What Does Russia Want in Cyber Diplomacy? A Primer

Xymena Kurowska

Cite as: Kurowska, Xymena. 2020. "What Does Russia Want in Cyber Diplomacy? A Primer." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 85-105. London: Rowman & Littlefield International.

More information about the book and The Hague Program for Cyber Norms is available on:

www.thehaguecybernorms.nl

Chapter 5

What Does Russia Want in Cyber Diplomacy?

A Primer[1]

Xymena Kurowska

The standard analytical narratives regarding Russia's behavior 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 (Kurowska 2014), or to anger over apparent disrespect received from other international actors (Larson and Shevchenko 2014). Demand for status recognition is a key factor in Russia's international conduct (Krickovic and Weber 2018; Schmitt forthcoming; Neumann 2016, 1996), which finds its expression in Russia's regular insistence on acknowledging its indispensability to the international order (Lo 2015, 47). Despite declarations of pragmatism in foreign policy (Omelicheva 2016; Casier 2006), 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, toward the UK representative during a Security Council session in April 2017: famously, "Look at me!" and "Don't you dare insult Russia again!" (RFE 2017). Many looked away mortified, but Safronkov's superiors in the Ministry for Foreign Affairs commended his behavior, as part of resistance toward Western attempts at hegemonic imposition (Schreck 2017).

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.[2] 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.

This chapter brings these issues to 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 chapter unpacks a core trope in Russia's strategic diplomatic communication more broadly: that is, the notion of "democratizing" 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 capitalizes on the West's own subversion and betrayal of the liberal ethos. Russia's strategy to advance its "democratization" agenda resembles "trickstery" (Kurowska and Reshetnikov 2018b): 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 chapter 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 chapter concludes with the suggestion that Russia's posturing in cyber diplomacy is not a security threat as such but a "normative threat" (Creppell 2011) to the liberal way of life. As such, it is a manifestation of an ideological struggle that liberal cyber-norms 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 concerns 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 U.S.-sponsored reaffirmation of UN Group of Governmental Experts (UN GGE) (General Assembly 2018a) and the Russia-sponsored launching of the Open-Ended Working Group (OEWG) (General Assembly 2018c), marks the final breakdown of international consensus on the issue.[3] In Russia's cyber narrative, it is, however, taken as a positive breakthrough, fortuitously overlapping with the twenty-year anniversary of 1998 when Moscow tabled its first draft resolution on Information and Communication Technology in the General Assembly's First Committee on Disarmament and International Security (Kommersant 2018, 6). In 2018, Russia in fact successfully sponsored two resolutions, the abovementioned one launching OEWG and another, adopted in the Third Committee of the General Assembly on cybercrime (General Assembly 2018b), both framed as a significant way forward instigated by Russia's cyber diplomacy (Chernukhin 2019). 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 the fundamentally "ungovernable" cyberspace. The OEWG resolution sets thirteen rules, norms, and principles (in comparison with the eleven laid out in the U.S.-sponsored resolution) of responsible state behavior that are the first "rules of the road" in history with regard to this issue —despite them formally being "recommendations for considerations by States" (Ibid.). Specifically, the resolution includes a re-assertion of cultural diversity, enshrined in the UN Charter, in global Internet governance. The launch of OEWG is presented as ushering in a genuine democratization 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 in cybercrime matters and promoted by the group of the "like-minded," the Budapest convention is opposed by Russia and others 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 Third Committee, 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 (Nakashima 2019). This is, in broad terms, the crux of "the like-minded" position. Russia, similar to some other non-Western actors, charges the West with maintaining digital inequality and infringement of sovereignty in the pursuit of upholding the liberal world order. The remainder of the chapter unpacks the Russian perspective on the current state of "unpeace" (Kello 2017, 78) that thus unfolds in cyberspace and the tasks that the 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*, cyberspace promises Russia respect (уважение/uvazheniye), not only at the well-cultivated regional level, but, potentially, globally. It affords status recognition that Russia lost and craved 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" (Schmitt forthcoming, 20). *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" (Security Council 2013). 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 reference to the consensus that existing international law applies in cyberspace, which, supported by the norms of responsible state behavior, 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 emphasized particularly in US discourse, hinder technological development (Rõigas 2015). Russia's advocacy for the treaty relies on the claim to defend 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 to curb the liberal international order which legitimizes intervention into the domestic makeup of states, and thus a tool against the ad hoc decisions by the strong.

The notion of "the rules-based international order"[4] 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" (Lavrov 2019). Such rhetoric, as the chapter 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 instrumentalization of such a concern for both tactical and strategic gains, increasingly inform political positions in the global governance of Internet.

Finally, Russia's advocacy of an international cyber treaty has another snappy line: International law applies in cyberspace but even experts do not know how, and there is a reason for it. The very term "responsible state behavior 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 Information and Communication Technology (ICT) (Strel'tsov, Sharyapov, and Yashchenko 2016, 6, para. 1.7.). The use of international customs and general principles of law is, further, unpromising in this area given the lack of a common understanding of some objects of legal regulation; for example, the use of ICT as a means of warfare (Ibid). 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 default Russian position: the objection to changing "basic principles of international law" in order to replace them with the doctrines of "limited sovereignty" (Igor Ivanov cited in, Averre 2009, 586).

This sacrosanct understanding of international law as above politics has been interrogated in the Western doctrine of international law as a political move in itself (Klabbers 2004; Koskenniemi 2011). 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 United States.

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 "securitization"[5] 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 savior. 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, Director of the Department of International Information Security in Russia's Ministry of Foreign Affairs (Andrey Krutskikh cited in, Kommersant 2019b) is an example of the securitizing discourse about the world at the brink of a cyber catastrophe. Russia substantively likens the hazards of nuclear weapons and digitalization because of the technological implications of the scale of threat and interlinkages between them (Sharikov 2018a). The very initiation of the cyber debate in the context of international security within the UN First Committee on Disarmament was justified in terms of the dangers of "information weapons" (the term now formally withdrawn but hardly forgotten) and modeled on the nuclear nonproliferation regime. Russia hoped to emulate the parameters of the nuclear regime for information security in cyberspace to mediate Western superiority in that domain (cf. Chernenko 2018). 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 remains dominant.

The image of the new Cuban crisis has a wider appeal, however. 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 (Vladimir Yermakov cited in, Permanent Mission 2019b, 2). An impoverished country with tangibly little to mold the 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" (cf. Nocetti

2018). 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 managed to create a taboo over such potential use (Tannenwald 1999). By contrast, cyberspace means of disruption and interference may be, and are, in common use.

In rhetoric, Russia's chief preoccupation is then with the militarization 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, like that of 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 democratizing international relations, read containing the 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, indeed, apply is marked by different understandings of the role of international law as such.[6] The consensus is, therefore, hardly a reason to celebrate. The recent recommendation that national governments append to UN GGE reports their explanation of how international law applies in cyberspace is a move toward 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 toward an end beyond itself (Collins 2019, 196). 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" (Ibid). 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 toward 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.

The core to the Russian interpretation is the preponderance of the statist discourse of international law, with the emphasis on the classic understanding of sovereignty and a categorical rejection of the notion of the individual as a subject of international law (Dmitry 2017). At the same time, the individual becomes increasingly empowered in the Western discourse on international law which also shifts toward transnational, rather than state-based, solutions. The glorification of the state in the Russian legal doctrine (Mälksoo 2015, 100) 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" rather is the United States, or the "West" by extension, and not the Russian government (Ibid, 81).[7] International law "à la Russe serves to restrain the exercise of American power" (Lo 2015, 95).

When the Russian foreign minister Lavrov repeats the mantra of the double standards in the application of international law (Lavrov 2016) and denounces "attacks on international law" (Sergey Lavrov cited in, Kommersant 2019a), 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 (Alexander Bastrykin cited in, Kommersant 2016, 20).

Such grievances are appealed to in Russia's pursuit of the "democratization" of international relations, even as the agenda serves the Russian doctrine of multipolarity, rather than the cause of a genuine democratization 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 (Kurowska 2014; Makarychev and Morozov 2011). A pole is also understood as an actor capable of producing order or generating disorder, usually a regional power with a global outreach. 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 order (Kagan 2008). 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 the normative, as well as political, influence. The principle is rather 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" (Cooley 2019, 22).

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 a 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 whole-hearted 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, specifically those such as, for example, 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 (Hopf 2002, 225). From this position, norms, including cyber norms, must be or should become binding, as a transitionary step toward codification. The current politically, rather than formally, binding character of cyber norms is, therefore, unsatisfactory for Russia as it reflects the suboptimal state of the regulation of the cyber domain.[8]

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 (cf. Kurowska 2019). 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 behavior in cyberspace. A global value-bound community, which does not need a binding legal instrument because it can act on a case-by-case basis on

shared understandings, is an embodiment of hegemony in this interpretation. Attempts to design and implement new cyber norms are supported because they are in Russia's interests of regulating the Internet; but they need to be monitored as they potentially penetrate the state and pose the risk of "norm weaponization" in the interests of liberal interventionism.

DEMOCRATIZATION 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 exposes 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 (Andrey Krutskikh cited in, Permanent Mission 2019a, 3). It often pushes Western countries into defensive positions, even as Russian "democratization speak" is recognized 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 (Astrov 2011, 6). As defined by Hedley Bull, great power management consists of two practices: managing relations among 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 (Bull 1977, 205-6; Astrov 2011). Within the framework of great power management, and in line with the doctrine of multipolarity, "democratization" of international relations denotes the decentralization of power from the United States, 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 GGE 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 of responsible state behavior and the question of the applicability of international law in cyberspace. The failure of the 2017 UN GGE is attributed by Andrey Krutskikh to Western experts' monopolization of the leadership of the group and the need of Russia to resist

that (Andrey Krutskikh cited in, Kommersant 2019b, 6). It is the realization 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 (General Assembly 2018c). From then on, it proceeded to label the UN GGE as a U.S.-promoted mechanism driven by experts who act in their personal capacity, which makes it unrepresentative and exclusionary.

The statements about the final draft of the OEWG-launching resolution in the First Committee on November 8, 2018 demonstrate a successful application of "democratization" rhetoric for contesting the liberal order. Russia denounced the UN GGE, ironically given its role in instantiating the process, as "the practice of some club agreements [that] should be sent into the annals of history" (Disarmament and International Security Committee 2018). "The like-minded" responded with pledges to strengthen capacity building and envisaging 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 the UN membership to shape Internet governance decisions, and, second, as returning sovereign states to the driver's seat of making such decisions (Andrey Krutskikh cited in, Permanent Mission 2019c, 3), 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 the OEWG advocacy, Russia seeks to break its own marginalization, 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 diplomatic downfall experienced in November 2019, after the generally positive atmosphere around the launch of the OEWG in June and September 2019, shows how "democratization agenda" is but a tool in the geopolitics of global Internet governance. The First Committee session on November 6, 2019 saw, again, two votes over competing resolutions. The U.S.-sponsored document (General Assembly 2019a) elaborates on and reasserts the primacy of the UN GGE and concedes to "also welcoming" rather than only noting the launch of the OEWG. The Russian-sponsored, and little-consulted, document (General Assembly 2019b) prioritizes the OEWG while "also welcoming" the UN GGE and underscoring the status of both as independent mechanisms under United Nations auspices that should work in parallel toward peace and stability in ICTs. This

head-on rhetorical confrontation between the two main cyber orators creates confusion and divisions among "the like-minded." Caught 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" (EEAS 2019). Switzerland, chairing the OEWG, voted in favor. A closer look at the underpinnings of Russia's cyber narrative may help better manage the confusion it generates.

"DIGITALIZATION IS DANGEROUS"—THE DOCTRINE OF INFORMATION SECURITY

The staple of the Russian cyber narrative is that digitalization 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 realization of the power of the social media during the Arab Spring, drove home by the extent of anti-regime protests in Russia in 2012 (Pigman 2019). 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 threats of information warfare and dangers stemming from foreign governments' exploiting information and communication technologies for undermining state sovereignty, political independence, and territorial integrity (MID 2011). Every year since 1998, Russia has put forward resolutions at the United Nations 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 as a continuous state of flux between peace and war (Franke 2015, 42).

Russia's understanding of what constitutes information security merits scrutiny in this context. In contrast to the 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 (Sharikov 2018c). 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 (Nocetti 2018, 187). 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 (Kokoshin 2006, 26); 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 (Sharikov 2018b, 172–4).

The Kremlin's expansion of a "digitally sovereign" Russia program is, therefore, a defence of the state against both the discontent of their own citizens and uncontrolled 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 November 1, 2019 and will be incrementally rolled out in the coming years, envisages technical arrangements in case of disconnection from the rest of the Internet, as, 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. The "Runet" logic is, in essence, defensive of the regime. But it is also a local response to challenges of digitalization at the global scale, which calls for a greater technological sovereignty and economic protectionism. The championing of data localization 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, United States, data localization constitutes a crucial part of state digital sovereignty. If, in the United States, information regime data belongs to tech companies, and 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 (Sharikov and Stepanova 2019).

GLOBALIZING INFORMATION SECURITY THROUGH REGIONAL PLATFORMS

The regional promotion of a counter-liberal order commenced in the late 1990s by mainstreaming the counternorms of civilizational diversity and traditional values, the old-new rearticulation the norm of sovereign equality (cf. Cooley 2015). Russia could not afford, however, a global model of illiberal contestation for the utter lack of legitimacy, both in terms of its own standing and the strength of the liberal order at that 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 to regional platforms its own solutions for countering the vulnerabilities of digitalization. Within the framework of the Shanghai Cooperation Organization (SCO), it has, for example, streamlined the norm of digital sovereignty in contrast to the U.S.-advocated "cyber-freedom" and in 2009 facilitated the SCO agreement for cooperation to ensure "international information security." Initiated in a 2011 letter to the UN General Assembly by the Russian coalition (gathering China, Uzbekistan, and Tajikistan), it includes a pledge that states subscribing to the Code "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" (General Assembly 2011). The 2011 proposal also banned the use of the Internet for military purposes, but was criticized for the very attempt at formalization, the inconsistency with the multistakeholder approach, the de facto justification of censorship in the name of national sovereignty, and the overemphasis on terrorism and extremism to the neglect of cross-border law enforcement cooperation (Rõigas 2015). The 2015 updated version retracts the term "information weapons" that generated much controversy and states the commitment that human rights apply online as they do offline, but submits this recognition to national security prerogatives (Kavanagh 2017, 25). 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 "democratization," 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 concerned with the cyberspace being unregulated, are increasingly puzzled at the West's refusal of the international cyber treaty, and are inclined toward the 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 "free, safe, open, and secure" Internet will not alleviate such concerns and challenges. This is the immediate leverage that regional regulation entrepreneurs do 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 turn them to its own advantage. Its traditionally strong regional expertise and the historical record of playing on regional grievances during the Cold War come in

handy especially strongly vis-à-vis colonial legacies and the extractive post-colonial policies that proliferate in cyberspace. The strategy of empowering regional organizations as responsible for regional security in accordance with the UN Charter adds legitimacy to this self-serving endeavor. Many regional actors recognize the "pragmatist" logic of this rhetoric. 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 decolonization and de-hierarchization. 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.

CONCLUSION

Cyber diplomacy has become a way of revendicating and revalorizing Russia's global role, another rendition of the old "Gentlemen, Russia is back!" (Rossiyskayagazeta 2007). That declaration after the Munich speech (Putin 2007) which 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. It depicts the Internet as the ultimate contemporary security threat to monger fear and justify extraordinary measures, and champions the cause of regulation in one breath. 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 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 is, however, 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 democratization and freedom at the level of the cyber citizen. The liberal cyber regime should hence reinvigorate its holistic commitment to the individual as the center 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- rather than security state-based model of democratization in international relations. The major challenge in this process is to "de-securitize" the politics of the global governance of the Internet and reformulate the parameters of the debate about digital society.

NOTES

1. I thank Patryk Pawlak and Mika Kerttunen for detailed comments on this chapter. I would also like to acknowledge research opportunities provided by EU Cyber Direct Team and non-attributable conversations with national diplomats participating in the UN processes. I further thank Bibi van den Berg and Dennis Broeders for numerous textual and terminological suggestions. Philip Conway helped with copy editing. The views expressed in this chapter are solely mine and I bear responsibility for any possible mistakes. A version of this paper was first published by EU Cyber Direct. Reprinted here with permission.

2. See Giles and Hagestad (2013) for an analysis of terminological misunderstandings in the domain of cyber and information security as evident in the policy documents by Russia, China, United States, and United Kingdom.

3. For an alternative view, see Tikk and Kerttunen (2018).

4. "The rules-based international order" has not been neatly defined but it can be understood 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" (Association of Australia 2015, 3).

5. 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 (Buzan, Wæver, and de Wilde 1998, 25). The successful securitization of ICT by the Russian Federation was noticed by Tikk and Kerttunen (2018, 56, 58).

6. Some authors speak of the Russian version as "a simulacrum or concave mirror to Western use" (Mälksoo 2015, 185). See Tikk and Kerttunen (2018), for examples, of how specific concepts of international law have been differently understood across a range of actors participating in the UN GGE.

7. This can also be interpreted as a "pragmatist relation to truth," which opens another line of interpretation of the Russian agenda of democratizing international relations. On the domestic culture of the pragmatic relation to truth as manifested in pro-Kremlin trolling, see Kurowska and Reshetnikov (2018a).

8. I thank Mika Kerttunen for highlighting this point to me.

BIBLIOGRAPHY

Association of Australia, United Nations. 2015. *The United Nations and the Rules-Based International Order.* Accessed November 23, 2019. https://www.unaa.org.au/wp-content/uploads/2015/07/UNAA_RulesBasedOrder_ARTweb3.pdf.

Astrov, Alexander. 2011. "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, 1–24. Farnham: Ashgate.

Averre, Derek. 2009. "From Pristina to Tskhinvali: The Legacy of Operation Allied Force in Russia's Relations with the West." *International Affairs* 85 (3): 575–591.

Bull, Hedley. 1977. *The Anarchical Society: A Study of Order in World Politics*. London: Macmillan.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Casier, Tom. 2006. "Putin's Policy Towards the West: Reflections on The Nature of Russian Foreign Policy." *International Politics* 43 (3): 384–401.

Chernenko, Elena. 2018. "Russia's Cyber Diplomacy." In *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, edited by Nicu Popescu and Sergiu Secrieru, 43–49. Paris: EU Institute for Security Studies.

Chernukhin, Ernest. 2019. *Mezhdunarodnaya informatsionnaya bezopasnost': uspekhi Rossii v OON [International Information Security: Russia's Successes at the UN]*. Russian International Affairs Council. Accessed November 23, 2019 https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-uspekhi-rossii-v-oon/.

Collins, Richard. 2019. "Two Idea(l)s of the International Rule of Law." *Global Constitutionalism* 8 (2): 191–226.

Cooley, Alexander. 2015. "Authoritarianism Goes Global: Countering Democratic Norms." *Journal of Democracy* 26 (3): 49–63.

Cooley, Alexander. 2019. "Ordering Eurasia: The Rise and Decline of Liberal Internationalism in the Post-Communist Space." *Security Studies* 28 (3): 588–613.

Creppell, Ingrid. 2011. "The Concept of Normative Threat." *International Theory* 3 (3): 450–487.

Disarmament and International Security Committee, General Assembly of United Nations . 2018. 31st meeting in the 73rd session of the General Assembly. New York.

Dmitry, Dubrovsky. 2017. "Lauri Mälksoo. Russian Approaches to International Law. Oxford: Oxford University Press, 2015." *Laboratorium: Russian Review of Social Research* 9 (1): 146–151.

EEAS. 2019. "EU Explanation of Vote—United Nations 1st Committee: Information and Telecommunications in the Context of International Security." https://eeas.europa.eu/delegations/un-new-york/70041/eu-explanation-vote-%E2%80%93-united-nations-1st-committee-information-and-telecommunications-context_en.

Franke, Ulrik. 2015. *War By Non-Military Means. Understanding Russian Information warfare.* Swedish Defence Research Agency. http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf.

General Assembly, United Nations. 2011. International Code of Conduct for Information Security. New York: A/66/359.
General Assembly, United Nations. 2018a. Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Edited by 1st Committee of the General Assembly of the United Natons. New York.
General Assembly, United Nations. 2018b. Countering the Use of Information and Communications Technologies for Criminal Purposes. Edited by 3rd Committe of United Nations General Assembly. New York.
General Assembly, United Nations. 2018c. Developments in the Field of Information and Telecommunications in the Context of International Security. Edited by 1st Committe of United Nations General Assembly. New York: A/RES/73/27.
General Assembly, United Nations. 2019a. Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Edited by 1st Committee of the General Assembly of the United Nations. New York: November 6, 2019.
General Assembly, United Nations. 2019b. Developments in theFfield of Information and Telecommunications in the Context of International Security. Edited by 1st Committee of the General Assembly of the United Nations. New York: November 6, 2019.
Giles, Keir, and William Hagestad. 2013. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." *5th International Conference on Cyber Conflict (CyCon)*: 1–17.
Kagan, Robert. 2008. *The Return of History and the End of Dreams*. New York: Knopf.
Kavanagh, Camino. 2017. *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.
Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
Klabbers, Jan. 2004. "Constitutionalism Lite." *International Organizations Law Review* 1 (1): 31–58.
Kokoshin, Andrei. 2006. *Real'nyi suverenitet v sovremennoi miropoliticheskoi sisteme [Real Sovereignty in a World Political System]*. Moscow: Evropa.
Kommersant. 2016. "Pora postavit' deystvennyy zaslon informatsionnoy voyne [It's time to put an effective barrier to the information war]." Accessed November 23, 2019. https://www.kommersant.ru/doc/2961578.
Kommersant. 2018. "Rossiya i SSHA peretyagivayut vsemirnuyu pautinu [Russia and the USA are pulling the World Wide Web]." Accessed November 23, 2019. https://www.kommersant.ru/doc/3797617.
Kommersant. 2019a. "Ataki na mezhdunarodnoye pravo priobretayut opasnyye masshtaby [Attacks on international law are becoming dangerous]." Accessed November 23, 2019. https://www.kommersant.ru/doc/4109238.
Kommersant. 2019b. "Rossii nechego skryvat' i nechego boyat'sya [Russia has nothing to hide and nothing to fear]." Accessed November 23, 2019. https://www.kommersant.ru/doc/3923963.
Koskenniemi, Martti. 2011. *The Politics of International Law*. London: Hart Publishing.

Krickovic, Andrej, and Yuval Weber. 2018. "What Can Russia Teach Us About Change? Status-Seeking as a Catalyst for Transformation in International Politics." *International Studies Review* 20 (2): 292–300.

Kurowska, Xymena, and Anatoly Reshetnikov. 2018a. "Neutrollization: Industrialized Trolling as a Pro-Kremlin Strategy of Desecuritization." *Security Dialogue* 49 (5): 345–363.

Kurowska, Xymena, and Anatoly Reshetnikov. 2018b. "Russia's Trolling Complex at Home and Abroad." In *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, edited by Nicu Popescu and Sergiu Secrieru, 25–32. Paris: EU Institute for Security Studies.

Kurowska, Xymena. 2014. "Multipolarity as Resistance to Liberal Norms: Russia's Position on Responsibility to Protect." *Conflict, Security & Development* 14 (4): 489–508.

Kurowska, Xymena. 2019. *The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation.* Paris: EU Institute for Security Studies. https://eucyberdirect.eu/content_research/the-politics-of-cyber-norms-beyond-norm-construction-towards-strategic-narrative-contestation/.

Larson, Deborah Welch, and Alexei Shevchenko. 2014. "Russia Says No: Power, Status, and Emotions in Foreign Policy." *Communist and Post-Communist Studies* 47 (3): 269–279.

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

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

Lo, Bobo. 2015. *Russia and the New World Disorder*. London and Washington, DC: Chatham House and Brookings Institution Press.

Makarychev, Andrey, and Viatcheslav Morozov. 2011. "Multilateralism, Multipolarity, and Beyond: A Menu of Russia's Policy Strategies." *Global Governance* 17 (3): 353–373.

Mälksoo, Lauri. 2015. *Russian Approaches to International Law*. First Edition ed. Oxford: Oxford University Press.

MID. 2011. Convention on International Information Security. Accessed November 24, 2019. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

Nakashima, Ellen. 2019. "The U.S. Is Urging a No Vote on a Russian-Led U.N. Resolution Calling for a Global Cybercrime Treaty." *The Washington Post*. Accessed 23 November 2019. https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html?wpisrc=nl_cybersecurity202&wpmm=1.

Neumann, Iver. 1996. *Russia and the Idea of Europe: A Study in Identity and International Relations*. 2nd ed. London: Routledge.

Neumann, Iver. 2016. "Russia's Europe, 1991–2016: Inferiority to Superiority." *International Affairs* 92 (6): 1381–1399.

Omelicheva, Mariya Y. 2016. "Critical Geopolitics on Russian Foreign Policy: Uncovering the Imagery of Moscow's International Relations." *International Politics* 53 (6): 708–726.

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

Permanent Mission, of the Russian Federation to the United Nations. 2019b. 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. New York: October 11, 2019.

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

Pigman, Lincoln. 2019. "Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion." *Journal of Cyber Policy* 4 (1): 22–34.

Putin, Vladimir. 2007. Speech and Discussion at Munich Conference on Security Politics. Accessed July 27, 2019. http://special.kremlin.ru/events/president/transcripts/24034.

RFE. 2017. "'Look At Me!'—Russian UN Envoy Demands Attention." Accessed November 23, 2019. https://www.rferl.org/a/russia-uk-un/28427527.html.

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

Rossiyskayagazeta. 2007. "Sergey Yastrzhembskiy: Gospoda, Rossiya vernulas'! [Sergey Yastrzhembsky: Gentlemen, Russia has returned!]." Accessed November 23, 2019. https://rg.ru/2007/02/22/yastrgemsky.html.

Schmitt, Oliver. forthcoming. "How to Challenge an International Order. Russian Diplomatic Practices in Multilateral Security Organisations." *European Journal of International Relations*.

Schreck, Carl. 2017. "'Look At Me!': Russian UN Envoy's Rant Stirs Buzz Back Home." Accessed July 10, 2019. https://goo.gl/xsS6Ga.

Security Council, of the Russian Federation. 2013. 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]. http://www.scrf.gov.ru/security/information/document114/.

Sharikov, Pavel, and Natalia Stepanova. 2019. "Podkhody SSHA, ES i Rossii k probleme informatsionnoy politiki [US, EU and Russia's approaches to information policy]." *Sovremennaya Evropa* 2: 73–83.

Sharikov, Pavel. 2018a. "Artificial Intelligence, Cyberattack, and Nuclear Weapons—A Dangerous Combination." *Bulletin of the Atomic Scientists* 74 (6): 368–373.

Sharikov, Pavel. 2018b. "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 (3): 170–188.

Sharikov, Pavel. 2018c. "Understanding the Russian Approach to Information Security." Accessed November 23, 2019. https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/.

Strel'tsov, A. A., R.A. Sharyapov, and V.V. Yashchenko. 2016. 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.

Tannenwald, Nina. 1999. "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use." *International Organization* 53 (3): 433–468.

Tikk, Eneken, and Mika Kerttunen. 2018. *Parabasis. Cyber-Diplomacy in Stalemate.* Norwegian Institute of International Affairs (Oslo).

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.