relationship with, and the role of, the private sector in international cyber security, they have acknowledged that such a relationship exists, or needs to be established. The 2015 report concludes that "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 momentum for the private sector to insert their views and proposals into the process. It also emphasizes the need to allocate the responsibility and accountability for cyber security issues more broadly than to governments.

Inviting to academic curiosity and elaborations, the relationship between the UN GGE recommendations and pre-existing norms and rules require further clarification. Some of the instruments that States have deemed relevant in the context of international information security include OECD Guidelines for the Security of Information Systems,[100] the Budapest Convention [101] and ITU ITRs. [102] Furthermore, the ongoing EU cybersecurity reform, combining significant developments in network and information security,[103] personal data protection,[104] cybersecurity[105] and cyber diplomacy,[106] offer valuable leads for how the GGE recommendations could be implemented. Furthermore, studies indicate a significant body or principles, norms and rules that are applicable to various aspects of cyber security and point out the need to thoroughly study and implement the pre-existing norms before offering new normative instruments.[107]

---

[100] 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 that apply 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. More information can be found in 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/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm.

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

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

[103] 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.

[104] 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).

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

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

[107] See Eneken Tikk (2018) Future Normative Challenges. Paul Cornish (Ed.) Handbook on Cybersecurity (OUP, forthcoming 2018).

Scholars could also provide useful assistance in analyzing the recommendations as to their novelty, expected outcomes, and the preconditions and support mechanisms for their implementation.[108] 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 cyber security might mitigate some of the issues that currently the GGE is expected to address and has found challenging.

The pause that the 2017 no-consensus outcome has created, offers a window to develop and enhance national prowess to narrow the digital gap, address every day cyber security issues and reduce perceived insecurity; develop regional normative initiatives that build on shared threats, capabilities; study State and legal practice to become informed 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 cyber security. There is an obvious lack of international cyber policy lead in the industry with Microsoft as the most prominent cyber norms entrepreneur.

Engagement from the civil society and academia will prepare the international community for what inevitably lies ahead: a continued push for a convention that would refine State power and international security in cyberspace, creating much sought predictability *of affairs*.[109] 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. All States should form 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 when it comes to identifying, comparing and promoting international norms. So far, only 70 countries are reported to have developed a national cyber security strategy[110], although call for a strategy could be an emerging norm of its own.[111]

While the GGE format itself is unable to accommodate a larger participation, individual Experts and participating States could invite regional discussions and contribute their points of view by written submissions in the underlying First Committee process. More than 60 States have shared their experience and views about ways to mitigate peace and security risks stemming from State uses of ICTs. [112] National undertakings and experiences in providing international cyber security and stability are questions of practical importance

[108] Eneken Tikk has developed a ten-step schema, a 'norms test', to evaluate the need and develop the scope of norm proposals. See Eneken Tikk (2018) Future Normative Challenges. Paul Cornish (Ed.) Handbook on Cybersecurity (OUP, forthcoming 2018).
[109] See Illustration 3 explaining the international cyber policy goals and instruments of the Russian Federation.
[110] Mika Kerttunen, "National Cyber Security Strategies: A Normative Reading" in O.Y. Bos and Eneken Tikk (eds.) *Legal Perspectives on Cyber Stability* (The Hague: T.M.C. Asser Press, 2018).
[111] The need for a national cyber security strategy required under the African Union Convention on Cyber Security and Personal Data Protection (Article 24 (2)) and the EU NIS Directive (Article 2a).
[112] See Annex D.

and add value for the purpose of mutual understanding and commonly accepted standards of behavior.

National experience, however, might reveal what could have constituted another choking factor in the 2016/2017 dialogue. Albeit costly and serious at national, corporate and individual levels, (very) few cybersecurity problems are or have become direct questions of international peace and security. Some countries doubt the existentiality of threats posed by uses of ICTs that both Russia and the United States forcefully advertise. To follow the GGE's own language, the suggested 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 of 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. Data breaches, website defacements, increasing cybercrime and botnet topologies, more than they speak of the potential of cyber warfare, testify of a cyber crisis surface where the risk of unwanted or unforeseen developments cannot be effectively prevented due to the still low awareness or obvious capacity gaps. Therefore, the GGE has, without necessarily meaning to, developed at least two separate agendas of international cybersecurity: one that can be understood and explained by way of traditional geopolitics and where the likelihood of conflict or no conflict does not depend significantly on ICT as such. Absent ICTs, the relationships between the US, China, Russia, Iran and North Korea remain largely the same. What geopolitics cannot exhaustively explain, is the surface of potential cyber crisis that has emerged by way of extensive adoption of ICTs across the world, without due acknowledgment of the accompanying risks and ways of their mitigation. Jumping on the international information highway has been too fast, too soon, for countries that are not able to run sustainable information systems and services: States that have to run on Windows XP, cannot be helped by any of the UN GGE recommendations.

Also, despite the cyber threat mantra, the UN Security Council has not once examined cyber security as a threat to international peace and security. Yet the UN First Committee is a platform for disarmament and international security issues. Absent evidence of cyber threat that amounts to threat to international peace and security, the GGE is unlikely to provide actionable guidance to the international community. It will fall upon the next GGEs to critically revisit their mandates and convince the international community of the gravity of the threat and the actual need for, of its product.

5. Conclusion

None of the findings described in this paper are fatal for the GGE process. Although the GGE is in a critical condition, it is far from dead. There are strong proponents for keeping up the process and it is likely to return sooner or later. Regardless of whether the GGE survives or not, the real question is what we have learned from the process so far, and the 2016/2017 flat line in particular.

Although the GGE cannot change or create international law, it does flag important considerations for further discussions about it. There is little settled State practice with regard to the use of ICTs, let alone near-universal 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 would likely result in even stronger counter-narratives and stands. While there is 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 reading 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 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 of existing remedies. Whether States taking refuge in existing legal principles giving them the widest freedom of behavior is acceptable or not, is the most pressing issue for the coming years. It is a question that requires an answer from every sovereign nation.

While the US and the like-minded want current international law to be clarified, and the Sino-Russo coalition seeks *lex specialis* on State development and uses of ICTs, both sides need to offer more convincing evidence to substantiate their arguments and propositions.[113]

There is a potentially high price to pay for the lack of conceptual and methodical coherence in the international cyber norms discourse. Absent a structured and framed dialogue between States, any guidance to the international community becomes subject to competing interpretations, and thus often meaningless. Failure to assign the right meaning and weight to facts, determine factors of causality in cyber security issues, and define appropriate remedies, are likely to prolong searches for shared understanding and agreement.

It is essential that the GGE no-outcome will not be interpreted as leaving the world in the dark, but as showing that additional light needs to be shed on how to maintain international

[113] To offer more grounded argumentation the authors have launched a feasibility study to investigate national and expert opinion on different proposals of and models for cyber convention as well as the feasibility of these thoughts.

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 a few others, existing international law and responsible State practices, to start with. The speed at which the international community is able to create effective remedies to international cyber security issues, does not have to be dictated by experts. A still useful guidance for the way forward is to be found in the US submission in 1999: the international community needs to do a substantial amount of systematic thinking before going further. To facilitate this, Member States should seek ideas and insights from a broad range of experts in our respective Governments and societies.[114]

To accept, for the purpose of argument, that there is a threat to international peace and security resulting from uses of ICTs, one should at the same time notice that the main actors in any such conflict are longstanding members of the GGEs. Therefore, actual implementation of the GGE guidance even only by States represented in the Group, would significantly reduce the risk of the feared cyber conflict. Consequently, time is 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. Russian 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*.[115]

In the light of the above, there is space, in the international cyber security dialogue, for another GGE as well as other formats and venues. What has been missing is an independent, neutral platform that would serve as a glue between the different initiatives and agendas, able to focus on less politicized reading of views and progress, and thereby ready to offer guidance and advice to and between these agendas and initiatives.

[114] US submission in 1999.
[115] See https://www.kommersant.ru/doc/3496533.

6. Eulogy

As the search for accepted standards of responsible State behavior in cyberspace continues, there is an essential contribution that the GGE, regardless of the political controversies surrounding it, has made. A pragmatic reading of the GGE reports reveals that over a relatively short period of time, experts have built a roadmap that any country, regardless of their political system or capacity level will find useful in developing basic understanding and awareness of the requirements and means of international cyber security.

For the purpose of introducing the roadmap, it is useful to dismiss the somewhat controversial classification of norms, rules, principles and confidence-building measures. Each Group has provided guidance and directions on upholding the rule of law in the context of State uses of ICTs, on exchange of national views and information, critical infrastructure protection as well as incident prevention and mitigation. These leads and recommendations are actionable, or at least serve as food for thought for national, regional, and further international engagement.

Drawing from the three GGE reports, States should be able to contextualize and prioritize the respective recommendations and guidelines in their national cyber security issues and situation. While hardly any country is in the position or has the need to implement the whole roadmap at once, its guidance is applicable in national cyber security strategy and legislation process. Supporting it as a framework of thinking and further discussion would duly acknowledge the GGE work and outcomes.

Annex A: UN GGE International Cybersecurity Roadmap

	Norms, Rules and Principles	CBMs and Capacity Building
Upholding the rule of law	States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (13 c)	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 (16 d i)
	States should respect resolutions on the promotion, protection and enjoyment of human rights on the Internet (13 e)[i]	Establish focal points and cooperation for the provision of assistance in investigations (17 b)
	States should intensify cooperation against criminal and terrorist use of ICTs, harmonize legal approaches and strengthen practical collaboration between law enforcement and prosecutorial agencies (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 (17 e)
	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 (13 d)	Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions (26 f)
Exchange of views and information		Voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs (16 c)
	Prevent practices that are acknowledged to be harmful or that may pose threats to international peace and security (13 a)	Voluntary sharing of national views and information on best practices for ICT security (16 c)
		Voluntary sharing of national views and information on national organizations, strategies, policies and programmes relevant to ICT security (16 c) (26 a)
		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 (26 b)
	In developing and applying measures to increase stability and security in the use of ICTs (13 a)	Establish focal points and cooperation for the exchange of information on malicious ICT use (17 b)
		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 (16 b)
CI Protection	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)	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 (16 d)
	States should take appropriate measures to protect their CI from ICT threats (13 g)[ii]	States should seek to facilitate cross-border cooperation to address CI vulnerabilities that transcend national borders (16 d)

	States should respond to appropriate requests for assistance by another State whose CI is subject to malicious ICT acts (13 h 1)	The development or mechanisms and processes for consultations on the protection of ICT-enabled CI (16 d ii)
		The development of technical, legal and diplomatic mechanisms to address ICT-related requests (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 (16 d iv)
Incident Prevention and Handling	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 (13b)	Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents (17 a)
	States should respond to appropriate requests to mitigate malicious ICT activity aimed at the CI of another State emanating from their territory, taking into account due regard for sovereignty (13 h 2)	Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role (17 c)
		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 (17 d)
	States should not conduct or knowingly support activity to harm the information systems of authorized emergency response teams of another State (13 k 1)	The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents (16 a)
	A State should not use authorized emergency response teams to engage in malicious international activity (13 j 2)	Consider categorizing CERT as critical infrastructure (17 c)
		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 incidents, for timely response, recovery and mitigation actions (26 c)
		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 (26 c)
		Exchanges of information and communication between national CERTs bilaterally, within CERT communities, and other forums, to support dialogue at political and policy levels (26 d)
		Increased cooperation to address incidents that could affect ICT or CI that rely on ICT-enabled industrial control systems, including guidelines and best practices among States against disruptions perpetrated by non-State actors (26 e)
Other	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 (13 i 1)	

	States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (13 i 2)	Voluntary sharing of national views and information on vulnerabilities and identified harmful functions in ICT products (16 c)
	States should encourage responsible reporting of ICT vulnerabilities (13 j 1)	
	States should share information about available remedies to vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure (13 j 2)	
	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)	
	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)	

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 2006-2017

	2006[iii]	2007[iv]	2008[v]	2009[vi]	2010[vii]	2011[viii]	2012[ix]	2013[x]	2014[xi]	2015[xii]	2016[xiii]
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
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	

	2006[iii]	2007[iv]	2008[v]	2009[vi]	2010[vii]	2011[viii]	2012[ix]	2013[x]	2014[xi]	2015[xii]	2016[xiii]
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
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

	2006[iii]	2007[iv]	2008[v]	2009[vi]	2010[vii]	2011[viii]	2012[ix]	2013[x]	2014[xi]	2015[xii]	2016[xiii]
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
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

Annex D: Replies from Governments 1999–2017

	99[xiv]	00[xv]	01[xvi]	02[xvii]	03[xviii]	04[xix]	05[xx]	06[xxi]	07[xxii]	08[xxiii]	09[xxiv]	10[xxv]	11[xxvi]	12[xxvii]	13[xxviii]	14[xxix]	15[xxx]	16[xxxi]	17[xxxii]
Afghanistan																			X
Albania																		X	
Argentina						X													
Armenia															X				X
Australia	X												X			X		X	
Austria																X			
Bangladesh									X										
Belarus	X																		X
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						

	99[xiv]	00[xv]	01[xvi]	02[xvii]	03[xviii]	04[xix]	05[xx]	06[xxi]	07[xxii]	08[xxiii]	09[xxiv]	10[xxv]	11[xxvi]	12[xxvii]	13[xxviii]	14[xxix]	15[xxx]	16[xxxi]	17[xxxii]
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		
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[xxxiii]													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											

	99[xiv]	00[xv]	01[xvi]	02[xvii]	03[xviii]	04[xix]	05[xx]	06[xxi]	07[xxii]	08[xxiii]	09[xxiv]	10[xxv]	11[xxvi]	12[xxvii]	13[xxviii]	14[xxix]	15[xxx]	16[xxxi]	17[xxxii]
US	X					X							X						
Venezuela						X													

[i] Human Rights Council and UNGA resolutions
[ii] UNGA resolutions
[iii] A/61/389
[iv] A/62/386
[v] A/63/385
[vi] A/64/386
[vii] A/65/405
[viii] A/66/407
[ix] A/67/404
[x] A/68/406
[xi] A/69/435
[xii] A/70/455
[xiii] A/71/28
[xiv] A/54/213
[xv] A/55/140 and A/55/140/Add.1
[xvi] A/56/164 and A/56/164/Add.1
[xvii] A/57/166 and A/57/166/Add.1
[xviii] A/58/373
[xix] A/59/116 and A/59/116/Add.1
[xx] A/60/95 and A/60/59/Add.1
[xxi] A/61/161 and A/61/161/Add.1
[xxii] A/62/98 and A/62/98/Add.1
[xxiii] A/63/139
[xxiv] A/64/129 and A/64/129/Add.1
[xxv] A/65/154
[xxvi] A/66/152 and A/66/152/Add.1
[xxvii] A/67/167
[xxviii] A/68/156 and A/68/156/Add.1
[xxix] A/69/112 and A/69/112/Add.1
[xxx] A/70/172 and A/70/172/Add.1
[xxxi] A/71/172
[xxxii] A/72/315
[xxxiii] On behalf of the States members of the European Union that are Members of the United Nations.