Cybersecurity in a Complex Environment

Transatlantic Divergences and Diplomatic Achievements*

Tim Maurer

This article is the English original of the article "Cybersicherheit in einem komplexen Umfeld. Transatlantische Divergenzen und diplomatische Errungenschaften", published in: **VEREINTE NATIONEN – German Review on the United Nations**, Vol. 64, 2/2016, pp. 51–55.

Tim Maurer directs the Cyber Policy Initiative of the Carnegie Endowment for International Peace in Washington, D.C., and is Nonresident Fellow of the Global Public Policy Institute in Berlin.

The international community has become increasingly alarmed by cyberspace incidents in recent years. The United Nations is one of the key forums for the discussion on a possible regulation of the cyberspace. This article outlines the history of the negotiations to date and illustrates future challenges. The effective implementation of the recent agreement on a strategy of optional norms will be crucial.

In December 2015, a cyber-attack caused a blackout in Western Ukraine. The effect was limited, the blackout lasted only for a few hours until operators switched to manual controls, and it was not the first blackout as part of the conflict. Only a few weeks earlier conventional bombs had caused a more prolonged blackout on Crimea. However, this incident is noteworthy because it is the first known blackout during a conflict to have been caused by malware. Similarly, just a year earlier, President Barack Obama, in an unprecedented move, publicly accused North Korea for having hacked Sony Pictures Entertainment. In short, the blackout is only the latest in a series of high profile incidents in recent years illustrating the deteriorating cybersecurity environment.

The international community has become increasingly alarmed by these developments and diplomatic efforts have been ramping up. One of the key forums of these discussions is the United Nations - the UN General Assembly's First Committee to be precise, when it comes to cybersecurity in the context of international peace and security. Dating back to a first draft resolution introduced by the Russian Federation in 1998, the First Committee has been discussing the issue of "Developments in the field of information and telecommunications in the context of security".[1] However, it was not until President Obama took office that this

*This article is partly based on Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?, Discussion Paper 2011-11, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2011, www.belfercenter.ksg.harvard.edu/experts/2304/tim_maurer.html

[1] UN Doc. A/RES/53/70, 4 December 1998.

debate started to intensify. As part of the Obama administration's shift in foreign policy toward more engagement, the U.S. government started to actively promote the idea of international cybersecurity norms and, more recently, the vision for "international cyber stability".[2]

There have been several important diplomatic developments in this field during the past eight years. In 2010, the permanent five members of the UN Security Council, Russia, China, the United States, the United Kingdom, and France together with ten additional UN member states acknowledged that "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century".[3] Three years later, a similar group agreed that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[4] This was a major milestone after several countries initially contested the notion that the existing international law applies, instead arguing for the development of new law for cyberspace. A consensus report developed by a group of 20 UN member states in 2015 provided further insight into the application of existing international law and norms governing cyberspace.[5]

At the same time, it is important to note that all of these agreements have been codified in reports of groups of governmental experts (GGE) established by the UN Secretary-General at the request of UN member states. The reports have not been adopted by the full UN membership (the last report has been "welcomed"). They therefore barely qualify even as soft law under international law standards. Moreover, the norms outlined in these documents are voluntary. Their implementation and whether they will stick depends on the political will of the various states and the internal coherence of their bureaucracy. This article outlines the history of this discussion at the United Nations distinguishing five different phases. It also provides an analysis of the developments in recent years and an outlook for the future in the concluding section.

As the Obama administration is nearing its end, it remains an open question what direction this agenda will take in the future under a new U.S. administration. Moreover, as the fifth GGE will convene in the fall of 2016, the question will be whether its enlarged membership of 25 states will focus on broadening and deepening the GGE reports' legitimacy and adoption by the UN membership or focus on making further progress on substance. How to operationalize the provisions from the previous reports will be a crucial task to imbue them with meaning and to

[2] White House. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, D.C. 2011; Department of State, International Security Advisory Board. Report on A Framework for International Cyber Stability, Washington, D.C., 2014.
[3] UN Doc. A/65/201, 30 July 2010, p. 2.
[4] UN Doc. A/68/98, 24 June 2013, p. 8.
[5] UN Doc. A/70/174, 22 July 2015.

actually improve the security environment. Last but not least, another question the international community will need to address is what will follow the fifth GGE. There seems to be little appetite for a sixth GGE. Will it instead morph into an open-ended working group or another institutional framework? And how will it integrate nongovernmental actors ranging from industry to civil society and the tech community?

Historical Background: The United Nations and Cybersecurity

In 1998, the Russian Minister of Foreign Affairs at the time, Igor Ivanov, wrote to the UN Secretary-General on September 23, 1998, requesting the circulation of a new draft resolution on "Developments in the field of information and telecommunications in the context of security".[6] Every year since, the Russian government has introduced a resolution on this issue in the UN General Assembly's First Committee. Sergey Ivanov, Russia's Minister of Defense from 2001 to 2007, later explained that "Russia wants to develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security". [7]

However, the Russian government's proposal for a treaty on information security was met with significant skepticism. According to Ronald Deibert, professor of political science and director of the University of Toronto's Citizen Lab, "Russia has been pushing for arms control in cyberspace, or information-weapons control. Most people dismiss this as disingenuous, and I tend to agree. Most observers see it as Russia's attempt to constrain U.S. superiority in the cyber domain. Russia is more concerned about color revolutions and mobilization on the Internet by dissident and human rights groups – and trying to eliminate the United States' ability to support that type of social mobilization – than it is about protecting the Internet."[8] Wall Street Journal reporter Siobhan Gorman also points out that the U.S. considers a treaty premature based on the concern that a treaty would not prohibit countries like Russia and China to use third parties to circumvent the treaty.[9]

Generally, the discussions about cybersecurity at the United Nations can be divided into two main groups: negotiations focusing on the "politico-military" dimension of cybersecurity and those focusing on "the criminal misuse of information technologies".[10] This article is limited to

[6] Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007.
[7] Christopher A. Ford, The Trouble with Cyber Arms Control, The New Atlantis. A Journal of Technology & Society. Vol. 29/2010, p. 65.
[8] Ronald Deibert, Tracking the emerging arms race in cyberspace, Bulletin of the Atomic Scientists, Vol. 67, Isssue 1, 2011, p. 6.
[9] Siobhan Gorman, U.S. Backs Talks on Cyber Warfare, The Wall Street Journal, 4 June 2010.
[10] UN Doc. A/RES/55/63, 4 December 2000.

the politico-military stream which is concerned about how "[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States.[11] So far, the UN Security Council has not seized this matter. Instead, the First Committee of the UN's General Assembly and the aforementioned process since this initial proposal in 1998 has been at the center of these discussions which can be divided into four phases:

Phase 1: The Beginning (1998–2004)

Following the Russian Minister's letter to the UN Secretary-General, the 1998 draft resolution was adopted by the General Assembly without a vote on 4 January 1999.[12] The resolution for an "international computer security treaty"[13] focused on the following key elements. First, it mentions the military potential of information and communication technology[14] and for the first time in a UN document expresses concern about the use of such technology "inconsistent with the objectives of maintaining international stability and security".[15] Second, it mentions the need to prevent cyber-crime and cyber-terrorism, and third, invites member states to inform the Secretary-General notably on their views regarding "definitions" and the development of "international principles".[16] In subsequent years, the Russian government continued to introduce this resolution as its sole sponsor which was then adopted by the General Assembly yet without any further action other than some member states submitting reports to the UN Secretariat to share information as requested by the resolution. In short, the resolution lay mainly dormant.

Phase 2: Contentious Politics (2005–2008)

In 2005, an important change took place in the First Committee. It is President George W. Bush's second term and a historic low in UN–U.S. relations after the failed 2005 World Summit. The draft resolution introduced by Russia is adopted but goes to a recorded vote for the first time in its history. The U.S. is the only country voting against the resolution on October 28.[17] Subsequently, the draft resolution introduced in 2006 is no longer sponsored by the Russian

[11] UN Doc. A/RES/53/70, 4 December 1998.
[12] Ibid.
[13] John Markoff, Step Taken to End Impasse Over Cybersecurity Talks, The New York Times, 16 July 2010.
[14] Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007.
[15] UN Doc. A/RES/53/70, 4 December 1998, p. 2.
[16] For an analysis why definitions are such an important issue in this discussion, see Tim Maurer/Robert Morgus, 'Cybersecurity' and Why Definitions Are Risky, The International Relations and Security Network, 10 November 2014.
[17] UN Doc. A/60/452, 16 November 2005.

Federation alone.[18] The People's Republic of China as well as Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan are now co-sponsors of the draft resolution and are joined by others in subsequent years.[19]

Around the same time, major newspapers are publishing articles with 'cyber-warfare' making major headlines in 2007 following the Distributed Denial of Server (DDoS) attack against Estonia and in 2008 during the Georgian-Russian war. While the academic debate about what constitutes 'cyber-warfare' continues to this day, the headlines certainly increased the public's general awareness of this issue. It also increased political decision-makers sensitivity including initial discussions whether a cyber-attack could trigger NATO's article 5.[20]

Phase 3: From Contestation to Engagement (2009–2013)

While media are increasingly reporting about cybersecurity threats around the world, the Bush administration has been succeeded by the administration of President Obama pursuing not only a "reset" policy with regard to Russia but also in the United Nations. In fact, the New York Times reported that in November 2009, "a delegation led by Gen. Vladislav P. Sherstyuk, a deputy secretary of the Russian Security Council and the former leader of the Russian equivalent of the National Security Agency, met in Washington with representatives from the National Security Council and the Departments of State, Defense and Homeland Security. Officials familiar with these talks said, the two sides made progress in bridging divisions that had long separated the countries. Indeed, two weeks later in Geneva, the United States agreed to discuss cyberwarfare and cybersecurity with representatives of the United Nations committee on disarmament and international security".[21]

In the wake of these developments, draft resolutions in the First Committee are again adopted without a vote starting in October 2009 during the pre-2005 period. Moreover, in January 2010, the Obama administration presented a position paper with the objective to bring the various parties closer together.[22] Later that year, Richard Clarke states in his latest book "Perhaps I should admit that I rejected the Russian proposal […] the U.S. had to stand almost alone in the UN in rejecting cyber talks, we said no […] and we have kept saying no for over a decade now […] it may be time for the United States to review its position on cyber arms control."[23] In fact, the U.S. government's change of heart leads to the U.S. co-sponsoring the draft resolution for

[18] UN Doc. A/C.1/61/L.35, 11 October 2006.
[19] Ibid.
[20] Ian Traynor, Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 16 May 2007.
[21] John Markoff/Andrew E. Kramer, In Shift, U.S. Talks to Russia on Internet Security, The New York Times, 13 December 2009.
[22] John Markoff, Step Taken to End Impasse Over Cybersecurity Talks, The New York Times, 16 July 2010.
[23] Richard A. Clarke/Robert Knake, Cyber War: The Next Threat to National Security and What To Do About It, New York 2010, pp. 218–219.

the first time after having voted against it between 2005 and 2008. The draft resolution differs in two important aspects to its previous versions. It omits the reference and attempt to come up with definitions which some argued would have been a first step towards a cyber arms control treaty. In a similar vein, it substituted the reference to “international principles” with references to “international concepts” and “possible measures”.

Phase 4: Initial Agreements and Substantive Progress (*2013–2015)*

As the diplomatic engagements on cybersecurity ramp up, the substantive discussions evolve, as well. Back in 2004, the First Committee had established a first GGE hoping that this smaller group consisting of representatives of only 15 UN member states would be able to make more progress on the substance of the draft resolution. However, this first GGE due to present a report in 2005 ultimately failed to come to a common position. According to A.A. Streltsov, a member of the Russian delegation at the GGE meetings and member of the Cryptography Academy of the Russian Federation, “The main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of ‘hostile’ use of ICTs for politicomilitary purposes.”[24]

A second GGE was established in 2009, another sign of the change that occurred with the new U.S. administration. This time the GGE did come to a consensus and initial agreement stating that “Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century”.[25] The threat is considered to be large enough to pose a risk to “international peace and national security”. The 2010 GGE report was an important milestone for its symbolism and a diplomatic success given the previous political climate.

In fact, the Washington Post published an article titled “15 nations agree to start working together to reduce cyberwarfare threat” stating that “A group of nations – including the United States, China and Russia – have for the first time signaled a willingness to engage in reducing the threat of attacks on each others' computer networks.” The article further points out that “The Russians proposed a treaty in 1998, that would have banned the use of cyberspace for military purposes”, and the journalist quotes Robert Knake as considering the new development as being “part of the Obama administration's strategy of diplomatic engagement” because in the words of an Obama administration official “There's been an increased understanding of the international need to address the risk".[26]

[24] Anatolij A. Streltsov, International information security: description and legal aspects, United Nations Institute for Disarmament Research (UNIDIR), Geneva 2007, pp. 6–7.
[25] UN Doc. A/65/201 v. 30.7.2010, p. 6.
[26] Ellen Nakashima, 15 nations agree to start working together to reduce cyberwarfare threat, The Washington Post, 17 July 2010.

However, the 2010 GGE report was vague in substance. A first substantive breakthrough occurred only three years later. In a resolution now sponsored not only by Russia but also co-sponsored by three dozen countries, the Secretary-General was asked to establish a new GGE in 2012 to submit a report at the 68th session in 2013.[27]

This new GGE moved beyond the initial agreement highlighting in its 2013 report that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[28] In other words, what Streltsov described as the "main stumbling block" to a consensus report nearly a decade earlier had been removed. The international community, including the U.S., Russia, and importantly, China, now agreed that international law including international humanitarian law applied online as well as offline. It is worth nothing that this agreement is part of a broader trend of the international community affirming that existing international law and rules apply online as well as offline, for example, the UN Human Rights Council agreed in 2012, that "the same rights that people have offline must also be protected online."[29]

In the meantime, as the diplomatic engagement around cybersecurity started to intensify with the new administration in the U.S. and against the background of increasingly alarming media reports about a deteriorating security environment, new substantive proposals started to circulate. In 2011, the White House published its "International Strategy for Cyberspace" while Russia and China collaborated through the Shanghai Cooperation Organization to develop a draft "International code of conduct for information security."[30] It became clear that while the U.S. government was now willing to engage on this issue, the differences dating back to the 1990s persisted.

According to Joseph Nye, "For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that measures banning offense can damage defense against current attacks, and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the internet. Nonetheless, the United States has begun formal discussions with Russia. Even advocates for an international law for information operations are skeptical of a multilateral treaty akin to the Geneva Conventions

[27] UN Doc. A/65/405, 9 November 2010, p. 5.
[28] UN Doc. A/68/98, 24 June 2013, p. 8.
[29] Library of Congress, U.N. Human Rights Council: First Resolution on Internet Free Speech, 12 July 2012.
[30] White House. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, D.C., 2011; UN Doc. A/66/359, 14 September 2011.

that could contain precise and detailed rules given future technological volatility, but they argue that like-minded states could announce self-governing rules that could form norms for the future".[31]

It was therefore a surprise to many observers that the fifth GGE was able to move beyond the 2013 GGE report and become even more detailed in substance. Not only had the group been enlarged from 15 to 20 states but it also met against the background of the conflict in the Ukraine significantly increasing geopolitical tensions. In fact, half way into the process, various GGE members put the chances of an agreement only at 50/50. Ultimately though, the GGE adopted a new consensus report outlining a set of specific norms, for example, protecting authorized emergency response teams and critical infrastructure. For example, the 2015 GGE report states that "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." And while the report included four of the five norms U.S. Secretary of State John Kerry outlined in his speech in Seoul, Korea, in spring 2015, it also included proposals from other countries such as language focusing on supply chain integrity that can also be found in the aforementioned draft international code of conduct.

Where does the path lead to?

The fifth GGE will start to convene in fall 2016 also marking the beginning of the fifth phase in this process. After the initial agreements and substantive progress in recent years, the two main questions the international community now faces is how to broaden the legitimacy of these agreements and how to implement them so they will lead to an actual improvement in the security environment.

Apart from operationalizing the language into concrete action, recent events also raise the question how to interpret existing agreements and what happens in case of violations. For example, the norm focusing on critical infrastructure posits that "A State should not conduct or knowingly support ICT activity…that…impairs the use and operation of critical infrastructure to provide services to the public."[32] What difference does it make that it says "should not" rather than "must not", for example, in the hypothetical case that the blackout in Ukraine was the result of state sponsored malicious activity? If this were a violation, what would be the consequences?

[31] Joseph S. Nye Jr, Cyberpower, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, p.18.
[32] Ibid.

With regard to legitimacy, the new group has been enlarged to now 25 member states and a record number of states have expressed an interest to participate to the UN Secretariat. The selection of the GGE members will be an important indicator and play an important part to broaden the buy-in of the UN membership. Looking beyond the fifth GGE, what will the process look like moving forward? Will the GGE become an open-ended working group or will it transition into another institutional set-up potentially integrating nongovernmental actors? And how will it interact with other ongoing discussions, for example, with China about economic espionage and the related recent bilateral and G20 statements as well as the discussions about surveillance in the General Assembly's Third Committee? Balancing a more inclusive process and increasing number of participants with progress on substance will be a challenge.

Last but not least, as diplomats tackle these questions, a broader and increasingly urgent challenge that decision-makers need to address is the widening gap between the diplomatic progress and achievements and the continuously deteriorating security environment and proliferation of capabilities. Apart from state actors and questions of internal policy coherence, nonstate actors are becoming increasingly daring. This also raises the question which institution is the appropriate forum and most nimble and effective for this discussion to move forward.