Contest and conquest: Russia and global internet governance

JULIEN NOCETTI

It has become part of conventional wisdom to consider cyberspace as an arena for strategic competition among states. There are many and varied recent illustrations of the prominence of cyberspace in international political and security concerns—for example (in no particular order), the leakage by Edward Snowden of information regarding US government surveillance programmes; the release of the Mandiant report, which disclosed the existence of Chinese units cyber-spying on the United States, and the subsequent intense high-level talks between China and the US on cyber security; and NATO's publication of the Tallinn Manual, which sets out to define the legal framework applying to cyberwarfare. This trend is reflected in the politicization of internet-related issues in global internet governance and cyber security forums, as displayed at the World Conference on International Telecommunications (WCIT) that took place in Dubai in December 2012 under the aegis of the United Nations to revise an international treaty that affects the way the internet is governed, and the ongoing debate on the internationalization of internet 'critical resources' (i.e. the internet infrastructure—root servers, exchange points, connections—and IP addresses and domain names).

This growing politicization of 'all things digital' illustrates three major current trends. First, many governments are attempting to exert sovereignty in cyberspace in the same way as they do in physical domains. The fact that private companies are dominant in this complex ecosystem is unsettling to many policy-makers, as is the unfettered internet access of their fellow citizens.

Second, governments are struggling to keep up with the pace of technological change, with technology evolving faster than law-making efforts; this disparity is calling into question the very nature of the Westphalian nation-state and its capacity to adapt to current challenges, leading to a profound reconfiguration of government-to-government and government-to-citizen relationships in the twenty-first century.

Third, there is a developing sense, underpinned by demographic factors, that the internet environment is quickly becoming more international and less western-centric. Over the next decade, the internet's centre of gravity will shift to the east and south. Even in 2012, 66 per cent of internet users were living in the non-western world, and the number of users across the globe is expected to rise

International Affairs **91**: 1 (2015) 111–130

from 1.9 billion in 2010 to 3 billion by 2016.[1] But there are also profoundly political factors involved: an increasing number of governments are no longer comfortable with the current system of internet governance and are seeking to challenge the historical dominance of the United States in the cyber domain.

Particularly prominent among these dissenting governments is Russia, whose foreign policy establishment has been seeking over the past decade to challenge the international consensus on a number of issues.[2] Today, as the international internet ecosystem becomes more volatile, Moscow is eager to shift the western narrative on the current global internet governance regime, over which the United States retains considerable leverage.[3]

The management of the World Wide Web is emerging as a leading issue of twenty-first-century global governance. For the Kremlin, the internet is indubitably a foreign policy tool, and it consequently strives to take the lead on global cyber governance and security issues as the membership, mandates and management of the institutions for cyber management increasingly become objects of international contention. In accordance with its views on the international system and law, Moscow upholds the traditional understanding of sovereignty and the principle of non-intervention at the core of its policy towards global internet matters. As a result, it conceives of cyberspace as a territory with virtual borders corresponding to physical state borders, and wishes to see the remit of international laws extended to the internet space, thereby reaffirming the principles of sovereignty and non-intervention as it understands them. Russia's active involvement in promoting international norms to guide states' behaviour in cyberspace across the global arena reflects this largely state-centric approach to internet-related issues. Moscow's stance on global internet governance also originates in a strained domestic political context since 2011–12 and a fear that the so-called Arab Spring uprisings might well be duplicated in Russia. Domestically, therefore, the internet is increasingly perceived as a threat by Russian leaders, who are seeking to impose strict regulation on the internet infrastructure and social networks. In both respects—on the international scene and within Russia—the Kremlin eyes the US superiority in the cyber domain with disfavour, and aims at constraining it.

This article sets out to explore Russia's multifaceted internet governance policy, and argues that Moscow is crucially involved in the politicization of global cyber issues, to a large extent owing to the inextricable interweaving of the Russian Federation's domestic and external affairs.

[1] Data collected on http://www.internetworldstats.com (as of 15 Feb. 2014), accessed 15 Feb. 2014. See also David Dean, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda and Paul Zwillenberg, *The $4.2 trillion opportunity: the internet economy in the G-20* (Boston: Boston Consulting Group, March 2012).

[2] See e.g. Andrei P. Tsygankov, 'Preserving influence in a changing world: Russia's grand strategy', *Problems of Post-Communism* 58: 2, 2011, pp. 28–44.

[3] Tim Maurer, 'Cyber norm emergence at the United Nations: an analysis of the UN's activities regarding cyber-security', Discussion paper 2011-11 (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, Sept. 2011).

International Affairs 91: 1, 2015

The significance of domestic perceptions and factors

To assert that the uprisings in the Arab world have had a profound impact on the minds of Russian political elites is an understatement. Reflecting on the sustained use of digital technologies—microblogs such as Twitter, video platforms such as YouTube and social networks such as Facebook—in the revolutionary processes in Tunisia, Libya and Egypt, the Kremlin and Russian law enforcement agencies started to monitor closely the impact of the political use of networked technologies upon social mobilization and democratic transition.[4]

The Arab awakening was followed by an election cycle in Russia—a parliamentary ballot in December 2011 and a presidential vote in March 2012—that quickly reawakened Russian leaders' anxiety over the 'power of networks'. Indeed, the political leadership feared a ripple effect in Russia as mass protests in the country's biggest cities—primarily Moscow and St Petersburg—were in large part coordinated on and facilitated by the use of digital technologies.[5] Alexei Navalny, a popular lawyer and blogger, and member of the non-systemic opposition,[6] took full advantage of his online-born 'crowdsourcing' projects to denounce the corruption of state officials and corporations, before virally spreading his motto against 'the party of crooks and thieves' (the ruling party United Russia) on web platforms and becoming a *cause célèbre* in the West.

In other words—though this is not a new concern—the Kremlin is increasingly seeing the internet as politically disruptive because it enables citizens to circumvent government-controlled 'traditional' media, most importantly television. Hence the series of laws discussed and passed in the state duma since Vladimir Putin's return to the Kremlin in May 2012, the most revealing of these creating a 'single register' of banned websites that contain child pornography, advocacy of drug abuse and drug production instructions, and suicide advocacy, which came into force on 1 November 2012. Analysts say that the blocking of both individual websites and IP addresses may require service providers to acquire deep-packet inspection (DPI) technology, which is a form of filtering used to inspect data packets sent from one computer to another over a network, and thus enables its users to track down, identify, categorize, reroute or stop internet traffic. This would make it easier to block particular and increasingly popular services, such as Skype, or pages such as individual Facebook groups.[7] Members of both parliamentary houses are promoting further legal initiatives, and the most prominent

[4] Julien Nocetti, 'Russie: le web réinvente-t-il la politique?', *Politique étrangère* 77: 2, Summer 2012, pp. 277–89. On the Arab awakenings, see Manuel Manrique and Barah Mikaïl, *The role of new media and communication technologies in Arab transitions*, FRIDE Policy Brief no. 106, Dec. 2011 (Madrid: Fundación para las Relaciones Internacionales y el Diálogo Exterior).

[5] Nicole Bode and Andrei Makarychev, 'The new social media in Russia: political blogging by the government and the opposition', *Problems of Post-Communism* 60: 2, 2013, pp. 53–62.

[6] The non-systemic opposition refers to opposition parties that are 'excluded' from the political system because they lack both a representation in the structures of state power and contacts with the ruling group. They predominantly use unconventional methods of political struggle, have limited resources, are particularly active on social networks, and enjoy little trust among citizens. See Ivan Bol'shakov, 'The nonsystemic opposition', *Russian Politics and Law* 50: 3, May–June 2012, pp. 82–92.

[7] Andrei Soldatov and Irina Borogan, 'The Kremlin's new internet surveillance plan goes live today', *Wired*, 1 Nov. 2012.

International Affairs 91: 1, 2015

Russian rulers regularly speak out in favour of greater internet regulation and more highly organized policing structures. The 2012 legislation reflects the Russian authorities' perception that controlling 'their' national cyberspace constitutes a twofold challenge both to governance and to political legitimacy.[8]

More strikingly, the scandal involving the United States National Security Agency (NSA), sparked by Edward Snowden's leakage of documents from June 2013, revived the push for tighter controls over the internet in Russia, on the basis that the privacy policies adopted by transnational companies such as Google, Facebook, Twitter and others pose a threat to Russia's digital sovereignty—and consequently national security. Several members of both houses of the parliament suggested that all servers on which Russian citizens' personal data were stored should be located in Russia, and started a media campaign to bring global web platforms under Russian jurisdiction—either requiring them to be accessible in Russia by the domain extension .ru, or obliging them to be hosted on Russian territory.[9] Deputy Prime Minister Dmitry Rogozin claimed that services such as Facebook and Twitter are elements of a larger American campaign against Russia, while state duma members called for tighter regulations on state officials' internet activity, based on the concern that Russian bureaucrats commonly discuss or upload government secrets in communications hosted on American websites (mainly gmail).[10] Though not specific to Russia, plans to promote national networking technology, set up a secure national email service and encourage regional internet traffic to be routed locally are well in the spirit of the times in Moscow. All these claims tend to legitimize and revive the longstanding call for a 'national operating system' that would reduce the Russian dependency on Microsoft Windows.

The assumption that digital technologies are used by the West to topple regimes in countries where the opposition is too weak to mobilize protests has thus come to define the Kremlin's approach to the internet both in Russia and globally (see below). Domestic factors therefore play a crucial role in shaping Russia's internet policies, though the Russian authorities' stance towards the internet is not (yet) fully homogeneous. Different groups, which promote their own agendas and visions of Russian objectives, can be roughly divided into two main categories. The pioneers of Runet[11]—mostly the technical community that introduced the internet in Russia in the 1990s and the not-for-profit structures 'governing' the national segment, along with IT entrepreneurs and active users of the 'blogosphere'—basically form the 'doves'; these groups view the internet as a means to further innovation and economic modernization, and believe that it should remain free of government control. This group also includes some of those working in the presidential administration and the Ministry of Telecommunications during

[8] Julien Nocetti, '"Digital Kremlin": power and the internet in Russia', *Russie.NEI.Visions*, no. 59 (Paris: Institut français des relations internationales, April 2011), p. 9.

[9] Sergei Zheleznyak, 'My dolzhny obezpechit' tsifrovoi suverenitet', *Ekonomika i Zhizn'*, 19 June 2013.

[10] 'Rogozin schel sotsseti elementom sovremennoi kibervoiny', RIA Novosti, 7 June 2013. See also Vladimir Zykov, 'Za peresylku dokumentov cherez Gmail chinovnikam grozit do 20 let', *Izvestia*, 11 June 2013.

[11] 'Runet' is the term commonly used to define the Russian internet. It is also sometimes used to describe the Russian-language internet.

International Affairs 91: 1, 2015

Dmitry Medvedev's presidency who were dealing with e-government projects and the country's digital modernization.[12] Importantly, it also includes some elements within the Ministry of Foreign Affairs, especially among the younger, more internet-aware diplomats, reflecting a deep and largely inter-generational split within the administration in attitudes towards the internet.[13] This group has been overshadowed by a more security-oriented grouping comprising the Russian Federation's Security Council, the General Prosecutor, the Ministry of Internal Affairs, the Federal Security Service, and political figures from the dominant party United Russia and its youth-affiliated organizations such as Nashi and Rosmolodezh. Bodies associated with the Civic Chamber—such as the League for a Safer Internet—and the recently created Kremlin-backed Foundation for the Development of Civil Society[14] also contribute to the introduction and dissemination of a security-driven approach to the internet, favourable to increased online monitoring and further regulation by law enforcement agencies.

Individuals can also play a substantial role in shaping the politicians' views on internet issues: Alexei Chadayev, for example, former 'ideologist' to United Russia, was key in promoting a 'direct internet democracy' in Russia, and leading IT businessman Igor Ashmanov has for years been promoting the development of a 'national search engine' and advancing 'information sovereignty' both in Russia and abroad.[15] In particular, Ashmanov—whose wife, Natalya Kasperskaya, was formerly married to computer security expert Yevgeny Kaspersky—has been actively defending the government's initiatives to increase government control over the internet, to criminalize anonymous web browsing in Russia, and to promote pro-Kremlin bloggers. His diverse set of skills closely matches the Kremlin's need for internet analysis, information control and promotion of pro-government content.[16]

Fundamentally, the Russian government's approach to the internet looks simultaneously both inwards and outwards, with draft legislation and public statements running alongside policy initiatives at the regional ('near abroad') and global level, and international events influencing Russia's policy-making in this sphere. For some, this approach is intimately connected with the inherently authoritarian nature of the Russian regime, continuing a century-long habit of muzzling dissenting voices by whatever medium is currently available.[17] For others, the strategy is attributable to the fact that Russia is a relatively young nation-state still

[12] Author's interview with a former Russian deputy minister for telecommunications, Moscow, July 2011.

[13] Author's interview with an expert from the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Feb. 2013.

[14] The Foundation for the Development of Civil Society, headed by a former deputy head of internal politics in the presidential administration, Konstantin Kostin, released a report in September 2012 expressing alarm about the threats posed by foreign web companies to Russia's stability. Early in 2013 another like-minded foundation was created by former Nashi (pro-Kremlin political youth movement) spokesperson Kristina Potupchik, with the particular aim of hiring bloggers to counter the opposition on social networks. On this, see Alyona Sivkova, 'Kreml' delaet stavku na blogerov', *Izvestia*, 30 July 2013.

[15] On this last point see Igor Ashmanov, 'Informatsionnyi suverenitet: novaya real'nost'', presentation at iForum (Ukrainian Forum of Internet Professionals), Kiev, 24 April 2013.

[16] Anastasia Golitsyna, 'Ashmanov otpravilsya vo Vetnam na poiski', *Vedomosti*, 13 Dec. 2011.

[17] Author's interviews with academics in Moscow, Dec. 2012 and Feb. 2013.

insecure about its sovereignty, and hence more strongly committed to a backward-looking, sovereigntist approach to internet governance.[18]

Beyond the Arab Spring and Snowden syndromes, it is clear that Russia has deep concerns about the principle of uncontrolled exchange of information in cyberspace, and about the presumption that national borders are of limited relevance in the cyber realm.[19] The slogan 'content as threat' encapsulates the Russian perception that digital technologies can be used as tools *against* Russia. In Russian documentation it is expressed more fully as the 'threat of the use of content for influence on the socio-humanitarian sphere'. The notion of content as threat is reinforced by the projection onto foreign partners of Russia's own preconceptions of how international relations work, and by the presumption that a primary aim of western powers is to disrupt and undermine Russia. Beyond this lies a deeper and more nebulous unease about the vulnerability of Russia's national culture to outside influences. This is another facet of the holistic approach to information security in Russia which, as Keir Giles argues, remains largely unrecognized in the West.[20]

Not surprisingly, the ongoing conflict with the West over Ukraine provides the perfect context to justify the aforementioned projects towards 'information sovereignty'. In April 2014 President Putin publicly described the internet as a 'CIA project'; this came at the same time as an avalanche of internet laws, including imposing stricter rules on bloggers and proposals such as forcing internet service providers to use domain name system (DNS) servers located inside Russia. Rumours about an internet 'kill switch' have added to the general picture of a 'tightening of the screws' of the internet in Russia.[21]

A state-centric approach to internet governance

Examining how Russian authorities conceive of the internet domestically reveals a great deal about their approach towards global cyber governance. In many ways, Russia takes a neo-Hobbesian view of the internet, seeing it largely as a chaotic domain, use of which reinforces global anarchy (as understood in International Relations theory). To the Russians, internet governance *per se*[22] has now entered the global political 'premier league'. In other words, far from being a merely technical matter, global internet governance is envisioned as an issue of high

[18] Milton Mueller, 'Are we in a digital Cold War?', paper presented at the GigaNet workshop, 'The global governance of the internet: intergovernmentalism, multistakeholderism and networks', Graduate Institute, Geneva, 17 May 2013.

[19] Keir Giles, 'Russia and cyber security', *Naçao e Defesa* 5: 133, 2012, pp. 69–88.

[20] Giles, 'Russia and cyber security'.

[21] Anastasia Golitsyna, 'Soviet bezopasnosti obsudit' otklyuchenie Rossii ot global'nogo interneta', *Vedomosti*, 19 Sept. 2014.

[22] In this article 'internet governance' is taken to mean 'all shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet': the definition proposed by the UN-initiated World Summit on the Information Society (WSIS) in 2005. This definition has been contested by various groups across political and ideological lines. For a discussion on internet governance and on the role of the nation-state in it, see Milton Mueller, *Networks and states: the global politics of internet governance* (Cambridge, MA: MIT Press, 2010).

politics in which states—and the interstate balance of power—play an essential role.[23]

Reasserting state sovereignty

The current internet governance regime clashes with Russia's preferences in two distinct ways. First, the legacy of denationalized liberalism associated with the internet's early development is still a powerful force shaping the internet's operations and the social, economic and political norms associated with its use. Instead of traditional, intergovernmental institutions, there are private sector-based, transnational forms of governance, alongside a widespread ethic of self-regulation and civil society support for internet freedom. This is what has been framed as the multi-stakeholder model, in which governments, private companies and non-governmental organizations exist alongside one another in non-hierarchical relations. Against this, Russia has for years articulated its views on the 'policy vacuum', identified as the institutional gap within the current internet governance ecosystem. These fundamentally consist in reasserting state sovereignty over internet governance—more precisely, in shifting the balance of participation from a network-to-network system to a government-to-government system in which experts would be required to participate indirectly—through government actors much less well informed on the issues.[24] For Russian observers, then, Russia could be considered an advocate of a 'digital Westphalia', meaning that it supports increased state control over online space—even though this would ultimately result in limitations on the open network concept that made the internet possible[25]—and defends the principle of non-interference in the internal affairs of other states.

Second, the privileged role of the United States in the current internet governance regime, especially its influence over the Internet Corporation for Assigned Names and Numbers (ICANN)—via a contract between the organization and the US Department of Commerce[26]—rankles with the Russians. Although in many respects denationalized liberalism and US pre-eminence are at odds with each other, it is not surprising that Russia sees them as related and mutually reinforcing. In Russia's state-centric view, internet freedom and the US doctrine of the 'free flow of information' are merely tools that a hegemonic America uses to subvert

[23] Author's discussions at the seventh international forum 'Partnership between state, civil society, and business in the field of international information security', Garmisch-Partenkirchen, Germany, 22–25 April 2013. See also Hannes Ebert and Tim Maurer, 'Contested cyberspace and rising powers', *Third World Quarterly* 34: 6, 2013, pp. 1054–74.

[24] Author's interviews with internet governance specialists, Moscow, Oct. 2011 and Feb. 2013.

[25] Yelena Zinovieva, 'Tsifrovoi Vestfal'?', analysis on MGIMO website (Moscow State Institute of International Relations), 26 March 2013, http://www.mgimo.ru/news/experts/document236588.phtml, accessed 8 Nov. 2014.

[26] The Department of Commerce and ICANN have a contract between them whereunder they carry out the Internet Assigned Numbers Authority (IANA) functions together. The IANA department oversees global IP address allocation, autonomous system number allocation, root zone management in the domain name system (DNS), and other internet protocol-related symbols and numbers.

other states and penetrate them with its own world-view and values.[27] In private meetings, even before the NSA-related scandal, Russian officials tend to emphasize the US supremacy over the network, and claim that it is necessary to prevent the emergence of an 'internet Frankenstein' (see below for recent developments).[28]

Within a broader perspective, the cyber policy promulgated by Russia in opposition to the existing US-led multi-stakeholder regime appears as a combination of two—not necessarily contradictory—approaches. One can be labelled intergovernmental, and seeks to tame US leadership by transferring authority to an international governmental organization (IGO) in order to embed US power 'in rules and institutions that channel and limit the ways that power is exercised'.[29] The other may be labelled a sovereigntist approach and focuses on establishing traditional territorial control over cyberspace, reasserting a Westphalian notion of sovereignty through an IGO such as the International Telecommunication Union (ITU).

Actors and decision-making processes

Contrary to common preconceptions, there is no homogeneity of views on internet governance and cyber security matters within the Russian decision-making elite. The presidential administration, the Security Council of the Russian Federation, the various law enforcement agencies and the Ministry of Telecommunications all from time to time promote their own agendas, leading to incoherence in the messages reaching foreign internet communities.

Within the government, internet governance and regulation are managed by the Ministry of Telecommunications, with the support of the Ministry of Foreign Affairs (MFA) in international forums. The MFA has recently been attempting to reinforce the expertise of Russia's diplomatic community on 'all things cyber' and to ensure (not always successfully) that its representatives speak with one voice on these topics: in March 2012 the ministry created a new position of special coordinator, with the rank of ambassador-at-large, charged with overseeing 'the political use of information and communication technologies'. Andrei Krutskikh, who had previously worked as deputy director of the Department of New Challenges and Threats at the same ministry, was appointed to the post.[30] In June 2014 he was appointed 'special envoy of the president for international information security', leading the country's internet governance and cyber security efforts globally.

Generally speaking, while the Ministry of Telecommunications tends to focus more on technical issues surrounding internet governance and regulation

[27] Yelena Chernenko, 'Rossiya vystupit za internatsionalizatsiyu interneta', *Kommersant'*, 3 Dec. 2012. On the interaction between the US 'open door' and internet policies, see Daniel McCarthy, 'Open networks and the open door: American foreign policy and the narration of the internet', *Foreign Policy Analysis* 7: 1, 2011, pp. 89–111.

[28] Author's discussions in Garmisch-Partenkirchen, Germany, 22–5 April 2013.

[29] G. John Ikenberry, *Strategic reactions to American preeminence: great power politics in the age of unipolarity* (Washington DC: United States National Intelligence Council, 2003), p. 14.

[30] Yelena Chernenko, 'V MIDe poyavilsya kurator interneta', *Kommersant'*, 20 March 2012. The ministry may also create an 'Office for International Information Security', which will deal exclusively with cyber security issues.

processes, taking part in all major internet governance initiatives, the MFA has engineered a security-driven internet governance agenda, clearly reflected during the WCIT-12 summit in Dubai in December 2012.[31]

Russia's Security Council (SC) has emerged as the most important body in terms of policy-shaping and decision-making on international cyber policy issues in Russia over the past few years—with an evident emphasis on cyber security and cyber defence. The British expert Andrew Monaghan notes that 'from a purely consultative body harvesting expert advice from across government, the SC has become a policy-forming body … the role of the SC has crystallized, and it has become a more serious, coherent organ; its powers are more streamlined and defined in an orderly way.'[32] Its deputy secretary Nikolai Klimashin specifically dealt with domestic and international information security until his resignation in December 2013, serving as a link between the Kremlin, the country's law enforcement agencies, and regional (Shanghai Cooperation Organization, Collective Security Treaty Organization, etc.) and international organizations (UN bodies, the OSCE, etc.). One of the Security Council's channels for exercising influence abroad is Moscow State University's Institute for Information Security Issues (IISI), which since the mid-2000s has been holding an annual International Forum for Information Security, usually in Garmisch-Partenkirchen (Germany). This institute has played a key role in formulating policy recommendations to the top decision-makers and in echoing Russia's cyber security policy to foreign audiences. It has been known particularly for a series of negotiations it led with American senior officials and experts on establishing a terminology for critical concepts relating to cyber security.[33] The institute is also engaged in bilateral 'track 2' meetings with European and Asian officials and experts, with the evident aim of influencing them on 'information security' issues. However, while IISI has been fairly successful in marshalling support, it has not produced as much scholarly output as would be expected.[34]

Civil society activity related to internet governance in Russia is at only a moderate level. There are very few civil society organizations that have a continuing interest and participation in internet governance issues; and although there is a noticeable increase in the number of academics and young think-tank experts engaging in these matters,[35] most of their work is published in Russian, thus limiting their outreach to audiences in non-Russian-speaking countries. The Russian chapter of the UN-led Internet Governance Forum (IGF), which has so far held five of its annual meetings in Moscow, has been quite successful in bringing together Russian and foreign experts, government and business representatives, and the 'internet community' with substantial civil society participation,

[31] Author's discussion with a Russian expert involved in the negotiations, Moscow, Feb. 2013.

[32] Andrew Monaghan, 'Putin's Russia: shaping a "grand strategy"?', *International Affairs* 89: 5, Sept. 2013, p. 1229.

[33] These negotiations are reflected in Karl Frederick Rauscher and Valery Yaschenko, eds, *Russia–US bilateral on cyber security: critical terminology foundations* (Moscow: East–West Institute and Information Security Institute, April 2011).

[34] Author's interviews with several representatives of the IISI, Moscow, Oct. 2011 and Dec. 2012; Garmisch-Partenkirchen, April 2013; Paris, June 2013.

[35] Author's talks with internet governance experts, Moscow, April 2013.

International Affairs 91: 1, 2015

in discussing a wide range of internet governance-related problems—apparently without the organizers coming under any substantial governmental pressure. At the fourth meeting in April 2013, the Russian government was even subjected to direct criticism, and a clear discrepancy was highlighted between government policy and reality.[36]

The business sector is fairly active in trying to influence Russia's national and global positions on information technology (IT) affairs. The IT industry is quite close to the IT departments of both the presidential administration and the state government (Ministry of Telecommunications); however, it still remains to be seen how successful the efforts of Russian non-state actors will be in advancing their own agenda on global internet governance.

Internationalizing internet governance

As noted above, Moscow is attempting to end the United States' 'cyber stewardship',[37] having grown weary of what it sees as Washington's 'unilateral globalism' over the network. Even before the NSA scandal, Russia had also been keen to denounce the United States' 'double standards' *vis-à-vis* the internet.[38]

On the diplomatic level, Russia promotes a system of international supervision in which security considerations play a significant role. To this end, Moscow works through both UN-led international organizations and regional forums such as the Shanghai Cooperation Organization (SCO), the Collective Security Treaty Organization (CSTO) and the BRICS grouping of Brazil, Russia, India, China and South Africa to promote its more centralized and top-down approach to internet governance among sympathetic countries.

De-Americanizing the internet?

Moscow has been advancing the internationalization of internet governance at both regional and international levels for over a decade. To Russian leaders dealing with internet matters, the internet is clearly and rapidly becoming more international and less western-centric. The reason most frequently invoked is a demographic one: by 2020, there will be 2 billion more internet users in the world, 90 per cent of whom will be in non-OECD countries. This shift to the non-western world has nevertheless provided Russia and other authoritarian and emerging countries with an opportunity to assertively question the US leadership over the internet. Indeed, Russia, like China and some Middle Eastern nations (particularly in the Gulf), considers the US stance on cyber politics to be largely hypocritical: while preaching the tearing down of 'digital borders' that have emerged in some authoritarian countries, US intelligence organizations have been recording and exploiting

[36] The present author participated in this event.

[37] The expression is from Roger Hurwitz, in 'Taking care: four takes in the cyber steward', paper presented at Cyber Dialogue 2012, 'What is stewardship in cyberspace?', University of Toronto, March 2012.

[38] As expressed for example by former Minister for Telecommunications Igor Schegolev: 'Miru nuzhen kodeks povedeniya v seti', *Vedomosti*, 20 Jan. 2012.

International Affairs 91: 1, 2015

mass surveillance data—without any control,[39] thus undermining Washington's 'ability to act hypocritically'.[40] Likewise, as noted above, Moscow is infuriated by America's stranglehold on the web in terms of both infrastructure (networks, monopoly in terms of internet naming and addressing) and the pre-eminence of American companies. The Russians note, for instance, that of the 13 root servers that are essential to the functioning of the entire internet, ten were originally located in the United States, and the other three are on the territory of US allies (Japan, the Netherlands and Sweden).

For these reasons the Russians think that the bulk of the debate on internet governance should not take place within the transatlantic framework, preferring to participate in various global internet governance forums on the basis of a North–South axis.[41] Overall, Russian representatives in international conferences like to stress the necessity to internationalize internet governance on the basis of its becoming a 'global commons', complacently adopting a rhetoric redolent of Soviet-era pronouncements on the Third World with the aim of influencing positions on the issue in the global South.[42]

The launch of a Cyrillic domain name in mid-2010, which put an end to the monopoly of Latin characters on the internet, was in this respect a case in point. Although Russia was not alone in obtaining from ICANN the right to use non-Roman scripts, as the accord also applied to Arabic, Chinese, Hebrew, Japanese and Korean characters, Moscow contributed significantly to raising the issue of internet literacy for Russian-speaking users not proficient in the use of Latin script.[43] It should be noted, however, that the Russians never publicly criticized the market-oriented dimension of internet governance—unlike, for example, a large part of the expertise from the Indian subcontinent, which tends to remain steeped in Marxist paradigms.[44]

Emphasis on norm-making and policy coordination

Russia's international cyber-policy agenda has developed on two levels, international and regional. In all channels of negotiation—and more visibly at the United Nations—Moscow has been instrumental in blurring the lines between internet governance and cyber security.

First, Russia has been proactively engaged in norm promotion through international institutions, especially the main forums of internet governance: ICANN, the ITU and the IGF. Many scholars have already observed that these institutions

[39] Thomas Gomart, 'De quoi Snowden est-il le nom?', *Revue des deux mondes*, Dec. 2013, p. 102.

[40] Henry Farrell and Martha Finnemore, 'The end of hypocrisy: American foreign policy in the age of leaks', *Foreign Affairs* 92: 6, Nov.–Dec. 2013.

[41] Interview with author in *Le Monde*, 'Gouvernance du Net: La Russie mène une politique d'influence', 7 Dec. 2012. See also Ebert and Maurer, 'Contested cyberspace and rising powers'.

[42] See 'My za internatsionalizatsiyu upravleniya internetom', interview with Andrei Krutskikh in *Kommersant'*, 16 June 2014.

[43] Author's interview with representatives of the Russian national registry, Moscow, July 2011.

[44] See e.g. Abu Bhuiyan, *Internet governance and the global south: demand for a new framework* (Basingstoke: Palgrave Macmillan, 2014); and Prabir Purkayastha and Rishab Bailey, 'U.S. control of the internet: problems facing the movement to international governance', *Monthly Review* 66: 3, July–August 2014.

are coming under new pressures as governments assert themselves more forcefully in cyberspace.[45] As a consequence, the focus of some of these forums is shifting: in technical governance forums, for example, previously unpoliticized or largely technical issues are becoming the objects of intense political competition.

As a case in point, Russia and the Russian-speaking countries of the former Soviet Union have adopted a wide-ranging engagement with forums such as the ITU and the IGF to promote policies that synchronize with national laws surrounding information security. Russia's President Vladimir Putin has himself pleaded several times that global cyberspace should be governed by international institutions operating under the United Nations—and that the ITU was the institution best placed to regulate the internet. Not surprisingly, Russia's policies have been vocally supported by the former (2007–2014) Secretary General of the ITU, Hamadoun Touré, who is fluent in Russian, having completed his higher education in the Soviet Union. Russia has been particularly eager to give both rhetorical and financial support to the ITU telecommunication development sector (ITU-D)—whose core mission is 'to foster international cooperation and solidarity … in the creation, development and improvement of telecommunication/ICT equipment and networks in developing countries'[46]—and to sponsor some developing countries in that forum in return for vocal support for Russian initiatives within the United Nations' internet governance forums.[47] Every year since 1998, Russia has put forward resolutions at the United Nations to prohibit 'information aggression', which is widely interpreted to mean ideological attempts, or the use of ideas, to undermine regime stability.

What is noteworthy is that the international institutions that are primarily focused on technical coordination of the internet—the Internet Assigned Numbers Authority (IANA), ICANN, the IETF (Internet Engineering Task Force) and RIRs (Regional Internet Registries)—have become increasingly politicized and subject to securitization pressures. Governments whose strategic interests are oriented around legitimization of national controls are viewing these cyberspace governance forums as important components of a broader, more comprehensive international policy engagement. In 2010, a coalition of Russian-speaking countries, supported by China and India, put forward a proposal through a sub-meeting of the ITU to give governments veto power over the decisions adopted by the ICANN Board of Directors on naming and addressing.[48]

Beyond the emblematic case of ICANN, the IETF provides an illustrative example of how a 'traditional' multi-stakeholder organization has been subject to political pressure from governments. Since its foundation in the mid-1980s the IETF has helped shape the majority of the internet's core networking protocols (such as

[45] See Eric Brousseau, Meryem Marzouki and Cécile Méadel, eds, *Governance, regulations and power on the internet* (New York: Cambridge University Press, 2012).

[46] According to the ITU-D website page, http://www.itu.int/en/ITU-D/Pages/About.aspx, accessed 8 Nov. 2014.

[47] Author's interview with a French official, Paris, Nov. 2011.

[48] This initiative was variously interpreted as a 'de-Americanization' and a bureaucratization of the internet. See Gregory Francis, 'Plutocrats and the internet', CircleID, 4 Oct. 2010, http://www.circleid.com/posts/20101004_plutocrats_and_the_internet/, accessed 15 March 2014; Igor Naumov, 'Minkomsvyazi predlagaet deamerikanizirovat' internet', *Nezavisimaya Gazeta*, 6 Oct. 2010.

TCP/IP) and the protocols for the internet's basic applications (for example, SMTP for email). Critics of the IETF, such as Russia and China, have stressed the fact that Americans have dominated the organization from the beginning, arguing that this makes it nothing more than an instrument of US political and commercial interests.[49] Since its meeting in Vancouver (November 2013), the IETF has moved cyber security issues to the top of its list of priorities, indicating an increasing susceptibility to governmental pressure; it is likely that this organization will become one of the top 'spaces to watch' in the internet governance ecosystem.

In 2011 Moscow scored a couple of successes in its international initiatives on information security. In September, Russia submitted, along with China, Uzbekistan and Tajikistan, a proposal for an International Code of Conduct for Information Security to the UN General Assembly. While this was not a proposal for a new institution, it certainly suggested a new process and power arrangement in global internet governance by calling for action on cyber security at UN level. Essentially, the code would increase governmental power over the internet, and it contains no multi-stakeholder dimension. The resolution proposed twelve voluntary commitments based on, among other things, 'the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States'. Although voluntary, the code aimed to clear more ground for a governmental role in internet governance, the preamble stating that 'policy authority for internet-related public issues is the sovereign right of States'. At roughly the same time, a draft Convention on International Information Security was released at an 'international meeting of high-ranking officials responsible for security matters'[50] in Yekaterinburg. The draft neatly illustrates many divergences between Russian and western preconceptions about the nature of the internet and the basic assumptions on how it should be governed.[51]

Taken together, the two documents propose to significantly strengthen the power of the state in cyberspace relative to non-government actors. But they also provide an alternative vision for undecided countries that may incline naturally towards state-dominated models of governance, and towards echoing Russia—and China—in viewing with disfavour the destabilizing potential of the internet and cyberspace more broadly. More recently, in October 2013 Russia submitted to the UN First Committee a draft resolution on international information security—which was signed by only 17 countries, mostly from the developing world in Asia, Latin America and Africa.

Second, Russia has pursued its attempt to shift the western narrative over internet governance via policy coordination through regional organizations. Some

[49] Jonah Force Hill, *Internet fragmentation: highlighting the major technical, governance and diplomatic challenges for US policy makers* (Cambridge, MA: John F. Kennedy School of Government, Harvard University, Spring 2012). The author reports that of the more than 6,000 'requests for comments' (technical reports that often lead to standards) drafted between 1986 and 2012, 4% originated from Chinese engineers, and less than 1.5% from Russia.

[50] International meeting of high-ranking officials responsible for security matters, Yekaterinburg, 21–22 Sept. 2011.

[51] Giles, 'Russia and cyber security', pp. 75–7.

International Affairs 91: 1, 2015

of these forums attract little attention, meeting in relative obscurity, and thus take actions well away from the spotlight that are ignored or overlooked by activists and others concerned with internet freedom and cyberspace governance. But the actors who comprise them treat them seriously, and use them as vehicles of policy coordination and information sharing.[52] One illuminating example is the SCO, whose members comprise China, Russia and all the Central Asian republics excepting Turkmenistan.[53] The SCO aims to share information and coordinate policies around a broad spectrum of cultural, economic and security concerns, among them cyberspace policies. Generally speaking, experts see the SCO as a regional vehicle of 'protective integration' against international norms of democracy and regime change, with shared information policies being seen as critical to that end.[54] Since 2009 SCO member states have been bound by an agreement on 'cooperation in the field of ensuring international information security'; and in 2011 the SCO issued a statement on 'information terrorism', which drew attention to its members' shared and distinct perspective on internet security policy. The Code of Conduct discussed above was proposed by SCO states, which formulated global standards for 'unacceptable state behavior' in cyberspace.

Although highly secretive, SCO meetings are likely to become important vehicles of policy coordination, giving unity, normative coherence and strength to the individual countries beyond the sum of its parts. A similar role is also played by the meetings of the CSTO, which increasingly focus on cyber-related threats, with a clear emphasis on Central Asia since the Arab Spring.[55] Besides, if agreements reflect the desires of the organizations' dominant members, they nonetheless provide models for other groups of states which are considering a regional approach to cyber security—for instance the Gulf Cooperation Council (GCC).

The BRICS grouping is also used as a vehicle for cooperation on cyber issues. At the policy level, all the BRICS states have shown an interest in internet governance and cyber security. Yet here different priorities are evident. There was no joint BRICS proposal for a code of conduct on information security or for a new internet governance body. Despite the increased institutionalization of the BRICS as a coalition and despite various proposals contesting the role of the United States regarding the internet, the group is divided and formal proposals have been submitted through either IBSA (India–Brazil–South Africa) or the SCO.[56] Generally speaking, the key differences are between those states that favour an intergovernmental approach based on international cooperation and those preferring to adopt a strict 'sovereigntist' cyber policy.

[52] Ronald Deibert and Maashi Crete-Nishihata, 'Global governance and the spread of cyberspace controls', *Global Governance* 18: 3, July–Sept. 2012, pp. 339–61.

[53] The SCO's members are China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan. Afghanistan, India, Iran, Mongolia and Pakistan have observer status, and Belarus, Turkey and Sri Lanka are considered dialogue partners.

[54] Author's interview with a Russian academic, Moscow, Oct. 2011. See also Roy Allison, 'Virtual regionalism, regional structures and regime security in Central Asia', *Central Asian Survey* 27: 2, 2008, pp. 185–202.

[55] See Yelena Chernenko's interview with CSTO General Secretary Nikolai Bordyuzha: '"Est' veshchi, kotorye dlya nas zapretny"', *Kommersant'*, 26 March 2013.

[56] Ebert and Maurer, 'Contested cyberspace and rising powers'.

Russia's active participation in ITU meetings provided good examples of Moscow working through regional and international organizations to propagate norms of state control. Much has been written on the December 2012 ITU–WCIT summit in Dubai. Here states disagreed over the content of a new set of International Telecommunication Regulations (ITRs). These included provisions that some countries argued could create political cover for other states to assert claims of sovereignty in order to regulate internet content within their borders. Some governments that signed the new ITRs clearly had an agenda to increasingly bring internet governance under the auspices of the UN, where states (rather than private stakeholders) dominate. Eighty-nine countries signed the controversial ITR amendment—including Russia, China, South Africa, Indonesia, etc.—and 55 did not.[57] Russia played a key role in proposing the above-mentioned amendment; however, its position was leaked shortly before the summit, forcing the Russian authorities, under international pressure, to re-examine their most controversial suggestions, especially the amendment conferring 'equal rights' on ITU member states in managing the internet's core functions.[58] The WCIT-12 made clear that international competition to shape internet governance has entered a more, and increasingly, contentious phase.

A mostly US-centric cyber policy

As argued above, to Russian leaders the internet is a virtual extension of the United States under absolute US control—a control which it seeks to contest. Increasingly active in forging new alliances and trying to reformulate norms and standards, Russia has also been engaged in direct cyber diplomacy with the United States.[59] Clearly, while endeavouring to shape the international dialogue on cyberspace, Moscow also aims to 'bilateralize' internet governance and cyber security issues by establishing an exclusive and direct dialogue of equals with the United States on this issue.

There is clear evidence that the dialogue between the two countries is not easy: they have divergent approaches towards the way the internet should be governed, and have reacted differently to major international events surrounding internet governance and cyber security. Bilateral consultations have focused particularly on

[57] For a comprehensive map of signatory and non-signatory countries, see Mike Masnick, 'Who signed the ITU WCIT treaty … And who did not?', *TechDirt*, 14 Dec. 2012, https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml, accessed 22 Feb. 2014.

[58] Russia's agenda at WCIT-12 did not apparently reflect general consensus among the leadership, the presidential administration and the Security Council opposing the Ministry of Telecommunications on several issues. See Yelena Chernenko, 'Rossiya vystupit za internatsionalizatsiyu interneta', *Kommersant'*, 3 Dec. 2012.

[59] See e.g. John Markoff and Andrew Kramer, 'In shift, US talks to Russia on internet security', *New York Times*, 12 Dec. 2009; 'Joint Statement by the Presidents of the USA and the Russian Federation on a new field of cooperation in confidence building' (Washington DC: White House, Office of the Press Secretary, 17 June 2013). See also the papers published by the East–West Institute summarizing the negotiations between the Russian and American High-Level Expert Group on information security between 2009 and 2011: Franz-Stefan Gady and Greg Austin, eds, *Russia, the United States, and cyber diplomacy: opening the doors* (Moscow: East–West Institute, 2010); Karl Frederick Rauscher and Andrey Korotkov, eds, *Working towards rules for governing cyber conflict: rendering the Geneva and Hague Conventions in cyberspace*, Russia–US Bilateral on Critical Infrastructure Protection (Moscow: East–West Institute, 2011).

International Affairs 91: 1, 2015

reaching a consensus on critical terminology defining cyber/information security, an issue on which the two governments have had different priorities. According to Russian experts, the US terms *cyber security* and *cyberspace* are primarily technological, whereas the Russian terms *information security* and *information space* are seen as having broader philosophical and political meanings. The technology is perceived as only one of many components, and not even the most important one, in Russia's understanding of information security.[60] Conversely, the main priorities for US cyber security policy are to safeguard domestic technologies from disruptions, unauthorized access or any other kind of interference, thus emphasizing the technological aspects of cyber security.

Beyond discussions on terminology, the two governments have pursued a series of confidence-building measures, the latest being the establishment of a 'cyber-hotline' between the US cyber security coordinator and the Russian deputy secretary of the Security Council, for use in the event of a need to directly manage a crisis situation arising from an ICT security incident. This step was taken on the fringe of the G8 summit in Northern Ireland in June 2013[61]—just when leaked details of network surveillance and espionage programmes by the NSA were stirring up international concern about how deeply US intelligence is reaching into IT operations worldwide. A month later the formation was announced of a bilateral presidential group on information security, tasked with easing tensions between Washington and Moscow and carrying on the implementation of confidence-building measures.[62] This initiative was timely, as in August 2013 Putin signed an 'international information security strategy to 2020', which deals with the main (real or perceived) digital threats Russia faces and the initiatives Moscow is promoting at global and regional levels—the document being widely seen as a response to the 2011 US 'international strategy for cyberspace'.[63]

Given its perceived inferiority in relation to the West in communications technology,[64] Russia views the major world economies' building up of their potential for information warfare with great concern. Russian official documents stress that this development could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as the global information infrastructure. Consequently, Russia is determined to restrict offensive cyber activity and cyber weapons. In this respect, the increasingly institutionalized dialogue with Washington also serves as a way to call for the prevention of cyberspace militarization. Indeed, while the United States has said it wants a peaceful cyberspace, Moscow accuses Washington

[60] Author's discussions with Russian experts and officials, Moscow, July and Oct. 2011. See also Keir Giles and William Hagestad, 'Divided by a common language: cyber definitions in Chinese, Russian and English', Fifth International Conference on Cyber Conflict, Tallinn, June 2013.

[61] *Fact sheet: US–Russian cooperation on information communications technology security* (Washington DC: White House, Office of the Press Secretary, 17 June 2013).

[62] Yelena Chernenko, 'RF i SShA popytayutsya snizit' napryazhenie v seti', *Kommersant'*, 22 July 2013.

[63] *Osnovy gosudarstvennoi politiki Rossiyskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti na period do 2020 goda* (Moscow: Security Council of the Russian Federation, Aug. 2013).

[64] Amy Wilson, 'Computer gap: the Soviet Union's missed revolution and its implications for Russian technology policy', *Problems of Post-Communism* 56: 4, 2009, pp. 41–51.

of militarizing the internet through the establishment of a Cyber Command and the development of offensive capabilities such as Stuxnet.[65]

Here again, Russian proposals to ban or regulate cyber weapons cannot be separated easily, or at all, from the authoritarian state's imperative of maintaining domestic political control.[66] Nor can Russian concerns be separated from global internet governance issues, as Moscow sometimes uses 'traditional' internet governance venues to advocate an international legal regime of non-proliferation of 'information weapons'.

The Tallinn Manual, which as noted above was published by NATO in March 2013 with the goal of establishing international legal norms applicable to cyber warfare, has aroused a particular interest in the Russian general staff: for the military leadership, the manual 'legalizes' cyber war, and legitimates large-scale cyber operations like Stuxnet or Flame.[67] More broadly, Russia criticizes the constant rise in US budget allocations for cyber operations.[68]

It is clear that recent global internet governance and security venues have seen Cold War policies being brought into the twenty-first-century cyber arena.[69] While some point to the Nuclear Non-Proliferation Treaty as an appropriate precedent, others argue that a global consensus on cyber security could be best achieved by pursuing deterrence strategies.[70] Russia has conspicuously opted for the first strategy, which enables its policy-makers to follow Moscow's longstanding foreign policy objective of promoting legally binding international treaties—while in this case also developing its own cyber capabilities.[71]

However, Moscow's international internet policy might well have unintended results. Russia has excessively bilateralized cyber issues with the United States—and it is unlikely that the country is one of the key 'cyber emerging powers' Washington is to 'target' for both diplomatic and commercial reasons.[72] For the US government, WCIT-12 clearly marked a watershed: emerging internet powers such as India or Brazil, with a rising internet economy and strong cyber security

[65] Russian officials have been trying for a couple of years to drum up support for the idea that 'information warfare' is a crime against international peace and security. See Adrian Croft, 'Russia says many states arming for cyber warfare', Reuters, 25 April 2012. Stuxnet, a joint US–Israel project, is a computer virus first discovered in June 2010 known for reportedly destroying roughly a fifth of Iran's nuclear centrifuges by causing them to tear themselves apart.

[66] Christopher Ford, 'The trouble with cyber arms control', *The New Atlantis*, no. 29, Autumn 2010, p. 62.

[67] Yelena Chernenko, 'Rossiya poshla v mirnuyu kiberataku', *Kommersant'*, 29 April 2013. A year before the manual's publication, Dmitri Rogozin, First Deputy Prime Minister in charge of the military–industrial complex, announced the imminent creation of a Cyber Command that would bring together skills in information warfare. Flame is a modular computer malware discovered in 2012 and used for targeted cyber espionage in Middle Eastern countries. The *Washington Post* claimed that Flame was jointly developed by the US and Israel to slow down Iranian nuclear efforts.

[68] The 2014 budget request includes a 20% increase over 2012; the US Cyber Command is reportedly expanding by more than fivefold. See John Negroponte, Samuel Palmisano and Adam Segal, eds, *Defending an open, global, secure, and resilient internet*, Independent Task Force Report no. 70 (New York: Council on Foreign Relations, June 2013), p. 35.

[69] See e.g. Alexander Klimburg, 'The internet Yalta', *Commentary*, Center for a New American Security, Washington DC, 5 Feb. 2013; Michal Joseph Gross, 'World War 3.0', *Vanity Fair*, May 2012. US Secretary of State John Kerry called cyber-attacks a 'twenty-first century nuclear weapons equivalent' in January 2013.

[70] Nazli Choucri, *Cyberpolitics in international relations* (Cambridge, MA: MIT Press, 2012), p. 173.

[71] Author's interview with a Russian expert on information security, Moscow, Feb. 2013.

[72] Negroponte et al., *Defending an open, global, secure, and resilient internet,* pp. 58–9.

concerns, are still considered 'swing states' by Washington in the context of internet governance, as both countries have long been committed to the multi-stakeholder rules, and yet also wish to involve greater state resources in the cyber environment. The problem for Russia is that conflicts between its own agenda and those of such countries might contribute to marginalizing Russian initiatives at the global level, the latter being overwhelmingly focused on the security component of internet governance.

Today, and especially with regard to the NSA-related scandal, global South leaders do not hesitate to use internet issues to raise their international profile. Brazil's President Dilma Rousseff, for example, engaged in internet diplomacy with ICANN to suggest a 'globalization' of the organization's activities and promote a 'new model' of internet governance to be forged after a global meeting in São Paulo—called NETmundial—in April 2014.[73] Such a proposal inevitably attracted a great deal of attention from many in the international community, and once again highlighted the risk Russia runs of losing the 'power of initiative' in contesting the US lead in internet governance. Russia, which is experiencing a great geopolitical contraction, can hardly mobilize any 'brand appeal' in this realm. At the NETmundial gathering Russia clearly felt uncomfortable in a multi-stakeholder arena: the Russian delegation refused to sign the outcome document—along with Cuba and India—claiming that it is non-internationally binding, and that 'rules were changed [before the meeting] and [Russia's] contributions ignored'.[74]

In parallel to this Brazil meeting, western initiatives, panels and events on the future of internet governance have mushroomed, initiated in response both to the growing importance of internet governance on the global political agenda and to internationally binding conventions proposed by Russia and China—as demonstrated at the ICANN-affiliated 'High-Level Panel on Global Internet Cooperation and Governance Mechanisms' chaired by Estonian President H. T. Ilves (initiated in December 2013), and the CIGI–Chatham House 'Global Commission on Internet Governance' headed by Swedish Foreign Minister Carl Bildt (established in January 2014). If the Snowden leaks contributed somehow to legitimize the Russian—and Chinese—approaches to controlling online activity, support for seceding from the global internet has now spread far beyond post-communist countries. German Chancellor Angela Merkel proposed to build a 'European internet', while Brazil plans to lay an undersea communications cable directly to Europe to reduce the country's reliance on the US. References to the US 'digital colonialism' and 'military-digital complex', and calls to 'dismantle' Google, are no longer coming from authoritarian regimes or advocates of alter-globalization, but increasingly emanate from European parliamentarians and entrepreneurs.[75]

[73] Milton Mueller, 'The core internet institutions abandon the US government', Internet Governance Project, 11 Oct. 2013, http://www.internetgovernance.org/2013/10/11/the-core-internet-institutions-abandon-the-us-government/, accessed 4 May 2014.

[74] Position of the Russian Federation on the outcome of the NETmundial Internet Governance Meeting, Permanent Mission of the Russian Federation to the United Nations, 23 June 2014, http://www.russiaun.ru/en/news/rus_nigm, accessed 8 July 2014.

[75] Julien Nocetti, 'Puissances émergentes et internet: vers une troisième voie', *Politique étrangère* 79: 4, Winter 2014–2015.

Conclusion: power politics in play

This article illustrates an unquestionable trend: internet governance has become an increasingly divisive foreign policy issue. The disagreement over amendments to the ITRs gave marked emphasis to this growing tension. Since the Dubai ITU summit in 2012, broad coalitions of states have been emerging to contest the traditional multi-stakeholder internet governance model, as well as to foster their own policy agendas, with a particular focus on expanding the role of the state in internet governance and empowering the United Nations to further debate and discuss internet issues. In all of this, the developing world is playing an active role: in particular since the Arab Spring, the scale of the internet's economic and social implications has driven internet policy and regulation rapidly up policy-makers' agendas, with governments now sharply alert to the potential for disruption caused by access to digital communications.

It is not surprising that it is the younger nation-states that seem to be the most strongly committed to a neo-Westphalian approach to internet governance. In many respects, the battle over the vision of internet governance cannot be characterized entirely accurately as between authoritarian, undemocratic states and liberal, freedom-loving states; it is also, and indeed more centrally, a conflict between long-established, cosmopolitan states and newer states that do not yet feel safe in their sovereignty. Russia fits into the latter category, as a relatively young nation-state that has been experiencing, since the chaotic 1990s transition to a free market economy and pluralism, a potent feeling of insecurity. This feeling stems in part from the complex interactions between state authorities and the media ecosystem since the 1980s, when Soviet leaders tolerated increased access to previously suppressed information, thus opening the 'information gates' to the masses. In the 2000s, with Russia striving to recover its full sovereignty and struggling against the 'permeability' of its neighbourhood, Putin gradually saw the information revolution—driven by the considerable growth in (domestic) internet access—as one of the most pervasive components of US expansionism in the post-Soviet sphere, most notably in Russia itself. Russia's policy on global internet governance issues therefore cannot be separated from a domestic political context in which digital technologies are increasingly used for purposes of contention by an active and articulate 'netizen' middle class.

At the same time, internet governance has become a real strategic issue where substantial political, economic and social stakes meet. At present the debate about the future of the governance regime is carried on between small silos of experts, and is increasingly political. The calls for change will not fade away: indeed, as some large emerging economies approach and even overtake western economies, shifts on global governance are increasingly likely to occur. Caught in between these 'two worlds', Russia is asserting state power in cyberspace governance as much as it can in UN-led multilateral organizations, regional security groupings and expert gatherings. This policy goes far beyond merely technological and military aspects—it encompasses multifaceted diplomatic practices in a constantly

changing environment subject to periodic 'strategic surprises' (e.g. the publication of secret information by Julian Assange's WikiLeaks and Edward Snowden, or the disclosure of the Stuxnet computer worm, etc.) that the Kremlin uses to extend its reach and its instruments of leverage.

The significance of internet governance issues in international politics is likely to go on increasing. Are we likely to see the development of a peaceful internet coexistence, or are we ineluctably headed for a 'Cold Internet War', as internet governance scholar Wolfgang Kleinwächter has suggested?[76] This is difficult to predict, but arguments assuming a translation of Cold War-style policies into the twenty-first-century global internet arena will inevitably crystallize at the next World Summit for Information Society in 2015 in a much more strained way than in Dubai, magnifying the resort to 'perceptions warfare'. By then, Russia's positions are unlikely to have altered in any way; for in the wake of Snowden's revelations proposals by policy-makers are unlikely to soften, and controlling the narrative now appears a realistically attainable objective for the Kremlin.

[76] Wolfgang Kleinwächter, 'Internet governance outlook 2013: "Cold internet war" or "peaceful internet coexistence"?', CircleID, 3 Jan. 2013, http://www.circleid.com/posts/20130103_internet_governance_outlook_2013/, accessed 8 Nov. 2014.