Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU

Eva Claessen

To cite this article: Eva Claessen (2020) Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU, Journal of Cyber Policy, 5:1, 140-157, DOI: 10.1080/23738871.2020.1728356

To link to this article: https://doi.org/10.1080/23738871.2020.1728356

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 1, 140–157
https://doi.org/10.1080/23738871.2020.1728356

Routledge
Taylor & Francis Group

Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU

Eva Claessen

Centre for Global Governance Studies, KU Leuven, Leuven, Belgium

ABSTRACT

In the face of the rising political stake associated with the Internet, states are increasingly vying for a bigger role in its governance. Within a climate of an array of threats associated with the online information space, the attention is turning towards the governance of the internet infrastructure itself, comprising both the physical (the collection of cables computers, servers and routers that make up the network) and the virtual infrastructure (protocols, social media platforms and search engines that make it possible to navigate and use the internet). The question of sovereignty is not only increasingly reflected in the legislation of political actors like Russia, but also recently in EU discourse in relation to technological resilience and cyber security. This article aims to map out the impact of the securitisation of the internet infrastructure in the Russian and the EU approach to internet governance.

Abbreviations: CII: Critical Information Infrastructure; CIIP: Critical Information Infrastructure Protection; DDoS: Distributed Denial of Service attack; GAC: Governmental Advisory Committee to ICANN; IANA: Internet Assigned Numbers Authority; ICANN: Internet Corporation for Assigned Names and Numbers; ISP: Internet Service Provider; IXP: Internet Exchange Point; SORM: Sistema Technicheskich Sredstv Dlya Obespecheniya Funktsij Operativno Rozysknych Meropriyatij (System of technical resources to secure the function of operative-investigative activities); TLD: Top-Level Domain Name; UN GGE: United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; UN OEWG: United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

ARTICLE HISTORY
Received 16 May 2019
Revised 6 November 2019
Accepted 7 January 2020

KEYWORDS
Securitisation; internet governance; internet infrastructure; cyber sovereignty; Russia; EU

Introduction

Within the context of rising challenges emanating from the online information space, states are increasingly faced with the dilemma of how to provide an adequate response to threats posed in an area that is inherently decentralised and non-hierarchical in its

CONTACT Eva Claessen Eva.Claessen@kuleuven.be

architecture. Due to a growing awareness of the use of information operations on the internet by state actors in the wake of the 2007–2008 cyberattacks on Estonia and Georgia, the Snowden revelations in 2013 and the use of hybrid actions and disinformation by Russia during and after the height of the Ukraine crisis, there is a shift in the debate on how to manage and regulate the internet. This shift is expressed in an increased focus on the role and responsibility of state actors in achieving a secure and resilient internet. As Milton Mueller (2017, 417) asserts, the dawn of these new challenges to state actors has led to cybersecurity claims being 'used to enmesh various aspects of the Internet in foreign policy and military conflicts, as well as in other national forms of regulation and control in which states are privileged'.

Furthermore, security claims seem to form a fertile basis for arguments of state-actors aimed at (re)asserting their role in the area of internet governance. The characterisation of cyberspace as a domain for military action in 2016 by NATO, for example, has led to increasing efforts from both Western states and Russia to provide an international normative framework to protect against operations by state actors in cyberspace. In some ways, this explicit characterisation of cyberspace as a space for military contention, affirmed the assertion by Russia itself that the information space is being used to achieve political-military goals, a point which was made in the 2000 Doctrine for Information Security:

> [One of the sources of threats for the information security of the Russian Federation is] the development by a range of states of the concept of information warfare, which foresees the creation of means to exert a dangerous influence on the information sphere of other countries of the world, the disruption of the normal functioning of the information and telecommunication systems, the preservation of information resources and the acquisition of unauthorized access to them.

As Maria Ristolainen (2017, 114) posits, this tendency towards the militarisation of the internet is uncovering new ways to approach the challenges posed by the instrumentalisation of the internet by state actors as 'both Western and Russian cyberspace and/or information space is becoming a new space within which states may act and reassert traditional notions of sovereignty – yet through contradictory "open" and "closed" approaches'.

The appearance of these two different approaches can also be viewed within the development of cyber norms through the UN and the working groups for Information Security, the UN GGE and the UN OEWG. Since the development of cyber norms is marked by these two diverging approaches to sovereignty, the way they are presented by their proponents can be decisive. Because of this an effective strategy is necessary. These strategies can be viewed from the perspective of the process of "strategic norm construction", through which political actors as strategists manipulated shared normative frames for their political ends" (Kurowska 2019, 1). An example of this is visible in the efforts by Russia to advance its normative framework on information security through the UN, as it routinely contests Western dominance in the creation of this normative framework and accentuates the need to respect the sovereign equality of states (Idem, 10).

A current example of efforts by Russia to secure and centralise control over its online information space is the recent introduction of the package of laws concerning the 'autonomous Russian Internet' (Russian State Duma 2019). This draft law foresees the introduction of 'regulation of the routing of traffic and the control of compliance to these rules'

(idem). It would make it possible to 'limit access to the resources with prohibited information not only at the level of the site address, but also by preventing the transmitted traffic' (idem).

In practice, this would mean that internet traffic within Russia could only go through internet exchange points (IXPs) that are pre-approved by the institution issuing control and supervision of the internet, Roskomnadzor. A registry of IXPs is set to be created and will require the 'proprietors or other owners of Internet exchange points' to register with Roskomnadzor (Government of the Russian Federation 2019a). Additionally, the idea of the creation of a 'duplicate' internet infrastructure is launched. This duplicate infrastructure would operate in the case of 'the inability of Russian network operators to connect to servers abroad' to ensure the operability of the Russian internet at all times (Russian State Duma 2019). In preparation for the enactment of this law, annual exercises have been approved to test the security and resilience of the Russian internet infrastructure in case of 'specific situations where threats to the stability, security and integrity of the functioning of the Internet on the territory of the Russian Federation arise' (Government of the Russian Federation 2019b).

Within the EU as well, the aforementioned challenges have started up a debate on the need to introduce measures aiming to achieve technological and information sovereignty. As Tim Maurer et al. (2015, 54) posit, the use of the term 'technological sovereignty' is still rather vague as it is used as an 'umbrella term to suggest a spectrum of different technical and non-technical proposals, ranging from the construction of new underseas cables to stronger data protection rules'. The use of this term has been recently put forward by the Commission President, Ursula von der Leyen, as a priority for the new EU commission (European Commission 2019) and was featured during the hearing of Margrethe Vestager who postulated for the agenda on 'A Europe fit for the Digital Age'. During the hearing she put the term 'technological sovereignty' in the context of the 'development of key value chains and technologies that are of strategic importance for Europe', which should be 'open, truly European, innovative and lead to widespread knowledge dissemination' (Vestager 2019). In many ways the term itself seems to point towards the need to achieve a certain degree of technological autonomy as well as securing against foreign surveillance.

This shift in focus to the management and protection of the internet infrastructure can be viewed from the perspective of what Francesca Musiani et al. (2016, 4) have dubbed 'the turn to infrastructure' in internet governance. These authors put forward the claim that there has been a significant turn in internet governance due to the assertion of the role of state responsibility in this area. They argue that states have recognised that 'points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money information, and the marketplace of ideas in the digital sphere' (Idem).

Both the EU and Russia seem to be privy to this realisation, as the development of internet policy and legislation has moved its focus away from purely measures of content regulation towards the issuing of legislation aiming to secure internet infrastructure. However, while security arguments are mirrored by both actors, a key difference in approach needs to be highlighted. The EU's approach to cyber and technological sovereignty starts explicitly from the point of view of it being a common effort to achieve a secure and resilient cyberspace. As Georg Christou (2019, 279–280) posits, 'governance in relation to cyberspace reflects the fact that disruption has been framed as a collective threat, which, if

not addressed effectively through EU rules, norms and regulations, will affect the economic and social development of the EU and its member states'. The importance of enhancing security on the level of internet infrastructure through concerted efforts has come to the fore in EU policy as well. The adoption of the NIS directive in 2016 is a notable example of this, as it 'seeks to ensure a minimal institutional capability for reporting cyber incidents across member states and so manage the risks associated with cyberattacks' (Christou 2019, 279).

This difference in approach is also present in the way both actors position themselves in the debate on the development of global cyber norms. While Russia takes on a 'closed' approach to sovereignty (Ristolainen 2017, 114) by emphasising the principle of non-intervention and the sovereign authority of the state in the protection of its information space, the EU takes on a more 'open' approach. As it departs from the idea of the need for collective actions to achieve a secure and resilient cyberspace, the EU appears to take on a both inward- and outward-looking position to the development of its normative framework in cyberspace. In policy development, it aims to take on the role of a norm entrepreneur by promoting its norms outside the borders of the Union.

What impact does this move towards to the securitisation of Internet Infrastructure have on the EU and Russian stance on global internet governance? This article aims to uncover how the logic of securitisation impacts the stances in both cases on management and regulation of the internet infrastructure. To do this, the article zooms in on the development of their respective understanding of key concepts impacting the logic behind cybersecurity strategy, and more specifically the security of internet infrastructure. For the purpose of this article, internet infrastructure is defined as the collection of physical (routers, cables, IXPs and ISPs, etc.) and virtual (online navigation tools, search engines and protocols, etc.) resources that make networked communication and the transmission of data possible. The point of focus of this article follows Laura DeNardis and Francesca Musiani (2016, 4), who study the term within the scope of their thesis of a turn towards internet governance by infrastructure, which takes into account the impact of 'the ecosystem of institutions, laws and private ordering' of the infrastructure on modes of internet governance. The main guiding elements are definitions of, and approaches towards, information security and cybersecurity on the internet in general and the impact of this logic on the EU and Russian stances on internet governance. The article starts from the hypothesis that in both cases the following tendencies are present in their approach towards this issue: a greater focus on the securitisation of the internet infrastructure and the need for greater independence of national or regional segments of the internet from foreign control. It is the purpose of this article to outline how these tendencies impact upon the formulation of cyber policy, creating two different approaches to internet infrastructure protection.

The securitisation of internet infrastructure

This article contributes to the framework of the Copenhagen School on securitisation (Buzan, Waever, and de Wilde 1998). The idea behind securitisation is that 'an issue is given sufficient saliency to win the assent of the audience, which enables those who are authorised to handle the issue to use whatever means they deem most appropriate' (Balzacq, Léonard, and Ruzicka 2016, 494). The application of the securitisation framework

to the online information space is increasingly relevant as recognition is growing that cybersecurity goes 'beyond a mere technical conception of computer security, when proponents urged that threats arising from digital technologies could have devastating social effects' (Hansen and Nissenbaum 2009, 1155).

Furthermore, debate in the international community is increasing on how to approach the development of a normative framework regulating and outlining the parameters for state behaviour and responsibility in cyberspace. Because of this, actors engage in the 'strategic construction of norms', by leveraging already established convergences of interests and identities to attract other actors to its normative frame (Kurowska 2019, 6). Security arguments are leveraged in relation to both the issuing of domestic legislation aimed at securing and managing internet infrastructure, as well as in debates within international organisations such as the UN. For states like Russia, which emphasise the primacy of state sovereignty, linking sovereignty arguments with security threats forms a useful instrument, as 'threats to sovereignty provide the state with an institutional interest to temporarily subordinate the interests of its citizens to its own, under the assumption that its functions are irreplaceable' (Van Veen 2007, 14). Since the international stance on the development of a normative framework to approach internet governance constitutes an influential element in the construction of the domestic approaches of both the EU and Russia, it is necessary to look into the development of internet governance since its inception as a commercial medium in 1991. This part will give an overview of the roots of discussions on internet governance, namely: (1) the allocation of domain names; and (2) the dominant role of the US in the regulation and management of internet governance.

The advent of the internet in the 1990s as a globally used communication and information medium gave way to discussions of how its infrastructure and content should be managed and regulated. Prior to its commercialisation and the democratisation of its usage, internet regulation rested on ad hoc solutions mostly initiated by private actors and the expert community. In this framework, the philosophy that the medium should be self-regulated prevailed (Radu, Chenou, and Weber 2014, 4). This was expressed in the creation of the International Ad Hoc Committee (IAHC), which brought together members of IANA, the Internet Society, the IAB, the National Science Foundation, the World Intellectual Property Foundation and the ITU. The IAHC recognised the need to bring together all the 'stakeholders' in the development of the internet (Internet Society 1996). This organisation focused mainly on the allocation of domain names and presented the self-regulatory principle as being advantageous, seeing as 'the current and future Internet name space stakeholders can benefit most from a self-regulatory and market-oriented approach to Internet domain name registration services' (The Internet Community 1997). However, the implementation of the IAHC memorandum of understanding for the Internet Community was short-lived due to the creation of ICANN in 1998, which took responsibility over the functions put forward in the memorandum (Radu, Chenou, and Weber 2014, 5). The idea of a self-regulatory system of internet governance rests on the view that the internet architecture and infrastructure itself does not allow for a top-down regulation. In this way the internet's freedom is viewed as having been 'engineered into its protocols' (Mueller 2010, 2).

Apart from the issue of state control, another seminal point of debate in internet governance is the perception of the dominant role played by the United States. The basis of

this discussion is mostly centred on the statute of ICANN, one of the only institutions in global internet governance which was originally contracted under the US Department of Commerce (Christou 2016, 37). It performs the crucial roles of allocating IP numbers and domain names, managing the registry of domain names, and allocating top-level domains (TLDs) to local registries. Due to strategic and commercial interests tied to the allocation of adequate domain names, the implications of one actor dominating the process are a continual point of debate.

Both issues came to the fore with a resolution presented to the UN by Russia in 1998 on the 'Developments in the sphere of informatisation and telecommunication in the context of international security' (UN GA 1998). The main point put forward was the need for enhancing the role of states in the face of 'the potential use of these [information] technologies and resources for aims that are not compatible with ensuring international stability and security, and which can negatively influence the security of states' (Idem).

Partly because of this resolution, the WSIS summit was put into place under the auspices of the ITU and set out to 'coordinate with other international organisations and with the various partners concerned'.[1] As Milton Mueller (2010, 55) argues, the WSIS process highlighted the division between two models of global internet governance: (1) based on agreements between sovereign, territorial states, with the internet portrayed as a national resource falling under the category of information and telecommunications technology; (2) based on private contracting among transnational non-state actors, but relying in some respect on the global hegemony of a single state.

However, in the current context of state actors claiming a bigger role in internet governance, as well as a growing focus on achieving a sufficient degree of technological autonomy to ensure the security and resilience of their respective information spaces, the second model of internet governance put forward by Milton Mueller (2010, 55) is called into question. Under the influence of a growing number of threats in cyberspace and the widening of the meaning of cybersecurity to include not only 'insecurities related to networked computers', but also 'threats arising from digital technologies that could have devastating social effect' (Hansen and Nissenbaum 2009, 1155), the tension between both governance models has intensified. Furthermore, as states are turning towards regulation of internet infrastructure in view of these rising challenges, the limits and boundaries of state sovereignty in the online information space are increasingly called into question. The nature of these growing tensions will be explored further in the cases of Russia and the EU.

Russia: internet governance in the context of information confrontation

To determine the logic behind Russia's securitisation of the internet infrastructure, it is first essential to go into an overview of its definition of *information* and the *information space*. This is all the more relevant since, as Natalya Kovaleva (2018, 134) points out, most of the focus is on the way Russia uses new technologies to its advantage 'to challenge democratic values', while there has been a very 'limited inquiry into the ways in which the Kremlin attempts to control its own information space'. This is key, since the fact that Russian authorities approach the online information space from the point of view of it belonging in the sphere of 'physical territoriality' has a significant impact on policymaking decisions. Because of this, it attaches the concept of state sovereignty and territorial

integrity quite closely to the regulation of the information space (Kovaleva 2018, 141–142). Efforts within this context have resulted in the accentuation by Russia of the primacy of principles of international law relating to sovereignty, among which is the principle of non-intervention, to be upheld and applied to the online information space (Nocetti 2015, 112). Domestically, this is expressed in the belief in the authority and responsibility of the state to ensure that the information space respects 'the stability of the constitutional order, sovereignty, and the territorial integrity of the Russian political, economic and social stability in the unconditional provision of law and order and the development of equal and mutually beneficial international cooperation' (Doctrine for Information Security 2000).

Another factor that influences policy formation is the fact that the word *information* in the context of information warfare or information operations is used to include both the communication component and the technological component of security in the information space and in cyberspace. A good example of this dual use of the term 'information' is present in the broad definition of 'information space' in the Doctrine for Information Security (2016):

> The information space is understood as the conglomerate of information, objects of informatisation, information systems, sites on the information and telecommunication network of the "Internet", networks, information technologies, and subjects, the activity of which is linked to the formation and processing of information, the development and use of the aforementioned technologies, the ensuring of information security, as well as the collection of mechanisms regulating the corresponding societal relations.

The implication of this broad definition allows for the circumvention of the division between the 'information space' (relating to communication dissemination and reception) and 'cyberspace' (encompassing all physical and non-physical components used to store, modify and exchange data using computer networks [Schmidt 2013]). The fact that the word 'cyber' (kiber) is not used anywhere in the Doctrine for Information Security is another testament to the all-encompassing definition of information security as both relating to 'information-psychological' security and 'information-technological' security. The flexible use of this term is important since it has a significant hand in the muddling of the term *information warfare*. Russian, unlike Western, thinking does not make a distinction between *cyber-* and *information warfare* (Giles 2016, 9).

Threats to information security from the Russian perspective are not limited to threats emanating from the content of online communication, but also include threats to the systems and the infrastructure used to disseminate this content. The broad use of the concept of *information operations* to include both the technological and psychological component also allows for the listing of a broad range of military tools to be used in this sphere. This line of reasoning is present in contemporary Russian military thinking which puts the emphasis of military action on non-military, indirect and asymmetric measures aimed first and foremost at capturing the hearts and minds of the population of the target state (Gerasimov 2013; Chekinov and Bogdanov 2013).

This logic of the need to protect information technology tools and simultaneously to use them to their advantage is not limited to military circles in Russia but is present across different policy fields. This is evident in the *Foreign Policy Concept* of the Russian Federation (2016), in which information security is put forward as one of the policy priorities to 'counteract threats connected to the use of information-communication

technologies and impede their use for military-political purposes' (Idem), while at the same time focusing on the 'development of own effective resources of information influencing on public opinion abroad' (Idem).

Another example of this is the contribution of Irina Yarovaya[2] to the Moscow Conference on International Security in 2017, where she listed several characteristics of the contemporary information space:

> It is global, it's universal, but it doesn't have any legal regulation, it completely violates sovereignty and, in fact, today information weapons are weapons of mass destruction. When we talk about influence on the conscience of a person, as a carrier of civil rights and freedoms, a carrier of that same sovereignty that ensures the sovereign security of every country, the information space today is not just vulnerable, but unprotected by international accords and treaties. (Yarovaya 2017)

The push for more governmental oversight in internet governance has resulted in several moves to regulate and centralise control over internet infrastructure on the domestic front, as well as an increasingly assertive stance in the international arena. Domestically, the evolution towards centralising control over internet resources has been ongoing since 2011. Before this, Russian authorities, in their creation of internet controls, opted to focus on legal and normative pressures in combination with technical surveillance equipment that enable the control of and access to information resources (Deibert and Rohozinski 2010, 7). This type of second and third generation controls were not aimed as much at filtering information outright, as they were at shaping and affecting 'when and how information is received by users' (Idem, 16). Until the Ukraine crisis began in 2013, the use of measures related to technical capabilities was limited to the three different versions of SORM equipment with the first one adopted in 1995 already (Konradova and Schmidt 2014), the most recent of which is used to collect information on internet traffic as well as the storage of user data and communication over the internet for up to six months (Minkomsvyaz 2018). The first real regulating measures on content came after the Bolotnaia revolution in 2012. This legislation was mostly aimed at the regulation of content and the establishment of a moral code of conduct on the Russian internet with the installation of the law on the protection of children against harmful information (Russian State Duma 2011) and the law against insulting religious beliefs (Russian State Duma 2013).

A break in Russia's style of regulation and control can be found after the Snowden revelations in 2013 and certainly in the wake of the crisis in Ukraine in 2014. These events preceded the rising tensions with the West that found a focal point in mutual accusations of information operations and cybersecurity threats. With the installation of a new Doctrine for Information Security in 2016 and an increased focus on information and cybersecurity in other policy documents, the issue of restructuring the internet infrastructure to allow for a more direct control of internet traffic in Russia came to the fore. Testament to this were the first large-scale joint exercises by the Ministry of Communication, the Ministry of Defence and the FSB aimed at the 'protection of the Russian segment of the Internet' (Minkomsvyaz 2014), the results of which constitute the basis for the current law on the autonomous Runet. Another significant example is the installation of the Yarovaya package in 2016 (Russian State Duma 2016), that ambitiously requires ISPs to save data to up to six months. This new generation of internet laws shows a break with the previous

wave in 2011–2013 with the former focusing mainly on content regulation on moral grounds and the latter taking a turn towards the co-optation of internet infrastructure to fulfil political aims (Ermoshina and Musiani 2017, 43).

Another development in this area is Russia's growing focus on the 'import substitution of ICT products' for its own national products. To this effect, a law was introduced on the 'preference for Russian operating systems in public procurement' (Russian State Duma 2015). The rationale behind this was explained by Putin in 2015:

> We have been witnesses of the fact, that our competitors, opponents, use their advantages, use our carelessness and, you could say, our gullibility, as well as contemporary forms of influencing with political aims, in a political struggle. Of course, we have to think about this, and we do think about this. And it's not even about these restrictions and sanctions, that we often talk about now. It is about the fact that we have to implement our own software products, and so-called 'iron'[3] (hardware) for our own high-tech development. (Putin 2015)

These domestic developments on the internet regulation front can also be linked to the international level. As Julien Nocetti (2015, 115) argues, 'the Russian government's approach to the Internet looks simultaneously 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 policymaking in this sphere'. This is exemplified by the fact that Russia, since the end of the 1990s, has been both active and vocal in global internet governance. The importance attached by Russia to security assurances in the information space on the basis of international law is present in its first resolution put to the UN on information security in 1998 (UN 1998). This resolution expressed the concern 'that these technologies and resources can potentially be used for purposes inconsistent with the objectives of international stability and security and may have a negative impact on the security of states' (Idem).

Russia's subsequent proposals to the UN have followed this line of thinking. Examples are efforts initiated by Russia and China within the framework of the SCO to issue a code of conduct for the information space with letters in 2011 and 2015. The language in this code of conduct (UN GA 2015) points to the interpretation of interventions in the information space as incursions on the 'territorial integrity' and sovereignty of states, essentially putting up virtual borders for their 'national information space' (Idem). Using *telecommunications* to refer to the internet implies that it is characterised as a national resource since telecommunication infrastructure in the traditional sense is, in most cases at least, partially state-owned (Cogburn 2016, 32). The same issue exists with Russia's insistence on giving the ITU (International Telecommunications Union) recognition as the international organisation dealing with the internet. Furthermore, discourse emphasising the primacy of the protection of state sovereignty is reflected in Russia's argumentation in these proposals to the United Nations, which can be exemplified by its push towards the creation of an Open Ended Working Group (OEWG) to be open to all interested parties, as opposed to the UN GGE, which is only open to 25 member states. This proposal was made within the framework of Russia's introduction of its 13 cyber norms to provide 'traffic rules' in the information sphere (MID 2018). In Russia's explanatory communication on the website of the Ministry of Foreign Affairs, the primacy of state sovereignty was put forward as one of the main principles enshrined in this text (MID 2018), as states 'have a primary

responsibility for maintaining a secure and peaceful information and communications technology environment' (UN 2018).

As this overview showed, the logic of securitisation has been a consistent element in thinking in Russian policy circles on the internet and the management and regulation of its infrastructure, both domestically and globally. Both in the domestic and the international approach, principles of sovereignty were invoked in the argumentation on the creation of policy aiming at centralising control of internet infrastructure. While Russia's approach to internet governance has been shut down regularly in the international arena, the blurring of information security and cybersecurity issues seems to be gaining in effect across the board. In the next section we explore whether this development takes place in EU internet governance as well.

EU: resilience building in the information- and cyberspace

In comparison to the Russian case, the EU's initial approach towards internet governance was not so infused with the need for the securitisation of this space. As Myriam Dunn Cavelty (2018, 312) notes, the issue of security in the EU's approach to internet governance only came to the fore properly after the cyberattacks on Estonia in 2007. Before this, the main point of focus was rather to stimulate and secure the development of the Information Society in Europe (idem). This point is exemplified by the 1994 Action Plan for the Information Society, which was created on the basis of an atmosphere of optimism towards the advantages that the use of this new information technology presented in developing a knowledge-based 'information society' (European Commission 1994).

This point was reinforced by the 2000 Lisbon Council conclusions, which reiterated the idea of an 'information society for all' with a focus on how to use the internet to its full potential in view of economic development (European Parliament 2000). While the atmosphere of optimism about the potential of the new information technology was prevalent, the need to set 'new rules of the game' (European Commission 1994) in view of these developments came to the fore in the Action Plan for the Information Society (1994). More specifically, the Action Plan urges for the creation of new legislative initiatives, as well as better resource allocation for the development of the information society. This was all the more poignant in view of the 'race going on at the global level, notably by the US and Japan', seeing as 'Those countries, which will adapt themselves most readily will de facto set technological standards for those who follow. It also underlines the global nature and calls for proper coordination mechanisms and the advancement of international negotiations' (European Commission 1994).

The EU's role in internet governance was focused on a global effort at tackling the difficulties associated with the deployment of the information society and the commercialisation of the internet. In tackling these problems, it highlighted the role of the private sector in the 'rapid establishment of a clear and stable regulatory framework, notably with regards to market access, intellectual property rights, data protection and copyright' (European Commission 1994). This focus on the need to include the private sector in policy formation is an example of the EU's early stance on how to approach problems of internet governance. This can be illustrated as well by the role played by the European Union regarding the status of ICANN. From its creation in 1998, the establishment of ICANN to oversee the allocation of domain names and numbers, triggered a discussion on the

role of governments in this organisation. Seeing as this institution was set up as a US-based private non-profit corporation under the auspices of the US Department of Commerce, this implied that ICANN was 'contractually and politically beholden to the US government' (Mueller 2010, 61–62).

While the US maintained a supervisory role over this organisation, other governments and intergovernmental organisations, such as the EU, were relegated to an advisory role in a 'Governmental Advisory Committee' (Christou and Simpson 2007, 154). It is not surprising that initiatives of the EU regarding ICANN were aimed primarily at internationalising the institution by advocating for a bigger role of the GAC. In doing so, the EU emphasised the 'need to create a public-private sector partnership' (Christou and Simpson 2007, 157). This implied a shift from self-regulation of the internet by non-state actors under supervision of the US, to more co-regulatory (partnership) practices (Idem). The discussion on the role of the GAC in ICANN reached a key turning point during the WSIS process (2003–2005), in which the EU actively called for cooperation based on the multistakeholder model under global oversight, where the role of the US government is diminished to an advisory role within the GAC together with other governmental actors (Klimburg 2011, 9; Mueller 2010, 74–75) This first discussion on the nature and statute of ICANN was an important step in the EU's formation of its stance within global internet governance, which was expressed in the conclusion of the EU's contribution to WSIS 2006:

> The EU believes that a new cooperation model is needed in order to give substance to the provisions in the WSIS Declaration of Principles regarding the crucial role of all stakeholders within Internet governance, including governments, the private sector, civil society and international organisations. Existing Internet governance mechanisms should be founded on a more solid democratic, transparent and multilateral basis, with a stronger emphasis on the public policy interest of all governments. (European Commission 2006a)

The main driver for the EU's advocating for an internationalised status for ICANN was the establishment of the institution as an independent organisation, based on a multistakeholder model and the *equal* advisory role of all states in the GAC (Christou and Simpson 2007, 161). Cybersecurity issues were mostly addressed in view of the use of the internet as an economic infrastructure, where 'current threats are now motivated by profit rather than "fame"' (European Commission 2006b), with threats aimed mostly at industry and enterprises, as well as individual users (identity theft and credit card fraud).

The catalyst that brought cybersecurity forward as a priority in EU internet policy, as well as imbuing the EU with a sense of urgency to take concrete steps towards the creation of comprehensive common efforts across all EU member states, was, as mentioned earlier, the cyberattacks on Estonia in 2007 (Christou 2019, 285). Following the removal of a Soviet war memorial from a park in Tallinn, the three-week-long attack featured distributed denial of service (DDoS) assaults involving botnets of computers against governmental, banking, media and political party websites in Estonia (Kaiser 2015, 11). Due to the societal and political impact of the attack on Estonian day-to-day life, the issue of cybersecurity captured the full attention of the global security policy community (Tikk 2010, 109).

The cyberattacks on Estonia and Georgia led to some essential changes in the EU approach towards cybersecurity and internet governance. Firstly, the need for a common framework to organise Critical Information Infrastructure Protection (CIIP) was put forward, seeing as 'simple experiments are now turning into sophisticated activities

performed for profit or political reasons' (European Commission 2009a). Critical Information Infrastructure (CII) was defined as 'ICT systems that are critical infrastructures for themselves or that are essential for the operation of Critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)' (European Council 2008). Because of this rather broad definition of what constitutes a CII, the identification of the CIIs present is a key factor in CIIP (European Commission 2009a). The implication of the characterisation of the internet infrastructure as a part of the CIIP is that its protection and security became a politicised issue spanning several different policy issue areas, among which are the financial sector as well as areas relating to the societal and political stability of member states and the Union. This was reflected in the 2011 follow-up document entitled 'On Critical Information Infrastructure Protection – achievements and next steps: towards global cyber-security' (European Commission 2011):

> New and technologically more sophisticated threats have emerged. Their global geo-political dimension is becoming progressively clearer. We are witnessing a trend towards using ICT for political, economic and military predominance, including through offensive capabilities. 'Cyber-warfare' or 'cyber-terrorism' are sometimes mentioned in this context. (Idem, 3)

The second change is regarding the EU stance towards the public-private partnership in internet governance. The definition of the internet as a critical resource and infrastructure implies greater involvement of governments in the regulation and management of this resource. As the 2009 document on 'Next steps in Internet governance' states, while the day-to-day management of the internet should be left to private-sector leadership,

> non-governmental stakeholders must recognise that Internet users world-wide […] have a legitimate expectation that their governments will guarantee that any current or future governance arrangements will reflect the public interest of society as a whole and will not be subject to capture by narrow commercial or regional interests. (European Commission 2009b)

A recent change in EU policy towards Internet governance was the call for a more active approach in the creation of norms in the international arena. As made clear in both documents detailed above, challenges posed by threats in cyberspace should be addressed with common efforts, not only across member states, but also across the world. This was put forward in the 2012 European Parliament resolution 'On Critical Information Infrastructure Protection':

> [The European Parliament] recalls that international cooperation is the core instrument for introducing effective cyber-security measures; recognises that at present the EU is not actively involved on an ongoing basis in international cooperation processes and dialogues relating to cyber-security; calls on the Commission and the European External Action Service (EEAS) to start a constructive dialogue with all like-minded countries with a view to developing a common understanding and policies with the aim of increasing the resilience of the internet and of critical infrastructure; maintains that, at the same time, the EU should, on a permanent basis, include internet security issues in the scope of its external relations, inter alia when designing various financing instruments or when committing to international agreements which involve the exchange and storage of sensitive data

These three changes were further built upon in the 2013 Cybersecurity Strategy by clarifying the EU approach towards the protection of the internet. Firstly, in the formulation of principles for cybersecurity, the tension is addressed between the growth in importance of the internet and the fact that limited to no governmental oversight or regulation was

given (European Commission 2013). In this vein, the creation of a comprehensive cybersecurity strategy across member states on the EU level in the development of cyber-defence policy is promoted, which would be expressed in the context of the future NIS directive (European Parliament and European Council 2016). This directive pays special attention to the need for setting minimum requirements regarding the reporting across member states and industries of cyberthreats, so that rapid action can be undertaken (Idem).

An added element in the 2013 Cybersecurity Strategy is the necessity of protecting the 'same norms, principles and values that the EU upholds offline' (European Commission 2013) in the online sphere, namely 'fundamental rights, democracy and the rule of law' (Idem). The presentation of the protection of these principles comes in the context of the perception of the Arab Spring as one of the examples where the internet 'provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies' (Idem). At the same time, another contradictory element added at this time was the need for the development of the EU's own industrial and technological resources for cybersecurity to address the 'risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers' (Idem). Both elements can be framed within the context of the rising stake of states in maintaining social and political stability, not only within geographical borders, but within the transnational framework of the global internet. Within this framework, greater self-sufficiency in the development and use of ICT systems, as well as wider recognition of the European principles regarding internet governance, further aids in the creation of a resilient and stable *information society*.

On a foreign policy level as well, the EU has taken a more active role within the creation of a common international normative framework. Within this context, the EU has taken on a stance that emphasises the need for shared norms and values in cyberspace as a basis on which to build network resilience. As is put forward in the EU's *Cybersecurity Strategy*: 'cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union' (European Commission 2013). This point on the need to apply 'the same norms, principles and values that the EU upholds offline to the online', namely 'fundamental rights, democracy and the rule of law', (Idem) is reiterated by the EU in its 2017 Joint Communication on *Resilience, Deterrence and Defence*. In this document it is stated that 'as a complement to International law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts' (European Commission 2017). Additionally, the point is put forward about the need for further development of 'cyber dialogues' to be 'complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace' (Idem). However, Xymena Kurowska (2019, 12) makes the point that this position reflects a 'repertoire of normative power Europe', in which the EU takes on the responsibility of knowledge and expertise dissemination on the implementation of cyber norms as well as fostering and promoting their implementation without full recognition that all UN member states should contribute to the process. The potential of the EU to be an influential norm setter is definitely there, as it has made some significant strides to ensure the resilience and security of its internet infrastructure through measures such as the GDPR, which provides rules for the transfer of data of EU citizens, as well as a legislative basis to ensure citizens' privacy (EU Parliament and European Council

2016a) and the NIS directive, which provides a framework for concerted efforts to report, and communicate about, cyberattacks between member states (European Parliament and European Council 2016b). However, as the EU is increasingly taking on the role of norm-maker or 'forward-looking cyber player' (European Union 2016, 42) in cyberspace and internet governance, this inward-outward position, in which norms are made to fit the EU situation and later promoted abroad, needs to be reflected upon carefully. As there is increasing recognition by the EU of the need to ensure 'strategic autonomy' or, as it is more recently being called, 'technological sovereignty' in cyberspace, it becomes increasingly difficult to balance an 'open' approach towards sovereignty in cyberspace with putting forward a normative and legislative framework impacting upon existing internet infrastructure if third parties don't agree to implement these norms.

Conclusion

This article has provided a look into the respective stances on internet governance of Russia and the EU and the increased importance of internet infrastructure in this context. In both cases, the logic and pivotal events behind their respective shift towards increasing securitisation rhetoric were explored. As challenges towards the resilience of internet infrastructure are coming under increasing public scrutiny both the EU and Russia appear to put more emphasis on the responsibility of states to play a greater role in internet governance.

In the Russian case, this article has delved deeper into the impact of the dual meaning of *information,* in a technological sense and a communication sense, on its approach to internet governance. The point was made that even though the Russian policy of the last five years seems to have taken a more assertive turn towards the use and regulation of the internet infrastructure, its approach towards this medium as a matter of national, regional and international security has featured in a consistent evolution from its commercialisation in Russia in 1994 until now. The heightened tension with the West and the EU is reflected in the recent implementation of this framework of thought that has been under development since the beginning of the 2000s. Arguments underpinning this logic of securitisation seem to continually turn towards the use of sovereignty principles in international law, such as the principle of non-interference and territorial integrity. Taking on the perspective that the online information space is tied to the principle of territoriality (Kovaleva 2018, 141–142), Russia's approach towards centralising control over internet infrastructure domestically appears to be reinforced by its stance on the primacy of the state in international internet governance.

When looking at the EU, the overview of the documents given above seems to show a shift in the EU approach towards internet governance and infrastructure. This is expressed in a move towards a more inward-looking approach, in areas where considerations of cybersecurity seem to have the upper hand. The pivotal moments in this respect can be linked to perceptions of Russian aggression in cyberspace, among which are the 2007–2008 cyberattacks against Estonia and Georgia, the more recent hybrid warfare strategies used in the conflict in Ukraine in 2014 and the rising tension over the increase in disinformation campaigns and use of strategic communication. However, the EU's approach towards the issue of state responsibility in this respect differs fundamentally from the Russian approach. Whilst advocating for more autonomy in cyberspace as well as a form of technological sovereignty, the EU takes on an approach that is both inward- and outward-looking. As it takes on the role of norm entrepreneur, both within and

without the borders of the Union, it puts forward the aim to set both political and legal precedents on how to best manage and regulate the internet.

Notes

1. *Resolution 73 of the ITU Plenipotentiary Conference Minneapolis 1998,* WSIS.
2. Irina Yarovaya is the Deputy Chairwoman to the Russian State Duma and was also the initiator of a package of anti-terrorism laws, which obliged ISPs to save personal data of citizens for up to six months. This package of laws was later dubbed the 'Yarovaya Package'.
3. Iron or 'zhelezo' in Russian is used as a term for 'hardware'. The quotation marks around the word 'zhelezo' were also present in the original quote by Vladimir Putin.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Eva Claessen is a PhD researcher in Russia studies at the Leuven Centre for Global Governance Studies (GGS). Her research is situated within the framework of the project CONNECTIVITY, which focuses on how differences between prominent states' conceptualisation of international norms impact upon cooperation in the international system. The aim of CONNECTIVITY is to generate novel insights into how international cooperation may be fostered amidst the crisis of the current global order. In this context her research aims to identify the mode and logic behind Russia's contestation in the area of the governance of the information space. To do this, she studies the impact of Russian perceptions of international norms and values on its approach towards Internet governance and cybersecurity on a national, regional and international level.

References

Balzacq, T., S. Léonard, and J. Ruzicka. 2016. "'Securitization' Revisited: Theory and Cases." *International Relations* 30 (4): 494–531.

Buzan, B., O. Waever, and J. de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Rien.

Cavelty, M. D. 2018. "Europe's Cyber-Power." *European Politics and Society* 19 (3): 304–320.

Chekinov, S. G., and S. A. Bogdanov. 2013. "The Nature and Content of a New-Generation War." *Military Thought* 10: 12–23.

Christou, G. 2016. *Cybersecurity in the EU: Resilience and Adaptability in Governance Policy*. New York: Palgrave Macmillan.

Christou, G. 2019. "The Collective Securitisation of Cyberspace in the European Union." *West European Politics* 42 (2): 278–301.

Christou, G., and S. Simpson. 2007. "Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation." *European Journal of Communication* 22 (2): 147–164.

Cogburn, D. L. 2016. "The Multiple Logics of Post-Snowden Restructuring of Internet Governance." In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, 25–46. New York: Palgrave MacMillan.

Deibert, R., and R. Rohozinski. 2010. "Control and Subversion in Russian Cyberspace." In *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*, edited by J. Zittrain, R. Deibert, R. Rohozinski, and J. Palfrey, 16–34. Massachusetts: The MIT Press.

DeNardis, L., and F. Musiani. 2016. "Governance by Infrastructure." In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, 3–24. New York: Palgrave MacMillan.

Doctrine for Information Security. 2000. *Novaya Gazeta*. http://www.ng.ru/politics/2000-09-15/0_infodoctrine.html.
Doctrine for Information Security. 2016. *Rossijskaja Gazeta*. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.
Ermoshina, K., and F. Musiani. 2017. "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era." *Media and Communication* 5 (1): 42–53.
European Commission. 1994. *Europe's Way to the Information Society: An Action Plan*. Publications office of the EU. https://op.europa.eu/en/publication-detail/-/publication/deed9eb9-0b6e-11e4-a7d0-01aa75ed71a1/.
European Commission. 2006a. *Towards a Global Partnership in the Information Society: The Contribution of the EU to the Second Phase of the World Summit on the Information Society (WSIS)*. EUR-Lex. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0181:FIN:EN:HTML.
European Commission. 2006b. *A Strategy for a Secure Information Society – "Dialogue, Partnership and Empowerment"*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&from=EN.
European Commission. 2009a. *Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience*. EUR-Lex. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149.
European Commission. 2009b. *Internet Governance – The Next Steps*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0277.
European Commission. 2011. *On Critical Information Protection – 'Achievements and Next Steps: Towards Global Cyber-Security*. EUR-Lex. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF.
European Commission. 2013. *Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*. EEAS. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
European Commission. 2017. *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450.
European Commission. 2019. *The von der Leyen Commission: For a Union That Strives for More*. European Commission Press Release Database. https://europa.eu/rapid/press-release_IP-19-5542_en.htm.
European Council. 2008. *On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG.
European Parliament. 2000. *Lisbon European Council 23 and 24 March 2000, Presidency Conclusions*. European Parliament. http://www.europarl.europa.eu/summits/lis1_en.htm.
European Parliament. 2012. *On Critical Information Infrastructure Protection – Achievements and Next Steps: Towards Global Cyber-Security*. European Parliament. https://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167.
European Parliament & European Council. 2016a. *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
European Parliament and European Council. 2016b. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
European Union. 2016. *Shared Vision, Common Action: a Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. EEAS. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
Gerasimov, V. 2013. "The Value of Science Is Its Foresight: New Challenges Require a Rethinking of the Forms and Means of Warfare." *Voenno-Promyshlennyj Kur'er*. https://www.vpk-news.ru/articles/14632.
Giles, K. 2016. *Handbook of Russian Information Warfare*. Rome: NATO Defense College.

Government of the Russian Federation. 2019a. *On the Approval of the Rules to Implement a Register for Internet Exchange Points*. Gosudarstvennaya Sistema Pravovoj Informatsii. http://publication.pravo.gov.ru/Document/View/0001201910210026?index=0&rangeSize=1.

Government of the Russian Federation. 2019b. *On the Approval of the Regulations on Conducting Exercises to Ensure the Sustainable, Safe and Comprehensive Functioning of the Internet and the Public Communications Network in the Russian Federation*. Gosudarstvennaya Sistema Pravovoj Informatsii. http://publication.pravo.gov.ru/Document/View/0001201910210025.

Hansen, L., and H. Nissenbaum. 2009. "Digital Disaster, Cyber Security and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155–1175.

Internet Society. 1996. *Formation of International Ad Hoc Committee (IAHC)*. https://www.internetsociety.org/history-timeline/formation-of-international-ad-hoc-committee-iahc/.

Kaiser, R. 2015. "The Birth of Cyberwar." *Political Geography* 46: 11–20.

Klimburg, A. 2011. "Ruling the Domain: (Self)Regulation and the Security of the Internet." Paper distributed at the 11th meeting of the ICANN Studienkreis.

Konradova, N., and H. Schmidt. 2014. "From the Utopia of Autonomy to a Political Battlefield: Towards a History of the Russian Internet." In *Digital Russia: The Language, Culture and Politics of New Media Communication*, edited by M. Gorham, I. Lunde, and M. Paulsen, 72–104. New York: Routledge.

Kovaleva, N. 2018. "Russian Information Space, Russian Scholarship and Kremlin Controls." *Defence Strategic Communications* 4: 133–171.

Kurowska, X. 2019. "The Politics of Cyber Norms: Beyond Norm Construction towards Strategic Narrative Contestation." *EU Cyber Direct: Research in Focus.* p. 18.

Maurer, T., I. Skierka, R. Morgus, and M. Hohmann. 2015. "Technological Sovereignty: Missing the Point?". In *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. Tallinn: NATO CCD COE Publications.

MID. 2018. *O prinyatii Genassambleej OON rossijskoj rezolyutsii po mezhdunarodnoj informatsionnoj bezopasnosti. Ministerstvo Innostrannych Del' Rossijskoj Federatsii* [On the Approval by the General Assembly of the UN of the Russian Resolution on International Information Security]. http://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3437775.

Minkomsvyaz. 2014. *The Ministry of Communication, the FSB and the Ministry of Defence Have Done Exercises for the Protection of the Russian Segment of the Internet*. https://digital.gov.ru/ru/events/31441/.

Minkomsvyaz. 2018. *Requirements to the Equipment and Soft- and Hardware Used by the Organizer of the Distribution of Information on the Internet in the Information Systems Operated by Him to Conduct Operational-Search Activities by the Authorized State Bodies to Ensure the Safety of the Russian Federation and to Implement Measures to Achieve the Goals Outlined in the Tasks Assigned to Them*. MFISoft. https://www.mfisoft.ru/upload/iblock/1f9/1f9d8d2ff9df2de804fb607d3c866da0.pdf.

Mueller, M. L. 2010. *Networks and States*. London: MIT Press.

Mueller, M. L. 2017. "Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings." *Digital Policy* 19 (6): 415–428.

Musiani, F., D. L. Cogburn, L. DeNardis, and N. S. Levinson. 2016. *The Turn to Infrastructure in Internet Governance*. New York: Palgrave MacMillan.

NATO. 2016. *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Nocetti, J. 2015. "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy." *Internet Policy Review* 4 (4): 1–19.

Putin, V. V. 2015. "Molodyezhnyj forum 'territoriya smyslov na klyazme.'" *Prezident Rossii*. http://kremlin.ru/events/president/news/49985.

Radu, R., J. M. Chenou, and R. H. Weber. 2014. *The Evolution of Global Internet Governance*. Berlin Heidelberg: Springer.

Ristolainen, M. 2017. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security within Russia and the West." *Journal of Information Warfare* 16 (4): 113–131.

Russian State Duma. 2011. *On the Implementation of Changes in Certain Legislative Acts of the Russian Federation Regarding the Adoption of the Federal Law "on the Protection of Children against*

Information That Is Harmful for Their Health and Development." Gosudarstvennaya Sistema Pravovoj Informatsii. http://pravo.gov.ru/proxy/ips/?docbody=&nd=102149554.

Russian State Duma. 2013. *On the Implementation of Amendments to Article 148 of the Criminal Code and to Certain Legislative Acts of the Russian Federation to Counter the Insult of Religious Beliefs and Feelings of Citizens*. Rossijskaya Gazeta. https://rg.ru/2013/06/30/zashita-site-dok.html.

Russian State Duma. 2015. *On the Introduction of Changes into the Law "on Information, Information Technologies and on the Protection of Information" and to Article 14 of the Federal Law "on the Contract System in the Area of Purchase of Products, Works and Services for Ensuring State and Municipal Needs"*. Konsultant. http://www.consultant.ru/document/cons_doc_LAW_144624/2c1e3551b4209a9fa5744534f7525ac7430624eb/.

Russian State Duma. 2016. *On the Introduction of Changes into the Federal Law "on Counteracting Terrorism" and Separate Legislative Acts of the Russian Federation Establishment of Additional Measures to Combat Terrorism and Ensure Public Safety*. Gosudarstvennaya Sistema Pravovoj Informatsii. http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102404066.

Russian State Duma. 2019. *On the Introduction of Changes into the Law on Information, Information Technologies and on the Protection of Information*. Gosudarstvennaya Sistema Pravovoj Informatsii. publication.pravo.gov.ru/Document/View/0001201905010025.

Schmidt, M. N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press.

The Internet Community. 1997. *Establishment of a Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU)*. http://web.archive.org/web/19971211190257/http://www.gtld-mou.org/gTLD-MoU.html.

Tikk, E. 2010. "Global Cybersecurity – Thinking about the Niche for NATO." *SAIS Review* 30 (2): 105–119.

UN GA. 1998. *Resolution Adopted by the General Assembly: A/RES/53/70. Developments in the Field of Information and Telecommunications in the context of international security*. UN. https://undocs.org/A/RES/53/70.

UN GA. 2015. *Developments in the Field of Information and Telecommunications in the Context of International Security (A/69/723). Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General*. UN. https://undocs.org/A/69/723.

UN GA. 2018. *Document A/C.1/73/L.27: Developments in the Field of Information and Telecommunications in the Context of International Security*. UN. https://undocs.org/A/C.1/73/L.27.

Van Veen, Erwin. 2007. "The Valuable Tool of Sovereignty: Its Use in Situations of Competition and Interdependence." In *Bruges Political Research Papers*. 1–29. College of Europe.

Vestager, M. 2019. *Answers to the European Parliament: Questionnaire to the Commissioner-Designate: Margrethe Vestager, Executive Vice-President-Designate for a Europe Fit for the Digital Age*. European Parliament. https://www.europarl.europa.eu/news/en/hearings2019/commission-hearings-2019/20190910STO60707/margrethe-vestager-denmark.

Yarovaya, I. 2017. "Discussion Session No. 2 at the MCIS 2017: Security of the Information Space and Freedom of Access to Information – Conflicting Relationships." *Ministerstvo Oborony*. https://www.youtube.com/watch?v=m4W693_IVbA&featuare=youtu.be.