POLICY BRIEF
February 2022
EU-Russia Relations Series

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES

BAD OPTIONS ONLY?

TRANSFORMING EU-RUSSIA RELATIONS IN CYBERSPACE

ABSTRACT

Relations between the EU and Russia are strained. Even though both actors declare full agreement to the United Nations (UN) framework of responsible state behaviour in cyberspace, they disagree regarding most of its provisions. Can this situation be transformed? What is the scope for cooperation if, as we suggest, options for transformation are limited? We address these questions by taking stock of the clashing EU-Russia positions in the UN cyber governance debate. Strikingly, despite the gravity of the situation, neither the EU nor Russia seems to take the other totally seriously in cyber diplomacy.

This policy brief places the EU-Russia dispute on cyberspace within two paradigmatically different models for the global governance of the internet – the state-centred and intergovernmentalist approach favoured by Russia, which Russia describes as an internationalisation of the debate, and the EU programmatic advocacy of multistakeholderism. We conclude that a structural change in the EU-Russia relationship on cyberspace is not in sight. We recommend instead better use of what we call a stagnation scenario, understood as a global if contested conversation in the context of the UN Open-Ended Working Group (OEWG). Despite Russia's triumphalism regarding the establishment of the OEWG as a realisation of its diplomatic goals, the spirit of the global cyberagora that the OEWG instigates is hardly in line with Russia's conservative vision of the international system. This constitutes an opportunity for the EU, and for its declared democratic ideals, if it stands up to the challenge of normative cyber contestation.

AUTHORS

DR XYMENA KUROWSKA
Associate Professor of International Relations at Central European University in Vienna, Austria

DR PATRYK PAWLAK
Brussels Executive Officer, EU Institute for Security Studies

FRIEDRICH EBERT STIFTUNG
FES Regionalbüro für Zusammenarbeit und Frieden in Europa
FES Regional Office for Cooperation and Peace in Europe

Fondation Jean Jaurès

AMICUS EUROPAE
FUNDACJA ALEKSANDRA KWAŚNIEWSKIEGO

Democracy | Development | Dialogue
FMS
Foundation Max van der Stoel

FONDAZIONE GRAMSCI

TABLE OF CONTENTS

About FEPS

The Foundation for European Progressive Studies (FEPS) is the think tank of the progressive political family at EU level. Its mission is to develop innovative research, policy advice, training and debates to inspire and inform progressive politics and policies across Europe.

FEPS works in close partnership with its 68 members and other partners, including renowned universities, scholars, policymakers and activists – forging connections among stakeholders from the world of politics, academia and civil society at local, regional, national, European and global levels.

European Political Foundation - Nº 4 BE 896.230.213 | Avenue des Arts 46 1000 Brussels (Belgium)

www.feps-europe.eu | Twitter/Instagram: @FEPS_Europe | Facebook: @FEPSEurope

THE FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)

European Political Foundation - Nº 4 BE 896.230.213
Avenue des Arts 46 1000 Brussels (Belgium)
www.feps-europe.eu
@FEPS_Europe

FRIEDRICH-EBERT STIFTUNG REGIONAL OFFICE FOR COOPERATION AND PEACE IN EUROPE (FES ROCPE) BRUSSELS

Reichstratsstr. 1-1010 Vienna, Austria
https://peace.fes.de
@FES_ROCPE

FONDATION JEAN JAURÈS

12 Cité Malesherbes, 75009 Paris
www.jean-jaures.org
@j_jaures

FOUNDATION AMICUS EUROPAE

Aleja Przyjacioł 8/5, 00-565 Warsaw, Poland
https://fae.pl
@FAE_pl

FOUNDATION MAX VAN DER STOEL (FMS)

Leeghwaterplein 45, 2521DB Den Haag, Netherlands
https://www.foundationmaxvanderstoel.nl
@FMS_Foundation

FONDAZIONE GRAMSCI

Via Sebino 43a, 00199 Rome, Italy
https://www.fondazionegramsci.org

Introduction

The antagonism in the relations between Russia and the European Union (EU) has become a new normal. The recent calls by Russia to review the security architecture in Europe are yet another reflection of Moscow's rejection of the western encroachment on Russia's perceived spheres of influence. Importantly, the EU will not 'reform', or even tame Russia's contestations. Russia is adamant that it has been short-changed in the post-cold war period and it acts out its resentment across global diplomatic venues.[1] Political circles in Russia see the EU, and the west more broadly, as set on destabilising Russia and overturning its system of governance – a process that Russia commonly refers to as regime change.[2] In such imagery, the lack of control over content and the circulation of (digital) information precipitates regime change. Russia's objective to bring global cyber governance into line with its domestic agenda is a function of this preoccupation. Russia's diplomatic effort consists accordingly in cultivating a discourse of the imminent danger that cyber and digital developments pose, and in lobbying for 'international information security' as an apparently adequate response to that perceived threat. Such a sense of urgency is less pronounced on the part of the EU. The lack of urgency can in principle contribute to more peaceful global cyber relations. In the short term, however, this creates an imbalance of diplomatic investment: the internal support for strengthening EU cyber diplomacy is relatively lukewarm in comparison to Russia's activism.

The EU finds it difficult to take Russia's declarations about the future of cyberspace seriously. It interprets Russia's insistence on 'information security' as a cover for containing domestic dissent by limiting access to information and freedom of expression online. Russia's alleged involvement in cyber operations targeting western societies, which range from espionage to disinformation and election interference to a paralysis of civilian infrastructure, only exacerbates the disparity between Russia's narrative of cyber responsibility and its actions that undermine cyber stability. Ultimately, Russia's cyber posture is regarded as a threat to the integrity of global and domestic democratic institutions because its conduct fails to meet the threshold of state accountability, where state rights come together with state duties. In a nutshell, while the EU recognises that Russia talks the talk, the EU is not convinced that Russia also walks the walk.

This controversy adds to the impasse in EU-Russia relations and affects the scope for cooperation on global governance of the internet under the United Nations (UN). Can the EU and Russia find any common ground in shaping the rules of responsible state behaviour in cyberspace? Or are their visions incommensurable? This policy brief argues that a structural change in their relationship is not in sight. Tweaking the relations or nudging Russia to implement the norms of responsible state behaviour in a particular way – through persuasion, coercion, or deterrence for example – will not succeed. The paradigmatic difference between how Russia and the EU envisage the regulation of the internet

[1] Schmitt, O. (2020) 'How to challenge an international order: Russian diplomatic practices in multilateral security organisations', *European Journal of International Relations*, 26(3): 922–946.
[2] Giles, K. (2021) 'What deters Russia' (www.chathamhouse.org/2021/09/what-deters-russia).

is often captured by the juxtaposition of intergovernmentalism and multistakeholderism. Yet the implications of this difference, and the embellishment of such difference, are not fully appreciated. We therefore start with an elucidation of how the clash between these principles of governance leads to 'contested multilateralism' in the cyber domain. This section is followed by a more detailed audit of the EU's cyber policies and their relevance for EU-Russia cyber relations at the UN. We conclude with an analysis of four different scenarios for EU-Russia relations in cyberspace: stagnation, fragmentation, accommodation, and conversion. As our analysis shows, only the first two scenarios – neither of which is ideal – offer a realistic vision for the future.

Contested multilateralism in cyberspace

Russia considers that the only legitimate platform for making rules with a universal global scope is the UN. Several reasons explain this belief. As a primarily intergovernmental organisation, the UN adheres to equal rights and responsibilities resulting from the principles of non-intervention and sovereign equality. It is a multilateral organisation in the classic sense of the word – that is, a forum to facilitate coordination among self-interested sovereign states, with peace being in the interest of all. The 'one country–one vote' rule can be used to reduce functional inequalities among UN member states: a country that is cutting-edge in technology and a country that is not at the forefront of developing Information and Communication Technologies (ICTs) each have one vote. It is therefore not surprising that Russia champions multilateral discussion at the UN on the regulation of cyberspace. Concerned about its technological, economic, and ideological disadvantage within the multistakeholder model of internet development, Russia has sought to streamline the management of the internet through the UN ever since the late 1990s.[3] Within the UN, Russian diplomacy has additionally lobbied to transfer internet management prerogatives to the International Telecommunications Union (ITU) so that the ITU becomes a body that develops and implements legal norms and standards in the area of internet governance.[4] Russia's official justification for this is the alleged ineffectiveness of the multistakeholder model of internet governance,[5] although its immediate purpose is to weaken the sway of the admittedly less controllable multistakeholder practices.

Over the last two decades or so, the UN and its bodies have become a battleground between different visions of cyberspace. Russia's role in shaping these global conversations is undeniable. Indeed, it was Russian diplomacy in the late 1990s that brought the issue of the impact of ICTs on international security to

[3] Chernenko, E. (2018) 'Russia's Cyber Diplomacy' in N. Popescu and S. Secrieru (eds) *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, Paris: EU Institute for Security Studies, pp. 43–49.

[4] Maxim Parshin, Deputy Minister of the Ministry of Digital Development, Communications and Mass Media, IGF 2020 High-Level Leaders Track: UN Wrap-up, 17 November 2020 (https://youtu.be/3GxCREczsko?t=1292) (21:32, in Russian).

[5] 2nd Inter-regional Conference on Information Security and Informational Interaction in the Central Federal District, 21 April 2021 (https://youtu.be/5qzrrKTBv3M?t=7163) (from 01:59:23, in Russian).

the attention of the international community in the First Committee on disarmament and international security.[6] The initiation of the cyber debate in this context was justified by the dangers of 'information weapons'[7] (a term now formally withdrawn but hardly forgotten) and the debate was modelled on the nuclear non-proliferation regime. Through several reiterations of the UN Group of Governmental Experts (GGE),[8] which was established under the umbrella of the First Committee, UN member states have now developed a framework for responsible state behaviour in cyberspace that builds on four key pillars: the applicability of international law; norms, rules, and principles of responsible state behaviour; confidence-building measures (CBMs); and capacity building. These pillars have also become key axes of contestation between Russia (supported by China), which pursues a state-controlled vision of cyberspace, and the EU (along with other like-minded countries),[9] which promotes a decentralised model of governance.

Russia's activism within the UN system has gradually raised the EU's concerns about the role of the UN regarding the regulation of cyberspace. Indeed, Russia has successfully customised its standing call for the 'democratisation' of international relations in order to make the call fit its cyber diplomacy agenda. In particular, Russia's appeals to "internationalise internet governance"[10] helped mobilise support for the establishment in 2018 of the Open-Ended Working Group (OEWG),[11] which has a mandate duplicating that of the GGE.[12] The head Russian cyber diplomat, Andrey Krutskikh,[13] characteristically described the OEWG as "a triumph of Russian diplomacy against the backdrop of escalation of the

---

[6] Chernukhin, E. (2019) '*Mezhdunarodnaya informatsionnaya bezopasnost': uspekhi Rossii v OON [International Information Security: Russia's Successes at the UN]*', Russian International Affairs Council (https://russiancouncil.ru/en/news/riac-holds-russia-uk-seminar-on-information-security/).and Informational Interaction in the Central Federal District, 21 April 2021 (https://youtu.be/5qzrrKTBv3M?t=7163) (from 01:59:23, in Russian).

[7] Thomas, T.L. (2020) 'Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice', *The Cyber Defense Review* 5(2): 125–44.

[8] The UN Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security is a UN-mandated working group that has been convening since 2004 in a format of initially 15 and then 25 governmental experts. Its most notable accomplishment has been the building of consensus that international law applies in cyberspace and an agreement on 11 norms of responsible state behaviour in cyberspace. For details on the latest round of UN GEE, see: www.un.org/disarmament/group-of-governmental-experts/.

[9] 'Like-minded countries' is a descriptor used by the group of mostly western countries that advocate liberal governance of the internet in accordance with the multistakeholder model and the applicability of human rights online.

[10] This is a recurring term that expresses the primacy of intergovernmentalism wherein Russia insists on "preserving the sovereign right of the states to regulate the national internet segment" and on developing "global governance policy at the intergovernmental level" – see Ernst Chernukhin, special coordinator at the Russian Ministry of Foreign Affairs on issues of political use of ICTs, Big National Forum for Information Security, 12 February 2021 (https://youtu.be/naN4_OglSFs?t=5015) (starts at 1:05:16, in Russian).

[11] The Open-Ended Working Group on Developments in the Field of ICTs (OEWG) in the context of international security includes all UN membership – see resolution A/RES/73/27 (https://undocs.org/A/RES/73/27). For details of the process see: www.un.org/disarmament/open-ended-working-group/.

[12] Disarmament and International Security Committee, 31st meeting in the 73rd session of the UN General Assembly, 8 November 2018 (https://media.un.org/en/asset/k1w/k1w4nmdnk6).

[13] Special representative of the President of the Russian Federation for international cooperation in the field of information security, Director of the Department of International Information Security of the Ministry of Foreign Affairs of the Russian Federation.

international situation by some countries."[14] But Russia's rhetoric of broadening the equal participation of all states in the design of global cyber governance, regardless of their cyber technological status, should not be taken at face value. When Vladimir Putin insists that "it is important to jointly develop and agree on universal and fair-for-all rules on the responsible behaviour of states in the cyberspace with clear and easy-to-follow criteria for acceptable and unacceptable actions and to make them legally binding,"[15] he does not necessarily mean a system where all stakeholders are equal and free to contribute. In fact, scholars have argued that Russia's resort to universal norms is opportunistic and divisive. The evocation of norms may paradoxically serve to undermine them, at least in their liberal rendition.[16] This is not an incorrect diagnosis[17] but its usefulness is limited because it obstructs envisaging productive scenarios of how to co-exist or perhaps even cooperate with Russia on cyber matters.

The EU views Russia's exploitation of multilateral organisations as a strategy to chip away at the dominance of the west. Although the EU remains committed to multilateralism, it increasingly questions what issues should be debated in which venues and what the rules of engagement should be, with a clear preference for preserving the status quo whenever possible. When this is not feasible, the EU engages in contestation. The EU's initial concern over Russia's disingenuous advocacy for the democratisation of the UN cyber debate, as potentially undermining the acquis of the GGE, was soon replaced by the call to manage the growing Russian influence. The outcome was a fragile balance of power that covered over a fundamental friction. However, the schism between the OEWG and the GGE ended in 2021 with the adoption of a single resolution in the First Committee that supports the OEWG on the security of and in the use of ICTs for 2021–2025.[18] The return to a single-track process in the First Committee and the establishment of the OEWG as the leading format means that the GGE process is effectively defunct. This moral and political win boosts the Russian position. Meanwhile, a distinct EU voice is hardly audible. Indeed, the EU's one important initiative to transcend the present entrenchment has hardly taken off the ground. The French proposal, supported by the EU, Egypt and a number of other countries – a Programme of Action (PoA) for advancing responsible state behaviour in cyberspace[19] –

---

[14] TASS (2021) 'Russia Says the UN OEWG Will Start its Work in June', 13 March (https://tass.ru/politika/10895625). On 15 March 2021, the Russian Ministry of Foreign Affairs issued a statement on the OEWG's final substantive report. The statement says that the report "enshrines basic approaches advanced by Russia and its partners in the area of international information security" (https://mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4632970).

[15] Security Council meeting, Novo-Ogaryovo, Moscow Region, President of Russia Office, 26 March 2021 (http://en.kremlin.ru/events/president/news/65231).

[16] Kurowska, X. and Reshetnikov, A. (2021) 'Trickstery: pluralising stigma in international society', *European Journal of International Relations* 27(1): 232-257.

[17] Lo, B. (2015) *Russia and the New World Disorder*, London and Washington DC: Chatham House and Brookings Institution Press.

[18] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/RES/76/19, 8 December 2021 (https://undocs.org/en/A/RES/76/19).

[19] See Géry, A. and Delerue, F. (2020) 'A New UN Path to Cyber Stability' (https://directionsblog.eu/a-new-un-path-to-cyber-stability/).

has as of yet failed to transform the parameters of the debate.[20]

Cyber diplomacy: auditing EU-Russia relations

The EU came to the discussions about international security and cyberspace relatively late. Since the late 1980s, the EU's primary focus has been on setting rules for digital trade and services that serve to promote and consolidate the European single market. With the establishment of the European External Action Service (EEAS), the EU's interest in a broadly defined cyber diplomacy has gradually grown, mostly because of the establishment of a dedicated team working on the international dimension of cyber-related policies such as internet governance, cybercrime, human rights, and international security. These broader policy goals were reflected in the 2013 EU Cybersecurity Strategy and the 2015 Council Conclusions on Cyber Diplomacy.[22] Both documents reaffirmed the EU's focus on promoting the rules-based international order and its commitment to the emerging UN-negotiated framework of responsible state behaviour in cyberspace that was shaped by the debates in the UN GGE.[23] Although not legally binding, the framework has become the main point of reference for identifying threats to international security in cyberspace. This focus carves an old-new role for the EU as a normative cyber power.

The history of the EU's cyber diplomacy would be incomplete without a clear acknowledgment of the role that Russia has played in the emergence of cybersecurity on the EU's foreign and security policy agenda. It was Russia's cyber operations against Estonia in 2007 and Georgia in 2008 that accelerated the discussion about the EU as an actor in cyberspace. From the early days, the EU's relations with Russia on cyber-related issues have been shaped by a broader political context. The polarisation of the relationship increased in the aftermath of the illegal annexation of Crimea, and in the aftermath of Russia-sponsored disinformation campaigns, including on the war in Syria, the downing of flight MH-17,[24] and the use of chemical weapons in the Salisbury attack. These irritations have influenced EU-Russia relations at both bilateral and international level, further deepening the existing chasm between the EU and Russia over the future of cyberspace governance. As a consequence, Russia and the EU view each other as antithetical to the political model of governing that the other pursues domestically and internationally. They are not at war, at least as far as we define war in international politics, but they may be stuck in what Lucas Kello calls "unpeace",[25] a form of

---

[20] See: https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-concept-note-final-12-2-2020.pdf; and www.un.org/press/en/2021/gadis3673.doc.htm.

[22] Council of the European Union (2015) Council Conclusions on Cyber Diplomacy, 11 February (https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf).

[23] Two consensus reports adopted by the UN GGE in 2011 and 2013 laid the foundations for the substantive work that was continued in the following years. The reports of 2015 and 2021 complement these reflections.

[24] EuvsDisinfo (2017) 'Flight MH17 three years on: getting the truth out of Eastern Ukraine', 7 July (https://euvsdisinfo.eu/flight-mh-17-three-years-on-getting-the-truth-out-of-eastern-ukraine/).

[25] Kello, L. (2017) *The Virtual Weapon and International Order*, New Haven: Yale University Press.

hostile but under-the-threshold of war relations. The following sections of this policy brief offer an audit of the EU-Russia relationship in order to assess whether there is room for engagement on cyber-related issues in these conditions.

Bilateral relations

The EU-Russia exchanges at the UN regarding cyberspace are informed by the two parties' interactions in other contexts. Despite Russia's declared commitment to a peaceful use of cyberspace, the EU criticises the Russian authorities for supporting malicious cyber activities against the EU,[26] its member states or its allies. The most prominent examples include the so-called 'Macron Leaks'[27] (never formally attributed by the French government to Russia but with substantial evidence provided by the US), the reports of Russian support for Catalan separatists,[28] and more recently the probing by German federal prosecutors into alleged Russian hacking attacks on lawmakers.[29] Since 2019, Russian hackers, government officials and entities involved in the Cloud Hopper, WannaCry and NotPetya attacks have been placed on the EU's cyber sanctions regime.[30] The EU and its member states have also expressed their solidarity with the US on the impact of malicious cyber activities, notably the SolarWinds cyber operation. Even though the EU has not formally attributed this operation to Russia, it has recalled the assessment of the US that this operation was conducted by Russia.[31] In September 2021, the EU High Representative issued a statement on behalf of the EU to denounce malicious cyber activities targeting numerous members of parliaments, government officials, politicians, and members of the press and civil society in the EU – all attributed to Russia.[32] The statement also called on Russia to adhere to the norms of responsible state behaviour in cyberspace.

These developments have placed EU-Russia relations on a collision course with little room for cooperation. Despite the EU's commitment to preventing conflicts in cyberspace, the European bloc has not engaged in bilateral dialogue with Russia on cyber-related issues. Instead, it has invested in strengthening its own resilience and developing a cyber deterrence doctrine to dissuade foreign powers – Russia but also China – from undertaking attacks

---

[26] European Commission (2021) Joint Communication on EU-Russia relations - Push back, constraint and engage, 16 June (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021JC0020).

[27] Jeangène Vilmer, J-B. (2019) *The "Macron Leaks" Operation: A Post-Mortem, Atlantic Council*, June (www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf).

[28] Lautman, O. (2021) *Catalonia: Where There's Trouble There's Russia*, 27 September, Centre for European Policy Analysis (https://cepa.org/catalonia-where-theres-trouble-theres-russia/).

[29] Deutsche Welle (2021) 'Germany investigates suspected Russian cyberattacks', 9 September (www.dw.com/en/russians-hacking-german-election/a-59137152).

[30] Council of the EU, Council Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 30 July 2020 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN).

[31] Council of the EU (2021) Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation, 15 April (https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/).

[32] Council of the EU (2021) Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes, 24 September (www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/?&web_view=true).

against targets in the EU or its allies. Both the EU Cyber Diplomacy Toolbox of 2017 and the EU Cybersecurity Strategy of 2020 aim at strengthening the EU's capacity to prevent, deter, and respond to such activities.[33]

Although there are no signs of détente in EU-Russia bilateral relations, several member states have invested in bilateral cyber-related dialogues with Russia. This is linked to the fact that despite closer cooperation at the EU level, the EU member states still retain sovereignty over any decisions about war and peace. Some countries have therefore recognised the need to maintain open channels of communication for de-escalation as well as cooperation on issues of common interest, such as the fight against cybercrime or terrorist use of cyberspace. The Netherlands, for instance, undertook some initial inter-agency consultations on cybersecurity with Russia in September 2021. The agenda included preventing conflicts and any kind of confrontation, as well as the peaceful use of cyberspace and strengthening international cooperation in "countering informational crimes".[34] During the same month, a French delegation also visited Moscow to discuss cyber-related issues.[35] These moves might suggest that the EU member states – even those like the Netherlands whose relations with Russia are particularly tense following the Dutch expulsion of Russian diplomats in 2020[36] – recognise the need to engage in dialogue with Russia despite the unfavourable political climate.

International level

In the context of UN cyber diplomacy, EU-Russia relations have been shaped by normative contestation and diverging ideas about the international order and global and domestic governance. The basic overarching differences include the understanding of sovereignty and non-interference as international norms. Domestically, these differences pertain to an emphasis on regime stability, on the part of Russia, and the focus on liberal democracy, the rule of law, and the adoption of a particular normative framework that reflects these values, on the part of the EU.[37] Russia's core concerns, which shape the objectives of its cyber diplomacy, include preoccupation with its diminished international status, the objection to 'normative activism' (– that is, to the expectation of adoption of and compliance with western norms that are articulated not as a legal agreement but through, in Russia's interpretation, coercive social norms),[38] and the US monopoly over the internet,[39] concealed within the multistakeholder model by technical elevation of private companies and civil society.

The objective of Russia's cyber diplomacy

---

[33] European Commission (2020) The EU's Cybersecurity Strategy for the Digital Decade, 16 December (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

[34] TASS (2021) 'First Russian-Dutch consultations on cybersecurity take place in The Hague', 17 September (https://tass.com/politics/1339323).

[35] See interview with Henri Verdier, the French Ambassador for Digital Affairs, regarding Russian-French consultations on cyber security for *Kommersant*, 30 September 2021. (https://www.kommersant.ru/doc/5008187).

[36] Deutsch, A. and Sterling, T. (2020) 'Dutch expel two Russian diplomats for suspected espionage', *Reuters*, 10 December (www.reuters.com/article/netherlands-russia-idUSKBN28K2AT).

[37] Morozov, V. (2022) 'The normative deadlock in EU-Russia relations Hegemony without influence' in T. Romanova and M. David (eds) *The Routledge Handbook of EU-Russia Relations*, Oxon: Routledge, pp. 48-57.

[38] Ibid

[39] See a characteristic recent statement by the Federation Council, the upper chamber of the Russian Parliament, 'Federation Council Asserts that US Government Entities Have Usurped Control over the Internet,' *RIA Novosti*, 27 January 2021 (https://ria.ru/20210127/sovfed-1594743673.html).

is thus twofold.[40] First, to prove Russia's indispensability in this domain and return it to the decision-making table, and, second, to create the conditions for promoting the Russian initiative to develop and adopt within the UN "a universal [cyber] international treaty based on generally recognised principles and norms of international law and meeting common interests in the information sphere."[41] Importantly for Russia, the development of any universal agreements, as well as the coordination of ways to resolve the existing problems in the ICTs sphere, must remain the prerogative of states with exclusive sovereignty in this area, and in defiance of big tech companies which "compete with the state and replace legitimate democratic institutions, while limiting the fundamental rights and freedoms of citizens."[42] The design and implementation of new cyber norms is supported in principle because it is in Russia's interest of regulating cyberspace – but it has to be monitored because it potentially penetrates the state and poses a risk of uncontrollable 'normative activism'.

The notion of 'the rules-based international order' (with the existing international law and norms of responsible state behaviour at its core) that is promoted by the EU cyber agenda is strongly contested in Moscow as a replacement for, rather than a continuation of, international law-based order. Indeed, Russia regards this notion as an attempt to "usurp the decision-making process on key issues" through "[replacing] the universally agreed international legal instruments and mechanisms with narrow formats, where alternative, non-consensual methods for resolving various international problems are developed in circumvention of a legitimate multilateral framework."[43] This is a formulation that comes from Russia's statist and procedural discourse of international law, which emphasises the classic understanding of sovereignty and categorically rejects the notion of the individual as a subject of international law.[44]

As signalled above, the doctrine of information security[45] is also a core area of divergence. While the EU and those that are like-minded with it fear this doctrine to be yet another Russian attempt to bring more governmental control over cyberspace, Russia stresses the dangers of digitalisation as a potential source of "destabilisation of any society and a pressure on state power."[46] While, for the like-minded, cyber security predominantly denotes protection of the communication infrastructure, and, ideally, free access to information, Russia believes that the doctrine of information security highlights

---

[40] Kurowska, X. (2020) 'What Russia wants in cyber diplomacy. A primer,' in D. Broeders and B. van den Berg (eds) *Governing Cyberspace: Behaviour, Power and Diplomacy*, London: Rowman & Littlefield International, pp. 105–125.

[41] Deputy Chairman of the Russian Security Council, Dmitry Medvedev, '75 Years UN - old problem, new challenges and global solutions,' *Russia Today*, 24 October 2020 (https://russian.rt.com/world/article/795600-dmitrii-medvedev-oon-75-let).

[42] Deputy Minister of Foreign Affairs, O.V. Syromolotov, 'Internet Has Become a Platform for Political Manipulations,' TASS, 5 February 2021 (https://tass.ru/interviews/10631379).

[43] Lavrov, S. (2019) 'World at a Crossroads and a System of International Relations for the Future,' *Russia in Global Affairs* (https://eng.globalaffairs.ru/articles/world-at-a-crossroads-and-a-system-of-international-relations-for-the-future/).

[44] Mälksoo, L. (2015) *Russian Approaches to International Law*, Oxford: Oxford University Press.

[45] Doctrine of Information Security of the Russian Federation (www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163).

[46] Deputy Minister of Foreign Affairs, O.V. Syromolotov, 'Internet Has Become a Platform for Political Manipulations,' *TASS*, 5 February 2021 (https://tass.ru/interviews/10631379).

the responsibility of the government to secure the information itself (– that is, its content because it can become a tool of influence and can thus undermine national sovereignty).[47] The Kremlin's investment in the digitally sovereign Russia is, therefore, a defence of the state against such vulnerabilities.[48] Internationally, Russia has uploaded this approach onto the UN debate on internet regulation through its sponsorship of The International Code of Conduct for Information Security, which was initially submitted to the UN General Assembly in 2011, and was then submitted in revised form in 2015 by member states of the Shanghai Cooperation Organization.[49]

Transformation in EU-Russia relations

While Russia and the EU agree that the cyber domain needs some type of regulation, the scope of agreement probably ends there. To assess the chances of transforming EU-Russia relations in cyberspace, we analyse four different scenarios that are developed on the basis of different configurations of the structural characteristics of each party's ideal (intergovernmentalism or multistakeholderism) and the level of conflict (high or low). These four scenarios are listed below.

1. **Stagnation** – whereby the current declaratory or actual commitment to promoting responsible state behaviour in cyberspace continues among the current levels of conflict. The impasse persists, concealing or blurring the fundamental difference between the two different logics of governance that inform various coalitions of the like-minded – with the EU and Russia on opposing sides.
2. **Fragmentation** – whereby the EU recognises that the Russian vision of cyberspace is impossible to contain, which results in the partition of the internet along different models of governance. In this scenario, the EU begrudgingly accepts at least a temporary geopolitical and regulatory parallelism, the defeat of the universal idea of open, free, and secure cyberspace, and thus of a liberal consensus. The EU does not, however, renounce its normative and regulatory commitments and continues to promote them. The level of conflict is high and so are the economic and social costs globally and locally, with the prospect of the breakdown of the internet as we know it.
3. **Accommodation** – whereby the EU accepts intergovernmentalism and state control as the superior form of internet governance, and thus de facto acquiesces to the Russian vision. This is accompanied by a broader political détente between the EU and Russia. In this scenario, the level of political conflict between Russia and the EU decreases because of the EU making a significant political concession.

---

[47] Sharikov, P. (2018) 'Informatsionnyy suverenitet i meshatel'stvo vo vnutrenniye dela v rossiysko-amerikanskikh otnoshenyiakh [Information sovereignty and interference in domestic affairs in the Russian-US relations]', *Mezhdunarodnyye protsessy* 16 (3): 170–188.

[48] Kurowska, X. (2020) 'On the geopolitics of Russia's Sovereign Internet Law,' ISPRI Dossier, (www.ispionline.it/en/pubblicazione/geopolitics-russias-sovereign-internet-law-25428).

[49] For a brief historical background of the Code of Conduct and comparative analysis of 2011 and 2015 versions, see https://citizenlab.ca/2015/09/international-code-of-conduct/#1.

4. **Conversion** – whereby EU-Russia relations undergo a structural transformation as a result of profound political changes in Russia, the adoption of a civil liberties code similar to that declared by the EU, and the implementation of a multistakeholder model which elevates non-state actors. The level of the EU-Russia cyber conflict decreases significantly.

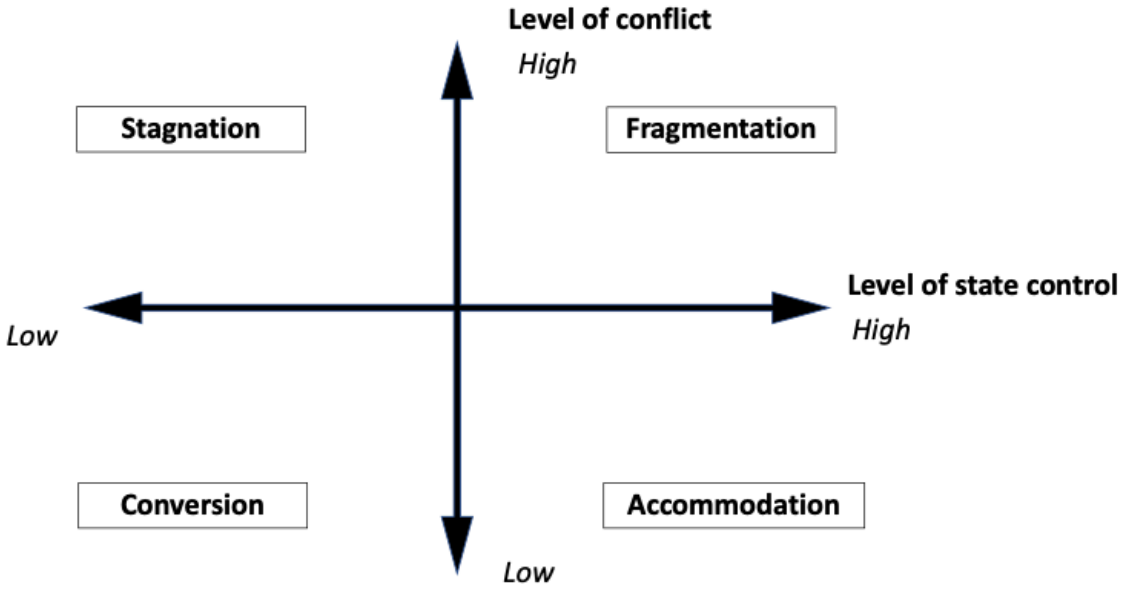


Figure 1. Four scenarios for transformation in EU-Russia cyber relations

We rule out two scenarios which, in light of their modality to eliminate conflict, would be transformative: accommodation and conversion. Accommodation envisages adoption of the Russian sovereigntist agenda of a government-controlled internet that trumps individual freedoms and establishes national cyber borders. It also foresees the strictly intergovernmental framework for the global cyber regime. Conversion meanwhile presupposes that Russia incorporates the western understanding of the multistakeholder model, with the state being just one actor among others. While accommodation is antithetical to the EU's posture, conversion is antithetical to Russia's posture, despite the post-cold war hope for Russia's normative merger with the west.

The two remaining scenarios assume varying degrees of conflict which can or cannot then be managed or channelled in productive ways. Fragmentation is a radical scenario but it is not to be excluded. Indeed, certain elements of it are already manifest – for example Russia's attempts at establishing a sovereign internet and its calls for data localisation. The danger of fragmentation materialises when the restraints of stagnation, or the grind of everyday diplomacy, give way to the escalation of conflict.

Stagnation disappoints because of the perpetual tug of war and the pretence of commonality that requires continuous affirmation. However, it offers a modicum of acknowledgment of difference and options for mediating such difference through controlled contestation within recognised global institutions. We therefore propound that stagnation is both a realistic and ultimately a worthy way forward that prevents full-blown fragmentation.

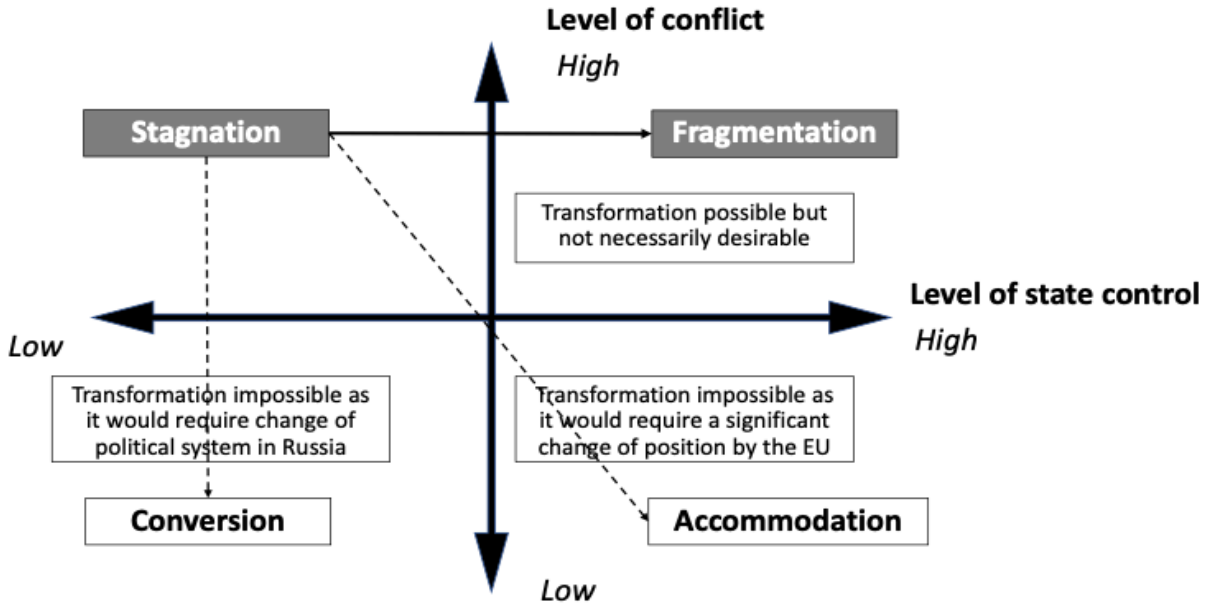


Figure 2. Pathways for transforming EU-Russia relations in cyberspace

Least bad option: stagnation

The stagnation scenario features institutionalised maintenance of the current divisions within the existing global fora, with the potential for escalation to open conflict or antagonistic disengagement that can lead to fragmentation. In the stagnation scenario, geopolitical boundaries consolidate, with under-the-threshold-of-war activities potentially provoking a deliberate or accidental outbreak of armed conflict. **Nevertheless, stagnation has its virtues as it provides space for low intensity conflict among high political tensions while at the same time acknowledging a plurality of models for cyberspace governance. In the stagnation scenario, the multistakeholder model coexists with the intergovernmentalist approach without any party being a clear winner or making significant concessions.** All countries agree – independently of their views towards the multistakeholder approach – that "the area of international security and peace is particularly sensitive and remains by and large a core responsibility of states. Meanwhile, there is no denying that non-state actors play an important role, especially when it comes to

cybersecurity, and that stakeholders have much to offer in terms of expertise and possible solutions."[50] Even though not ideal from the EU perspective – at least not to the extent that the conversion scenario would be – it is the least bad option from the perspective of the process and the policy outcomes.

Regarding the process, the stagnation scenario assumes the existence of multiple tracks within the First Committee of the UN General Assembly that become spaces of contestation between Russia and the EU.[51] In its bid to launch the OEWG in late 2018, Russia might have paradoxically encouraged productive developments in cyber governance that it had not intended. Russia's aim was geopolitical, to break through the alliance of the like-minded that prevented Russia from shaping the GGE process. Opening up the debate to all the UN membership was a means towards this aim.[52] The OEWG quickly evolved to become a "cyber General Assembly,"[53] which was Russia's intention. But the OEWG also re-asserted the importance of global civil society, which Russia would prefer to avoid. An informal intersessional consultative meeting of the OEWG with industry, non-governmental organisations, and academia in December 2019 was unprecedented in its scope of involving non-state actors.[54] Tellingly, no Russian civil society actors spoke in this gathering; also tellingly, there were no fundamentally dissenting voices that would express a more structural critique.[55] However, bringing global civil society to bear on cyber security issues, which had previously been restricted to state actors and powerful non-state actors already embedded in global governance, cracked open the silos of the global governance of the internet. Even though Russia attempted to prevent the broader participation of civil society and non-state actors in the OEWG deliberations,[56] it later underlined this aspect as a "distinctive feature" of the OEWG. Even if merely declaratory, or disingenuous, Russia's recognition of the role of global civil society is a crack in its own model of governance wherein civil society actors need an ideological approval of the state to function. In this context, the OEWG can further the democratic understanding of global civil society wherein civil society actors serve as watchdogs that monitor governmental activity and expose abuses of power. The support of the like-minded for that latter vision is an important strategy of revitalising the agendaof free and open internet. The subsequent OEWG, which will continue until

---

[50] Lauber, J. and Eberli, L. (2021) 'From confrontation to consensus: taking stock of the OEWG process', *Cyberstability Paper Series*, The Hague Centre for Strategic Studies, September, p. 7, (https://cyberstability.org/wp-content/uploads/2021/09/From-Confrontation-to-Consensus-Taking-Stock-of-the-OEWG-Process.pdf).

[51] Hofmann, S. and Pawlak, P. 'Governing Cyberspace: Framing Strategies, Porous Policy Boundaries, and Evolving Regime Complexes', Working Paper, forthcoming 2022.

[52] Andrey Krutskikh in an interview for *Kommersant*, 26 March 2019 (www.kommersant.ru/doc/3923963).

[53] Statement by Vladimir Shin at the online consultations of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 19 February 2021 (https://front.un-arm.org/wp-content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-19.02.2021.pdf).

[54] United Nations, Outcome report of the Informal Multistakeholder Consultation on OEWG Zero Draft Report (https://front.un-arm.org/wp-content/uploads/2021/03/Outcome-Report-of-the-Informal-Multistakeholder-Consultation-on-OEWG-zero-draft.pdf).

[55] United Nations, Outcome report of the Informal Multistakeholder Consultation on OEWG Zero Draft Report (https://front.un-arm.org/wp-content/uploads/2021/03/Outcome-Report-of-the-Informal-Multistakeholder-Consultation-on-OEWG-zero-draft.pdf).

[56] Revised consensus-aimed draft report of the OEWG tabled by the Russian Federation, 9 February 2021 (https://front.un-arm.org/wp-content/uploads/2021/02/RF-Revised-consensus-aimed-OEWG-draft-report-ENG.pdf).

2025, is another expression of Russia's ambition to turn the OEWG into a regular institutional dialogue at the UN[57] and thus mitigate the concentration of influence over global cyber regulation. Unsurprisingly, Russia vehemently opposes any initiatives that would undermine this initiative, in particular the Franco-Egyptian proposal for a PoA supported by the EU. While the details of the PoA are not yet clear, Russia was keen to discredit this project as allegedly an attempt of "westerners" to "hijack" the First Committee process by "inventing" a new track.[58] However, Russia's real concern seems to be the EU's potential to capitalise on numbers – that is, the participation of 27 EU member states that can use PoA proposed tools, such as implementation reports, to promote the EU's best practice and "impose" it "as a golden standard for the entire word."[59] In this setup, EU-Russia relations at the UN will turn into a regular competition for votes whereby each vote is considered as just one battle – some more meaningful than the others – in the long-term struggle.

In terms of policy outcomes, stagnation has a good starting point in that all parties are familiar with each other's positions. In this scenario, contestation over norms or principles of international law constitutes and is accepted as a normal state of affairs in EU-Russia relations. Russia and the EU both have distinct, partly conflicting and partly overlapping – at least rhetorically – narratives about the global governance of the internet that cannot be wished away by either party. They will understandably vie for global support for their respective storylines and subsequent adoption of the proposed policy solutions that put those respective visions in practice. The important element in this stagnation scenario (as opposed to the fragmentation scenario) is that the global nature of the internet is preserved, without significant repercussions for global connectivity.

In order to make the stagnation scenario work to its advantage and to navigate it effectively, the EU first needs to accept that this is the best outcome it can hope for in the current international environment. This implies one major adaptation – which is accepting that Russia simply sees the governance of cyberspace differently from the EU. In this sense, cyber diplomacy is not immune to a value-driven and political conflict that underpins other areas of EU-Russia relations.[60] Second, the EU needs to accept Russia's claims and concerns as legitimate, without necessarily agreeing with them. This means recognising that Russia's narrative about international security in cyberspace is not just the tale of a malicious spoiler, even if it is told from the position of deep-seated resentment. Some EU actors will object to such recognition as a form of indulging the resentment, or more dramatically, as appeasement. This is not the rationale behind the stagnation scenario. Recognition

---

[57] United Nations (2021) Developments in the field of information and telecommunications in the context of international security, A/RES/75/240, 4 January (https://undocs.org/en/A/RES/75/240).

[58] Statement by Vladimir Shin at the online consultations of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 19 February 2021 (https://front.un-arm.org/wp-content/uploads/2021/02/Russian-Federation-statement-at-informal-OEWG-session-19.02.2021.pdf).

[59] Ibid

[60] Kurowska, X. (2019) 'The politics of cyber norms: Beyond norm construction towards strategic narrative contestation' (https://eucyberdirect.eu/research/the-politics-of-cyber-norms-beyond-norm-construction-towards-strategic-narrative-contestation).

of difference, in combination with the EU's assertive cyber diplomacy, is simply more rational than hopes for Russia's conversion. Russia, however, does not necessarily perceive the EU to be an important player in UN debates about international security in cyberspace – it much prefers to reach deals directly with the United States, which it considers as the leader of the western bloc. The challenge is therefore to demonstrate that such a perception is unfounded. Third, and relatedly, the EU needs to use the First Committee debates as an opportunity to engage in dialogue with Russia on responsible state behaviour in cyberspace, but also to contest what it disagrees with more convincingly, and perhaps in novel ways.

The EU has several options to mediate the high level of conflict and avoid undesirable antagonistic fragmentation. **On the doctrinal level**, the EU needs to rethink to what extent adopting military frameworks of analysis and military vocabulary supports the EU's purpose of peaceful cyber relations, and the EU's positions at the UN. The best and most unfortunate example of unnecessary securitisation has been the poorly substantiated incorporation of the notion of deterrence into EU cyber policy.[61] Rather than mimic the speak adopted by NATO or the United States, whose cyber doctrine is rooted in defence policy, the EU should restate its commitment to the peaceful resolution of disputes and to conflict prevention – a language that would also resonate better with partners in the Global South. Russia's diplomatic practice is known for its resort to confrontational theatricality and tirade,[62] and such conduct will continue. Russia will use every opportunity to call out the EU's double standards when it comes to turning a blind eye on the violation of international norms by its allies – in particular the United States – but not missing any occasion to point the finger at Russia or China. However, rather than joining the confrontational or military speak reactively and by resort to buzzwords, such as deterrence in this case, the EU should communicate its normative commitments with a high level of transparency and accountability towards EU citizens. But it should also appeal to the interest of states in tapping into the benefits of a global digital economy – which only an open, free and global internet can facilitate. Issuing statements by the High Representative of the EU for Foreign and Security Policy (HRVP) about the common EU stance on cyber incidents, and on the EU's readiness to impose sanctions, as well as public and non-public demarches are a good tool to signal the consistency of the EU's posture.

On the operational level, the EU needs to make better use of its foreign policy and security tools in promoting its positions on the international stage in order to translate its global engagements into concrete support in international organisations, especially the UN. This recommendation is not new and has been broadly recognised in cyber diplomacy circles at the EU and member state levels. However, translating this goal into practice lags on several fronts. There is an urgent need for better coordination between the cyber sector in the EEAS and other thematic divisions, such as digital transition or strategic communication, regional desks and EU delegations, as well as between the EEAS and the European

---

[61] European Commission (2020) The EU's Cybersecurity Strategy for the Digital Decade, 16 December (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

[62] Marten, K. (2017) 'President Trump, keep in mind that Russia and the West think about negotiations very, very differently' (www.washingtonpost.com/news/monkey-cage/wp/2017/07/25/president-trump-keep-in-mind-that-russia-and-the-west-think-about-negotiations-very-very-differently/).

Commission services. Despite the adoption of policy frameworks and solutions that aim to bring different actors together – such as the Cyber Diplomacy Toolbox or the EU Cyber Diplomacy Network – turf wars and questions of competence (also between the EU member states) still hold the EU back and diminish the impact that it might play globally. Indeed, the EU currently remains one of a few key players that do not have a dedicated high-ranking diplomat to represent their positions on cyber and digital issues. Establishing the post of an EU Special Representative for Cyber Issues could nevertheless potentially remedy the leadership vacuum at EU level and pull together various EU workstreams to ensure their complementarity.[63] All these tools and coordination should then be deployed to expose the inconsistencies of the Russian positions as well as the benefits of the EU's own proposals.

The ultimate bad option? Fragmentation

Contrary to the stagnation scenario where the EU contests the Russian approach to cyber governance and attempts to contain it at the global level, **the fragmentation scenario implies that the EU recognises the Russian vision of cyberspace as impossible to contain, resulting in the partition of cyberspace along different models of governance. The fragmentation scenario envisages a formation of cyber regional orders that regulate the governance of the internet in regional-specific ways.** In principle, regionalism enhances the legitimacy and effectiveness of regulatory solutions because it relies on local expertise and arrangements. Regionalism and delegation to regional organisations as per Chapter VIII of the UN Charter also mediate concentration of global power. It is in this spirit that the GGE consultations in 2019 and 2020 envisaged a constructive role for regional organisations such as the EU, the Organization of American States, or the African Union. **In this scenario, however, regional institutions become stumbling blocks rather than building blocks for global multilateralism. This is because they develop into regional security alliances with a militaristic posture towards one another, which ultimately increases the overall sense of global insecurity.** Multiple regional cyber regimes can balance against each other, but the outcome can only be a fragile equilibrium established on hostility, with individual players dismissing the role of certain organisations as inadequate.[64]

This new cyber regionalism is already in the making. The Commonwealth of Independent States (CIS), the regional security alliance on the post-Soviet space, signed a statement on cooperation around international information security in which it also stressed the need to adopt a UN cybercrime convention, acknowledged the importance of "developing cooperation on issues related to the use and management of national segments of the internet" and singled out "the need to expand the role of the ITU in this context."[65] NATO has also been at the forefront of regional military cyber solutions. At the same time, new proposals are put forward to unsettle the existing normative orders. For example, the launch of the UN process to negotiate a new cybercrime treaty clearly challenges the legal and institutional

[63] Pawlak, P. (2019) 'Rebooting the EU's cyberdiplomacy', *European Cybersecurity Journal*, Vol. 5, Issue 2, pp. 52-59 (https://cybersecforum.eu/wp-content/uploads/2021/06/ECJ-VOLUME-5-2019-ISSUE-2.pdf).

[64] We have seen this, for instance, with Russia's dismissal of the Organization for Security and Co-operation in Europe (OSCE) as an organisation where discussion about the European security order can take place.

[65] CIS Heads Adopt a Joint Statement on Cooperation in the Area of International Information Security,' CIS Internet Portal, CIS News, 18 December 2020 (https://e-cis.info/news/564/89858/).

framework that was established globally by the Council of Europe Convention on Cybercrime. Proposals for a 'New Internet Protocol (NIP)' to become the global standard also challenge the traditional model of multistakeholder internet governance. If accepted, NIP would give states more control over cyberspace under the cover of more security and safety for citizens. The emergence of two competing internet orders would imply further fragmentation and undermine the global nature of the internet as we know it. Such breakdown of connectivity and interdependence not only increases rivalry but also removes a powerful brake on the offensive operations of states – that is, potential negative spillovers in their own territories.

In this type of fragmentation scenario, the EU begrudgingly accepts at least a temporary geopolitical and regulatory parallelism but remains committed to ultimately securing the predominance of the EU vision for cyberspace. An increased securitisation of discussion in regional organisations would also imply that in order to be taken seriously the EU would need to invest in strengthening its cyber offensive capabilities. In the context of the First Committee, this means that the EU recognises the impossibility of reaching a consensus with Russia on a universal approach to responsible state behaviour in cyberspace. The EU thus enters competition with Russia for the 'hearts and minds' of other states by establishing closer partnerships with regional organisations or advocating new bodies and organisations that would challenge the intergovernmentalist model proposed by Russia. In Russia's interpretation, the PoA may already be a move in this direction.

Although Moscow has traditionally been a promoter of regional organisations, this scenario is not necessarily ideal for Russia itself, in that its own international standing has suffered as a consequence of repeated accusations of malicious cyber activities and violations of international law. Its resulting isolation in major international venues has turned Russia into one of the strongest advocates of the central role of the UN in setting the future norms for cyberspace governance. During the OEWG, Russia insisted – albeit inaccurately – that there is a "universal consensus that the UN has a leading role" on international security in cyberspace and that efforts of regional organisations "should remain in line with the work under the UN auspices (…) not to duplicate it and not to contradict or undermine it in any other way".[66]

The fragmentation scenario exhibits high levels of conflict and polarisation which make it unlikely that the EU and Russia would propose reliable global frameworks of deconflicting and peaceful settlement. This scenario would also imply more rigid divisions in the debates around principles of non-interference, sovereignty, and peaceful resolution of dispute that would multiply across the whole UN system. Russia's reliance on sovereignty and non-intervention as the flagship concepts of its vision for cyberspace have resonated particularly well with states that wish to exercise more governmental control over 'their' cyberspace in the fight against cybercrime and information manipulation, and that fear western retribution for such policies. Because fragmentation cannot be fully excluded, the EU should take several mediating steps. It will be crucial that regional organisations do not become hostage

[66] Revised consensus-aimed draft report of the OEWG tabled by the Russian Federation, 9 February 2021 (https://front.un-arm.org/wp-content/uploads/2021/02/RF-Revised-consensus-aimed-OEWG-draft-report-ENG.pdf).

to any one principle of cyber governance as dictated by powerful sponsors. They thus need sufficient capacities to realise their globally compatible yet locally crafted solutions. In this way, the acknowledgment of difference can be consolidated in a bottom-up way and inform the UN processes, thereby contributing to the global culture of bona fide contestation. In other words, the prevention of fragmentation as a militaristic form of cyber regionalism lies in the capacity for self-determined regionalism. This currently seems unworkable given the level of political polarisation between major powers that influence the policies of key regional organisations. Proposals made by Mexico and Australia, among others, to focus on implementation of the framework for responsible state behaviour and the creation of a Survey of National Implementation[67] are regularly rejected by Russia, which argues that the contours of the responsible state behaviour framework are far from being settled.

This scenario of fragmentation is not in the EU's interest, but that does not mean the EU should not prepare for it, especially since certain initiatives by Russia and China are clearly aimed at promoting their own vision of cyberspace under the guise of trade or security partnerships. An important element of this scenario is that Russia by itself does not have the sufficient gravitas or capacity to push for change to the existing models of governance in cyberspace and needs to rely on China – the only other partner with ideological, technological, and military muscle. **On the doctrinal level**, this is nevertheless an opportunity for the EU to reinvent itself as a normative cyber power. The currently dominant approach in Brussels suggests the adoption of a more transactional approach to working with third countries and regional organisations. But such an approach needs to be carefully calibrated. Even if the EU's message might be attractive, its delivery will be equally important in order not to feed into Russia's strategic communication about western cyber neocolonialism. The EU should instead grow an attitude of partnership with regional actors, without the condition of normative and political acquiescence. It should also support their locally driven strategies of capacity development towards full participation in the global discussions about cyber-related issues. At the end of the day, the success of the EU's capacity building might be measured better in the number of different regional positions that emerge in the global debates rather than the level of compatibility with EU views. The General Data Protection Regulation (GDPR) or Network and Information Security (NIS) Directive are just two examples of how EU norms and standards can become global benchmarks thanks to their perceived value rather than conditionality mechanisms. This may appear counterintuitive to the standards of conditionality, but the multitude of competent, capable, and relatively self-reliant cyber actors constitutes a better strategic environment than a militaristic cyber fragmentation. It also speaks to the spirit of genuine multistakeholderism more broadly. The EU needs to renew its commitments in this realm by investing in the diversity of global digital civil society and by supporting stakeholders that do not have the capital of Big Tech.

On the operational level, this scenario of fragmentation poses a particular challenge for the EU because it undermines the global

[67] United Nations (2021) Proposal for National Survey of Implementation of United Nations General Assembly Resolution 70/237, 22 February (https://front.un-arm.org/wp-content/uploads/2021/02/Joint-Proposal-Survey-of-National-Implementation-FINAL-REV-3-.pdf).

nature of cyberspace on which the EU builds its digitalisation agenda and partnerships with some regions of the world. The EU's best bet to encourage other states on board – and consequently regional organisations – is therefore to focus on promoting tools and mechanisms that enhance cooperation around strengthening resilience and the digital economy. Reinforcing this message among the partner countries in practice implies that digital policies need to become an integral component of the EU's cyber diplomacy. Regarding the approach towards Russia, the EU needs to invest more in strategic communication that exposes the contradictions between Russia's narrative and practice, in particular when it comes to promoting the focus on cyber capacity-building, Russia's insistence on sovereignty and non-interference, and its practices that prevent other states from involving their civil society organisations in the discussions at global level.

Conclusions

This paper contextualises the current impasse between the EU and Russia within a broader horizon. To begin with, Russia capitalises on global hypocrisies in preaching but not delivering on genuine multilateralism. Russia does this in particular through outreach with those that are truly concerned with, and have been affected by, the deepening of the global digital divide. Furthermore, Russia exploits any hint of discriminatory conduct (including in the complexities of attribution in the aftermath of cyberattacks) as proof of Russophobia in the international arena. Russia is given an ear, even if it is not believed, because there are large constituencies in international society which are disgruntled over the past and present global inequalities. In such advocacy, Russia uses forms of normative relativisation that disorient the normative power Europe.

Looking at the level of overall conflict between the EU and Russia, as well as their views on the role of states in governance of cyberspace, we propose four different scenarios in which this complicated EU-Russia relationship could be managed and transformed: stagnation, fragmentation, accommodation, and conversion. Having rejected the latter two as politically unlikely, we conclude that a deep transformation of EU-Russia cyber relations at the UN is not plausible. We suggest, however, that realising the potential unleashed at the UN – in particular within the OEWG – may be the best way to manage the stagnation scenario, and thus to manage EU-Russia relations effectively, within the existing constraints. This is because the OEWG is in fact a space of contestation which cannot be readily hijacked – where all parties can advertise their small victories but where ultimately none should gain an upper hand. The OEWG gives Russia the rhetorical means to claim a diplomatic triumph while in fact it better reflects the EU's normative commitments in international politics. Russia will strive to pull the OEWG towards intergovernmentalism – but the EU should pull it towards multistakeholderism. In the process, both Russia and the EU will evoke the framework for responsible state behaviour in cyberspace. While they may understand this framework differently, and while they continue to accuse each other of hypocrisy, the OEWG creates a space to practise deconfliction, sometimes by the performance of commonality. Handling such contestation without becoming dogmatic or defensive, especially in times when international politics becomes a populist playground, will be a challenge.

Finally, we point to two main dilemmas associated with the EU's response. At the doctrinal level, the EU's turn away from promoting cyber resilience and conflict prevention towards deterrence as a dominant concept in defining the EU's cyber posture may cost Brussels the support of other actors that are committed to the peaceful resolution of disputes. At the operational level, the EU's biggest weakness lies in the disconnect between digital and cyber policies from a broader foreign and security policy agenda. Unless the EU leadership approaches cyber diplomacy as a tool to promote the EU's vision for the digital world while at the same time using the digital policies as vehicles for the EU's values and norms – as Russia does consistently – it risks being relegated to the second league of cyber players.

About the authors

DR XYMENA KUROWSKA

Xymena Kurowska is Associate Professor of International Relations at Central European University in Vienna. She is an International Relations theorist practising interpretive policy analysis. She has published and taught in the areas of European security policy, cyber diplomacy, Russia in global politics, international political sociology, critical security studies, and narrative approaches in knowledge production. She is a co-editor of the *Journal of International Relations and Development*. She holds a PhD in Political and Social Sciences from the European University Institute in Florence and an MA in International Relations from Warsaw University.

DR PATRYK PAWLAK

Patryk Pawlak is the EUISS Brussels Executive Officer and leads the Institute's work on cyber and digital issues. He is a project director for the EU Cyber Direct – European Cyber Diplomacy Initiative, an EU-funded multimillion-Euro project that supports the EU's engagement on cyber diplomacy and digital policies worldwide. In this capacity, he is also co-editor of Directions Blog on cyber, digital and tech issues. Dr Pawlak's work focuses on the EU's cyber and digital policies, in particular the role of cyber capacity-building policy and confidence-building measures. He regularly contributes to the ongoing international and regional processes focused on cyber issues. He holds a PhD in Political and Social Sciences from the European University Institute in Florence and an MA in European Studies from the College of Europe.

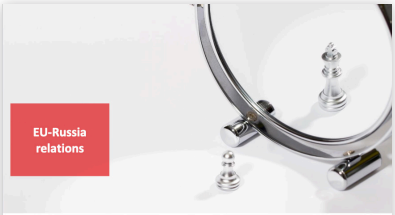
Cover photo: Shutterstock / FOTOGRIN

This Policy Brief was produced with the financial support of the European Parliament. It does not represent the view of the European Parliament.

ON SIMILAR TOPICS

Recommendations to the EU in light of Russian policy towards the Eastern Partnership

By Jakub Benedyczak



Mirror images In EU-Russia relations

By Irina Bolgova

EU-Russia relations in the light of Russia's engagement in the Middle East and North Africa

By Agnieszka Bryc

EU-Russian relations: Normative rivalry or pragmatic partnership?

By Barbara Roggeveen

Is Russia interested in multilateralism and should the EU engage with it?

By Angela Romano

The Role of Sanctions in current and future EU-Russia Relations

By Tatiana Romanova