Regional Perspectives on Cyber-Security: Formation and Evolution

Stelian Dumitrache, Christopher Jolliffe,
Sandra Rector and Oliver Woodhall

University Consortium Annual Conference
5-6 October 2017, Washington DC

Introduction

The cyber weapon is a recent addition to the arsenal of states. Some commentators regard the advent of cyberspace as the most significant transformation in security affairs since the development of nuclear weapons. Indeed, some nations already regard it as an integral element of their national defence apparatus. Yet strangely at the same time, the integration of cyber realities and theory into the field of international relations is in its infancy, and gaps in security doctrine persist at the most elemental level. Recent work on the area identifies national perceptions as being shaped by events. Whether cyber-security reaches elites at the higher echelons of political leadership depends on a number of factors: personal interest, a direct experience of malicious cyber action, media attention, or the salience of cybersecurity on their national and international agendas. With this in mind, this paper seeks to explore the underlying reasons behind differing national and regional perspectives, look for similarities, and identify areas for potential cooperation between our three regions: Russia, Europe, and the United States of America. (n.b. the term 'Europe' here is taken as referring to those member states of the European Union).

As a backdrop to our regional analysis, it is necessary to explore the term 'cybersecurity' and assess its application to our three areas. 'Cybersecurity' as we understand it, is a conceptually loaded multi-faceted term which can cover three key aspects: security of cyber infrastructure and data safety, informational-psychological security, and the institutional aspect of internet governance [ref]. We can see from analysing Western discourse that a narrower understanding of the term predominates – one concerned with the security of data and infrastructure. Whereas, in Russia and other areas of the globe including China, the term becomes conceptually broader – encompassing fundamental issues of regime security. Indeed, the term ' 'international information security' has been invoked to describe the position typical of Russia [Zinovieva, 2013]. Here, concerns over the security of data and critical infrastructures are coupled with those from potentially hostile information, attacks, and propaganda that could be used with the aim of undermining an incumbent regime. The inauguration of such conceptual broadening was promoted by the colour revolutions in Russia's 'near abroad' and the 2012, DDoS attacks on Golos during the Russian presidential election, and the 2011 Arab Spring, to name but a few of these junctures.

[The Problem of Attribution]

The development of new technologies shaping our ways to communicate in a networked society has also brought many new challenges, which in turn shape the way policy makers and experts try to address the

new issues. One problem which has arisen after the first international cyber attacks on Estonia and Georgia is the problem of attribution.

The problem of attribution is becoming increasingly difficult to solve. Being able to identify an attacker is prerequisite for being able to requite the attack (Tsagourias, 2012), or to build up an effective defence (Mejia, 2014). The ability to identify foreign attackers as well as domestic ones is crucial in order to press legal charges against them or to demand compensation for the damage done.

From a legal point of view there is a gap between the ability to punish civil perpetrators, who committed cyber crimes against state agencies or other private persons and the ability to sanction attacks carried out on behalf of a state against other states either by state actors, or private citizens often calling themselves "hacktivists". While many states nowadays have enough suitable laws addressing offenses tied to different forms of cybercrimes, there still isn't any kind of international framework in place, which could be used to address the issue of cyber attacks in a comprehensive way.

Possible ways to address the issue mentioned by scholars is the use of Article 2(4) of the UN Charta which is prohibiting the use of force against other states (Waxman, 2011) or the use of Article 51 of the UN Charter which defines the right to self-defence of individual states in the case of an attack (Tsagourias, 2012) combined with the use of the Law of Armed Conflict, which in turn sets certain limits to the scope of counterattacks (Mejia, 2014). They argue that a point can be made that cyber attacks carried out against other states can be interpreted as use of force. Nevertheless it becomes evident quite fast that such an interpretation and the according readiness of international actors to acknowledge cyber attacks as use of force depend heavily on the perception of the risks tied to such attacks and the opportunities they pose for different state actors. Therefore, so far, there isn't an international group of actors, which is big and powerful enough to address the issue on an international level in front of the UN.

Still, even when experts and politicians could agree on defining cyber attacks as use of force as described in the UN Charter, there still would be the problem of attributing such attacks to a state in a manner, which would be sufficient from a legal point of view. One approach proposed by scholars (Allan, 2008) is to use the Draft articles on Responsibility of States for Internationally Wrongful Acts (International Law Commission, 2001). The draft is in big parts based on two hallmark cases of international law: The so called "Nicaragua" case which addressed the support of Nicaraguan rebels through the US and the "Tadić" case, which was part of the International Criminal Tribunal for the former Yugoslavia. The draft proposes tests to assess whether actors acted under the direct control of a state or were instructed by a

governing state. Both instances would warrant the attribution of attacks to a state. The draft seems at first glance to be a good legal tool, because it provides a way to hold states responsible for attacks carried out by non-state actors as well. The tests described in the draft also seem to provide at least in theory a concise and comprehensive way to assess the contribution of state actors in attacks on other entities. Nevertheless, the hurdles to pass those legal tests are quite high, because they of course are supposed to prove beyond a reasonable doubt that certain state actors were involved in the attacks themselves, or that they provided support for the whole attack and not just only parts of it. Therefore the mentioned approach poses a possible way to address the problem of attribution but it has to be taken into account that the draft was written with classic conflicts in mind and is in many ways too restrictive for modern cyber attacks (Allan, 2008).

Besides the legal aspects mentioned the problem of attribution is furthermore also intrinsically paired with the problem of deterrence (Young, 2016). In classic warfare, especially during the Cold War, where there was an identifiable enemy, building up means of deterrence was an easier task for everybody involved. Simply put, most actors knew in which direction to point the missiles. Nowadays on the other hand, the situation changed dramatically.

Due to the fact, that it's hard to pinpoint the origins of many attacks it also became quite hard to build up a credible deterrence. As long as perpetrators can safely assume, that they're not going to be identified, any kind of threat of retaliation remains quite void in nature (Bendiek & Metzger, 2015).

Therefore the problem of attribution in the realm of cyber warfare, cyber espionage and etc. eventually has shifted the focus from trying to find useful means to attribute attacks to the perpetrators, to finding efficient means to defend oneself from those attacks and to maintain operations while under attack (Clark & Landau, 2011). Furthermore it showed that definitions used so far need to be adjusted and maybe even broadened in order to encompass all the aspects of cyber warfare. It's rather obvious by now, that the tools used in cyber attacks became more sophisticated and that possible consequences of cyber attacks in the real world have been neglected for too long.

[The European Perception]

Three decades ago, the European Union (EU) started to develop as a security actor. From the late 1990s on, a network of regulations and initiatives emerged in the area of cybersecurity, “aimed at fostering Member State (MS) awareness and shared concern” (Carrapico&Barrinha, 2017, p. 6). Only in the 2000s,

when the vulnerabilities to post-Westphalian threats become apparent, did cybersecurity become a priority in the EU's security strategy. This not only led to an increasing emergence of legally binding initiatives but also reinforced the idea that *coherence* was a crucial part of efficiency, and that this should be accomplished at the EU level. Coherence refers here to consistency and coordination between MS/institutions of the EU.

In 2013, the European Commission (EC) introduced the *EU Cyber Security Strategy*, the first coherent policy response to cyber threats. It is driven by three main motivations: (1) the economic motivation: because EU economic growth and health require a robust digital and telecommunications infrastructure, cyberspace should be, in the parlance of the strategy, `open, safe, and secure´; (2) the political motivation: reliable EU cybercapabilities require a multi-stakeholder governance model; (3) the ideological motivation: the same norms, principles and values that the EU seeks to uphold offline—the protection of fundamental rights like the protection of personal data, freedom of expression and the rule of law--should also be secured online (EU Cyber Security Strategy), which means that the strategy is based on political, social and economic rights stated in the Charter of Fundamental Rights of the EU.

The priorities of the strategy are the following: "enhance the cyber resilience of IT systems, reduce cybercrime and strengthen EU international cyber security policy and cyber defense" (European Council, 2017). Resilience aims at enhancing the level of preparedness, in order to ensure rapid recovery from cyber disruptions and deter adversaries from attempting attacks. In 2015, the EC presented the European Agenda on Security 2015-2020, which states cybercrime as a priority, together with terrorism and organized crime. As apparent in the most recent communiques[1], the EU follows a socio-economic approach to cyber security, i.e. it aims at enhancing prosperity, rather than accomplishing military objectives alone. This has been the case for three decades.

While Russia can implement coherent cybercapabilities, capacity building is a serious challenge in the EU because the sovereign MS each have their own *National Cyber Security Strategy (NCSS)*. Accordingly, one of the main challenges is the high level of fragmentation of cyber infrastructure, capabilities and priorities between the MS. The EU attempts to propose a common approach by founding agencies devoted to cybersecurity: *The European Cyber Crime Center (EC3)* aims to increase cooperation between MS. *The European Union Network for Information Security (ENISA)*, established in 2004, focuses on building up cyber resilience by helping MS to identify and strengthen weaknesses in their

[1] *The Digital Single Market Strategy* of 2015 and *The Communication on Strengthening Europe´s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* of 2016.

cybercapabilities. *The Network and Information Security Directive (NIS Directive)* is the first piece of EU-wide cybersecurity legislation and entered into force in 2016. It attempts to both build up MS cybersecurity capabilities by demanding that they have the relevant technical equipment, and strengthen inter-MS cooperation and information exchange by creating a cooperation group (EC: NIS Directive).

Although measures have been taken to build a coherent EU cyberspace policy and promote core values, limitations remain. As mentioned, the level of fragmentation between MS challenges efforts of capacity building in the EU. "While all MS acknowledge the need to act against cyberthreats, views differ significantly on how best to achieve network and information security" (European Parliament, 2015, p 48). In addition to these difference in norms and values, there is the challenge of balancing responsibilities between the sovereign MS and the powers of EU institutions: While defense falls into the responsibility of the sovereign MS, the *Common Security and Defense Policy (CSDP)* is an integral part of the *Union's Common Foreign and Security Policy (CFSP)* (EU Facts Sheet, 2017).

The highly differentiated set of responsibilities within the EU complicate the effort of establishing a common cyber infrastructure. In order to protect fundamental rights, democracy and the rule of law in the EU--online and offline--from increasing cyber threats, a cooperative, streamlined and coherent cyber infrastructure is crucial.

[Estonia's Cyber Attack in 2007]

In 2007, Estonia was targeted by a series of massive denial of service attacks. This first cyber attack on a state has also been called, by some commentators, *Cyber War I* (Klimburg, 2017, p. 59). The attacks followed the relocation of a soviet war memorial, the Bronze Soldier of Tallinn, to the outskirts of the city, which led to a serious dispute between the Estonian and Russian governments. The massive DDoS (Distributed Denial of Service) attacks, which took place over the course of three weeks, disabled the websites of Estonian government bodies, media, companies and banks. Estonia uses e-government services to large extent, which makes it especially vulnerable to cyber threats. The attacks were so severe that the government had to cut the global internet connection, i.e. prevent everybody but the domestic population from accessing the targeted pages. Despite the problem of attribution, "today, the cybersecurity community generally accepts that the FSB not only was guilty of allowing the attacks to happen but also ordered them directly" (Klimburg, 2017, p. 234).

A major digital initiative by the Estonian government—offering Estonian e-citizenship—can be seen as a consequence of the attacks. The initiative allows anyone who passes a background check and spends 64 USD to *become a citizen of a new digital nation for global citizens, powered by the Republic of Estonia*[2]. The benefits are twofold: (1) the e-card enables the new e-resident to open a bank account and start an online business; (2) Estonia "increased in size (and connections) in cyberspace" (Segal, 2017, p. 74), which distributes more broadly, i.e., to citizens of multiple nations, the effects of any cyber attack on Estonia. This is thought to raise the risk to an adversary of launching such an attack. These geopolitical implications compensate for the relative size (geography and population) and location of Estonia.

The series of attacks on Estonia in 2007 (and the extensive international media coverage) were a critical juncture in the development of the country's threat perception, which influences strategies and alters national leaders´ priorities with respect to the significance of cyberspace in their relations with other states. According to most analysts, "national perceptions of cyber threats largely conform to a country´s existing security priorities, but the global attention paid to incidents like Estonia (…) helped to elevate cybersecurity as a national security concern" (Lewis, 2014, p. 655-567). Nothing is more impactful on a government's understanding of its national security threats than having been attacked in a particular way, e.g. by having its crucial digital infrastructure compromised or disabled.

[The U.S. Perception]

The United States is widely thought of as the most capable nation in the world in terms of cyber capabilities (Maness and Valeriano 2015). The nation possesses a wide pool of individual and professional talent, as well as well-funded and technologically innovative cyber defence programs on a governmental level. However, as the world's sole superpower, the U.S. is often primary target for technologically accomplished dissident groups, terrorists, and rogue states that may have an interest in challenging the supremacy of the U.S. or in illegally seizing corporate, or scientifically sensitive data. Indeed, without the possession of a 'kill-switch' as witnessed in China, enabling the immediate cessation of external Internet traffic flows to China; nor, a detailed monitoring of all incoming Internet flows by the secret services, as in Russia, the U.S. remains highly vulnerable to cyber threats originating from beyond her borders. As a natural product of the foundation doctrines of personal freedom and economic liberalisation, 85% of Internet infrastructure in the United States lies in private hands (Cherian, 2011). This has complicated U.S. efforts to strike an optimal balance between these ideological principles on the

[2] Website of the Republic of Estonia:https://e-resident.gov.ee (as of 28 September 2017).

one hand, and security on the Internet on the other. Indeed, rogue or government-sponsored groups originating in China, which are responsible for over half of recorded cyber operations in the U.S. (Maness and Valeriano, 2015) have been able to steal many cases of sensitive data from the free and open American network. Botnets, allegedly from Russian sources, were able to infiltrate the U.S. Eastern power grid in 2009 and 2013.

Incidents of this nature had, and still do have, the potential to cause serious economic and strategic damage. The more 'plugged in' a nation is, the more it relies on cyber networks for vital domestic operations, the greater are the costs of being a victim of cyber malice. As such, in a manner consistent with the framework presented by (Lewis, 2014), it is this heightened exposure and vulnerability that most saliently influences perception. Concerns over cyber security permeate elite levels of business as well as governmental administrations with North American executives ranking the issue as their 4th highest risk priority [out of 50]. The comparison with a much lower ranking by Asian executives demonstrates the greater importance attached to securing cyber networks.

As with Europe, the United States' position can best be understood by examining the philosophical foundations of their dominating narratives. U.S. administrations have consistently sought to privileges transparency, the projection of human rights over the web, freedom of speech and association and free flows of information. The Western liberal philosophical tradition allows for the resultant fragmentation of cyberspace. This individual sovereignty, which impeded the approval of a U.S. equivalent of a 'kill switch' by Congress, can be contrasted sharply with the idea of state sovereignty and inviolability of sovereign borders into cyberspace expounded by authoritarian states such as Russia and China.

[The Russian Perception]

The contrasting cybersecurity policy of Russia to the USA and Europe rests on some clear distinctions. Firstly this a norm based view of the international system, that directly influences Russia's cybersecurity policy, and secondly an alternative view on what constitutes cyber security, that prioritises terminology focussed on information security.

It is argued that Russia's cyber policy is deeply informed by its own approach to the international system and law, in particular the privilege given to state sovereignty and the principle of non-intervention. (*Nocetti 112*) This is what will be referred to as Russia's 'cyber-norms', of which a crucial part is Russia's striving towards an international cyber space of digital sovereignties. Russia has been proactive in promoting these norms through multiple international institutions, and Russia's President Vladimir

Putin has stated on several occasions that global cyberspace should be governed by international institutions operating under the United Nations. (*Nocetti 122).*

The explanations for this approach vary. Whilst some put this down to a simple concern about the effects of massive cyber attacks on critical information infrastructures, some critics have identified Russia as a country that might be lagging behind in cyberspace, and the regulation provided by an international treaty on cyber security would be one way to gain control over the advancements rival states are making ahead of Russia (*Heickero* 50).

This has also been met with support from big cyber players. Russia, alongside Uzbekistan and Tajikistan, were joined by China in 2011 for the submission of a proposal for an *International Code of Conduct for Information Security* at the UN General Assembly. In considering this regional support some experts see a demographic shift to the non-western world of internet users which provides a greater opportunity for authoritarian and emerging countries to flex their authority in cyberspace.(*Nocetti 120)*. If one reflects upon the claimed 'resurgence' of Russia as an international player, the promotion of these alternate cyber-norms shapes cybersecurity for not just Russia, but regional hubs it is a part of, allow Russia greater status power in the international system, and most importantly as a normative power in cyberspace. This creates a greater challenge for cooperation between Russia and the West on this issue, as it is not a lone player in its views on cybersecurity, but instead has appealed successfully to gain leverage for some of these norms from countries within its regional order and outside.

The prevalence of the term *information security* in Russian discussion on cyber security is crucial to note. As Kier Giles points out, there is a conceptual gap that leaves "cyber" in terms of warfare being absent in Russian analysis. It has until recently being portrayed as a purely American phenomenon. (GILES 74). These concerns over cybersecurity predominately refer to concerns over information security, which is highlighted in the way Russia has been seen to view these features as a threat. *Information security* and *information space* are reflective of broader philosophical and political meanings. (*Nocetti 126)* As one analyst notes, where Western states discuss cyber security as its own stand-alone issue, Russia opts for a discussion on information security as an overall holistic concept, with cyber security as a subset of concerns *(Giles 70*). Tellingly, since 1998 every year at the UN, Russia has put forward resolutions to prohibit 'information aggression'.(*Nocetti 122*) Therefore, the role of information-psychological factors shows crucial divergence in Russia's approach. Explaining this is the context by which the policy developed, with the collapse of the Soviet Union and the wars in Chechnya, where the role of information and the psychological factor played significant roles in shaping the outcomes of these events. In a

Parliamentary hearing titled "*Russia and the Internet: The Choice of a Future",* in 1996, the head of the security body responsible for cyber affairs at the time characterised the internet as a whole as "a threat to national security", highlighting caution that existed in cyber policy making circles. (*Giles* 81). This developed into *The Information Security Doctrine of the Russian Federation 2000,* detailing the liberal provisions like the free exchange of information as similar to the trends in the West at the time, but also guaranteeing the protection of "strategically important" information from foreign activities directed against the interests of the Russian Federation in the information sector (*Heickero 18)*. Therefore, post-Soviet Russia's early cybersecurity policy prioritised a form of information governance, which highlighted the threat of information, particularly foreign, to national security.

Multiple social movements have arguably increased this threat in recent years. The events of the Coloured Revolutions, the protests after the 2011 Russian Presidential Election, the Arab Spring, and Ukraine's Euromaidan, have displayed the influence of information and internet access in posing a threat to regime security. Dmitri Medvedev's statement on the link between Western social networks and political unrest – They have been preparing such a scenario for us, and now they will try even harder to implement it' reflects the fear of regime survival and anti-Western inspired perceptions of cyber threats. (*Lewis 573-574*)

An updated version of the 2000 doctrine, *The Information Security Doctrine of the Russian Federation 2016* , reveals a significant strengthening of cybersecurity, albeit not explicitly. It stipulates that there should be developed a 'national system of Russian Internet segment management.' A major insight can be drawn from this. As mentioned previously, a lack of any international treaty on cyber space, has led to the Russian government fortifying its own cyber space. This therefore signals Russia's own digital sovereignty, contrary to the more "open" international internet space that can be seen in the American approach. A case in point is the ban on the social media platform LinkedIn due to the creators' refusal to allow the data of Russian users to be kept on servers outside of Russia, and early proposals to ban Facebook for similar reasons by Russia's telecom authorities. This signals a digital sovereignty where Russia's own rules must be respected when it comes to citizen data, and establishing its own internet space when an international treaty does not exist.

[Conclusion]

In our paper we analyzed and compared the formation of cyber security from the European, Russian and American perspectives; we also discussed the problem of attribution because of its unique effects on

security strategy. Before turning to the three national perspectives, we can summarize the attribution problem briefly. Since the ability to identify attackers is thought to be necessary for being able to counter the attack, build up an effective defense, or project credible deterrence, the technical difficulty of locating with certainty the source of cyber attack has led policy makers in recent years to focus more structural resilience. That means finding efficient means to defend against attacks and to maintain operations and critical functions while under attack (Clark&Landau, 2010).

The European perspective on cybersecurity is based on political, social and economic rights stated in the *Charter of Fundamental Rights in the EU*, aiming at an ´open, safe and secure´ cyberspace. The main challenge of cyber capacity building in the EU is the high level of fragmentation between the MS. However, in a similar vein to that of Europe, American perceptions of cybersecurity prioritise individual sovereignty, transparency and freedom of information. This erosion of borders, facilitated by digital technology is seen as a method of upholding their dominance and international influence. Conversely, Russian perspectives place heavy emphasis on national digital sovereignty, and is grounded in the narrative of the strong state. This is consistent with foreign policy exercises in other areas, and has been promoting through multiple international institutions.

The main discrepancy between the three regions is between their respective discourses on cybersecurity. EU and US discourse uses a narrower understanding of the term: primarily, it refers to security of data and infrastructure. Russian discourse employs a conceptually broader sense, which includes informational threats of all kinds under the rubric of regime security. Due to the lack of an international framework on cybersecurity, Russia aims at digital sovereignty, meaning a fortification of its own national cyberspace. As mentioned, the US and EU both prioritize an open cyberspace that facilitates transparency, freedom of speech and free flows of information, which defines another important divergence between the three regions. Finally, while Russia can implement a coherent cyber security strategy, capacity building is a challenge for the EU and the US. As mentioned, the EU is confronted with a high level of fragmentation between its MS; in the US fragmentation is a result from 85% of its national Internet infrastructure being in private hands (Cherian, 2011).

The case studies such as the Estonia DDoS attacks of 2007 show how such events have shaped the threat perception of relevant actors, and thereby informed their strategic policies concerning cyber security. Indeed, we would like to echo the following sentiments of Lewis (2014): “Cyberspace is better understood if we do not think of cyberspace as a domain, but rather adopt Clausewitzian notions and see it as an extension of interstate politics.”.

Recent work identifies that the major challenge in this area involves shifting from a reactive policy to a coherent, proactive cyber strategy that will efficiently contribute to the pursuit of national interests. This is likely to depend not only on learning the right lessons from previous attacks, but also on a major effort by the EU, the US, Russia, and other actors to engage in cooperative multilateral negotiations.

Bibliography

Allan, C. (2015). Attribution Issues in Cyberspace. *Chicago-Kent Journal of International and Comparative Law, 13*(2), 57–82.

Bendiek, A. & Metzger, T. (2015). *Deterrence theory in the cyber-century*. Retrieved from https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-MetzgerWP−Cyberdeterrence.pdf

Carrapico, H. & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies.* doi:10.1111/jcms.12575

Christou, G. (2014). *The EU's Approach to Cyber Security*. EUSC Policy paper series Autumn/Winter2014.

Clark, D. & Landau, S. (2011). Untangling Attribution. *National Security Journal, 2*(2).

Department of Defense (2011). *Department of Defense Strategy for Operating in Cyberspace.* Retrieved from https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy

European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved from http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec commen.pdf

European Commission (2015). *Digital single market: Bringing down barriers to unlock online opportunities*. Retrieved from https://ec.europa.eu/commission/priorities/digital-single-market/

European Commission (2015). *The European Agenda on Security*. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu agendaonsecurityen.pdf

European Commission (2016). *Strenghtening Europe´s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

European Commission (2016b). *The Directive on security of network and information systems (NIS Directive)*. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Council (2017). *Reform of cyber security in Europe*. Retrieved from http://www.consilium.europa.eu/en/policies/cyber-security/

European Parliament (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL

European Parliament (2017). Common Security and Defence Policy. Retrieved from http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_6.1.2.html#_ftn1

Giles, K. (2012). Russia and Cyber Security. *Nação e Defesa (Journal of Portuguese National Defence Institute), 133*, 69–88.
Heickerö, R. (2017). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. FOI Swedish Defence Research Agency.
International Law Commission (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Retrieved from http://www.refworld.org/docid/3ddb8f804.html
Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. London: Penguin Publishing Group.
Lewis, J. A. (2014). National Perceptions of Cyber Threats. *Strategic Analysis, 38*(4), 566–576. doi:10.1080/09700161.2014.918445
Maness, R. & Valeriano, B. (2015). *Russia´s Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*. Basingstoke: Palgrave Macmillan.
Mejia, E. (2014). Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. *Strategic Studies Quarterly, 8*(1), 114–132.
Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111–130. doi:10.1111/1468- 2346.12189
Samuel, A. (2011). Prospects for India-US Cyber Security Cooperation. *Strategic Analysis, 35*(5), 770-780.
Segal, A. (2017). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. New York, NY: PublicAffairs.
Soldatkin, V., Stubbs, J. & Teterevleva, A. (2016). *Russia upholds LinkedIn ban over data protection fears*. Retrieved from http://www.reuters.com/article/us-russia-linkedin/russia-upholds-linkedin-ban-over-data-protection-fears-idUSKBN1351PV.
The Ministry of Foreign Affairs of the Russian Federation (2017). *Doctrine of Information Security of the Russian Federation*. Retrieved from http://www.mid.ru/en/foreign policy/official/assetpublisher/CptICkB6BZ29/content/id/2563163.
Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict & Security Law, 17*(2). doi:10.1093/jcsl/krs019
Waxman, M. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law, 36*(2), 421–458.
Young, N. (2016). *The Blame Game: Attribution in the 2016 Elections*. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2016/nyoung.pdf
Zinovieva, E. (2013). *International Information Security*. Moscow: MGIMO University Press.