RESEARCH IN FOCUS

What does Russia want in cyber diplomacy? A primer

Xymena Kurowska
Central European University
December 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is
funded by the
European Union.

Contents

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).

Abstract

This paper examines the origins and current shape of Russia's priorities in cyber diplomacy, as well as its efforts to shape global governance of the Internet. These are discussed with regard to a larger paradigm of Russia's foreign policy since the late 1990s and its understanding of the digital domain as a threat to both the international order and the domestic regime. Russia has worked out a relatively consistent strategy of contestation of the liberal order in general and the liberal cyber regime in particular. Rhetorically, it builds on what it calls a 'democratisation' of international relations, of which the advocacy for the Open-Ended-Working-Group in global governance of the Internet is an example. It also relies on an interpretation of international law and international norms that challenges the notion of "the rules-based international order" as unlawful and resorts to regional arrangements which become a laboratory for global cyber initiatives. The core of Russia's cyber rhetoric is the pre-eminence of the state and the guarding of information security, which see the politically and cyber-empowered individual as a potential threat to regime stability.

Key points

> Russia is often portrayed as a spoiler in cyber diplomacy but such portrayal ignores the sources of Russia's cyber posture and its normative potential.

> While Russia has sought to counter the liberal order since the late 1990s, it previously lacked legitimacy, which it now tries to restore with its call for the Internet regulation.

> Russia conjures up in particular an understanding of international law and international norms which challenges the principle of "the rules-based international order" on the basis that it is "undemocratic."

> It seeks to mobilise grievances in international society; however, the aim is not to democratise decision-making. Rather, it is to secure an equal place at the decision-making table.

> The advocacy for OEWG may therefore backfire: it has created a 'cyber agora' which can prove difficult to steer towards Russia's cyber goals.

> The place of the individual in international cyber society remains the bone of contention. The liberal cyber regime should reinvigorate its holistic commitment to the individual as the centre of gravity.

Introduction

The standard analytical narratives regarding Russia's behaviour in global diplomacy, today, revolve around great power aspirations, revisionist power games, and a threat to liberal democracy as we know it. The Russian discourse can also, however, be parsed with reference to resentment, resulting from the sense of 'being betrayed' by the West,[1] or to anger over apparent disrespect received from other international actors.[2] Demand for status recognition is a key factor in Russia's international conduct,[3] which finds its expression in Russia's regular insistence on acknowledging its indispensability to the international order.[4] Despite declarations of pragmatism in foreign policy,[5] this status-related rationale often overshadows what would appear more rational courses of action. Demands for recognition may also result in embarrassment. One vivid example of the latter involved the emotional outburst by the acting Russian representative to the UN, Vladimir Safronkov, towards the UK representative during a Security Council session in April 2017: "Look at me!" he said famously, followed by, "Don't you dare insult Russia again!"[6] Many looked away mortified, but Safronkov's superiors in the Ministry for Foreign Affairs commended his behaviour, as part of resistance towards Western attempts at hegemonic imposition.[7]

“

> **The contestation over global Internet governance both manifests and indicates the emerging contours of a new international order.**

The current tit-for-tat clashes over models of global Internet governance, which effectively reinstate Russia to the highest echelons of international interactions, are redolent of the Cold War diplomatic ritual that Russia enjoys. It matters, once again, what Russia says. There is a timely narrative in this strategic communication, backed by effective diplomatic outreach, which is by no means 'cheap talk.' The contestation over global Internet governance both manifests and indicates the emerging contours of a new international order. Examining Russia's priorities in this struggle is not easy, however, due to radical political polarization but also a certain 'confusion-of-tongues.' In cyber diplomacy, or in international information security (as is the preferred term in the Russian discourse), actors use identical or similar terminology, but such terminology derives from different imaginaries about the international order, and, arguably, different imaginaries about the good life.[8] The place of the individual in international society remains the bone of contention across these ideational frameworks. It will inform, implicitly and explicitly, the normative stakes in global governance of the Internet for years to come, including with regard to technology-related questions.

[1] Xymena Kurowska,"Multipolarity as Resistance to Liberal Norms: Russia's Position on Responsibility to Protect," Conflict, Security & Development, 14 (2014): 489-508.

[2] Deborah Larson and Alexei Shevchenko, "Russia Says No: Power, Status, and Emotions in Foreign Policy," Communist and Post-Communist Studies, 47 (2014): 269-279.

[3] Oliver Schmitt, "How to Challenge an International Order: Russian Diplomatic Practices in Multilateral Security Organisations," European Journal of International Relations, forthcoming; Iver Neumann, "Russia's Europe, 1991–2016: inferiority to superiority," International Affairs, 92 (2016): 1381-1399.

[4] Bobo Lo, Russia and the New World Disorder (London and Washington, DC: Chatham House and Brookings Institution Press, 2015), p. 47.

[5] Mariya Omelicheva, "Critical Geopolitics on Russian Foreign Policy: Uncovering the Imagery of Moscow's International Relations," International Politics, 53 (2016): 708-726.

[6] Radio Free Europe/Radio Liberty, 13 April 2017. Accessed 5 October 2019. Available at https://www.rferl.org/a/russia-uk-un/28427527.html.

[7] Carl Schreck, "'Look At Me!': Russian UN Envoy's Rant Stirs Buzz Back Home," Radio Free Europe/Radio Liberty. Accessed 24 November. Available at https://www.rferl.org/a/look-at-me-russian-envoy-rant-stirs-buzz-russia/28428194.html.

[8] For an analysis of terminological misunderstandings in the domain of cyber and information security as evident in the policy documents by Russia, China, US, and UK see Keir Giles and William Hagestad, "Divided by a common Language: Cyber Definitions in Chinese, Russian and English," 2013, 5th International Conference on Cyber Conflict, Tallinn.

This paper brings these issues into sharp relief, contributing to a better-informed debate. In its substantive introduction, it lays out the basics of the current framing of Russia's cyber narrative. It then explains the priorities of Russian cyber diplomacy with reference to Russia's self-perceived standing and responsibility in maintaining peace and security. Crucial to grasping this position is understanding the conception of international law that Russia applies in cyberspace, how this ties back to its doctrine of multipolarity, and the peculiar interpretation of multilateralism that comes along with this. Further, the paper unpacks a core trope in Russia's strategic diplomatic communication more broadly: that is, the notion of 'democratising' international relations. This is a self-serving rhetorical trope, readily dismissed by the West as nonsense. But it is not without the potential to subvert the Western normative dominance in global Internet governance. This rhetoric appeals to genuine grievances over the existing inequalities in international society and capitalises on the West's own subversion and betrayal of the liberal ethos. Russia's strategy to advance its 'democratisation' agenda resembles "trickstery":[9] It is a mixture of a spoiler's tactic of sowing confusion, along with a sombre discourse of responsibility for international security.

The last two parts of this paper look more closely at, first, the doctrine of information security, which is fundamental for grasping Russia's cyber conduct at the juncture of its domestic and foreign policy, and, second, the regional effort to codify this doctrine, which is incrementally being uploaded globally. The paper concludes with the suggestion that Russia's posturing in cyber diplomacy is not so much a security threat per se but a 'normative threat'[10] to the liberal way of life. As such, it is a manifestation of an ideological struggle that liberal cybernorms entrepreneurs cannot afford to simply disparage or ignore. An analysis of exactly what is being contested can help to reform their effort. The rather urgent political question, in this context, involves how to smartly counteract being cast as a villain by Russia's narrative about the post-liberal world. In other words, the question is how to offer an appealing and inclusive alternative.

2018 – Reclaiming the debate

The adoption of two competing resolutions regarding global governance of the Internet in 2018 - the US-sponsored reaffirmation of the UN Group of Governmental Experts (UN GGE)[11] and the Russia-sponsored launching of the Open-Ended Working Group (OEWG)[12] - marks the final breakdown of international consensus on the issue. In Russia's cyber narrative, however, it is taken as a positive breakthrough, fortuitously overlapping with the 20-year anniversary of when, in 1998, Moscow tabled its first draft resolution on Information and Communication Technology (ICT) in the General Assembly's First Committee on Disarmament and International Security.[13] In 2018, Russia in fact successfully sponsored two resolutions: the above-mentioned one launching the OEWG and another, adopted in the 3rd Committee of the General Assembly on cybercrime.[14] Both were framed as a significant way

[9] Xymena Kurowska and Anatoly Reshetnikov, "Russia’s Trolling Complex at Home and Abroad," Hacks, Leaks and Disruptions. Russian Cyber Strategies, edited by Nicu Popescu and Sergiu Secrieru, (Paris: EU Institute for Security Studies, 2018), pp. 25-32.

[10] Ingrid Creppell, "The Concept of Normative Threat," International Theory, 3(2011): 450-487.

[11] General Assembly of the United Nations, "Advancing responsible State behaviour in cyberspace in the context of international security," 2018, New York: A/RES/73/266.

[12] General Assembly of the United Nations, "Developments in the field of information and telecommunications in the context of international security," 2018, New York: A/RES/73/27.

[13] Kommersant, "Rossiya i SSHA peretyagivayut vsemirnuyu pautinu [Russia and the USA are pulling the World Wide Web]," 12 November 2019, p. 6.

[14] General Assembly of the United Nations, "Countering the use of information and communications technologies for criminal purposes," 2018, New York: A/RES/73/187.

forward, instigated by Russian cyber diplomacy.[15] They are portrayed as a return to the original purpose of the UN track on International Information Security, as initiated by Russia in 1998, which is to create accountability in what is depicted as fundamentally "ungovernable" cyberspace. The OEWG resolution sets 13 rules, norms, and principles (in comparison with the 11 laid out in the US-sponsored resolution) of responsible state behaviour that are the first "rules of the road" in history with regard to this issue - despite them formally being only "recommendations for consideration by States".[16] Specifically, the resolution includes a reassertion of cultural diversity, enshrined in the UN Charter, in global Internet governance. The launch of the OEWG is presented as ushering in a genuine democratisation of global Internet governance and a potential space where negotiations over an international cyber treaty can be launched.

The aim of the resolution on cybercrime was, in turn, to launch a separate track on the matter in the UN, as an alternative to the Budapest Convention on Cybercrime. Drawn up by the Council of Europe in 2001 to foster international cooperation on cybercrime and promoted by the group of "the like-minded," the Budapest convention is opposed by Russia due to its paragraph 32b, which allows for transborder access to data during cybercrime investigations by the intelligence services. Russia's advocacy for a cybercrime treaty within the UN, recently bolstered by a new resolution adopted in the 3rd Committee mandating such efforts, is portrayed as part of the attempt to extend the control of the state over the Internet and curtail the political rights of the individual.[17] This is, in broad terms, the crux of "the like-minded" position. Russia, similar to some other non-Western actors, in return charges the West with maintaining digital inequality and infringement of sovereignty in the pursuit of upholding the liberal world order. The remainder of the paper unpacks the Russian perspective on the current state of "unpeace"[18] which thus unfolds in cyberspace and the tasks that Russian diplomacy sets for itself in this regard.

Priorities of Russia’s cyber diplomacy

The short answer to what Russia wants in and through cyber diplomacy is twofold. First, cyber promises Russia respect *(уважение/uvazheniye)*, not only at the well-cultivated regional level, but, potentially, globally. It affords status recognition that Russia lost and has been eager to regain since the unsuccessful attempt to integrate into the liberal world order in the early 1990s. Status thirst is, however, difficult to engage with in politics: It is a moving target and the approaches of Western countries are likely to "fall below Moscow's expectations to be treated as it feels it deserves".[19] Second, the long-standing priority of Russia's cyber diplomacy is "to *create conditions* [emphasis mine] for promoting internationally the Russian initiative to develop and adopt a Convention of International Information Security by United Nations Member States."[20] The *lex specialis* for the cyber domain may not yet be realistic, in other words, but Russia is working to prepare the ground for it.

"The like-minded" tend to justify their objection to an international cyber treaty by referring to the consensus that existing international law already applies in cyberspace, and that when this is supported

[15] Ernest Chernukhin, "Mezhdunarodnaya Informatsionnaya Bezopasnost': Uspekhi Rossii v OON [International Information Security: Russia's Successes at the UN]," presented at the Russian International Affairs Council on 4 February 2019. Accessed 23 November 2019. Available at https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-uspekhi-rossii-v-oon/

[16] Ibid.

[17] Ellen Nakashima, "The U.S. is urging a no vote on a Russian-led U.N. resolution calling for a global cybercrime treaty," The Washington Post, 6 November 2019.

[18] Lucas Kello, The Virtual Weapon and International Order, (New Haven: Yale University Press, 2017), p. 78.

[19] Schmitt, op.cit., p. 20.

[20] Security Council of the Russian Federation, "Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda [Foundations of the state policy of the Russian Federation in the field of international information security for the period until 2020]," 2013. Accessed 23 November 2019. Available at http://www.scrf.gov.ru/security/information/document114/.

by the norms of responsible state behaviour, it is sufficient to defend "the rules-based international order" in cyberspace. Negotiations over a new binding instrument would, in this context, only divert efforts from implementing what is already agreed upon; they would draw the world into an unnecessary, lengthy, and divisive struggle, and, as emphasised particularly in US discourse, hinder technological development.[21] Russia's advocacy for the treaty relies on the claim of defending the international order in its classic version, where binding legal instruments are a traditional form of regulation. An international cyber treaty is also portrayed as a means for curbing the liberal international order, which legitimises intervention into the domestic makeup of states, and thus as a tool against the ad hoc decisions of the strong.

> “
>
> **Russia's advocacy for the treaty relies on the claim of defending the international order in its classic version, where binding legal instruments are a traditional form of regulation.**

The notion of "the rules-based international order"[22] is particularly contested in this respect, as a replacement for, rather than a continuation of, an international law-based order. The idea is vehemently attacked in Russian diplomacy as an attempt to "usurp the decision-making process on key issues" by "[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."[23] Such rhetoric, as the paper lays out below in more detail, is self-serving; however, it is short-sighted of the West to disregard it. The concern with representativeness, and the instrumentalisation of such a concern for both tactical and strategic gains, increasingly inform political positions in global governance of the Internet.

Finally, Russia's advocacy of an international cyber treaty has another snappy line: International law applies in cyberspace but even legal experts are not sure how. The very term "responsible state behaviour in cyberspace" is, in the Russian interpretation, not clear. International procedural law, as a set of principles and norms governing the exercise of the rights and obligations of subjects of international law, is seen as being not adapted to the regulation of international relations in the field of ICT.[24] Furthermore, the use of international customs and general principles of law is unpromising in this area given the lack of a common understanding of some objects of legal regulation, such as the use of ICT as a means of warfare.[25] This almost sacrosanct portrayal of international law has been part of Russia's foreign policy for two decades. After the 1999 NATO operation in Kosovo, which Russia contested passionately, the then-minister for foreign affairs, Igor Ivanov, formulated what became a

[21] Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What’s New?," 2015. Accessed 11 November 2019. Available at https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/.

[22] "The rules-based international order" can be defined as "a shared commitment by all countries to conduct their activities in accordance with agreed rules that evolve over time, such as international law, regional security arrangements, trade agreements, immigration protocols, and cultural arrangements," see United Nations Association of Australia, "The United Nations and the Rules-based International Order," 2015. Accessed 23 November 2019. Available at https://www.unaa.org.au/wp-content/uploads/2015/07/UNAA_RulesBasedOrder_ARTweb3.pdf.

[23] Sergey Lavrov, "World at a Crossroads and a System of International Relations for the Future," Russia in Global Affairs, 20 September 2019. Accessed 11 November 2019. Available at https://eng.globalaffairs.ru/book/World-at-a-crossroads-The-future-system-of-international-relations-20199.

[24] Strel'tsov, A. A., R.A. Sharyapov, and V.V. Yashchenko, "Kratkiy kommentariy i predlozheniya k p.13 Doklada Gruppy pravitel'stvennykh ekspertov po dostizheniyam v sfere informatizatsii i telekommunikatsiy v sfere mezhdunarodnoy bezopasnosti [Brief comment and suggestions to paragraph 13 of the Report of the Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security]," Moskva: Institut problem informatsionnoy bezopasnosti Moskovskogo gosudarstvennogo universiteta imeni M.V.Lomonosova, 2016, p. 6, para. 1.7.

[25] Ibid.

default Russian position: the objection to changing "basic principles of international law" in order to replace them with the doctrines of "limited sovereignty."[26]

This sacrosanct understanding of international law as being above politics has been interrogated in the Western doctrine of international law as a political move in itself.[27] Despite its claim to neutrality and impartiality, international law is part of the way political power is used, critiqued, and sometimes limited. The Russian initiative to create conditions conducive to negotiating an international cyber treaty needs to be seen in this light: It is part of the process of imposing a particular vision of international relations, in the process critiquing and possibly limiting the power of Western liberal states, above all the US.

> “
>
> **Despite its claim to neutrality and impartiality, international law is part of the way political power is used, critiqued, and sometimes limited.**

Russia’s comeback as a « responsible cyber power »

The promotion of a dedicated and legally binding instrument in cyberspace belongs to Russia's twofold strategy. On the one hand, Russia engages in intense "securitisation"[28] of cyberspace: It invests in portraying everything cyber, or digital, as a grave security threat (see below). On the other, it takes up the role of a responsible great power which can be relied upon to counter this threat. Russia thus acts simultaneously as spoiler and saviour. This position yields distinct rewards: It provides discursive resources for Russia to frame itself as a concerned, influential and capable cyber leader for the non-Western, or post-liberal world. Thus, Russia returns to the global game of international order.

The analogy with the new 'Cuban missile crisis,' conjured up by Andrey Krutskikh, the Special Representative of the President of the Russian Federation on International Cooperation in Information Security,[29] is an example of the securitising discourse about the world at the brink of a cyber catastrophe. Russia substantively likens the hazards of nuclear weapons to those of digitalisation because of the technological implications of the scale of threat and interlinkages between them.[30] The very initiation of the cyber debate in the context of international security within the UN 1st Committee on Disarmament was justified in terms of the dangers of "information weapons" (the term now formally withdrawn but hardly forgotten) and modelled on the nuclear non-proliferation regime. Russia hoped to emulate the parameters of the nuclear regime for information security in cyberspace to mediate Western superiority in that domain.[31] Cyber debates predictably proliferated across the UN landscape to include all domains of international relations. But the security tone that Russia set back in the late 1990s has also become progressively dominant.

[26] Igor Ivanov cited in: Derek Averre, "From Pristina to Tskhinvali: the legacy of Operation Allied Force in Russia's relations with the West," International Affairs, 85 (2009): 575-591, p. 586.

[27] Martti Koskenniemi, The Politics of International Law, (London: Hart Publishing, 2011).

[28] Securitization in international relations is the process of state actors transforming subjects into matters of ‘security’: an extreme version of politicization that enables extraordinary means to be used in the name of security, see Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: a New Framework for Analysis, (Boulder, Colo.: Lynne Rienner, 1998), p. 25. The successful securitization of ICT by the Russian Federation was noticed by Eneken Tikk and Mika Kerttunen in their Parabasis. Cyber-diplomacy in Stalemate, (Norwegian Institute of International Affairs: Oslo, 2018), pp. 56 & 58.

[29] Andrey Krutskikh cited in Kommersant, "Rossii nechego skryvat' i nechego boyat'sya [Russia has nothing to hide and nothing to fear]," 27 March 2019.

[30] Pavel Sharikov, "Artificial Intelligence, Cyberattack, and Nuclear Weapons—A Dangerous Combination," Bulletin of the Atomic Scientists, 74 (2018): 368-373.

[31] Elena Chernenko, "Russia’s Cyber Diplomacy," in: Hacks, Leaks and Disruptions. Russian Cyber Strategies, edited by Nicu Popescu and Sergiu Secrieru, (Paris: EU Institute for Security Studies, 2018), pp. 43-49.

The image of the new Cuban missile crisis has a wider appeal, too. It excavates the frame of the Cold War Soviet-US relationship as ruling the world, and of the international order as it was fixed in 1945 by the victorious allies, with the caveat that China has risen in the meantime. This is a reinvigorating turn for Russia's long-frustrated aspiration to regain (even symbolically) parity with the West and the image of an imminent disaster is well-exploited. As the current mantra of Russian diplomats goes: "[U]nlike the US, Russia, as a *responsible* [emphasis mine] State, is not interested in new missile crises," but it has the obligation to mitigate US "destructive actions" in global politics.[32] An impoverished country with tangibly little to mould world affairs, but with a reputation in need of restoring, Russia can only gain from revamping its international role by becoming a responsible cyber power.[33] The role gives a shiny and topical veneer to an anachronistic understanding of the international order, reasserting Russia's special responsibility as the permanent member of the UN Security Council for shaping global cooperation and maintaining peace and security. The distinct advantage of the cyber domain is that it is highly 'actionable.' Nuclear weapons are, ultimately, not to be used; the international community has even manged to create a taboo over such potential use.[34] By contrast, cyber means of disruption and interference may be, and are, in common use.

> “
>
> **In practice, cyber diplomacy provides Russia with a global platform for uploading its long-cultivated regional effort to counter the liberal world order.**

In rhetoric, Russia's chief preoccupation is then with the militarisation of cyberspace, which adds urgency to global Internet regulation. In practice, cyber diplomacy provides Russia with a global platform for uploading its long-cultivated regional effort to counter the liberal world order. The frequency of cyberattacks and scandals, including the Snowden and Cambridge Analytica revelations, bolster Russia's claim of cyberspace as dangerous and lacking proper 'rules-of-the-road.' The growing populist sentiment at the global level further plays into the hands of the Kremlin, which has the ideological and operational resources to tap into this sentiment as a new structuring force in international politics. A key discourse in this respect is Russia's broad agenda of defending international law and democratising international relations (read: containing US hegemony), revamped in the rhetoric of fighting digital inequality.

International law and international norms in Russia’s cyber diplomacy

There is a missing link in the debate over whether international law applies in cyberspace. The explicit consensus that it does apply is marked by different understandings of the role of international law as such.[35] This consensus is therefore hardly a reason to celebrate. The recent recommendation that national governments append to the UN GGE reports their explanation of how international law applies

[32] Statement by Mr. Vladimir Yermakov, Head of Delegation of the Russian Federation to the First Committee of the 74th UNGA session, Director of the Department for Nonproliferation and Arms Control of the Ministry of Foreign Affairs of the Russian Federation, within the General Debate. Permanent Mission of the Russian Federation to the United Nations, New York: 11 October 2019, p. 2.

[33] Cf. Julien Nocetti, "Cyber Power" in: Routledge Handbook of Russian Foreign Policy, edited by Andrey Tsygankov, (London and New York: Routledge, 2018), pp. 182-197.

[34] Nina Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use," International Organization, 53 (1999): 433-468.

[35] Some authors speak of the Russian version as "a simulacrum or concave mirror to Western use," see Lauri Mälksoo, Russian Approaches to International Law, (Oxford: Oxford University Press, 2015), p. 185. See Tikk and Kerttunen, op. cit., for examples of how specific concepts of international law have been differently understood across a range of actors participating in the UN GGE.

in cyberspace is a move towards clarification. It will not, however, eradicate fundamental differences in interpretation.

The Kremlin interprets international law as the body of rules and conventions that govern relations between the major powers. Formally speaking, this reflects a procedural and pluralist understanding of international law as a particular kind of a legal system, with a commitment to legality in international politics as an end in itself rather than a means towards an end beyond itself.[36] This traditional positivist notion contrasts with a model of international law as a way to judge, in terms of its "functional capacity to actually pre-empt political choices and realise agreed-upon objectives".[37] In other words, for Moscow, international law regulates relations between states of different ideological disposition, without prejudice as to such disposition. "The like-minded" see international law more as a means towards upholding a liberal consensus, in this case an open and free Internet which belongs to the liberal vision of international order. As a result, there are different models of international law that apply in cyberspace.

Core to the Russian interpretation is the preponderance of the statist discourse of international law, with emphasis on the classic understanding of sovereignty and a categorical rejection of the notion of the individual as a subject of international law.[38] At the same time, the individual becomes increasingly empowered in the Western discourse on international law, which also shifts towards transnational, rather than state-based, solutions. The glorification of the state in the Russian legal doctrine[39] leads to a distinct twist on the very idea of law as "speaking truth to power": In the Russian rendition, the addressee of the 'truth of international law' is the US, or the 'West' by extension, and not the Russian government.[40] International law "à la Russe serves to restrain the exercise of American power".[41]

When Russian Foreign Minister Lavrov repeats the mantra of double standards in the application of international law[42] and denounces "attacks on international law",[43] it is this version of speaking truth to power that is being exercised. Such tirades may be interpreted as ludicrous and hypocritical by Western observers. It eludes these observers, however, that international law is often portrayed outside of the West as a hegemonic tool of the West. The Russian Investigative Committee chief, Alexander Bastrykin, taps into anti-hegemonic grievances in international society when he states that "international law and the justice based on it have increasingly become tools of [hybrid] war" against Moscow.[44]

Such grievances are appealed to in Russia's pursuit of a 'democratisation' of international relations, even as the agenda serves the Russian doctrine of multipolarity, rather than the cause of a genuine democratisation of decision-making in the international system. Simply put, multipolarity, or the polycentric world order, refers to a system in which power is distributed among at least three significant poles concentrating wealth and/or military capabilities and which are able to block or disrupt major political arrangements that threaten their major interests.[45] A pole is also understood as an actor

[36] Richard Collins, "Two Idea(l)s of the International Rule of Law," Global Constitutionalism, 8 (2019): 191-226, p. 196.

[37] Ibid.

[38] Dmitry Dubrovsky, "Lauri Mälksoo. Russian Approaches to International Law," Laboratorium: Russian Review of Social Research, 9 (2017): 146-151.

[39] Lauri Mälksoo, Russian Approaches to International Law, op. cit., p. 100.

[40] Ibid, p. 81.

[41] Bobo Lo, op.cit., p. 95.

[42] Sergey Lavrov, "Russia's Foreign Policy in a Historical Perspective," Russia in Global Affairs, 2 (2016). Accessed 27 July 2019. Available at https://eng.globalaffairs.ru/number/Russias-Foreign-Policy-in-a-Historical-Perspective-18067.

[43] Sergey Lavrov cited in Kommersant, "Ataki na mezhdunarodnoye pravo priobretayut opasnyye masshtaby [Attacks on international law are becoming dangerous]," 27 September 2019.

[44] Alexander Bastrykin cited in Kommersant, "Pora postavit' deystvennyy zaslon informatsionnoy voyne [It's time to put an effective barrier to the information war]," 18 April 2016.

[45] Andrey Makarychev and Viatcheslav Morozov, "Multilateralism, Multipolarity, and Beyond: A Menu of Russia's Policy Strategies," Global Governance, 17 (2011): 353-373.

capable of producing order or generating disorder, usually a regional power with a global reach. Multipolarity therefore means concentrating power in the hands of a few. When Russia speaks of a polycentric world order, it also projects a value system that would support such an order.[46] This builds on civilizational diversity; that is, the notion that countries should not have the right to judge each other's domestic practices and cultures. The principle is not politically neutral - the pole exerts normative as well as political influence. Rather, the principle is intended "to chip away at the authority of Western forms of order and empower regimes to dismiss liberal norms as intrusive and inappropriate for their culture".[47]

> “
>
> **Russia approaches international institutions as equalizers of liberal hegemony and as a means of guarding its own sovereignty, not as components of transnational regimes generating global governance**

Multipolarity is often conflated with multilateralism in Russian diplomacy, to the extent that it baffles external observers. Russia approaches international institutions as equalizers of liberal hegemony and as a means of guarding its own sovereignty, not as components of transnational regimes generating global governance, which contravenes sovereignty, or makes it 'conditional.' The insistence on the UN's central and coordinating role in world politics should be read in this light: It reasserts collective leadership by major powers through the Security Council, as fixed in 1945. It also constitutes a balancing mechanism to both prevent an imposition with regard to domestic governance and curb unilateral action based solely on national interest (i.e. the US' interest).

International law and international norms are crucial to maintaining this system, hence Russia's wholehearted commitment to them. They do so differently from how they are envisaged in the liberal paradigm, however. As explained above, in the Russian doctrine, international law is understood procedurally. The international cyber treaty is supposed to target the current 'loose' cyber regime based on the 'common law' logic that reflects, enables, and reproduces the liberal consensus. A dedicated legal instrument establishes procedural rules of the game, in a supposedly politically-neutral manner, to prevent acting on the liberal reflex. International norms such as sovereignty and multilateral decision-making have also been extremely important in the Russian foreign policy discourse because they help Russia maintain its technically great power status.[48] From this position, norms, including cybernorms, must be or should become binding, as a transitionary step towards codification. The current politically, rather than formally, binding character of cybernorms is therefore unsatisfactory for Russia as it reflects the suboptimal state of the regulation of the cyber domain.[49]

Norms are not, however, understood in accordance with the liberal idea of norm diffusion by enlightened norm entrepreneurs, as progressively adopted across the international community to constitute a uniform social glue and superior morality.[50] Quite the opposite: In the Russian doctrine, norms are in place in order to regulate conduct between states of a different normative makeup and, to be effective, they need to be formally binding. This is how Russia interprets the rules and norms of responsible state behaviour in cyberspace. An embodiment of hegemony in this interpretation is a global community, bound by liberal values, that does not need a binding legal instrument because it can act on a case-by-case basis on shared understandings. Attempts to design and implement new cybernorms are supported because they are in Russia’s interests of regulating the Internet. But such

[46] Robert Kagan, The Return of History and the End of Dreams, (New York: Knopf, 2008).

[47] Alexander Cooley, "Ordering Eurasia: The Rise and Decline of Liberal Internationalism in the Post-Communist Space," Security Studies, 28 (2019): 588-613, p. 22.

[48] Ted Hopf, Social Construction of International Politics: Identities & Foreign Policies, Moscow, 1955 and 1999, (Cornell University Press: Ithaka, 2002), p. 225.

[49] I thank Mika Kerttunen for highlighting this point to me.

[50] Cf. Xymena Kurowska, The Politics of Cyber Norms: Beyond Norm Construction towards Strategic Narrative Contestation, (EU Institute for Security Studies: Paris, 2019).

attempts need to be adequately monitored as they potentially violate the state and pose a risk of 'norm weaponization' in the interests of liberal interventionism.

Democratisation à la Russe

One of the curious political implications of cyber treaty advocacy is that it furthers a fundamentally conservative process - in the spirit of the post-1945 international arrangement - by imitating the progressive politics that expose digital inequality. A good illustration thereof is Russia's standing claim that developing states become "hostage to the cyber neocolonialism policy", as they also become the wasteland of the West's cyber refuse.[51] This often pushes Western countries into defensive positions, even as Russian 'democratisation speak' is recognised as instrumental given Russia's own practices of exclusion and domination.

The function of such rhetoric can be better understood, however, in the framework of great power management.[52] As defined by Hedley Bull, great power management consists of two practices: managing relations amongst themselves in the interest of international order, for example by preserving the balance of power, and exploiting dominance in relation to the rest of international society by acting either in concert or unilaterally.[53] Within the framework of great power management, and in line with the doctrine of multipolarity, 'democratisation' of international relations represents the decentralisation of power from the US, as the former hegemon, to a group of great powers, including Russia and now China. Despite the populist use of the term in Russia's cyber diplomacy, small states are instrumental in this configuration. They can be wooed or coerced for tactical purposes, but only great powers ultimately have the responsibility to manage the international order.

This rationale is an important qualification in evaluating Russia's advocacy of the OEWG as a parallel UN track to the UN GGE. Russia's initial support for the UN GGE followed the logic of the world being governed by a few - that is, great power management, here represented by governmental experts. Formally launched in 2004, the UN GGEs produced three reports in 2010, 2013, and 2015. The reports are not legally binding but they have become the main point of reference in the discourse over responsible state behaviour and the question of the applicability of international law in cyberspace. Andrey Krutskikh attributes the failure of the 2017 UN GGE to Western experts' monopolisation of the leadership of the group and Russia's need to resist that.[54] It is this realisation that Russia could not further advance its great power cyber goals within the UN GGE that led to a major diplomatic swerve in 2018 and the resolution which launched the OEWG. From then on, Russia proceeded to label the UN GGE as a US-promoted mechanism driven by experts who act in their personal capacity, making it unrepresentative and exclusionary.

The statements about the final draft of the OEWG-launching resolution in the 1st Committee on 8 November 2018 demonstrate a successful application of 'democratisation' rhetoric for contesting the liberal order. Russia denounced the UN GGE - ironically, given its role in instantiating the process - as

[51] Statement by Ambasador Andrey Krutskikh, Special Representative to the President of the Russian Federation for International Cooperation in the Field of Information Security at the First Session of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security. Permanent Mission of the Russian Federation to the United Nations, New York: 3-4 June 2019, p. 3.

[52] Alexander Astrov, "Great Power Management Without Great Powers? The Russian–Georgian War of 2008 and Global Police/Political Order," in: The Great Power (mis)Management: The Russian–Georgian War and its Implications for Global Political Order, edited by Alexander Astrov, (Farnham: Ashgate, 2011), pp. 1-24, p. 6.

[53] Hedley Bull, The Anarchical Society: a Study of Order in World Politics, (London: Macmillan, 1977), pp. 205-6.

[54] Andrey Krutskikh cited in Kommersant, "Rossii nechego skryvat' i nechego boyat'sya [Russia has nothing to hide and nothing to fear]," 27 March 2019, p. 6.

"the practice of some club agreements [that] should be sent into the annals of history".[55] The "like-minded" responded with pledges to strengthen capacity building and envisage merely a secondary and consultative role for the OEWG in implementing norms created by the UN GGE. This made them politically vulnerable to charges of maintaining the structural inequality of the global Internet governance. The Russian portrayal of the OEWG as, first, providing equal access to all UN members in order to shape Internet governance decisions and, second, as returning sovereign states to the driver's seat of making such decisions,[56] appealed to concerns over representativeness in non-Western constituencies.

The diplomatic feat of launching the OEWG unsettles the process of global Internet governance but it will not be easy to exploit. With its OEWG advocacy, Russia seeks to break its own marginalisation, yet it can simultaneously harm its overall objective, that is, achieving an equal status at the table of those shaping the global governance structures of the Internet. The OEWG constitutes 'a cyber agora', which in the long run can provide a platform for treaty negotiation. But it comes with agora-like politics, which cannot be easily channelled or made conducive to intimate deals among 'poles of power', something that Russia craves to be involved in.

“

The OEWG constitutes 'a cyber agora', which in the long run can provide a platform for treaty negotiation. But it comes with agora-like politics, which cannot be easily channelled or made conducive to intimate deals among 'poles of power'

Yet another diplomatic downfall experienced in November 2019, after the generally positive atmosphere around the launch of the OEWG in June and September of that year, shows the 'democratisation agenda' to be an element of cyber posturing in the geopolitics of global Internet governance. The 1st Committee session on 6 November 2019 saw, again, two votes over competing resolutions. The US-sponsored document[57] reasserts the primacy of the UN GGE and concedes to "also welcoming" rather than, as initially proposed, merely noting the launch of the OEWG. The Russian-sponsored - and little-consulted - document[58] prioritises the OEWG while "also welcoming" the UN GGE; it underscores the status of both as independent mechanisms under UN auspices that should work in parallel towards peace and stability in ICTs. This head-on rhetorical confrontation between the two main cyber orators creates conditions for confusion and division among "the like-minded". Finding itself between its commitment to working within both the OEWG and the UN GGE and its allegiance to "the like-minded" vision of cyberspace, the EU abstained rather than voting against the Russian-sponsored resolution. The explanation of the vote cited "the non-consensus based language" but reaffirmed the commitment to "work both within the UN GGE and the OEWG in a complementary and coordinated fashion, to promote and further build on the cumulative achievements of the previous UN GGEs".[59] Switzerland, chairing the

[55] First Committee, 31st meeting, General Assembly, 73rd session, Disarmament and International Security Committee, 8 November 2018. Accessed 24 November 2019. Recording available at http://webtv.un.org/meetings-events/general-assembly/main-committees/1st-committee/watch/first-committee-31st-meeting-general-assembly-73rd-session/5859574011001.

[56] Statement by the Special Representative of the President of the Russian Federation on International Cooperation on Information Security, Ambassador-at-Large A.V. Krutskikh. Permanent Mission of the Russian Federation to the United Nations, New York: 9 September 2019, p. 3.

[57] General Assembly of the United Nations, "Advancing responsible State behaviour in cyberspace in the context of international security," 2019, New York: A/C.1/74/L.49/Rev.1.

[58] General Assembly of the United Nations, "Developments in the field of information and telecommunications in the context of international security," 2019, New York: A/C.1/74/L.50/Rev.1.

[59] Delegation of the European Union to the United Nations - New York, "EU Explanation of Vote – United Nations 1st Committee: information and telecommunications in the context of international security," 7 November 2019. Accessed 23 November 2019. Available at https://eeas.europa.eu/delegations/un-new-york/70041/eu-explanation-vote-%E2%80%93-united-nations-1st-committee-information-and-telecommunications-context_en.

OEWG, voted in favour.[60] A closer look at the underpinnings of Russia's cyber narrative may help better manage the confusion it generates.

« Digitalisation is dangerous » - The doctrine of information security

The staple of the Russian cyber narrative is that digitalisation is dangerous. It is generally seen as *уязвимость/uyazvimost* (vulnerability). Domestically, it constitutes a disruptive tool with regard to regime stability, a view which consolidated in the realisation of the power of social media during the Arab Spring and was driven home by the extent of anti-regime protests in Russia in 2012.[61] Internationally, the Internet is portrayed as a dangerous instrument of foreign interference. The doctrine on information security laid out in the International Convention on Information Security stresses the threats of information warfare and the dangers stemming from foreign governments' exploitation of ICT for undermining state sovereignty, political independence, and territorial integrity.[62] Every year since 1998, Russia has put forward resolutions at the UN to prohibit "information aggression," which is interpreted to mean ideological attempts to undermine regime stability. Moscow seems to see itself in a particular situation vis-à-vis Western countries: a non-declared war, no peace context, but information warfare which is a continuous state of flux between war and peace.[63]

Russia's understanding of what constitutes information security merits scrutiny in this context. In contrast to Western approaches focused on technology, protection of communication infrastructure, and free access to information, the doctrine of information security relates to the responsibility of the government to secure the information itself and, therefore, ultimately national sovereignty.[64] If Western countries seek security of communication, the Russian government wants control over the content of information, since content can be used as a tool of influence in the socio-humanitarian sphere.[65] More broadly, two political principles are key to the doctrine. One is the understanding of "real sovereignty" as the stability of the political system, national unity, prevention of fundamental contradictions between the authorities, the society, and the elites;[66] in other words, prevention of political dissent. The other relates to the perception of the politically empowered individual, especially one who uses information technologies to advance their rights, as both a vulnerability and a security threat to the state.[67]

[60] This voting pattern was largely repeated in the UN General Assembly vote on 12 December 2019, with UK consistently voting against the Russia-sponsored resolution. For details of voting on both resolutions in the First Committee and the General Assembly see "Draft Resolutions, Voting Results, and Explanations of Vote from First Committee 2019." Accessed 18 December 2019. Available at http://reachingcriticalwill.org/disarmament-fora/unga/2019/resolutions.

[61] Lincoln Pigman, "Russia's Vision of Cyberspace: a Danger to Regime Security, Public Safety, and Societal Norms and Cohesion," Journal of Cyber Policy, 4 (2019): 22-34.

[62] Convention on International Information Security. Accessed 24 November 2019. Available at the website of the Russian Ministry of Foreign Affairs: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

[63] Ulrik Franke, War by Non-military Means. Understanding Russian Information Warfare, (Stockholm: Swedish Defence Research Agency, 2015). Accessed 24 November 2019. Available at http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf, p. 42.

[64] Pavel Sharikov, "Understanding the Russian Approach to Information Security," 16 January 2018. Accessed 23 November 2019. Available at https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/.

[65] Nocetti, op. cit., 187.

[66] Andrey Kokoshin, Real'nyi Suverenitet v Sovremennoi Miropoliticheskoi Sisteme [Real Sovereignty in a World Political System], (Moscow: Evropa, 2006), p. 26.

[67] Pavel Sharikov, "Informatsionnyy Suverenitet i Vmeshatel'stvo vo Vnutrenniye Dela v Rossiysko-amerikanskikh Otnoshenyiakh [Information Sovereignty and Interference in Domestic Affairs in the Russian-US Relations]," Mezhdunarodnyye Protsessy, 16 (2018): 170-88, pp. 172-4.

The Kremlin's expansion of a "digitally sovereign" Russia programme is therefore a defence of the state against both the discontent of its own citizens and unchecked Western influence. The development of the Russian segment of the information and communication network, known as *Runet*, is part of this agenda. The Sovereign Internet Law, which came into force on 1 November 2019 and will be incrementally rolled out in the coming years, envisages technical arrangements in case of disconnection from the rest of the Internet, for example due to foreign aggression. Russian telecom firms have to install, for this purpose, 'technical means' to re-route all Russian Internet traffic to exchange points approved or managed by Roskomnazor, Russia's telecom watchdog. While the *Runet* logic is essentially in defence of the regime, it is also a local response to challenges of digitalisation on a global scale, which often includes greater technological sovereignty and economic protectionism. The championing of data localisation also belongs to this agenda. Understood as storing data within the borders of the country where it was generated, and justified in terms of resisting the concentration of transnational data storage in California, data localization constitutes a part of states' digital sovereignty. If, in the US, information regime data belongs to tech companies, and if in the EU General Data Protection Regulation framework it belongs to the individual, in Russia data belongs to the state and must be strictly controlled by it.[68]

> “
>
> **The Kremlin's expansion of a ‘digitally sovereign’ Russia programme is therefore a defence of the state against both the discontent of its own citizens and unchecked Western influence.**

Globalising information security through regional platforms

The regional promotion of a counter-liberal order commenced in the late 1990s by mainstreaming the counternorms of civilisational diversity and traditional values - the old-new rearticulation of the norm of sovereign equality.[69] However, Russia could not afford a global model of illiberal contestation because of its utter lack of legitimacy, both in terms of its own standing and the strength of the liberal order at the time. Regional platforms have presently become regulation entrepreneurs, a laboratory for global cyber regulation and a space for coalition building for global cyber diplomacy.

Russia has uploaded its own solutions for countering the vulnerabilities of digitalisation to regional platforms. Within the framework of the Shanghai Cooperation Organization (SCO), it has, for example, streamlined the norm of digital sovereignty in contrast to US-advocated 'cyber freedom' and facilitated the SCO agreement for cooperation to ensure "international information security". Together with China, Uzbekistan, and Tajikistan, Russia proposed the Code of Conduct for Information Security in a 2011 letter to the UN General Assembly. It included a ban on the use the Internet for military purposes and a pledge that the subscribing parties "not use information and communications technologies and other information and communications networks to interfere with the internal affairs of other states or with the aim of undermining their political, economic and social stability".[70] The proposal was criticised for the very attempt of formalisation, the inconsistency of its state-centred approach with the multi-stakeholder model, the de facto justification of censorship in the name of national sovereignty, and the

[68]Pavel Sharikov and Natalia Stepanova, "Podkhody SSHA, ES i Rossii k Probleme Informatsionnoy Politiki [US, EU and Russia's Approaches to Information Policy]," Sovremennaya Evropa, 2 (2019): 73-83.

[69] Alexander Cooley, "Authoritarianism Goes Global: Countering Democratic Norms," Journal of Democracy 26 (2015): 49-63.

[70] General Assembly of the United Nations, "International Code of Conduct for Information Security," 2018, New York: A/66/359.

overemphasis on terrorism and extremism to the neglect of cross-border law enforcement cooperation.[71] The 2015 updated version retracts the term "information weapons" that generated much controversy and states the commitment that human rights apply as much online as they do offline, but still submits this recognition to national security prerogatives.[72] It also, however, introduces a provision not to take advantage of a "dominant position in the sphere of IT" (section 5), which is in line with the broader agenda of 'democratisation', and reiterates the role of governments in Internet governance (section 8), which may be interpreted as a continuous opposition to the multi-stakeholder model propagated by "the like-minded". This acquis clashes too violently with the liberal model of Internet governance to be uploaded in its entirety. Still, the regional cyber codification is attractive to many actors who are 1) concerned with cyberspace being unregulated, 2) increasingly puzzled at the West's refusal of the international cyber treaty, and 3) drawn towards state-controlled regulation of the Internet. The call for stricter regulation is gaining salience as it addresses many contemporary issues in cyberspace. The generic call for a "free, safe, open, and secure" Internet will not alleviate such concerns and challenges. This is the immediate leverage that regional regulation entrepreneurs possess.

While Russia did not fabricate the backlash against the hegemonic liberal world order and the reassertion of the conservative ideologies in these regions, it will rush to expedite such processes and use them to its own advantage. Its traditionally strong regional expertise and its historical record of playing on regional grievances during the Cold War come in handy, especially vis-à-vis colonial legacies and the extractive post-colonial policies that proliferate in cyberspace. The strategy of empowering regional organisations as being responsible for regional security in accordance with the UN Charter adds legitimacy to this self-serving endeavour. Many regional actors recognise the 'pragmatist' logic of this rhetoric. However, even if they do not necessarily fall for Russia's supposedly democratic campaign, their concern with structural inequality in the international system partially overlaps with Russia's agenda. What gets corrupted in the process of aligning such positions is the very ideal of decolonisation and de-hierarchisation. It is hijacked for Russia's pursuit of collective leadership by great powers, which will disregard the voices of those structurally disadvantaged in the system.

> “
>
> **Cyber diplomacy has become a way of revendicating and revalorising Russia's global role.**

Conclusion

Cyber diplomacy has become a way of revendicating and revalorising Russia's global role, another rendition of the old, "Gentlemen, Russia is back!"[73] That declaration after the Munich speech[74] that heralded a more active international politics by the Kremlin lacked, however, in the realm of legitimacy for many years to come. The realm of global Internet governance provides a new ground of legitimation because it strikes a peculiar balance between Russia being able to break and fix things. In the same breath, it depicts the Internet as the ultimate contemporary security threat to monger fear and justify extraordinary measures and it champions the cause of regulation. Russia often punches above its weight in this game and its cyber narrative is simplistic. But it exposes the hypocrisy and self-subversion of the liberal order on the global stage the way populists expose the liberal hypocrisy domestically. This is

[71] Rõigas, op. cit.

[72] Camino Kavanagh, The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century, (New York: The United Nations Institute for Disarmament Research, 2017), p. 25.

[73] Sergey Yastrzhembskiy cited in Rossiyskaya Gazeta, "Gospoda, Rossiya vernulas! [Gentlemen, Russia is back!]", 22 February 2007.

[74] Vladimir Putin, Speech and discussion at the 2007 Munich conference on security. Accessed 27 July 2019. Available at http://special.kremlin.ru/events/president/transcripts/24034.

where the normative threat of endangering the sustainability of the liberal way of life and the liberal international order manifests itself most clearly.

One of the distinguishing features of liberalism, however, is that it can reform and adapt itself while authoritarianism only learns how to be more effective. The Russian vision is, ultimately, anachronistic. It relies on control and subordination of the individual to the state, which ignores the extent of and the hunger for genuine democratisation and freedom at the level of the cyber citizen. The liberal cyber regime should reinvigorate its holistic commitment to the individual as the centre of gravity of international cyber society - not only as a free entrepreneur but as a political subject with a full spectrum of political rights and with community and national attachments as a source of self-expression rather than subservience. 'Leading by example', the old liberal means of persuasion, may have lost much of its charm as an effective strategy to achieve such aim. Its righteousness also becomes anachronistic in international society, underpinned by normative pluralism and the contestation of hierarchies, including those created by liberal social norms. The shift from paternalism to participatory modes of engagement in building sustainable cyber societies better corresponds to the realities of the contemporary world. It builds an alternative, human-based - rather than security state-based - model of democratisation in international relations. The major challenge in this process is to 'de-securitise' the politics of global governance of the Internet and reformulate the parameters of the debate about digital society, by taking a human-centred focus.

> “
>
> **The liberal cyber regime should reinvigorate its holistic commitment to the individual as the centre of gravity of international cyber society.**

About the author

Xymena Kurowska is Associate Professor of International Relations at Central European University and academic rapporteur on norms for EU Cyber Direct.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

This project is
funded by the
European Union.