TALLINN PAPERS

Elaine Korzak

Russia’s Cyber Policy Efforts in the United Nations

Tallinn Paper No. 11
2021

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Previously in This Series

No. 1 Kenneth Geers “Pandemonium: Nation States, National Security, and the Internet” (2014)

No. 2 Liis Vihul “The Liability of Software Manufacturers for Defective Products” (2014)

No. 3 Hannes Krause “NATO on Its Way Towards a Comfort Zone in Cyber Defence” (2014)

No. 4 Liina Areng “Lilliputian States in Digital Affairs and Cyber Security” (2014)

No. 5 Michael N. Schmitt and Liis Vihul “The Nature of International Law Cyber Norms” (2014)

No. 6 Jeffrey Carr “Responsible Attribution: A Prerequisite for Accountability” (2014)

No. 7 Michael N. Schmitt “The Law of Cyber Targeting” (2015)

No. 8 James A. Lewis “The Role of Offensive Cyber Operations in NATO’s Collective Defence” (2015)

No. 9 Wolff Heintschel von Heinegg “International Law and International Information Security: A Response to Krutskikh and Streltsov” (2015)

No. 10 Katrin Nyman Metcalf “A Legal View On Outer Space and Cyberspace: Similarities and Differences” (2018)

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). The expressions reflected are those of the author(s) alone; publication by the Centre should not be interpreted as endorsement thereof by the Centre, its Sponsoring Nations or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

The Tallinn Papers

The NATO CCD COE's Tallinn Papers are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarization of cyberspace, and technical. Focusing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by invitation, proposals dealing with issues of strategic importance and acuteness will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org

Russia’s Cyber Policy Efforts in the United Nations

Elaine Korzak[1]

Introduction

Unlike high profile cybersecurity breaches or incidents, international cyber policy discussions rarely make the news.[2] Even when they do, coverage is sporadic, simplified and limited to seemingly recent breakthroughs.[3] However, a closer look reveals that international discussions in a number of areas have been underway for quite some time, growing only more complex with an increasing number of forums and initiatives getting involved.

In the United Nations (UN), important negotiations aimed at regulating the activities of states and non-state actors in cyberspace began in the late 1990s. Despite increasing awareness, particularly in recent years, these discussions have remained largely obscure to wider audiences although their outcome can have wide-ranging consequences for both governments and non-governmental stakeholders, as is the case with governance regimes in other policy areas. Equally important, at least two very different visions for governance in cyberspace have emerged and are competing for votes among UN members. Like-minded states mainly from the Global North advocate an open, free and secure cyberspace that preserves the free flow of information globally, while another group led by Russia and China strive to establish a governance regime that would enable greater government control of cyberspace.[4]

This paper presents and examines the activities and views of Russia, one of the most (if not the most) important members of the latter group. Although Russia initiated discussions in the UN and has since actively shaped various processes, widespread awareness of the breadth and depth of Russian activities has been lagging. In particular, Russia’s long-standing engagement and consistency in its positions are frequently underestimated even while it continues to shape current negotiation dynamics. Thus, the following sections aim to raise understanding by providing an

[1] Elaine Korzak, PhD, LLM is an Affiliate at the Center for International Security and Cooperation (CISAC), Stanford University.

[2] See, for example, discussion of UN negotiations in ‘America rethinks its strategy in the Wild West of cyberspace’, *The Economist*, 28 May 2020. See also coverage of the SolarWinds incident, David Sanger, Nicole Perlroth and Julian Barnes, ‘As Understanding of Russian Hacking Grows, So Does Alarm’, *New York Times*, 2 January 2021.

[3] See, for example, John Markoff and Andrew Kramer, ‘U.S. and Russia Differ on a Treaty for Cyberspace’, *New York Times*, 27 June 2009; David Sanger, ‘U.S. and China Seek Arms Deal for Cyberspace’, *New York Times*, 19 September 2015; Shannon Vavra, ‘World powers are pushing to build their own brand of cyber norms’, Cyberscoop, 23 September 2019, available at https://www.cyberscoop.com/un-cyber-norms-general-assembly-2019/; Kevin Collier, ‘27 countries sign cybersecurity pledge with digs at China and Russia’, *CNN*, 23 September 2019, available at https://www.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html; and Edith Lederer, ‘UN gives green light to draft treaty to combat cybercrime’, *AP News*, 27 December 2019, available at https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15.

[4] See, for example, Tom Gjelten, ‘Shadow Wars: Debating Cyber ‘Disarmament’’, World Affairs (2010).

introductory overview of various Russian activities in the United Nations over the past two decades.

The first part presents the various initiatives, discussions and processes relating to cybersecurity that Russia has initiated or participated in. In particular, developments in the First Committee, the longest-standing and most prominent negotiation process, are detailed alongside more recent activities in the Third Committee related to a new framework to address cybercrime. The second part provides an overview of the key cyber policy positions characterising the Russian approach in the UN, which have also prompted concerns among like-minded and other states. Concluding remarks summarise the main findings to categorise Russia's actions in the United Nations as persistent, consistent and long-term oriented.

Overview of Russian Initiatives in UN Cyber Discussions

For more than two decades, Russia has played a critical role in cybersecurity discussions at the United Nations and beyond. Not only did it initiate the international debate in the late 1990s, but it has also acted as a major driver of various processes and initiatives ever since.

UN First Committee

The most prominent process has evolved under the auspices of the UN General Assembly and its First Committee tasked with matters of disarmament and international security. Russia initiated discussions in the Committee in 1998 with a draft resolution entitled 'Developments in the field of information and telecommunications in the context of international security'.[5] Broadly speaking, Russian officials argued that the information revolution could have potentially detrimental effects on international security and stability[6] and that advances in information and communication technologies (ICTs) could be used by terrorist, extremist or criminal groups.[7] Similarly, the application of these technologies by states' militaries could have potentially destabilising consequences affecting the national security of states.[8]

Ultimately, these concerns were taken up by the First Committee which noted that ICTs can be used 'for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States'.[9] In response, the Committee called

[5] Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary-General A/C.1/53/3. The draft resolution is contained in the same document as an appendix.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] UN General Assembly Resolution A/RES/53/70, p.2.

on member states to consider existing and potential threats in this field and to share their views on how to enhance the security of global ICT systems.[10]

This marked the beginning of a process that continues to this day. Over the years, discussions have gained prominence as the Committee's deliberations turned into the longest-running process dealing with cybersecurity issues in the UN or elsewhere.[11] Russia's role in this process has been a dominant one. Since 1998, Russia has traditionally sponsored and submitted a draft resolution almost every year with an increasing pool of co-sponsoring countries, ensuring that ICT security has become an integral part of the First Committee's agenda.[12]

Russia has also sought to influence and shape the trajectory of discussions in various ways. First, Russia has actively formulated and advanced its national views relating to cyberspace since the late 1990s. It has frequently submitted its official views on information security to the UN's Secretary-General, a mechanism provided for in the annual resolutions adopted by the First Committee.[13] In these and other policy documents, an overarching theme has been Russian calls for a new international legal framework to regulate activities in cyberspace. Such calls have been underpinned by distinct policy views rooted in Russian notions of information security, to which we will return later.

More importantly, Russia has promoted its viewpoints in all five Groups of Governmental Experts (GGEs) established by the General Assembly in the past 20 years, with a sixth currently underway.[14] GGEs are small groups of national experts that can be convened at the request of the UN General Assembly to study a specific set of questions. First proposed by Russia, the GGE format has evolved over the years into the main vehicle for discussions in the First Committee. While the first (2004-2005) and most recent GGEs (2016-2017) were unsuccessful, the work of the remaining three (2009-2010,[15] 2012-2013,[16] and 2014-2015[17]) culminated in reports that identify a number of international measures to address threats in cyberspace. Four elements in particular form what has come to be referred to as the international normative framework for

[10] Ibid.

[11] Discussions of cyberspace-related questions in other UN venues have been comparatively short-lived. The Second Committee of the General Assembly, dealing with economic and financial questions, considered critical infrastructure protection and the creation of a global culture of cybersecurity with a limited set of resolutions during the early 2000s. The Third Committee, tasked with social, humanitarian, and cultural issues, briefly considered the issue of cybercrime in 2000.

[12] See the list of annual General Assembly resolutions on the UN Office of Disarmament Affairs website, available at https://www.un.org/disarmament/ict-security/.

[13] See the description and list of annual reports on the UN Office of Disarmament Affairs website, available at https://www.un.org/disarmament/ict-security/.

[14] The first (2004-2005) and fifth (2026-2017) GGEs were not able to produce a report. The second (2009-2010), third (2012-2013) and fourth (2014-2015) GGEs arrived at consensus reports. The sixth GGE (2019-2021) is still underway. See also Factsheet with an overview of GGEs on the UN Office of Disarmament Affairs website, available at https://www.un.org/disarmament/ict-security/.

[15] 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.

[16] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98.

[17] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174.

responsible state behaviour in cyberspace: (1) The application of international law to the use of ICTs by states, in particular, the Charter of the United Nations; (2) eleven voluntary, politically-binding norms of behaviour for states to follow in cyberspace; (3) practical confidence-building measures to enhance transparency and predictability among states' policies and activities in cyberspace; and (4) international assistance and capacity-building efforts to enhance all states' capacity to protect their ICT environment.[18]

Since GGEs operate on the basis of consensus,[19] the outcome of a particular Group tends to reflect the international compromise attainable among the main players in cybersecurity discussions at that point. Having participated in all GGEs, and having chaired two of them,[20] the views of Russia have played an important role in the successes and failures of each GGE. Particularly enduring controversies around the application of international law, the need for additional norms and future discussion mechanisms reflect the influence of Russian views on the course of negotiations.[21]

Second, Russia has sought to shape the trajectory of discussions in the First Committee by continuously introducing new proposals, initiatives and discussion formats, albeit with varying degrees of success. In 2011 and 2015 Russia and a handful of other states submitted proposals for a voluntary '[i]nternational code of conduct for information security' to the First Committee.[22] The proposals identified states as the primary actors in cyberspace and laid out their rights and responsibilities. Both documents committed to the Charter of the UN, but with a particular emphasis on its provisions regarding sovereignty, state control and non-interference in the information space as important tenets governing state interactions. Although political declarations, both codes of conduct sought to distil principles that could later form the basis for binding international agreements guiding the behaviour of states. In the end, neither proposal was able to garner widespread support among UN member states.[23] Both proposed codes were backed most notably by China, which over the years has emerged as an important partner and supporter of Russian efforts.[24] However, the other co-sponsors (Kazakhstan, Kyrgyzstan,

[18] See 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, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98, and Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174.

[19] See GGE mandate in UN General Assembly Resolution A/68/243.

[20] Russian expert Andrey V. Krutskikh chaired the 2004-2005 and 2009-2010 GGEs.

[21] For a discussion of the 2016-2017 GGE outcome for example see, Elaine Korzak, 'UN GGE on Cybersecurity: The End of an Era?', *The Diplomat*, 31 July 2017, available at https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

[22] See Letter 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 A/66/359 and 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.

[23] The code of conduct did not find mention in UN General Assembly Resolution A/RES/66/24.

[24] China joined Russia as a co-sponsor of its annual resolution for the first time in 2006. Beyond the confines of UN discussions, both countries also entered into a bilateral agreement. See Elaine Korzak, 'The Next Level for Russia-China Cyberspace Cooperation?', *Net Politics*, 20 August 2015, available at https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation. For a discussion of the relationship between Russia and China see Adam Segal,

Tajikistan, Uzbekistan) were limited to Central Asian post-Soviet states that are seen as part of Russia's Near Abroad sphere of influence. Efforts outside the UN such as the 2009 agreement on International Information Security in the Shanghai Cooperation Organisation, have similarly focused on this region.[25]

In contrast to these earlier initiatives, Russia's most recent efforts have been more consequential for the course of cybersecurity discussions in the UN. Following the lack of progress in the 2016-2017 GGE, Russia proposed the creation of a new discussion format in 2018. Its draft resolution that year set up an Open-Ended Working Group (OEWG), moving cybersecurity deliberations to a forum open to all interested UN member states.[26] The OEWG convened in 2019 and was due to conclude with a report of its discussions to the General Assembly in 2020.[27]

With this initiative, Russia argued that UN negotiations would become 'more democratic, inclusive and transparent'.[28] The OEWG stood in contrast to the limited, and therefore the more exclusive format of the previous GGEs that had accommodated no more than 25 members. In effect, the move sought to succeed and supplant past discussion formats and establish an alternative negotiation platform that would be more conducive to multilateral negotiations for an international legally binding agreement for information security. Thus, among other things, the OEWG was tasked 'to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations'.[29] Other areas of discussion for the OEWG mirrored topics of previous GGEs, including the application of international law to the use of ICTs by states, norms of responsible state behaviour, confidence-building measures and capacity-building.[30]

However, several aspects of the Russian proposal were problematic for the United States (US) and other like-minded states.[31] In response, the US along with other sponsors submitted a competing draft resolution entitled 'Advancing responsible State behaviour in cyberspace in the context of international security'.[32] In stark contrast to the format of the OEWG, the resolution called for the creation of a sixth GGE for 2019-2021 to study the implementation of norms and the application of international law, effectively extending the long-standing GGE format.[33] Since Russia and its supporters continued to promote their draft resolution, deliberations in the First Committee culminated in the adoption of both resolutions setting up parallel processes. In the end, both draft resolutions were adopted by vote , with a majority of UN member states voting in

'Peering into the future of Sino-Russian Cyber Security Cooperation', *War on the Rocks*, 10 August 2020, available at https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/.

[25] Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, Yekaterinburg, 16 June 2009.

[26] UN General Assembly Resolution A/RES/73/27.

[27] Ibid.

[28] Ibid., p.5.

[29] UN General Assembly Resolution A/RES/73/27.

[30] Ibid.

[31] Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Net Politics*, 15 November 2018, available at https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[32] UN General Assembly Resolution A/RES/73/266.

[33] Ibid.

favour of both.[34] This represented a notable departure from prior practice in the First Committee under which one annual resolution submitted by Russia enjoyed broad support among member states and was adopted without a vote in almost every year of the Committee's discussions.[35] Over the years, the annual resolution garnered a growing number of co-sponsors, even including the US and other like-minded states at some points.[36] This prevailing, consensus-driven approach of 20 years came to an end with the historic voting on two resolutions in 2018.

The split created two negotiation processes – the OEWG and another GGE – that operate on the basis of consensus and have similar mandates, raising critical questions as to their potential outcomes and how their work relates to each other. Although participants initially stressed the need (and opportunity) for complementarity rather than competition between the two processes,[37] the 2018 developments in the General Assembly have set up inherent tensions that are still to be resolved. The effects of the unexpected COVID-19 pandemic have only exacerbated these tensions as both processes have been delayed. With the postponement of the final session of the OEWG from June 2020 to March 2021,[38] the discussions of both the GGE and the OEWG are supposed to conclude in the first half of 2021.[39]

Yet, even before both groups resumed their in-person meetings, Russia had again taken the initiative with a new proposal tabled during the 2019 General Assembly session.[40] Without awaiting the outcome of either the GGE or the OEWG, the Russian resolution proposed the creation of a new Open-Ended Working Group to run from 2021 until 2025 and submit annual progress reports and a final report of its work.[41] The mandate of the new Group is similar to the current one to ensure the 'uninterrupted and continuous nature' of the UN negotiation process and even provides for the option to establish thematic subgroups to facilitate its work.[42]

Unsurprisingly, this has not been universally welcomed, particularly in light of proposals from France and Egypt on how to align the GGE and OEWG processes in the future.[43] The US and

[34] Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Net Politics*, 15 November 2018, available at https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[35] Only between 2005 and 2008 the annual resolution was adopted by vote.

[36] For a collated overview see Eneken Tikk and Mika Kerttunen, *Parabasis. Cyber-diplomacy in Stalemate*, Norwegian Institute of International Affairs, 2018, pp. 83-86, available at https://www.nupi.no/nupi_eng/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate.

[37] See for example Opening address by Ms. Izumi Nakamitsu, High Representative for Disarmament Affairs at Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, New York, 9 December 2019, available at https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/12/HR-addresses-GGE-on-advancing-responsible-State-behaviour-in-cyberspace-.pdf.

[38] Report of the First Committee A/75/394, p.6.

[39] The OEWG adopted a final consensus report on 12 March 2021. See Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security A/AC.290/2021/CRP.2. As of writing the GGE has yet to conclude its work.

[40] UN General Assembly Resolution A/RES/75/240.

[41] Ibid.

[42] Ibid., p.3.

[43] See proposal for 'Joint Contribution – Programme of Action' on UN Office of Disarmament Affairs, Open-Ended Working Group website, available at https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

others introduced a resolution calling on the UN's members to first consider the outcome of the work of the current GGE and OEWG before deciding on any future work during the General Assembly in the fall of 2021.[44] Ultimately, both resolutions were adopted by majority vote, as was the case in 2018. This has created a host of questions as to the future direction of negotiations, even as the outcome of current processes remains open.[45] However, the creation of a more permanent negotiation platform along the lines of an OEWG or merged format rather than a complete return to the format of GGEs seems to have been cemented by Russia's various initiatives.

UN Third Committee

Similar dynamics can be observed in the UN's Third Committee dealing with social, humanitarian and cultural issues. Through a series of proposals and initiatives, Russia has actively advanced discussions on cybercrime in recent years. While conversations on cybercrime in the early 2000s remained inconsequential,[46] Russia's recent actions have had a potentially lasting effect by setting up a formal negotiation process for a new international treaty to combat cybercrime. As with the creation and extension of the Open-Ended Working Group in the First Committee, Russia's proposals were ultimately adopted by majority vote, albeit with significant opposition from like-minded states.[47] The absence of consensus reflects the differing views among states concerning the utility of existing international arrangements addressing cybercrime.

On one side, the US and like-minded states have promoted the Budapest Convention on Cybercrime, an international treaty which was adopted under the auspices of the Council of Europe in 2001 and entered into force in 2004[48] and is so far the only major international treaty addressing cybercrime, ratified by over 60 states.[49] The Convention seeks to promote a common criminal policy and facilitate cross-border law enforcement cooperation in cybercrime cases. Members of the Convention include countries with some of the world's largest ICT service providers that hold critical electronic evidence.[50]

[44] UN General Assembly Resolution A/RES/75/32.

[45] For a preliminary analysis see Josh Gold, 'Competing U.S.-Russia Cybersecurity Resolutions Risk Slowing UN Progress Further', *Net Politics*, 29 October 2020, available at https://www.cfr.org/blog/competing-us-russia-cybersecurity-resolutions-risk-slowing-un-progress-further.

[46] The Third Committee adopted a resolution on 'Combating the criminal misuse of information technologies' in 2000. A year later, discussions were deferred to the Commission on Crime Prevention and Criminal Justice. See UN General Assembly Resolution A/RES/55/63 and UN General Assembly Resolution A/RES/56/121.

[47] See UN Press Release 'General Assembly Approves $3.07 Billion Programme Budget as It Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-Fourth Session', 27 December 2019, available at https://www.un.org/press/en/2019/ga12235.doc.htm.

[48] For overview information see Council of Europe, Convention on Cybercrime website, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[49] The list of signatories is available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=QJwJsSg8.

[50] Joyce Hakmeh and Allison Peters, 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', *Net Politics*, 13 January 2020, available at https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

Supporters of the Budapest Convention called on states from all regions to become members. Like-minded states have also referred to the Convention's importance in the early years of the First Committee discussions on ICTs and international security. Following Russia's initiative in 1998, the US and others emphasised the need to address cybercrime as an urgent concern for the international community, thereby in part shifting attention away from Russian concerns over an arms race in cyberspace. To elevate the issue, the US and others sponsored a resolution in 2000 on '[c]ombating the criminal misuse of information technologies' in the Third Committee that invited UN members to enhance law enforcement cooperation, raise awareness and increase information sharing around cybercrime.[51] The US argued that: 'the key threat to cybersecurity originates in the relentless criminal attacks by organized criminals, individual hackers and non-State actors, including terrorists' and that '[f]rom this perspective, the benefits of cyberspace can best be protected by focusing … on the effective criminalization by States of the misuse of information technology'.[52] Thus, 'the United States of America and … other States have signed the Council of Europe Convention on Cybercrime'.[53] The ability to point to an existing multilateral agreement in the area of cybercrime also aided like-minded states in their rejection of Russian calls in the First Committee for an international legal treaty to regulate the development and use of ICTs.

On the other side, Russia and other states have long opposed the Budapest Convention on Cybercrime and have called for alternative arrangements. They have argued that it constitutes an outdated regional agreement that infringed principles of state sovereignty and non-interference, among other things.[54] The result has been a division between states with regard to the Convention and its utility in countering cybercrime, a stalemate that has dominated discussions for the past fifteen years.

Russia's recent actions in the Third Committee have interrupted this pattern. They have deepened existing divisions by seeking to create a new international cybercrime treaty as an alternative to or even replacement for the Budapest regime. In 2018, a Russian-sponsored resolution placed the topic of cybercrime on the Committee's agenda.[55] The resolution, which passed by majority vote,[56] asked the UN Secretary-General to collect member states' views 'on the challenges that they face in countering the use of information and communications technologies for criminal purposes'.[57] In 2019, Russia followed up with a resolution that established a committee of experts

[51] UN General Assembly Resolution A/RES/55/63

[52] US submission in Report of the Secretary-General A/59/116/Add. 1, pp. 3-4. See similarly UK submission in Report of the Secretary-General A/59/116.

[53] US submission in Report of the Secretary-General A/59/116/Add.1, p.4.

[54] Joyce Hakmeh and Allison Peters, 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', *Net Politics*, 13 January 2020, available at https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

[55] UN General Assembly Resolution A/RES/73/187, p.2. Earlier in 2018 Russia also published a 'Draft United Nations Convention on Cooperation in Combating Information Crimes', available at https://www.rusemb.org.uk/fnapr/6394.

[56] Detailed voting information is available at https://digitallibrary.un.org/record/1656199?ln=en.

[57] UN General Assembly Resolution A/RES/73/187.

to draft an international cybercrime treaty under the auspices of the UN.[58] Specifically, the resolution created an open-ended ad hoc intergovernmental committee of experts to 'elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes' beginning in 2020.[59] Due to the COVID-19 pandemic, however, the proceedings, including an organisational session intended to agree on an outline and modalities for the committee's activities, have been delayed.[60] Notably, the 2019 resolution was also adopted by majority vote with strong opposition from like-minded states, passing with a narrow margin of 79 to 60 votes and 30 abstentions.[61] Opposing states and human rights organisations have been wary that a new cybercrime treaty as envisioned by Russia would ultimately enable governments to assert increased control over activities online, raising human rights concerns.[62]

In many ways, the dynamics in the Third Committee are similar to and interlinked with the divisions that have become apparent in the First Committee. Russia, together with China, has been seeking to establish new international legal frameworks to regulate the use of ICTs. These overtures have been met with resistance from the US and like-minded states. While First Committee discussions have not so far resulted in formalised treaty negotiations, Russia's efforts have been more successful in the Third Committee with the recent creation of an ad hoc committee of experts to elaborate a new cybercrime treaty. This development will undoubtedly affect the approach of like-minded states in both processes as they have promoted and relied on the Budapest Convention in their diplomatic efforts.

Overview of Russian Policy Positions in UN Cyber Discussions

Following Russia's efforts across the UN, the subsequent sections offer an overview of the main policy views that these initiatives have sought to advance.

[58] UN General Assembly Resolution A/RES/74/247.

[59] Ibid.

[60] For postponement information see UN General Assembly Decision A/75/L.55. For information on the proposed outline and modalities of the committee see Background Paper Prepared by the Secretariat A/AC.291/2.

[61] See UN Press Release 'General Assembly Approves $3.07 Billion Programme Budget as It Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-Fourth Session', 27 December 2019, available at https://www.un.org/press/en/2019/ga12235.doc.htm.

[62] See for example issues raised by several non-governmental organisations in an open letter, 'Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online', available at https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf.

New International Regime for Information Security

An overarching theme of Russian activities in the UN has been its advocacy for the creation of a new international regime to regulate information security. Ever since the beginning of UN discussions in 1998, Russia has, in particular, stressed the need to negotiate a formal international legal agreement in this area.[63] While the Third Committee has recently established a committee of experts to produce a draft treaty on cybercrime, Russia's efforts in discussions on international security are still ongoing.

In the early days of the First Committee discussions, Russia, in part, called for new regulations since existing international law was perceived to be ill-equipped to effectively regulate novel uses of ICTs enabled by the information revolution. As a 1999 Russian position paper argued:

> *A fundamentally new area of confrontation in the international arena is in the making, and there is the danger that scientific and technological developments in the field of information and communications might lead to an escalation of the arms race. … We are referring to the creation of an 'information weapon', the use of which, depending on the level of a society's information technology and the vulnerability of its vital structures, can have devastating consequences, … and contemporary international law has virtually no means of regulating the development and application of such a weapon. … [T]here is an obvious need for international legal regulation of the worldwide development of civilian and military information technology.*[64]

Over the years, Russia's call for an international legal treaty has remained a central theme in its contributions in the First Committee, even as discussions on international law and norms of responsible state behaviour progressed with the work of the various GGEs. Particularly the 2012-2013 and 2014-2015 GGEs were able to achieve critical diplomatic compromises, acknowledging the applicability of international law, including the UN Charter. Notwithstanding, Russia noted as recently as June 2020 that the:

> *specific modalities of this applicability … [remain unclear and that] these practical aspects should be regulated by a specialized universal international legal instrument that would envisage criteria for how the existing norms of international law apply to the use of ICTs and would directly indicate the need for developing new norms. Time*

[63] See Russian submission in Report of the Secretary-General A/54/213. See also Eneken Tikk and Mika Kerttunen, *Parabasis. Cyber-diplomacy in Stalemate*, Norwegian Institute of International Affairs, 2018, available at https://www.nupi.no/nupi_eng/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate.

[64] Russian submission in Report of the Secretary-General A/54/213, p.8.

> *is ripe for such steps in regulating the use of ICTs under the current de facto 'legal vacuum'.*[65]

Thus, Russia still argues that there is a need for an international legal treaty, but its argument has evolved. Rather than negating the applicability or adequacy of international law, a treaty is presented as a critical means to clarify how existing international law applies to cyberspace. This approach also highlights the possibility of identifying and codifying additional legal norms.

Despite Russia's long-standing advocacy for a formal international agreement, the US and like-minded states have met the notion with considerable scepticism and continued opposition over the past two decades. This opposition stems, in part, from concerns over what type of activities or state behaviour such a treaty would seek to regulate, including through the introduction of additional legal norms. Like-minded states have, in particular, highlighted concerns over potential limitations of the free flow of information or content through greater government control.[66]

Russia has been cognisant of this opposition, acknowledging as recently as 2020 that 'reaching consensus on the elaboration of a universal legal basis … is impeded'.[67] Russia's First Committee initiatives and activities over the past two decades can thus be seen as attempts to build steppingstones or gradual multilateral support towards its treaty idea in the face of continuing opposition. For example, while the proposed codes of conduct (though ultimately unsuccessful) represented a set of voluntary international principles resembling multilateral declarations rather than an international legal agreement, they could have served as a rudimentary basis for a broader international agreement later on. Similarly, Russia has acknowledged that, pending consensus on a new international treaty, international efforts should be focused on norms, rules and principles of responsible state behaviour.[68] At the same time, it has been seeking to retroactively shape the set of norms agreed in the 2014-2015 GGE through the negotiations of the OEWG and its authorising resolution. Resolution 73/27 selectively listed some norms (but not others) from the 2015 GGE report resulting in a list of norms of state behaviour that Russia seeks to promote as a new reference point.[69]

Russia has also sought to create an institutional environment that could facilitate international treaty negotiations. To that end, its active support for the creation of more permanent or

[65] Statement by the representative of the Russian Federation at the online discussion of the second 'pre-draft' of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Moscow, 15 June 2020, p.4, available at https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

[66] See, for example, the US submission in Report of the Secretary-General A/59/116/Add. 1, p.3. See also discussion in Eneken Tikk and Mika Kerttunen, *Parabasis. Cyber-diplomacy in Stalemate*, Norwegian Institute of International Affairs, 2018, pp. 15-16, available at https://www.nupi.no/nupi_eng/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate.

[67] Commentary of the Russian Federation on the Initial "Pre-Draft" of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, p.3, available at https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

[68] Ibid.

[69] UN General Assembly Resolution A/RES/73/27.

institutionalised negotiation platforms under the First Committee has been a key component. Breaking with the long-standing format of GGEs, the Russian Federation opened discussions to all UN member states with its proposal for an OEWG in 2018. Similarly, its push to extend the Group's lifespan to 2025 even before current negotiations concluded aimed to effectively create an institutional venue that can serve as a treaty negotiation platform, or at the very least a precursor to it.

Russia's advocacy for an international legal treaty governing the use of ICTs has been an overarching and long-standing feature of its diplomatic dealings at the UN. Though its twenty-year efforts in First Committee discussions have not resulted in treaty negotiations given the opposition of other states, the notion of an international legally binding instrument remains a persistently recurring part of discussions to this date.

Notion of 'Information Security'

A distinct characteristic of Russian policy views in the UN and beyond stems from its perception of threats and risks in the ICT environment that, in turn, translate into comparatively broad understandings and concepts. These are denoted by the use of terms such as 'information security' or 'international information security', which reveal important differences to the terminology of cybersecurity preferred and commonly used by like-minded states in international diplomatic discussions.[70] These conceptual differences also help explain the reservations of other states towards Russian initiatives in UN discussions.

Broadly speaking, the Russian understanding of information security goes beyond concerns regarding the security of information and communication technologies systems and also includes the regulation of information or content flows. Relevant policy documents define information security as the 'protection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and *information per se*….'.[71] Threats to information security go beyond the targeting of ICT systems and interference with their proper functioning to include numerous concerns related to content. Threats perceived by Russia explicitly include:

> *The use of information to undermine the political, economic and social system of other States, … or to engage in the psychological manipulation of a population in order to destabilize society; …*

[70] The term "information security" can lead to confusion as it is also used by technical, business and other communities in like-minded states. However, in the context of international cybersecurity discussions, the terms "information security" and "cybersecurity" carry distinct meanings and are used deliberately by different states. See the UK's submission in Report of the Secretary-General A/68/156, p.15 for an example of differences of interpretation.

[71] See for example Russian submission in Report of the Secretary-General A/54/213, p.10 (emphasis added).

> *The transboundary dissemination of information in contravention of the principles and norms of international law and of the domestic legislation of specific countries; …*
>
> *The manipulation of information flows, disinformation and the concealment of information in order to corrupt the psychological and spiritual environment of society, and erode traditional cultural, moral, ethical and aesthetic values.*[72]

As a result, the regulation of information and information flows comprises an integral part of Russia's views for what a new international governance regime should cover. As an indication, the Russian-sponsored resolution of 2018 establishing the OEWG affirmed the 'right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news' and the 'duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda'.[73]

Such an expansive understanding of information security has prompted significant concerns among like-minded states and other stakeholders. The regulation of information and information flows is seen as particularly problematic, enabling human rights restrictions and impeding the free flow of information. In response, the applicability of international human rights law on- and offline has been stressed, with repeated references to the 'importance of respect for human rights and fundamental freedoms in the use of information and communications technologies'.[74]

Though Russia and its supporters have not denied the applicability of international human rights law to the ICT environment, their approach has been more nuanced. Human rights and fundamental freedoms are acknowledged, but the focus is shifted towards matters of implementation. Respect for human rights is placed within the national context. The exercise of internationally recognised human rights and fundamental freedoms, for example, the 'right[s] and freedom to search for, acquire and disseminate information', is based 'on the premise of complying with relevant national laws and regulations'.[75] As a result, Russian views incorporate an acknowledgement (and even emphasis) of human rights and fundamental freedoms while advancing expansive notions of information security that seek to regulate the use of information and information flows.

[72] Russian submission in Report of the Secretary-General A/55/140, p.5. See also the 2011 Russian proposal for a 'Convention on International Information Security', available at https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf.

[73] UN General Assembly Resolution A/RES/73/27, p.3.

[74] UN General Assembly Resolution A/RES/73/266, p.2.

[75] Letter 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 A/66/359, p.4. See also Russian submission in Report of the Secretary-General A/55/140, p.4.

Emphasis on State Sovereignty

Russian activities in the UN have been underpinned by an understanding of states and their governments as the primary actors responsible for the protection of the ICT environment.[76] The 2011 draft code of conduct stressed, for instance, 'all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space … from threats, disturbance, attack and sabotage'.[77]

This view of states as central, coupled with Russia's notion of information security, has resulted in an emphasis on certain international legal principles, most notably state sovereignty. Although Russia has not unreservedly acknowledged the applicability of international law, including the UN Charter, over the years, it has consistently chosen to emphasise certain elements of international law in its interventions.

These elements have been centred around the sovereign equality of states and the rights and responsibilities that flow from it. Policy documents and proposals have prominently featured calls to respect 'the sovereignty, territorial integrity and political independence of all States' and to recognise 'the diversity of history, culture and social systems of all countries'.[78] Equally important, state sovereignty also applies to states' jurisdiction over ICT infrastructure within their territory.[79] Related international legal principles that have been highlighted include non-intervention in the internal affairs of other states, the non-use of force in international relations and the peaceful settlement of international disputes.[80]

The selective emphasis of these international legal principles, all of which are enshrined in the UN Charter, suggests a rather defensive view of the state: seeking to maximise the autonomy of government action within its jurisdiction while minimising activities by other states or non-governmental stakeholders that are perceived as undue interference or intervention. States and their rights derived from the principle of sovereign equality are seen as the central elements in the governance of state activities in cyberspace. This emphasis on state sovereignty is underpinned by the Russian understanding that the information revolution ultimately constitutes 'a disruptive tool with regard to regime stability'; information flows can be used as a means to influence and undermine a state's political and social system.[81] The use of social media during the Arab Spring and anti-government protests in Russia in 2012 validated these views.[82] Thus, state sovereignty and the related legal principles stressed by Russia in the context of UN

[76] See, for example, Doctrine of Information Security of the Russian Federation, 5 December 2016, available at https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

[77] Letter 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 A/66/359, p.4.

[78] Ibid.

[79] See, for example, reaffirmation in UN General Assembly Resolution A/RES/75/240.

[80] See, for example, Russian submission in Report of the Secretary-General A/55/140, p.4.

[81] Xymena Kurowska, *What does Russia want in cyber diplomacy? A Primer*, EU Cyber Direct Research Paper, December 2019, p.12, available at https://eucyberdirect.eu/content_research/what-does-russia-want-in-cyber-diplomacy-a-primer/.

[82] Ibid.

discussions reflect its broader concerns of ensuring regime stability and guarding against undue (foreign) interference.

For other states, this emphasis is problematic as it signals increased government control in domestic jurisdictions and international mechanisms for internet governance. Coupled with Russia's notion of information security, the emphasis on state sovereignty again evokes human rights concerns. Russia's interpretations of sovereignty and its attendant rights could justify and enable abuses by states seeking to unduly assert greater government control to restrict information flows and access.

Preference for Intergovernmental Organisations

In line with its emphasis on the role of the state and state sovereignty in information security, Russia has strongly advocated that ICT-related discussions take place under the auspices of intergovernmental organisations, particularly the UN which is portrayed as a central organisation for multilateral security discussions since it 'most fully represents the interests of all countries'[83], and is thus able to ensure the consideration of cybersecurity issues in a 'global, comprehensive and non-discriminatory manner'.[84]

At the same time, the UN, along with other intergovernmental organisations, is by definition generally limited to states in terms of participation and (most importantly) decision-making.[85] Thus, Russia's preference for the UN reflects its position that states and national governments are the primary actors in information security. Other stakeholders, including the private sector, civil society and academia, play a subordinate role. While their respective roles and responsibilities are recognised, governments are ultimately seen as leading national efforts.[86]

Unsurprisingly, these views entail scepticism, if not rejection, of multistakeholder approaches that enable the active participation of non-governmental stakeholders on an equal footing with governmental actors. Russia has long been critical of the multistakeholder approach in internet governance, instead supporting calls for 'multilateral' governance mechanisms or arrangements that would privilege states and national governments.[87]

Similarly, Russia has resisted efforts to expand the participation of non-governmental stakeholders in the current negotiation processes such as the OEWG. While the mandate of the Group provided for 'consultative meetings' with business, non-governmental organisations and

[83] Russian submission in Report of the Secretary-General A/58/373, p.9.

[84] Ibid.

[85] Malcolm Shaw, *International Law* (Cambridge University Press: Cambridge, 2014, Seventh Edition), pp. 938-939.

[86] See for example the 2011 Russian proposal for a 'Convention on International Information Security', available at https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf.

[87] For an overview discussion see Julien Nocetti, 'Contest and conquest: Russia and global internet governance', *International Affairs*, 91:1 (2015), pp. 111-130.

academia that were seen as useful exchanges by many states,[88] Russia has stressed the importance of states' views expressed during formal negotiation sessions. Commenting on the institutional way forward and the draft text for the OEWG, Russia argued that 'the importance of [the] "multi-stakeholder approach" with emphasis on the contribution of [the] non-governmental sector, business and academia to ensuring responsible behaviour in the information space is artificially exaggerated'.[89] Overall, past Russian activities across the UN system and beyond have illustrated its commitment to multilateral formats and its considerable efforts to retain and advance negotiations accordingly.

Concluding Thoughts

International cybersecurity discussions have gained considerable momentum and prominence in recent years. Following slow and incremental advances for the better part of two decades, the past five to seven years have brought two major trend lines: signs of emerging international compromise followed by a fracturing of processes. The outcome documents of the 2012-2013 and 2014-2015 GGEs have established a baseline understanding for international consensus around responsible state behaviour in cyberspace that particularly like-minded states point to, but the creation and extension of the OEWG have set up an alternative negotiation platform to further develop this international consensus, complementing, contradicting, or possibly supplanting any discussions in the tried format of GGEs.

Russia has continuously played an important role in these developments. Ever since it initiated discussions in the late 1990s, it has sought to actively shape the trajectory of debate according to its views. This long-standing engagement and Russia's historical role may surprise many newcomers to the international cybersecurity discussions at the UN. However, over the years, Russia has emerged as an important actor in international cybersecurity discussions and a lead proponent for states favouring an information security approach to cyberspace. Its efforts have naturally yielded varying levels of success but have illustrated Russia's investment and commitment in the various UN processes. Having surveyed its activities and main cyber policy views, Russia's efforts across the UN system can be characterised as persistent, consistent and long-term oriented.

Russia has maintained an important role in UN discussions, in part since it has been persistent in its efforts. It has repeatedly introduced proposals and initiatives over the whole life span of

[88] UN General Assembly Resolution A/RES/73/27, p.5. See also information provided on UN Office of Disarmament Affairs, Informal intersessional consultative meeting of the OEWG with industry, non-governmental organisations and academia website, available at https://www.un.org/disarmament/oewg-informal-multi-stakeholder-meeting-2-4-december-2019/.

[89] Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Moscow, 15 June 2020, p.2, available at https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

discussions, even though its success has varied in light of opposition, particularly from the US and other states. Some initiatives have failed altogether to garner support, as was the case with the two proposed codes of conduct in 2011 and 2015. Others have shaped the course of discussions as is evident in the extension of the OEWG process in the First Committee or the creation of the ad hoc committee of experts in the Third Committee.

Russia has also been consistent in its main policy positions since it initiated discussions. Key tenets of its views include a broad understanding of ICT security as ‘information security’, resulting in an emphasis on the role of the state and state sovereignty. Efforts have been geared towards the creation of a new international governance regime, preferably negotiated between states under the auspices of the UN. While Russia has undoubtedly adapted its efforts in response to unfolding negotiation dynamics, its core views have remained remarkably stable (and predictable) over the years.

In addition to being persistent and consistent, Russian efforts in UN discussions have been focused on the long-term. Perhaps best encapsulated by Russia’s efforts for a new international legal regime for information security and the incremental steps towards that goal, the activities of Russia illustrate sustained long-term commitment for its policy positions over the past decades.

Taken together, these features provide insight into Russia’s past actions and can serve as important lessons for stakeholders engaging with Russia in the various upcoming negotiation processes.