
# Routledge Handbook of Russian Foreign Policy

Andrei P. Tsygankov

## Cyber Power

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9781315536934-13
Julien Nocetti
**Published online on: 29 Mar 2018**

# 11
# CYBER POWER

*Julien Nocetti*

FRENCH INSTITUTE OF INTERNATIONAL RELATIONS, PARIS

## Introduction

In June 2016, at the height of the Democratic National Convention in Pennsylvania, WikiLeaks disclosed some 20,000 emails revealing how the machinery of the Democratic Party had favored presidential elections' candidate Hillary Clinton and multiplied low blows to discredit the latter's opponent, Bernie Sanders, which aroused great confusion in the United States. U.S. law enforcement agencies then suspected Russian hackers, and opened an investigation on the existence of a large-scale covert influence operation by the Kremlin to meddle in the November presidential voting. A few months later, in October, the White House publicly acknowledged the implication of the Russian government in these cyberattacks, while the U.S. director for national intelligence described the Russian covert influence campaign as "ambitious" and designed to counter U.S. leadership in international politics (Priest et al., 2016; Rid, 2016).

A couple of years before, Russia's annexation of Crimea and the outburst of hostilities between pro-Russian separatists and loyal Ukrainian forces in Eastern Ukraine, gave rise to a particularly intense "information war" between Moscow and the West (labelled here as the United States and the European Union). Information warfare is perceived in Moscow as adapting to the situation in which Russia believes itself to be towards Western countries: a no-declared war, no peace context, but a permanent state of conflict which requires the use of alternative tools to weaken both the will and the capabilities of the enemy (Franke, 2015).

Both of these examples demonstrate how Russia uses the cyber realm for geopolitical advantage. This includes Russia's cyber capabilities and espionage motivation and its use of the Internet for information warfare. Truly, the cyber and information realms have been carefully integrated into Russian foreign policy's doctrines and practice, all the more so as Internet access has skyrocketed throughout the globe since the late 2000s, de-multiplying the latter's potential for reaching strategic objectives.

First amongst these, the Russian decision-makers are driven by a mostly defensive and risk-averse approach towards information and communications technologies (ICTs): they seek above all to counter any spillover of "Arab Spring"-like events to Russia and post-Soviet republics, thus seeing the Internet as a profoundly disruptive technology that threatens not only government-to-government relations but also, and more importantly, the stability and integrity of nations. In other words, domestic concerns do impact the formulation of Russia's foreign

policy, which is not a new phenomenon in itself but is considerably accelerated by the dissemination of networked technologies. The Kremlin's conception of cyber and information is thus a mostly *defensive* one, which is explicitly reflected in all Russian recent "security doctrines" and "foreign policy concepts."

Second, Russia, as a country seeking to challenge the international consensus on a number of issues since the mid-2000s, is eager to shift the Western narrative over the current global governance regime of the Internet, over which the United States still retains considerable leverage. Here, the Internet is a *subject* of international relations – all the more contentious since former National Security Agency (NSA)'s subcontractor Edward Snowden's disclosures on the United States' massive global electronic surveillance revealed a new form of "U.S. hegemony" in the eyes of the Kremlin. This approach underpins two major features: first is portraying the Internet as a dangerous place and instrument in the hands of a hostile United States – somewhat emphasizing Moscow's largely neo-Hobbesian view of international politics. Second is a U.S.-centric cyber/information foreign policy, driven by both a deep anti-Americanism persisting in the top Russian foreign policy and security elites, and a will to position Russia as an exclusive interlocutor to Washington in key international negotiations on, most notably, cyber norms. On the "information" level, Moscow seeks to stir up widespread distrust in the Western political system and values – understood as rule-of-law-based democracy. On the "cyber" level, Russia is eager to challenge NATO member states' reactions and capacities, while blurring the lines between cybersecurity and the Russian concept of information security.

This chapter does not seek to recount exhaustively the whole Kremlin's cyber and information policies during the "Putin years." Instead it first aims at comprehending in a novel way our understanding of Russia's foreign policy: indeed "things digital and cyber" have long been neglected, even largely ignored, in all the major works published on Russian foreign policy since the late 2000s.[1] This carelessness is all but restricted to Russia: it is also visible in the wider academic debate in international affairs (Powers and Jablonski, 2015) – although important works have recently been published, mostly in the United States (Mueller, 2010; Kramer and Müller, 2014; McCarthy, 2015; Owen, 2015; Segal, 2016). In such a context, overlapping Internet studies with the analysis of Russia's foreign and security policies appears necessary, and should help us in "reloading" our understanding of Moscow's initiatives, moves, and maneuvering towards the West and in a more general sense in the international arena – where information and cyber-related "events" frequently occur.

This chapter's second aim is to analyze Russia's "foreign internet policy" combining cyber and information elements – which is surprisingly a new approach – thus providing a *holistic view* of Russian "cyber power." While in the United States (and Europe) cyber security has been conceived of in a technical way, focusing on the security of hardware and software, i.e. not determining what content and information should be allowed online, Russia rather envisions "information security," thus encompassing the cognitive layer of cyberspace – in other words, *content*. That difference is key: mixing the *cyber* instrument and the *information* tool, even granting more significance to information, Moscow once again blurs the boundaries in order to shape a quickly evolving cyberspace/Internet governance along its sole national interests.

## Terminology and concepts

It should be no surprise that "cyber power" is inherently a U.S. concept, which has been defined as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" (Kuehl, 2009). In a more general sense it

can be described as the ability to control and apply typical forms of control and domination of cyberspace. Others approach the issue primarily from a military perspective (Starr, 2009). A slightly broader view is offered by Joseph Nye, who considers the most important application of soft (cyber) power to be outward-facing, influencing nations, rather than inward-facing. Just who has cyber power often relates back to questions of capabilities and resources. As Nye (2010) notes, "power depends on context and cyber power depends on the resources that characterize the domain of cyberspace." Traditional global powers such as the United States, China, and Russia seem to be the most dominant cyber actors because they have the resources, manpower, and money to support massive cyber operations (Valeriano and Maness, 2015: 25).

What is compelling about cyber power is the ability of the tactic to bleed into other arenas, suggesting that it is not a new and separate domain. What happens in cyberspace does not stay in cyberspace. Weakness displayed in the cyber arena can influence how states interact in all areas and levels; this has an impact on trust between states and corporations (Valeriano and Maness, 2015: 27).

The Russian equivalent to "cyber power" (*kiber sila*) is not used by Russian officials and academics – although it can sometimes be employed at think tank gatherings and forums in Moscow, but mostly in reference to the United States' own cyber power.[2] Generally speaking, "cyber" as a separate function or domain is not a Russian concept. The delineation of activities in the cyber domain from other activities processing, attacking, disrupting, or stealing information is seen as artificial in Russian thinking.[3]

However, the official Russian narrative and policy cannot but hide an ultimate goal which appears close to what has been described as *cyber power*. To the author, a top-Russian official in charge of international information security at the Ministry of Foreign Affairs once said that "Those in control of ICTs will be in control of financial flows, and then, world politics,"[4] suggesting a clear consciousness of the Internet's disruptive role in international politics as well as it being a new and huge source of power.

The phrase "cyber warfare" in Russian writing describes foreign concepts and activities, which do observe this distinction between information activities on computers and networks and those "in real life." Consequently, searches for "cyber" in Russian sources primarily return references to Western doctrine and thinking. It follows that any research on Russian capabilities and intentions which includes the word "cyber" risks providing fundamentally misleading results.

This includes above all the Russian view of *cyber security*, to which the Russians prefer the term *information security* (*informatsionnaya bezopasnost'*), which emphasizes the holistic span of information, where cyber is one component along with others. The Russians see information as being either artificial or natural. Cyber is artificial and is seen as the technical representation of information. In addition to what would be included in cyber, information also includes thoughts in one's head and information in books and documents. Further, they see a logical assumption that a discussion should encompass all information, and not just a subset (i.e. cyber) (Streltsov, 2010).

In other words, according to Russian experts, the U.S. terms *cyber security* and *cyberspace* are primarily technological, whereas the Russian terms for *information security* and *information space* are seen as having broader philosophical and political meanings.[5] The technology is perceived as only one of many components in Russia's understanding of information security and is not considered to be the most important one.[6] The Russian word most equivalent to the English "security" (*bezopasnost'*) denotes "protection"; their view of security of information includes therefore several dimensions: human, social, spiritual, and technical factors. Conversely, the main priorities for U.S. cyber security policy are to safeguard domestic technologies from disruptions, unauthorized access, or any other kind of interference.[7]

In the Russian construct, *information warfare* is not an activity limited to wartime. It is not even restricted to the "initial phase of conflict" before hostilities begin, which includes information preparation of the battle space (Antonovich, 2011). Instead, it is an ongoing activity of the state of relations with the opponent (Heickerö, 2010); "in contrast to other forms and methods of opposition, information confrontation is waged constantly in peacetime" (Slipchenko, 1998; Panarin, 2006, 2012) For Russia, contest with the West in the information domain has already begun. Ongoing information warfare is "a regular feature of the country's news and current affairs coverage."[8]

At the same time, some Russian authors while discussing the permanent nature of information confrontation have drawn a distinction between its nature in peacetime and wartime. According to this categorization, peacetime is mostly characterized by covert measures, reconnaissance, espionage, building capacities, and degrading those of the adversary, and maneuvering for advantage in information space. Wartime measures, by contrast, are deliberately aggressive, and include "discrediting [adversary] leadership, intimidating military personnel and civilians . . . falsification of events, disinformation, and hacking attacks" (Malyshev, 2000; Sharavov, 2000) Furthermore, "the main effort is concentrated on achieving political or diplomatic ends, and influencing the leadership and public opinion of foreign states, as well as international and regional organizations" (Donskov and Nikitin, 2005). If measured by these criteria, recent Russian activities in the information domain would indicate that Russia already considers itself to be in a state of war.[9]

Crucially, information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort, or destroy information. The channels and methods available for doing this cover an equally broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, YouTube videos, or direct approaches to individual human targets.[10]

## The Internet, cyber, and information in Russia's worldview

State-centrism (emphasis on state sovereignty) and anti-Americanism (pushing for "de-Westernizing" the Internet, fed by a quest for international recognition and prestige) are the "heart and lungs" of Russia's vision and policy on Internet-related issues at both domestic and global levels. On a "practical level," Russia considers information to be *militarized*, the aim being to reach informational superiority over the adversary (Gorbachev, 2013).

### *De-Americanizing the Internet*

In recent years, global issues connected to the Internet and its uses have vaulted into the realm of "high politics." Amongst these, Internet governance has long been ignored and restricted to small silos of experts; however, the leaks disclosed by Edward Snowden in June 2013 triggered a massive response to the historical "stewardship" of the Internet by the United States, destabilized foreign relations, and impacted geopolitics of cyberspace (Segal, 2016). Today, international politics has blended with individual actions (from Julian Assange's WikiLeaks to Edward Snowden) and the development of multinational corporations in a way never seen before. Stakes are high indeed: today 2.5 billion people are connected, and by 2030, the Internet is likely to represent 20% of the world's GDP (Dean, 2012). Beyond mere figures, Internet governance sharpens everyone's appetite – from big corporations to governments, as the Internet has taken such a place in our lives, and from freedom of expression to privacy, intellectual property rights

to national security (Nocetti, 2014a). Data encryption, as well as data localization, have more recently emerged as significant and contentious policy issues between the states-corporations-citizens' triangle (Farrell and Newman, 2016; Nocetti, 2016).

Unsurprisingly, a number of countries including Russia have been criticizing U.S. "hegemony" over the Internet (infrastructures, "critical resources" such as protocols, the domain names system, or normative influence, etc.). To a large extent, the Internet is the ambivalent product of the U.S. culture and the expression of its universalist and expansionist ideology. As U.S. policymakers emphasized the importance of winning the battle of ideas both during the Cold War and in the post-2001 period, the ability to transmit the United States' *soft power* via communications networks has been perceived as vital. U.S. policymakers have viewed the "free flow of information" as a means to by-pass authoritarian governments to allow the United States to "tell its story" directly to the people, allowing the targeted populations to understand that U.S. foreign policy is benign and thereby wean them away from radical ideologies (McCarthy, 2011).

Consequently, in recent years, particularly since the Arab uprisings in 2011, governments around the world have become more alert to the disruptive potential of access to digital communications. Thus the line between *technical* and *political* governance is being increasingly blurred by predominantly – but not exclusively – authoritarian governments who fear the "subversive power" of networked technologies from both a political and economic perspective (Yakushev, 2010, 2013). Demographic factors are also put forward: by the 2020s, the Internet's center of gravity will have moved eastwards – already in 2012, 66% of the world's Internet users were living in the non-Western world.[11] However, the reasons for questioning U.S. supremacy also lie in these countries' defiance towards the current Internet governance system, which is accused of favoring the sole interests of the United States (Nocetti, 2014b). As a result of these conceptions, *Moscow has been advancing the "internationalization" of Internet governance* at both regional and international levels since the mid-2000s. Russia, like China and some Middle Eastern nations, considers much of the U.S. stance on cyber politics to be hypocritical: while preaching the tearing down of "digital borders" that have emerged in some authoritarian countries, U.S. intelligence organizations have been recording and exploiting metadata without any oversight (Gomart, 2013: 102).

*The Kremlin fully considers the Internet as a foreign policy item*, and strives to take the lead on global cyber governance and security issues as international contention increasingly arises surrounding the membership, mandates, and supervision of the institutions for cyber management. Reflecting its views on the international system and law, Moscow upholds a traditional understanding of sovereignty and the principle of non-intervention at the core of its policy towards global Internet matters. This results in portraying cyberspace as a territory with virtual borders which correspond to real state borders, and in extending the remit of international laws to the Internet space. As a consequence, Russia is actively involved in promoting international norms that should guide states' behavior in cyberspace on the global arena, thus reflecting a mostly state-centric approach to Internet-related issues (see later) (Nocetti, 2015).[12]

## *The militarization of information*

In contrast to the common Western view of the Internet as an enabler and facilitator, many Russian analysts, experts, and commentators are guided by a much better established perception of insecurity online, and a greater openness to considering the Internet as a vulnerability (*Antirossiyskiy vector*, 2016). The Russian intelligence services publicly stress the potential for a detrimental effect on national security arising from being connected to the Internet.

The functional ("war on information warfare against Russia") and the geopolitical contexts are closely intertwined. The foreign policy doctrine treats information as a dangerous weapon: it

is a cheap, universal weapon, with unlimited range; it is easily accessible and permeates all state borders without restrictions. The information and network struggle (more frequently, the information-psychological struggle), including its extreme forms, such as information-psychological warfare and netwars, are means the state uses to achieve its goals in international, regional, and domestic politics, and also to gain a geopolitical advantage.

On 29 December 2014, the Security Council of the Russian Federation published a new version of the Military Doctrine of the Russian Federation. The comments accompanying the Russian doctrine emphasized the importance of informational operations in contemporary conflicts, and the inclusion of information into the country's defensive arsenal (Security Council, 2014).

By emphasizing the need for a reassessment of the global situation (the struggle of the world's leading countries for their interests are characterized by indirect actions, exploiting the potential for protest among local populations, radical and extremist organizations, as well as private military companies), the Security Council reiterated the anti-NATO and anti-American mantra which has constantly been present in successive editions of the Doctrine.

The new Doctrine conceives of information as a national security instrument amongst others. This is not new in Russia's approach – both the 2000 Military Doctrine and Doctrine on Information Security already emphasized that precise aspect. However, information warfare now features prominently in several sections of the Doctrine, which proves how fundamental the information factor has become in recent conflicts. Indeed, one of the main external military threats is identified as "the use of ICTs in a political-military purpose in order to act, against international law, sovereignty, political independence and territorial integrity of states, and to threaten international peace and security, and world and regional stability."

The Doctrine states a number of examples of information uses described earlier, as "the combined use of military force with political, economic, informational and other means, leading to an intense use of the protest potential of the population." This particular scenario, which imagines the population ganging up against its political leaders, is recurring in how Russians understand information warfare. This Doctrine also enumerates other informational threats as encouraging the youth to give up their historical, spiritual, and patriotic traditions, or to disturb governmental agencies and information infrastructures.

The new elements introduced in the Doctrine clearly suggest a blurring of the lines between external and internal threats. For some scholars, these signal the "militarization" of the Kremlin's domestic and foreign policies. By mobilizing and sensitizing the public to the threat from the West, the Kremlin legitimizes its military policy on both the domestic and international arenas (Darczewska, 2015: 12). The message to foreign audiences is more nuanced: the Doctrine supplies the so-called opinion-makers, and in practice the moderators with informational campaigns.

## The significance of the domestic factor

As a relatively young nation-state that has been experiencing a potent feeling of insecurity since the chaotic 1990s transition to a free market economy and pluralism, Russia has thus been adopting a threat-oriented lens towards the Internet. By extension, the country's Internet policy conveys a long-lasting security fear. 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 for full sovereignty and struggling against the "permeability" of its neighborhood, President Vladimir Putin gradually saw the information revolution – driven by the considerable growth in domestic Internet access – as one of the

most pervasive components of the U.S. expansionism in the post-Soviet sphere, most notably in Russia itself.

However, officials have long paid modest attention to the Russian Internet's development, supporting its benefits for the country's economy while tolerating some spaces online for dissenting activities (Etling, 2010). The first legal online restrictions were imposed in 2002–2003 on condition of fighting "extremism." In parallel, SORM-II, the technical system used by several law enforcement agencies to intercept and analyze the contents of telecommunications within Russia, extended its reach to monitoring the Internet.[13]

The authorities' approach drastically changed from 2011 when they observed citizens from some Arab countries mobilizing and coordinating their protest actions through networked technologies. These events – known as "Arab Spring" – did profoundly impact the minds of Russian political and security elites. 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 (Nocetti, 2012). The events in the Arab world did clearly reawaken the authorities' fear of "regime change" initiated from abroad, i.e. by the United States, through the use of digital tools.

These international developments inspired many in Russia who demanded substantial political changes after a decade of Vladimir Putin's rule characterized by rising living standards for the population guaranteed by the state in exchange for (most) political freedoms (Parker, 2014). During the years of Dmitry Medvedev as President of Russia (2008–2012), the Internet served as a substitute to the public sphere in Russia, equivalent to the role played by literature in the nineteenth century and independent media in the 1980s (Pipenko, 2010). Digital technologies have indeed been used by citizens in a "creative" way for mobilization purposes around a particular cause, addressing the politicians directly to solve such issues, thus going beyond both the legal online restrictions that have been imposed since 2002–2003, and overcoming the traditional distrustful attitude toward institutions among Russian society (Sidorenko, 2011). Overall, Internet users have become skillful in circumventing "legislative" obstacles online or at least mitigating their consequences. They learned to move their profiles quickly or duplicate them on Western social networks when popular blog platforms such as LiveJournal were subject to denial-of-service (DDoS) attacks. They massively use services such as TOR, and traditionally resort to humor to make a mockery of political authorities (Kastoueva-Jean and Nocetti, 2012).

The 2011–2012 election cycle in Russia – a parliamentary ballot in December 2011 and a presidential vote in March 2012 – reawakened Russian leaders' anxiety over the Internet's potential for political disruption. Indeed, the political leadership feared a ripple effect in the countryside, as mass protests in its biggest cities were mostly coordinated on and facilitated by the use of digital technologies (Bode and Makarychev, 2013). Likewise, the Kremlin felt irritated by the fact that the Internet enables citizens to circumvent government-controlled "traditional" media, most importantly television.[14]

More strikingly, the scandal which involved the National Security Agency (NSA) around Edward Snowden's leaked documents revived the push for tighter controls over the Internet in Russia, on the basis that the transnational companies' privacy policies (Google, Facebook, Twitter, etc.) pose a threat to Russia's digital sovereignty – and consequently national security. Several members from both houses of the parliament suggested locating in Russia all servers having Russian citizens' personal data, 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 (Zheleznyak, 2013).

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 years-old call for a "national operating system" that would reduce Russian dependency on Microsoft Windows.

In April 2014 Vladimir Putin publicly assimilated the Internet into a "CIA project." Rumors about an Internet "kill switch" being devised in Russia came after "cyber exercises" reportedly revealed vulnerabilities in the Russian Internet's security infrastructure preparedness against potential external aggression (Golitsyna, 2014). This produced calls for the creation of a self-contained system duplicating the root domain name system (DNS) architecture to keep the Russian Internet running in case of emergency, either externally – which is no longer seen as hypothetical in the current belligerent geopolitical context – or, in case of civil disorder and/or extremist action, internally.[15]

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. *Domestic factors therefore play a crucial role in shaping Russia's Internet policies*. Fundamentally, Russia has been adopting an "inside-outside" approach towards the Internet: (draft) laws and public speeches go hand-in-hand with policy initiatives at the regional (i.e. near abroad) and global level, while international events impact Russia's policy-making in this regard. For some, this approach cannot be split away from the inherently authoritarian nature of the Russian regime, which would perpetuate a century-long tradition of muzzling dissenting voices, whatever the medium used.[16] For others, this strategy can be explained by the fact that Russia is a relatively young nation-state still insecure about its sovereignty, hence the stronger commitment to a backwards-looking, sovereigntist approach to Internet governance (Mueller, 2013).

Beyond the "Arab Spring" and Snowden syndromes, it is clear that Russia has deep concerns on the principle of uncontrolled exchange of information in cyberspace, and over the presumption that national borders are of limited relevance there (Giles, 2012). "Content as threat" pertinently informs the Russian perception that digital technologies can be used as tools *against* Russia. In Russian documentation this is expressed as the "threat of the use of content for influence on the socio-humanitarian sphere."

This overall defensive mindset and stance led to a questioning of the reshaping of Russian foreign and security policies through cyber. The cyber domain is conceived of as an asymmetric weapon, in an unequal balance of power as Russia's conventional means remain inferior to NATO's. Back in 2007 Vladimir Putin claimed, "Our answers have to be based on intellectual superiority; they will be asymmetric and less costly." In short, the Russian strategy is one of a "cross-domain coercion"[17] that combines propaganda, cyberattacks, and the use of both conventional and nuclear forces, in an action aimed at blurring the distinction between war and peace, and preventing any quick and coordinated reaction from Western leaders. The successive hacks, leaks, dissemination of "fake news" are thus seen as complementary to the use of strategic bombers, missile defense systems, or tanks. In other words, the traditional vehicles for Russian power – the military, energy – are no longer sufficient to explain the transformation of Russian power. Cyber and information instruments do not contradict other foreign policy tools; they complement them, as Chief of Staff Valery Gerasimov clearly wrote in his articles (Gerasimov, 2013).

Government funding has been increasing in parallel with the Kremlin's interest in cyberspace. The appointment of Sergei Shoigu as Minister of Defense in November 2012 seemingly translated into a progressive and constant interest in strengthening both Russian capabilities and "human resources" dealing with cyber and information (Turovskiy, 2016).

The successive Russian military involvements in Georgia, and later in Crimea, Eastern Ukraine, and Syria, were the opportunity to test the country's enhanced capabilities in information and cyber. These were reflected in particular in the long-announced creation of "Information Troops," effective from February 2017 and which gather diverse profiles from hackers, specialists in sociolinguistics, psychology, and networks.

## Moscow's cyber diplomacy in practice

Russia wants to position itself in an *exclusive dialogue with the United States on defining norms in cyberspace*. On the one hand, the Kremlin noticed that since the annexation of Crimea in 2014 the United States dropped their strategic dialogue with Moscow on cyber security in favor of China – to the point of signing with Beijing a pact of non-aggression in cyberspace in 2015. *The redefinition of Internet geopolitics in favor of a China-U.S. "duopoly" irritates Russia*, which still considers itself as a cyber superpower. On the other hand, the Kremlin did not hide its irritation towards Barack Obama's reluctance to agree on a "Code of conduct" that would rule cyber war operations. Pushed by Russia, such an agreement would replace debates within the United Nations – a red line for the U.S. administration. *Moscow and Washington remain antagonistic on their approach towards cyber security*: unlike the United States that gives priority to technology and networks, the Russians want to include in any future agreement the cognitive layer of cyberspace.

## *Reshaping the debate on cyber norms*

In little more than a generation, the Internet has become the substrate of the global economy and governance worldwide. The convergence of the data economy, robotics, the Internet of Things, and (tomorrow) artificial intelligence overwhelms not only industrial production but also societies and the world's balance of power. All of this increasing interdependence implies vulnerabilities that governments and non-governmental actors can exploit. In such a volatile context, *Russia posits that the set of norms that governed state behavior before the rise of the Internet did not translate to state behavior in an Internet age* – in other words, a new digital age required new norms.

As a consequence, Russia has been pro-actively engaged in norm-promotion through international institutions. Now a highly contentious issue (Bradshaw, 2014), global Internet governance has seen a constant Russian involvement to introduce security concerns into previously unpoliticized or mostly technical issues and forums (Nocetti, 2015).

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 International Telecommunications Union (ITU) and the Internet Governance Forum (IGF) to promote policies that synchronize with national-level laws surrounding information security. Vladimir Putin himself several times pleaded that global cyberspace should be governed by international institutions operating under the United Nations – and that the ITU was the best placed institution to regulate the Internet. Notably, 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.

In a 2011 letter to the United Nations General Assembly outlining a proposal for an "International Code of Conduct for Information Security," the Russian coalition (gathering China, Uzbekistan, and Tajikistan) proposed a codification of this concept, stipulating that states subscribing to the Code pledge to "not use information and communications technologies and

other information and communications networks to interfere with the internal affairs of other states or with the aim of undermining their political, economic and social stability."

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" in the Russian city of 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.

Taken together, the two documents propose to significantly strengthen the power of the state in cyberspace vis-à-vis non-government actors, introducing raw security concerns. But they also provide an alternative vision for hesitant countries that may lean naturally toward state-dominated models of governance, and that side with Russia – and China – in decrying the destabilizing potential of the Internet and cyberspace more broadly.

At the regional level, Moscow uses regional organizations and forums to disseminate its views on cyberspace policies and the norms it seeks to push internationally. One illuminating example is the Shanghai Cooperation Organization (SCO).[18] 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.[19] Since 2009, SCO member states are bound by an agreement on "cooperation in the field of ensuring international information security"; and more recently, the SCO issued a statement on "information terrorism," which drew attention to the way in which the countries have a shared and distinct perspective on Internet security policy. The Code of Conduct discussed earlier was proposed by SCO states, which formulated global standards for "unacceptable state behavior" in cyberspace.

The BRICS format is also used as a vehicle for cooperation on cyber issues. At the policy level, the BRICS states have all shown an interest in Internet governance and cyber security. Yet there is a difference in prioritization. There was no joint BRICS proposal for a Code of Conduct on information security. Despite the increased institutionalization of BRICS as a coalition, and despite various proposals contesting the U.S. role regarding the Internet, the group is splintered, and formal proposals have been submitted either through IBSA (India-Brazil-South Africa) or the SCO (Ebert and Maurer, 2013). Generally speaking, the key differences are informed by states favoring an intergovernmental approach based on international cooperation and those preferring to adopt a strict "sovereigntist" cyber policy.

## *The Russia/China/U.S. triangle*

Increasingly active in forging new alliances and trying to reformulate norms and standards, Russia has also been engaged in an up-and-down cyber diplomacy with the United States (Markoff and Kramer, 2009; White House, 2013b). Clearly, while endeavoring to shape the international dialogue on cyberspace, *the aim for Moscow is to "bilateralize" cyber security and cyber warfare issues with Washington, reflecting a quest for an exclusive and direct dialogue on par with the United States* on this issue.

There is clear evidence that the dialogue between the two countries is not easy – they both have diverging approaches toward the security of cyberspace, and have reacted differently to major international events surrounding Internet governance and cyber security. Bilateral consultations particularly focused on reaching a consensus on critical terminology defining cyber/information security, as both governments have had different priorities from each other on

the issue. Beyond agreements on terminology, both governments have turned to a series of confidence-building measures, including the establishment of a "cyber-hotline" between the U.S. cyber security coordinator and the Russian deputy secretary of the Security Council, should there be a need to directly manage a crisis situation arising from an ICT security incident. The step was taken on the fringe of the G-8 Summit in Northern Ireland in June 2013 (White House, 2013a) – just when leaked details of network surveillance and espionage programs by the NSA were stirring up international concern about how deep U.S. intelligence is reaching into IT operations worldwide. A month later was announced the formation of a bilateral presidential group on information security, tasked with easing tensions between both capitals and carrying on the implementation of confidence-building measures (Chernenko, 2013).

Russia views the major world economies' build up of their potential for information warfare with great concern. As stressed by official Russian documents, 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 global information infrastructure. Consequently, Russia vehemently wants to restrict offensive cyber weapons (Croft, 2012; Peck, 2013). 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 they want a peaceful cyberspace, *Moscow accuses Washington of militarizing the Internet* through the establishment of a Cyber Command and the development of offensive capabilities such as *Stuxnet* (PIR-Tsentr, 2016).

More broadly, Russia criticizes the constant rise in the U.S. budget for cyber operations.[20] As far as norms are concerned, the U.S. concept of counter-measures sounds worrisome to Moscow. The Kremlin, as Beijing, is opposed to a key notion in Washington: the extraterritoriality of counter-measures, i.e. the possibility for a state attacked by another state via servers domiciled in a third country to respond to these servers.[21]

It is clear that recent global Internet governance and security venues have shown a portability of Cold War policies into the twenty-first century cyber arena (Gross, 2012; Klimburg, 2013). Using the nuclear non-proliferation treaty as an appropriate precedent, others note that a global consensus on cyber security could be best achieved by pursuing deterrence strategies (Choucri, 2012: 173). Russia has conspicuously opted for the first strategy, which enables its policy-makers to follow Moscow's long-standing foreign policy objective of promoting legally binding international treaties, whilst in this case developing its own cyber capabilities.[22]

Though largely U.S.-centric, Russia's international cyber policy has also sought to focus on China following the Russian "turn to the East" fostered by the Kremlin since 2014 (Trenin, 2016). The bilateral relationship has attracted speculation about whether it will continue to deepen into an alliance. The cybersecurity deal signed in 2015 between Moscow and Beijing seemed to mark further Sino-Russian cooperation in another arena – cyberspace. The pact has two key features: mutual assurance on non-aggression in cyberspace and language advocating cyber-sovereignty. The two sides agreed on a range of trust- and confidence-building measures and joint "promotion of norms of international law in order to ensure national and international information security," especially under the auspices of the platforms of the relevant international organizations: the United States, OSCE, and ITU. The agreement looks like an ambitious attempt at setting the rules of the game in cyberspace at a time when no such consent on norms of behavior seems currently feasible at a global level. Also, the Russia-China deal can be seen as a response to the 2015 U.S. cyber defense strategy, which directly identifies Russia and China among its key adversaries – both countries "have developed advanced cyber capabilities and strategies," while only mentioning the need for keeping a dialogue with China.

The two sides have not experienced big public fallout on mutual hacking so far,[23] which makes what seems like a non-aggression pact look more like a pre-emptive declaration of understanding, making a special point of this consensus to the external world.

Nevertheless, cyber-espionage is not the core of the Sino-Russian cybersecurity cooperation. Much like Russia and China's combined effort to oppose a U.S.-dominated world order, the insistence on "cyber-sovereignty" is a shared strategic interest that contrasts with the U.S. advocacy for "cyber freedom." This was further emphasized at the Wuzhen World Internet Conference, an annual meeting organized by Chinese government agencies first held in 2014, where Chinese politicians – including President Xi Xinping – together with Russian guests (high-level officials, experts) also forcefully promoted a norms-driven approach to cyberspace governance.

However, *for the Chinese the highest priority remains their strategic dialogue on cyberspace with the United States*. Beijing and Washington signed a non-aggression pact in cyberspace in autumn 2015 following years of negotiations on highly contentious issues between the two sides (cyber-warfare, cyber espionage) (Austin and Gady, 2012; Lieberthal and Singer, 2012). *The redefinition of global Internet geopolitics along a Sino-U.S. axis is not seen favorably in Moscow* – that might be a reason why the Russians "flex their muscles" in terms of cyber aggressions worldwide in order to test U.S. and NATO capabilities and reactions, and to reshape the cyber norms' debate. Moscow's U.S. election-related activities brought the importance of Russia's conceptualization of information security front and center in the United States, possibly making it harder for Washington to separate cyber security from information security.[24]

## *Russia's interference in the 2016 U.S. presidential election*

Russian involvement in the U.S. presidential election, as formally alleged by the Obama administration, represented a turning point in U.S.-Russia relationships and in international politics – at least as regards state conduct in cyberspace. The theft of a vast amount of data in mid-2016 belonging to the Democratic National Committee and other political organizations was allegedly the work of Russian hacker groups. Although Russian cyber operations are surrounded with high secrecy, some groups labelled as "APT 28" and "APT 29," also known respectively as "Cozy Bear" and "Fancy Bear," gained public attention during the election campaign as well as being under Washington's high scrutiny, as these are allegedly tied to Russian intelligence services. Barack Obama took the unprecedented step of imposing sanctions on the chiefs of the Main Intelligence Directorate (GRU) and the FSB (Jones, 2017). The alleged attacks from Moscow combined the technological dimension and intelligence-gathering capabilities of twenty-first-century hackers with the art of propaganda familiar with Cold War-era tactics.[25]

Overall, Russian interference in the U.S. election perfectly illustrated how the Russians view cyber, i.e. as an embedded part of the broader concept of information operations. Russian maneuvers aimed less at influencing the outcome of the election than at the perceptions (*soznanie*) Americans have about the reliability of their rulers and institutions. Sowing a general distrust towards the U.S. political system, directing voters toward candidates more lenient vis-à-vis Russian *Weltanschauung* and objectives, keeping the idea that Western leaders are indecisive, weak, divided: that is the longer-term Russian strategy. Moscow's larger goal is to strengthen the doubt in public opinion toward Western policies and values: liberal democracy, multiculturalism, and interventionism under the guise of "responsibility to protect."

Less costly than "traditional warfare," information and cyber instruments also prove considerably harder to be attributed to governments. In the case of the U.S. election, the Obama administration took several months to publicly attribute the hacks and leaks to Moscow – nevertheless

an unprecedented move given the escalation risks such a step can carry, all the more opening both a legal and technical "Pandora's box" for further cyber damage.

## Conclusion

The cyber realm is becoming a salient topic in international relations – no one doubts that. Russia so far has had a rather subtle "use" of the Internet/cyber instrument in its foreign policy, which remains under-estimated in academic and policy-oriented analyses. Like in other international issues, in cyberspace Russia does not have permanent allies. All Moscow's alignments are situational and conditional, serving primarily Russia's regional interests or, most notably, its world-order goals. *There is no Russian "grand strategy" related to cyber policy. Instead, the Kremlin constantly maneuvers, seizes opportunities wherever they are, and quickly reacts to international events*. The Snowden disclosures in 2014 immediately come to mind: in welcoming on its soil the U.S. whistleblower, Russia not only caused a major diplomatic blow to Washington, it also signaled a shift in the geopolitics of cyberspace, the consequence of which are still meaningful.

One of the major differences between Russia and the West on cyberspace is that the Russians primarily consider the cognitive layer of the network, i.e. the contents. The key word is *information*. In the Russian conceptual framework, this information can be stored anywhere and transmitted by any means – so information in print media, or on television, or in somebody's head, is subject to the same targeting concepts as that held on an adversary's computer or smartphone. Similarly, the transmission or transfer of this information can be by any means: so introducing corrupted data into a computer across a network or from a flash drive is conceptually no different from placing disinformation in a media outlet, or causing it to be repeated in public by a key influencer. *This holistic approach has also been underestimated – or misunderstood – in the West*, which has always been keen to create a clear separation between cybersecurity and information security.

Will the 2016 U.S. presidential election be a game-changer in the future? For the first time in history, the cyber tool has been directly accused of playing a pre-eminent role in determining the outcome of a vote through the meddling of a foreign power – Russia. Relying on both cyber-attacks and information operations, a confident Russia may use these as a particularly potent foreign policy instrument wherever it needs to dictate its interests. In other words, hydrocarbon pipelines and conventional military instruments are no longer sufficient to illustrate twenty-first-century Russian power: cyber power is definitely a core element in this triad.

## Notes

1 The author stresses the following books Lo, 2015; Tsygankov, 2013; Allison, 2013; and Mankoff, 2009.
2 Author's experience during closed seminars and internet forums, Moscow, April 2013, November 2014 and April 2015.
3 Author's interview with the deputy director of Moscow State University's Institute for Information Security Issues (IISI), Moscow, 13 December 2012.
4 Author's informal talk on the sidelines of an international seminar in Garmisch-Partenkirchen, Germany, 23 April 2013.
5 Author's interview with the deputy director of Moscow State University's Institute for Information Security Issues (IISI), Moscow, 20 October 2011 and 13 December 2012.
6 Author's discussions with Russian experts and officials, Moscow, July and October 2011. See also Giles (2012).
7 Author's discussion with an American official, Krakow, 29 September 2015. See also the U.S. *International Strategy for Cyberspace*, The White House, May 2011.
8 As described in a BBC Monitoring media survey (Ennis, 2016).

9 Multiple indicative examples include computer network operations targeting the U.S. in a practically overt manner, and Russia's new lack of concern at accompanying damage to its international reputation (Blake, 2016).
10 Closed seminar at IFRI, Paris, 10 March 2017.
11 Data collected from www.internetworldstats.com (as of 15 February 2014).
12 On Russia's activities on norms-making at the United Nations, see Maurer, 2011.
13 For a comprehensive analysis of early restrictive legislations over the internet in Russia, see Alexander, 2004.
14 However, television has so far remained the main source of information for a majority of Russians.
15 Even though a special Security Council meeting reassured that "no internet switch off" or state take-over is planned, it would be right to assume the further strengthening of Russia's internet at the level of critical cyber infrastructure as part of the national security capacities.
16 Author's interviews with academics in Moscow, December 2012 and February 2013.
17 The expression was coined by Dmitry Adamsky, 2015.
18 The Organization comprises China, Kyrgyzstan, Kazakhstan, Russia, Tajikistan, and Uzbekistan. India, Iran, Mongolia, Afghanistan and Pakistan have observer status, and Belarus, Turkey, and Sri Lanka are considered dialogue partners.
19 Author's interview with a Russian academic, Moscow, October 2011. Read also Allison, 2008.
20 Indeed, the 2014 budget request includes a 20% increase from 2012; the U.S. Cyber Command is reportedly expanding by more than fivefold (Negroponte et al., 2013: 35).
21 Author's talk with a French official, 29 September 2015.
22 Author's interview with a Russian expert on information security, Moscow, February 2013.
23 Russia's security firm Kaspersky Lab estimated that cyber-espionage attacks by "Chinese-speaking" groups against Russian targets increased 300 percent from December 2015 to February 2016.
24 Informal discussions of the author with American and British experts, Ditchley, 18 November 2016.
25 See, for instance, declassified U.S. Department of State (1981) reports on Soviet "active measures."

## References


Adamsky, Dmitry. 2015. "Cross-Domain Coercion; The Current Russian Art of Strategy," Ifri, *Proliferation Papers* No. 54, November.

Alexander, Marcus. 2004. "The Internet and Democratization: The Development of Russian Internet Policy," *Demokratizatsiya* 12, 4: 616.

Allison, Roy. 2008. "Virtual Regionalism, Regional Structures and Regime Security in Central Asia," *Central Asian Survey* 27, 2: 185–202.

Allison, Roy. 2013. *Russia, the West, and Military Intervention*, Oxford, UK: Oxford University Press.

*Antirossiyskiy vektor: zarubezhe SMI v 2015 g.* 2016. Moscow: Rossiyskiy Institut Strategicheskikh Isledovaniy.

Antonovich, P. 2011. "Cyberwarfare: Nature and Content," *Military Thought* 20, 3: 35–43.

Austin, Greg and Franz-Stefan Gady. 2012. "Cyber Detente between the United States and China. Shaping the Agenda," New York: East-West Institute.

Blake, Aaron. 2016. "The CIA Concluded that Russia Worked to elect Trump. Republicans Now Face an Impossible Choice," *The Washington Post*, 9 December.

Bode, Nicole and Andrei Makarychev. 2013. "The New Social Media in Russia: Political Blogging by the Government and the Opposition," *Problems of Post-Communism* 60, 2: 53–62.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond 2014. "The Emergence of Contention in Global Internet Governance," *The Centre for International Governance Innovation, Paper presented at the 9th Annual GigaNet Symposium, Istanbul*, 1st September. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809835.

Chernenko, Yelena. 2013. "RF i SShA popytayutsiya snizit' napryazhenie v seti", *Kommersant'*, 22nd July.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press.

Croft, Adrian. 2012. "Russia Says Many States Arming for Cyber Warfare," Reuters, 25 April.

Darczewska, Jolanta. 2015. "The Devil is in the Details: Information Warfare in the Light of Russia's Military Doctrine," OSW, *Point of View* 50, May.

Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark 2012. "The Internet Economy is Growing More than 10 percent Per Year in the G-20 Nations." www.bcg.com/publications/2012/technology-digital-technology-planning-internet-economy-g20-4-2-trillion-opportunity.aspx.

Donskov, Yu and O. Nikitin. 2005. "Mesto i rol' spetsial'nykh informatsionnykh operatsij pri razreshenii voennykh konfliktov," *Voyennaya mysl'* 6: 17–23.
Ebert, Hannes and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, 6: 1054–1074.
Ennis, Stephen. 2016. "Russia's Fixation with 'Information War,'" BBC News, 26 May.
Etling, Bruce, Karina Alexanyan, John Kelly, Robert Farris, John G Palfrey Jr and Urs Gasser, 2010. "Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization," Massachusetts, MA: Harvard University, Berkman Center for Internet & Society, October.
Farrell, Henry and Abraham Newman, 2016. "The Transatlantic Data War," *Foreign Affairs*, January/February. Online. www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war.
Franke, Ulrik. 2015. "War by Non-Military Means. Understanding Russian Information Warfare," Swedish Defence Research Agency (FOI), *Report*, March.
Gerasimov, Valery. 2013. "Tsennost' nauki v predvidenii", *Voenno-promychlennij kurier*, 27 February.
Giles, Keir. 2012. "Russia and Cyber Security," *Naçao e Defesa* 5, 133: 69–88.
Golitsyna, Anastasia. 2014. "Soviet bezopasnosti obsudit otklyuchenie Rossii ot global'nogo interneta," *Vedomosti*, 19 September.
Gomart, Thomas. 2013. "De quoi Snowden est-il le nom?" *Revue des deux mondes*, December.
Gorbachev, Yuri. 2013. "Kibervoina uzhe idet," *Novoe voennoe obozrenie*, 13, 12–18 April.
Gross, Michal Joseph. 2012. "World War 3.0," *Vanity Fair*, May.
Heickerö, R. 2010. "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," *Swedish Defence Research Establishment (FOI).*
Jones, Sam. 2017. "Russia Mobilises an Elite Band of Cyber Warriors", *Financial Times*, 23 February.
Kastoueva-Jean, Tatiana and Julien Nocetti. 2012. "Le LOL, nouvel avatar de la contestation en Russie", *Les Echos*, 8 November.
Klimburg, Alexander. 2013. "The Internet Yalta," Center for a New American Security, *Commentary*, 5th February
Kramer, Franklin, Stuart Starr and Larry Wentz (eds), 2009. *Cyber Power and National Security*, Washington, DC: National Defense University Press.
Kramer, Jan-Frederik and Benedikt Müller (eds), 2014. *Cyberspace and International Relations. Theory, Prospects and Challenges*, Berlin: Springer.
Kuehl, Dan. 2009. "From Cyberspace to Cyberpower: Defining the Problem," in Franklin Kramer, Stuart Starr and Larry Wentz (eds), 2009. *Cyber Power and National Security*, Washington, DC: National Defense University Press.
Lieberthal, Kenneth and Peter W. Singer. 2012. *Cybersecurity and U.S.-China Relations*, New York: Brookings Institution, February.
Lo, Bobo. 2015. *Russia and the New World Disorder*, New York: Brookings Institution, and London: Chatham House.
Malyshev, V. 2000. "Ispol'zovanie vozmozhnostey sredstv massovoy informatsii v lokal'nikh vooruzhennykh konfliktakh", *Zarubezhnoye voyennoye obozreniye*, 7: 2–8.
Maurer, Tim. 2011. "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, September.
Mankoff, Jeffrey. 2009. *Russian Foreign Policy: Return to Great Power Politics*, New York: Council on Foreign Relations and Rowman & Littlefield.
Markoff, John and Andrew Kramer. 2009. "In Shift, U.S. Talks to Russia on Internet Security," *The New York Times*, 12th December.
McCarthy, Daniel. 2011. "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet," *Foreign Policy Analysis*, 7, 1: 89–111.
McCarthy, Daniel. 2015. *Power, Information Technology, and International Relations Theory. The Power and Politics of US Foreign Policy and the Internet*, Basingstoke, UK: Palgrave Macmillan.
Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*, Cambridge, MA: MIT Press.
Mueller, Milton. 2013. "Are We in a Digital Cold War?" *Paper presented on 17th May at the GigaNet workshop The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and Networks*, Graduate Institute, Geneva. www.internetgovernance.org/2013/07/19/are-we-in-a-digital-cold-war/.

Negroponte, John, Samuel Palmisano, Adam Segal (eds.). 2013. *Defending an Open, Global, Secure, and Resilient Internet, Council on Foreign Relations, Independent Task Force Report* No. 70, June. www.cfr.org/report/defending-open-global-secure-and-resilient-internet.

Nocetti, Julien. 2012. "Russie: le web réinvente-t-il la politique?" *Politique étrangère*, 77, 2, Summer: 277–289.

Nocetti, Julien. 2014a. "Puissances émergentes et internet: vers une 'troisième voie'?" *Politique étrangère*, 4, Winter: 44–51.

Nocetti, Julien. 2014b. "Global'noe upravlenie Internetom: pochemu eto tak vazhno," *Rossijskij Soviet po Mezhdunarodnym delam*, 29 July.

Nocetti, Julien. 2015. "Contest and Conquest: Russia and Global Internet Governance," *International Affairs* 91, 1, January: 121–125.

Nocetti, Julien. 2016. "Vojna za Internet-dannye nachalas," Rossijskij Soviet po Mezhdunarodnym delam, 22 March.

Nye, Joseph. 2010. *Cyber Power*, Harvard Kennedy School: Belfer Center for Science and International Affairs, May.

Owen, Taylor. 2015. *Disruptive Power: The Crisis of the State in the Digital Age*, New York: Oxford University Press.

Panarin, I. 2006. *Informatsionnaya voyna i geopolitika*, Moscow: Goryachaya liniya

Panarin, I. 2012. "Vtoraya mirovaya informatsionnaya voyna – voyna protiv Rossii," *Kirill i Mefodiy*, 10 January

Parker, Emily. 2014. *Now I Know Who My Comrades Are: Voices from the Internet Underground*, New York: Sarah Crichton Books.

Peck, Michael. 2013. "Russia Says Cyberspace Is New Theater of War," Forbes.com, 20 August.

Pipenko, Maria. 2010. "Russian Blogosphere as a Public Sphere," *Journal of Siberian Federal University*, 4, 3: 526–535.

PIR-Tsentr. 2016. "Pravo voyny i kiber prostranstvo," PIR-Tsentr, 6 April.

Powers, Shawn and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*, Champaign, IL: University of Illinois Press.

Priest, Dana, Ellen Nakashima, Tom Hamburger. 2016. "U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections," *The Washington Post*, September 5.

Rid, Thomas. 2016. "How Russia Pulled Off the Biggest Election Hack in U.S. History," *Esquire*, October 20.

Security Council. 2014. "Ob itogakh operativnogo soveshchaniya Soveta Bezopasnosti Rossiiskoy Federatsii po voprosu 'O vnesenii utocheniy v Voennuyu doktrinu Rossiiskoy Federatsii", Security Council of the Russian Federation, 20 December, accessible at www.scrf.gov.ru/news/838.html.

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York: PublicAffairs.

Sharavov, I. 2000. "K voprosu ob informatsionnoy voyne i informatsionnom oruzhii", *Zarubezhnoye voyennoye obozreniye*, 10: 2–5.

Sidorenko, Alexey. 2011. "Blogery i gosudarstvo, tsifrovoy dualizm v Rossii," Ifri, *Russie.Nei.Visions* No. 63, December.

Slipchenko, V.I. 1998. "Future War (A Prognostic Analysis)," January.

Starr, Stuart. 2009. "Toward a Preliminary Theory of Cyberpower," In Franklin Kramer, Stuart Starr and Larry Wentz (eds), *Cyber Power and National Security*, Washington, DC: National Defense University Press.

Streltsov, A. 2010. *Gosudarstvennaya informatsionnaya politika: osnovy teorii*, Moscow: MTsNMO.

Trenin, Dmitri. 2016. "Aziatskaya politika Rossii: ot dvustoronnego podkhoda k global'noy strategii," Ifri, *Russie.Nei.Visions* No. 94, June.

Tsygankov, Andrei. 2013. *Russia's Foreign Policy: Change and Continuity in National Identity*, New York: Rowman & Littlefield, 3rd edition

Turovskiy, Daniil. 2016. "Rossijskie vooruzhennye kibersily", *Meduza*, 7 November.

U.S. Department of State. 1981. "Forgery, Disinformation, Political Operations", U.S. Department of State, Bureau of Public Affairs, *Special Report* No. 88, October. www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

*U.S. International Strategy for Cyberspace*. 2011. The White House, May. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, New York: Oxford University Press.

Yakushev, Mikhail. 2010. "Upravlenie Internetom: politiki i geopolitiki," *Indeks Bezopasnosti*, 2, 93, Summer.

White House. 2013a. "Joint Statement by the Presidents of the USA and the Russian Federation on a New Field of Cooperation in Confidence Building," The White House: Office of the Press Secretary, 17th June. https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0.

White House. 2013b. *Fact sheet: U.S.-Russian cooperation on information communications technology security*, The White House's Office of the Press Secretary, 17th June. https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

Zheleznyak, Sergei. 2013. "My dolzhny obespechiy' 'tsifrovoj suverenitet," *Ekonomika I Zhizn'*, 19th June.