European Journal for Security Research
https://doi.org/10.1007/s41125-020-00070-0

ORIGINAL ARTICLE

Russia's Critical Infrastructure Policy: What do we Know About it?

Christer Pursiainen[1]

Received: 10 June 2020 / Accepted: 14 October 2020
© The Author(s) 2020

Abstract
The article is an analytical state-of-the-art review of the Russian Federation's critical infrastructure policy, starting from the 1990s but zooming in on the current situation. The article discusses what does critical infrastructure mean in the Russian context. It explores the country's threat scenarios in this field, and asks what part is played by cyber security threats in this context. Further, the article elaborates the issue whether Russia's policy is focused on critical infrastructure protection, or has the country adopted the more recent concept of resilience that puts emphasis on adaptive measures and recovery. Finally, it is considered who are the actors in Russian critical infrastructure policy and, in particular, how does Russia deal with the fact that the respective infrastructure operators even in Russia usually are not directly state-owned entities, but private companies.

Keywords Russian critical infrastructure · CI protection · CI resilience · Cyber security · Russia's threat pictures

Critical infrastructure (CI) has since early 2000s gained importance in the European Union (EU) and its Member States (e.g. Pursiainen 2009, 2018; Aradau 2016; Lazari 2014). Consequently, there are many policies, multinational projects and multidisciplinary academic debates on the issue. At the same time, we do not know much about what is happening in the Russian Federation in this area. There is certainly very little interstate policy cooperation in this field between the EU and Russia in the era of tense relations and hybrid threats. There is neither much English-language literature on Russian critical infrastructure policy (for a rare exception, see Pynnöniemi and Busygina 2013). The scholars of traditional Russian security studies have not yet recognised the issue, and most Western CI scholars lack the language skills to this effect. Should one take a closer look at the issue, we may,

✉ Christer Pursiainen
christer.h.pursiainen@uit.no

[1] Faculty of Science and Technology, Department of Technology and Safety, Arctic University of Norway, Tromsø, Norway

Published online: 29 October 2020

however, find a rapidly growing body of official Russia's CI-related policy and regulative documents, rather vivid media discussion on especially cyber threats, and a steadily increasing Russian academic interest, especially in terms of engineering literature focusing on conceptual and modelling issues.

Hence the current study. The analysis is structured by some fundamental questions to capture the essential features of this multidimensional issue. It starts by setting the issue into a broader context of Russia's understanding of security. After that, the article traces back the emergence of Russia's more specific CI policy, and especially discusses the issue of what does CI mean in the Russian context. This is followed by a short discussion on what are the country's threat scenarios in this field. This leads to ask what part is played by cyber security threats in Russia's CI policy. Another strategic issue is scrutinised, namely whether Russia is focusing on CI protection, or has it adopted the more recent concept of resilience. Finally, the article discusses the roles of different actors in Russian CI policy.

1 Setting the Context: Russia's Broad Understanding of Security

Vulnerable infrastructure has naturally existed in Russia for a long time, yet this was—as in most Western countries—traditionally discussed with more generic concepts and policies rather than the more recent concept of CI. In Russia, this was specifically handled through terms such as 'national security', 'civil defence' and 'emergency situations'. This is largely the case even today. Yet one can see that a specific field of official policies, institutions and research has emerged since the mid-2000s that concentrates on CI in particular. It is however useful to firstly situate Russian CI policy within this more generic context, in order to understand its scope and limitations.

'National security' is perhaps the most overarching concept of the above-mentioned ones. The current Russian definition of national security is based on what in the Western literature is usually called the 'comprehensive security' approach. In addition, it includes elements of 'human security' in that it also assesses not only state security threats but also those from the perspective of individual citizens or society at large. Thus, while state-centred military-political security is still at the core of Russian national security discourse, the concept's official scope is much broader.

According to the current official definition (Ukaz 2015, Art. I, 6), national security entails the protection of 'the individual, society and the state from internal and external threats', ensuring the implementation of the constitutional rights and freedoms of citizens, a decent quality and standard of living, independence and territorial integrity, as well as sustainable social and economic development.

This is almost the same as 'civil defence', a Soviet-era term which in Russian use strongly resembles the way that the same concept was also used in some Western countries during the Cold War. The Yeltsin-era Federal Law on 'Civil Defence' dates back to 1998 (Federal'nyj zakon 1998), revitalised by the Putin-era presidential decree from 2016. Following the latter, the definition reads as follows: 'Civil defence is defined as a set of coordinated and unified political, military, socio-economic, legal, informational and special measures implemented by federal executive bodies, authorities of the subjects of the Russian Federation, local governments and organizations. [These measures are…] in the field of protecting the population, material and cultural values on the territory of the Russian Federation from the dangers arising from armed conflicts or as a result of these conflicts, as well as dangers of large-scale emergency situations of natural and technological character' (Ukaz 2016, Art. 1.2).

What in turn in the EU vocabulary is called 'civil protection' is in the Russian context simple 'emergency management', organised nationally and regionally under EMERCOM, a paramilitary Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters. Most of the traditional CI issues are included in its scope, and as such the issue is not a new one. In the post-Soviet Russia, already the Yeltsin era Federal law 'On protection of the population and territory from emergency situations of natural and technological character' (Federal'nyj zakon 1994) included many elements of typical CI policies, and the 1997 laws on industrial safety (Federal'nyj zakon 1997a, b), focusing on non-malicious hazards, are naturally closely related to typical CI protection.

In the main 1994 law (Art. 1, para 1), an emergency situation is defined as a situation in a certain territory that has developed as a result of an accident, a dangerous natural phenomenon, a catastrophe, a natural or other disaster that can result in human casualties, damage to human health or the environment, significant material losses and disruption of people's livelihoods. This definition has been detailed in lower-level regulation and strategies. As Petrova (2011, p 2228) points out, the more detailed criteria for an emergency demand that it is a situation causing 5 or more fatalities, injuring 10 or more people, disrupting the living conditions of 100 or more people, or incurring major damage amounting to more than, in the current European currency, EUR 100,000.

EMERCOM used to list emergencies by year, number and type, as well as their human consequences, on its website until 2017, after which the agency's statistics section disappeared. The three main categories were technology-generated emergencies, natural emergencies, and bio-social emergencies. The author of the current article compiled a concise survey for the period of 2013–2017 when the data were still available. While 'technology-generated emergencies' share of the total number of emergencies and related fatalities was striking, being overwhelmingly the biggest category within the range of around 100–200 emergencies annually, it must be noticed that a big majority of them were car accidents, defined as emergencies on the basis of the above criteria of fatalities/injuries. 'Natural emergencies' were usually in the annual range of 40–120 and 'bio-social emergencies' within 25–70, respectively. No publically available statistics on CI disruptions in particular can be found.

The International Disaster Database is even more inaccurate and scarce with its information, at least when it comes to CI disruptions. It tells us, for instance, that in 2018–2019 (24 months) Russia had 11 'technological disasters' (incl. 10 road, air and water transport and one miscellaneous events) and six 'natural disasters' (incl. one wildfire and five floods). For comparison, even if incommensurable in terms of metrics, during the same period EU-28 had 94 ‘natural disasters’ and 14 ‘technological disasters’ (EM-DAT Public, n.d.).

It seems that the publically available data are too rough and biased for us to draw any better picture about Russia’s CI disruptions in statistical terms. Yet, the issue as such was gaining importance early on in President Putin’s administration. The timing suggests that it might be 9/11 that triggered also Russia’s interest in CI protection, as it had done in the USA and the EU.

2 The Emergence of Russia’s Critical Infrastructure Policy

Pynnöniemi and Busygina (2013, p 565) argue that the joint session of Russia’s Security Council and the State Council in November 2003 ‘can be considered the starting point for the re-formulation of the Russian policy on CIP [critical infrastructure protection]’. In that meeting, President Putin raised the question of a new policy towards objects critical to national security and the need to protect them from man-made, natural and terrorist threats. The first principles of this policy were consequently formulated in a presidential strategy, literally an ‘Order’, from 2006 under President Putin (Osnovy 2006). Its updated version was published under President Dmitri Medvedev (Osnovy 2011/2017), with the latter extending up to 2020.

It has been claimed that 2014/2015 (after the annexation of the Crimean peninsula) marked a turning point in this development. Within a very short time, ten federal laws, two presidential decrees, more than 20 resolutions and orders of the Government, and more than 40 subordinate acts of federal executive bodies were adopted (Azanov et al. 2015). Thus, at the legislative level, in 2015 a more explicit notion of CI was added to the above-mentioned main law on emergencies (Federal’nyj zakon 2015; incorporated in the current version of: Federal’nyj zakon 1994). Translated literally, the concepts that were used were ‘critically important objects’ and ‘potentially dangerous objects’, which together comprise the official Russian-language equivalent of CI. The amendment made the Government (not mentioning any ministry in particular) responsible for establishing ‘the criteria for classifying objects of all forms of ownership of critical objects and potentially dangerous objects’, and for preparing and approving a list of critical facilities and a list of potentially dangerous objects, as well as the required performance requirements of these objects (2015, Art. 3).

While previous but lower-level presidential strategies (Osnovy 2006, 2011/2017) were also literally about ‘critically important objects’ and ‘potentially dangerous objects’, they nevertheless failed to define what kind of objects they are in any categorical terms. It seems that one of the first official definitions can be found in the context of critical information infrastructure (CII) and automated control systems (ACS) in a presidential strategy published in 2012 (Osnovye napravlenija 2012). It is almost the same definition that was subsequently presented in the 2015 version of the main law on emergencies. In the latter, the definition reads: ‘A critically important object is an object whose violation or termination of its functioning will lead to a loss of economic management of the Russian Federation, a constituent entity of the Russian Federation or an administrative and territorial unit of a subject of the Russian Federation, its irreversible negative change (destruction) or a significant decrease in the safety of the population' (Federal'nyj zakon 1994, incorporated amendment from 2015, Art. 1, para 3).

The concept of a 'potentially dangerous object' was also defined. This kind of object was characterised as 'an object on which buildings and structures of an increased level of responsibility are located, or an object on which more than five thousand people can simultaneously stay' (Federal'nyj zakon 1994, incorporated amendment from 2015, Art 1, para 4). A more detailed definition of this lesser level of criticality, compared to a 'critically important object', can be found in an earlier 2012 EMERCOM document. According to the latter, 'potentially dangerous objects' are such 'that use, produce, recycle, store, liquidate or transport radioactive, flammable or explosive, chemically or biologically hazardous material, as well as hydrotechnical objects, that may cause a real danger of an emergency situation' (Metodika 2012, Part 1, para 2).

In the same document, a methodology for prioritising the objects is presented, aiming at contributing to a national list of these infrastructures. It divides them into three main classes. First, objects where the highest state organs of Russia are or could, in certain circumstances, be placed. This obviously refers to bunkers or redundancy locations that all states have for their leadership in times of crises if under attack. Second, objects that could be used by terrorists in order to violate state security and destabilise state structures by pressuring the highest state organs in their decision-making. Third, objects whose termination of functions would lead to a threat to the national (information, economic, military, foreign policy, ecological, chemical, radiological and biological) security of Russia.

Besides 'critically important object' and 'potentially dangerous object', one can find other related concepts, such as a 'life support object' (some examples include water pump stations or food stores) and 'regime object' (such as military units). The use of all of these CI-related concepts is often unclear. Therefore, it has been noted that the lack of uniformity in the conceptual apparatus leads to confusion, which complicates the division of powers of special bodies for the protection of these objects (Strokin 2014b).

In any case, the 2015 amendments to the 1994 main Federal Law seemingly paid off and led to a concentrated effort to list the CI in Russia. One can currently find from open sources a full *sectoral* list of the 'critically important objects', including six sectors and under them 48 subsectors: (1) nuclear and/or radiation hazardous facilities; (2) chemically hazardous facilities; (3) biological hazardous facilities; (4) technogenic hazardous facilities; (5) fire and explosion hazardous objects; 6) objects of public administration, information and telecommunications infrastructure (KVO n.d.).

What do we know beyond the classification of the CI sectors presented above? The 2011 strategy document on CI (Osnovy 2011/2017, Art. II, 7) mentions that 'more than 90 million people (60 per cent of the country's population) live in zones of possible impact from damaging factors resulting from accidents at critical and potentially dangerous objects'. In one EMERCOM document (currently not available), the percentage shares of 'critically important objects' and 'potentially dangerous objects' from the total number in each of Russia's federal districts were presented in a map a couple of years ago (MChS, n.d.), reproduced in Table 1.

This information implies that CI facilities in Russia have been mapped in some detail at least. Indeed, one can find from open sources at least one Federal District's detailed list on its 'critically important objects' and 'potentially dangerous objects'. It is mentioned that the list had been approved by the Governor, based on the decision of the 'regional anti-terrorism committee'. The list consists of the names of 50 regional CI facilities and their addresses.

We can thus conclude that Russia's national CI policy is established and that it has been gradually incorporated into the legislation, expressed in official strategies and implemented on regional levels.

3 The Securitised All-Hazard Approach

In the Western CI debates and policies, there has been certain tension between whether one should focus on terrorism or on all possible threats, the latter often being referred to as the all-hazards approach (see e.g. Pursiainen 2009, 2018). Russia has faced the same challenge.

Terrorism is undeniably a real threat in contemporary Russia, resulting in approximately 3000 fatalities to date. Terrorist attacks became a more or less regular occurrence starting from the early 1990s, mostly connected to separatist movements, intensifying from late-1994 onwards on account of the Chechen wars. While terrorist attacks are seldom directly targeted against CI, either in Russia or elsewhere (Stepanova 2010), soft targets in Russia such as public transport and public buildings have been common objects, challenging the state in terms of undermining its ability to take care of the safety and security of its society and citizens. Lately, it seems that terrorism in Russia has become more closely connected to violent international jihadist movements. According to Russian intelligence sources, as President Putin publically stated in February 2017, around 4,000 Russians were then fighting for militant forces in Syria (*The Moscow Times* 2017), many of whom would create a terrorist threat in their Russian homeland in the future. The issue of possible

Table 1 Distribution of 'critically important objects' in the Russian Federation/Federal Districts

Distribution of 'critically important objects' in their RF/federal district	%
Central	25.57
Volga	18.16
Northwest	16.35
South	10.02
Siberian	9.73
Ural	9.61
Far East	6.44
North Caucasus	4.12

Source : MChS (n.d.), extracted from the map increase in radicalisation in the Central Asian countries and its spill over to Russia is also a realistic threat picture (Azimov 2020).

Yet the Russian approach to CI can to all intents be termed an all-hazards approach. The currently valid national security strategy (Ukaz 2015) provides perhaps the best overview of the range of threats that Russia's highest-level decision-makers prioritise in their generic security planning. It identifies seven groups of hazards, covering a huge spectrum of threat scenarios. Of these, some are only indirectly linked to CI, whereas others are such that CI is clearly an object of the threats.

First, the strategy pays attention to threats caused by intelligence and other activities by special services and organisations of foreign states or individuals, damaging Russia's national interests. Second, the strategy mentions the activities of terrorists and extremist organisations aimed at violently changing the constitutional system of Russia, thereby destabilising the work of public authorities, destroying the operations of military and industrial facilities, disrupting the life support facilities of the population, transport infrastructure, and in general terrorising the population. Third, the strategy raises as a national threat the activities of radical public associations and groups using nationalistic and religious extremist ideology, as well as foreign and international non-governmental organisations, financial and economic structures, and individuals. The fourth threat picture consists of the activities of criminal groups, including transnational organisations. Fifth, the national security strategy is concerned about activities related to the use of information and communication technologies for the dissemination and propaganda of the ideologies of fascism, extremism, terrorism and separatism. These are said to be aimed at inflicting damage on civil peace, and political and social stability in society. Sixth, the strategy discusses criminal encroachments, directed against a person, property, state power, or public or economic security. Finally, the national security strategy raises the issue of natural disasters, accidents and emergences, including those related to global climate change, the deterioration of the technical condition of infrastructure facilities, as well as fires.

Separate from the list of threats as such, special attention in the national security strategy is also paid to economic security in terms of supply chain and self-sufficiency. In short, this means that Russia should implement rational import substitution as well as the reduction of critical dependence on foreign technologies and industrial products. Furthermore, subjects such as science, education, health and culture, among others, find their own sections in this national security strategy, but in these fields Russia sees both threats and opportunities.

Other official documents are in line with the national security strategy but with slightly different emphases in terms of the order of priority. In the civil defence degree (Ukaz 2016), for instance, the threat of the outbreak of armed conflicts and the probability of epidemics, including those caused by new, unknown agents of infectious diseases in humans and animals, are mentioned.

All in all, the Russian approach seems to rely on a very broad basis of threat scenarios. While not that different from many current Western policies, the impression is that several fields of normal societal activities are currently securitised in Russia and have therefore become objects of state control and punishment. The practice has shown that legal labels such as extremism or terrorism have efficiently been used to discipline political opposition and dissidents (Kravchenko 2019). This concerns critical civil society activities, especially religious and other minorities, which can be now defined as anti-state forces following the new anti-extremism legislation (e.g. Nuñez-Mietz 2019; Østbø 2017).

4 Cybersecurity Threats and the FSB-led 'unified state system'

In Russian security research literature, CII has been a rather popular theme for some years now, often looking at Western experiences with the aim of enhancing Russia's own CII security (e.g. Smekalova 2019; Massel' et al. 2016; Kalashnikov 2013; Dodonov et al. 2007). The basic Russian assumption, analysed in some Western studies (e.g. Kari 2019; Kukkola et al. 2019), is that Russia is surrounded and constantly under the threat of external cyber attacks. While no official public statistics can be found, according to figures presented by Russian leadership, about 70 million cyber-attacks on Russian information resources are registered annually, including attacks against CI. The most public attention was paid to the August 2015 'spy planted' malware infection that hit some 20 Russian scientific and military institutions, defence contractors, and public authorities, as well as the massive November 2016 attacks against Russia's financial sector. Russian experts expect more attacks on production facilities and the Internet of Things devices (Tass 2017; Sayer 2016).

CII has not been highlighted in the above-discussed presidential decrees on national security (Ukaz 2015) and civil defence (Ukaz 2016), but it has remained a separate field in a way. This is so probably more from bureaucratic than political reasons. Yet it is clear that Russia is readying itself for cyber-attacks, and even a cyberwar, and the country is actively making both offensive and defensive preparations.

Focusing on the defensive side, thus taking Russia as the object of cyber threats, the regulatory activity in the field of CII started in the mid-2000s, but was not without its problems. In 2006, a bill 'On features ensuring the informational security of critically important objects in the informational and telecommunications infrastructure' was introduced. Following the generic Russian approach in security issues, the aim was to create a unified state-controlled system for all ICT in Russia, to establish a registry of critically important ICT objects, and to train a qualified staff to this effect. However, the bill was withdrawn, probably due to economic reasons and inter-agency conflicts. Different versions of this law bill remained circulating in the State Duma, but the bill never proceeded further until 2017.

Meanwhile, under then President Medvedev, a rather comprehensive presidential strategy about cyber threats was published (Osnovnye napravlenija 2012). The threat scenario is related to disruptions of the Automated Control Systems (ACS) and Supervisory Control and Data Acquisition (SCADA) of the 'critically important objects'. These threats might be malicious or non-malicious. They were said to potentially damage the country's foreign policy interests, law and order, or defence capability. Cyber-attacks may also cause accidents and disasters, lead to riots and societal unrest, or result in long disruptions in transport, production or technological processes.

At the very beginning of Putin's third term, a presidential decree was introduced entitled 'On the establishment of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation' (Ukaz 2013). Compared to the national security and civil defence decrees discussed above, which are dozens of pages long, this one-page decree is laconic and does not provide much information. Its only important message is that it conferred the authority in this field to the Federal Security Service (FSB), including the interaction with the owners of the country's often privately-owned information resources. However, the decree proved to be the beginning of a rather comprehensive CII policy.

In July 2017, a Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation' (Federal'nyj zakon 2017) was adopted. Some weeks before the new law was adopted, the Deputy Secretary of Russia's Security Council praised the Russian CII protection system, saying that the country had, following Putin's above-mentioned decree from 2013, already developed a state system 'to detect, prevent and eliminate the consequences of computer attacks on the information resources of the Russian Federation' (Sputnik 2017b). The FSB had namely in 2013 started to create a system known as 'GosSOPKA', whose purpose was to shield all government information resources under the protection of a single system with constantly monitored perimeters. The idea was that this shield would before long extend to all CI, with a shared information and command system. The system would be divided into response centres in different regions and government departments, coordinated by the FSB-led National Coordination Centre for Computer Incidents (hereafter federal CII agency). Such a subordinated response centre was, for instance, created by Russia's Central Bank and named the Financial Sector Computer Emergency Response Team (FinCERT, n.d.) for monitoring and responding to computer incidents in the credit and financial sphere. Through this sub-centre, banks could share information about cyber-attacks, analyse them, and obtain recommendations from Russia's intelligence agencies about how to defend themselves (Turovsky, Chs. 2 and 4, 2017).

The new CII 2017 law was designed to formalise this already existing system. Presenting the bill to the State Duma, the FSB's Deputy Director informed that Russia was now prepared to repel cyber-attacks and underlined that the Russian CII would use domestically-developed components only (Sputnik 2017a). In the research literature, often from scientific academies belonging to EMERCOM, one can, however, detect that the ACS in particular remained a weak link in CI and CII protection (e.g. Ivanov and Ryzhko 2016).

Being a horizontal concept, CII is related to the rest of CI. The following CI fields in particular are mentioned in the CII law (Federal'nyj zakon 2017): health, science, transport, communications, banking and other areas of the financial market, fuel and energy complexes, nuclear energy, defence, the space, missile, mining, metallurgical and chemical industry, as well as Russian entities and individual entrepreneurs that provide interaction for these systems or networks. The amendments made to the main law countering terrorism (Federal'nyj zakon 2016) reveal that cyber-attacks against air transport CII were increasingly seen as a realistic threat picture.

Russia has also tested extreme protective CII measures against foreign-based cyber-attacks. In February 2019, the country announced that its telecom operators will in the Spring 2019 try to disconnect the whole Russian network from a global information network. The test would be based on a long-prepared bill that was introduced in December 2018. According to the same bill, Russian telecom operators must be able to control all network traffic from Russia to nodes approved or controlled by the authorities. Network traffic control would be handled by Roskomnadzor, an authority that controls the mass media, and would filter out forbidden content from traffic. At the same time, Roskomnadzor would ensure that the communication between Russians remains within the borders of the country (See e.g. Cimbanu 2019). In December 2019, a bit delayed, it was informed that the test had been successfully implemented (BBC 2019).

Thus, the recent years have attested to increasing attention being paid in Russia to defensive cyber security. CII vulnerabilities are understood as systemic threats due to the sector's horizontal importance within CI in general. The basic legislation as well as institutions seem to be in place. While it is difficult to find any clear-cut evidence about the degree of success in Russian government's efforts, the fact that some of the best-known global companies in the field of cyber security are of Russian origin (e.g. Kaspersky Lab) gives some reason to think that Russia at least has the necessary know-how in this field. The obviously rapidly increasing (Russian-language) literature on CII, as well as the alleged Russian offensive capabilities in terms of attacking other countries' CI and CII (e.g. Lilly & Cheravitch 2020) underline this assumption.

5 Protection or Resilience?

Already for some time, in Western policies and debates, there has been a shift in emphasis from CI protection to that of resilience (see e.g. OECD 2019; Pursiainen 2018; Pursiainen and Gattinesi 2014). Complete protection can never be guaranteed, and achieving the desired guaranteed level of protection is normally not cost-effective in relation to the actual threats. Therefore, one should put more focus on adaptive measures and quick recovery. Has the paradigm shift from CI protection to that of resilience taken place in Russia?

The two concepts that are used in the EMERCOM document *Metodika* (2012), and subsequently repeated in many decrees and other regulations, are 'warning' and 'prevention'. In the President-confirmed strategy document on CI from 2011 (Osnovy 2011/2017), the main concepts referring to defensive activities are 'minimisation' of risks and increasing the level of 'protection'. The national security strategy (Ukaz 2015) envisages countering threats against CI through the improvement and development of a unified state system for 'preventing' and 'eliminating' emergencies. The same goes for most official strategy documents and legislation. The Russian approach seems to focus on the pre-crisis phase, paying scant or no attention to the during-crisis (response, adaptation) and even less to the after-crisis (recovery) phases.

In Russian academic CI or CII literature, the picture is somewhat more varied, although one mostly finds literature based on pre-crisis CI protection following typical risk assessment methodologies (e.g. Ban'shhikova and Nazarenko 2019; Jannikov et al. 2018) than more comprehensive CI resilience analyses. True, as Romanova (2017) notes, the very concept of 'resilience' as a single term is not established in the Russian language, and one can find several Russian words used instead. None of these words, such as the one Romanova uses, *stressoustojchivost'*, which would perhaps translate as 'stress sustainability', however, does entirely encapsulate the meaning of resilience as it is used in Western CI literature. This absence of an agreed-upon Russian translation may be a contributory factor as to why the resilience approach has been rather slow to emerge in Russia. Nonetheless, a body of Russian-language literature is taking shape that does discuss CI resilience, and more often CII resilience, using an approximate concept of one sort or another (e.g. Klimov et al. 2019; Zaharchenko and Korolev 2018; Sokolov et al. 2015; Kul'ba et al. 2013; Malinin et al. 2013; Malyshev et al. 2013; Dodonov et al. 2007).

The issue then is whether, as in Western countries, the resilience approach will penetrate Russia's official CI policy, and what does it entail. One can forecast that Russia sooner or later will adopt its own variation of resilience, following the example of the Western countries and organisations, for the very reason mentioned above that CI protection alone is an inadequate strategy. The difference compared to Western countries is, of course, that the Russian state can experiment and implement its solutions without taking into account civil liberties, property rights and democratic procedures that limit the Western political systems to introduce too much regulation.

6 Who are the Actors?

The hierarchy of authority in security-related issues in Russia is defined in several documents, for instance in the federal law on security from 2010 (Federal'nyj zakon 2010). It follows the typical pyramid of Russia's political system, starting from the President, the chambers of the Federal Assembly (Council of Federation and State Duma), the Government, the Security Council, and the local self-government bodies. The main coordination responsibility, however, lies with the President and the Security Council, with the latter being formed and headed by the President.

In practice, some line ministries or agencies are responsible for preparing the first draft laws and lower-level documents, and for implementing them when approved. Traditionally, EMERCOM has been responsible for 'safety' issues, including those related to CI, whereas the Ministry of the Interior is the main domestic 'security/malicious threats' body. The activation of international jihadist terrorism, as well as increasing tension between Russia and the Western powers, combined with the emergence of cyber threats, has brought the Russian intelligence services (especially the FSB) as well as clearly military organisations into the picture.

The possible tensions between Russian bureaucracies about power and authority in the field of CI policy have not often been discussed in public. In the legal debates, one can find some signs that the issue remains under discussion. It has been suggested, for instance, that the bodies of the Ministry of Interior, due to their specialised capabilities, should have a coordinating role in the activities to protect CI at the territorial level. While the FSB currently occupies a leading position in this area, it has been criticised for not having the resources to ensure a proper level of protection of CI facilities (Strokin 2014a).

One more actor's role is emphasised in related legislation on countering terrorism (Federal'nyj zakon 2006), namely the Armed Forces. They, and the 'voluntary forces' related to military and intelligence organisations, can in certain conditions be used to suppress terrorist acts. This provides domestic legal grounds for using Russia's Armed Forces against terrorist groups not only domestically but aslo abroad. A specific case is the semi-state security forces, particularly the so-called Wagner Group, which Russia uses in it foreign operations without seemingly legalising its existence or role (e.g. Marten 2019).

Where do private actors, such as CI operators, fit into the picture? In the national security strategy, they as such are not mentioned. Ensuring national security is the task of the state power and institutions of local administration in cooperation with the civil society, using political, military, organisational, socio-economic, information, legal and other measures. The main tool for 'ensuring state security and public security is the strengthening of the role of the state', especially by 'increasing the effectiveness of law enforcement agencies and special services, as well as state control'. The state bodies are 'to liquidate the foreign state's malicious acts against the Russian Federation, as well as strengthen the level of antiterrorist protection and safe functionality of the organisations of the defence-industrial, nuclear, chemical, fuel and energy complexes of the country, life support facilities of the population, transport infrastructure, and other critical and potentially dangerous facilities' (Ukaz 2015, Part IV, Art. 44, 45). Similarly, in the civil defence concept (Ukaz 2016), the system is described as a centralised government-led hierarchy. The state policy is implemented through the coordinated and purposeful activity of federal executive bodies, executive authorities of the constituent entities of the Russian Federation, and local governments. The federal Government ensures the implementation of a unified state policy in the field of civil defence.

While in many cases CI is, however, operated or owned by private actors in Russia too, in such fields as transport or ICT, for instance, the legislation is very clear about the fact that the operator or owner is legally responsible and liable for taking care of the registration and protection of their respective CI in the regulated way. The operators must give all the information about the related systems and operations to the executive bodies both automatically and when asked. Compliance with the requirements is subject to the federal control, including mandatory exercises and tests, as well as scheduled and unscheduled inspections (e.g. Federal'nyj zakon 2017).

The most important part of the non-cyber CI is run by state enterprises, and the rest is strictly monitored and controlled by regulation and direct state agency interference. The CII sector is somewhat different, more fragmented and more privately owned than the traditional CI sectors. CII is by definition such a field that Russian state agencies are often dependent on private actors, be they legal specialised IT security companies, or outright freelancer hackers forced or persuaded to cooperate, for both offensive and defensive purposes (Turovsky 2017). However, Russian state agencies have in recent years also started increasingly becoming CII part-owners or developers (Tass 2017).

From the very onset of the related CII regulation, the goal is a 'unified state system' (Osnovnye napravlenija 2012). When President Putin embarked on his third term, the so-called power institutions gained even more salience. The presidential decree on CII (Ukaz 2013) clearly reflects the idea that the field of cyber security is a subject for the intelligence community. The FSB almost has a monopoly over CII in some respects. The Ministry of Telecom and Mass Communications, which basically deals with ICT issues, seems to have very little say in CII matters. However, the mere physical CI protection is still largely connected to the emergency and civil defence ministry EMERCOM.

Under the latest CII legislation (Federal'nyj zakon 2017), the effort to establish a unified federal system under strict regulation in this field is obvious. Should this be or have been implemented, indicators for the significance of CII facilities would first be defined, based on social, political, economic and ecological significance, as well as the importance of the object for the country's defence, state security and public order. After this analysis, the CII will be divided into three priority groups, each with its own protection criteria. It is the obligation of the operator, be it private or public, to follow certain rules in order to evaluate the criticality of the ICT and to determine whether the facility should be classified as CII.

If so, the operator needs to assign a priority level to it. The operator must then submit the results of this self-analysis to the above-mentioned federal CII agency, who then independently reviews the evaluation. If it concludes that an ICT facility is a CII, it will be registered as such. In that case, the operator has to comply with the respective federal CII security regulations. Subject to scheduled and unscheduled audits as well as unrestricted access for the federal CII agency, the operator is obliged to respond to cyber incidents in accordance with federally adopted procedures. The operator and its employees may be criminally prosecuted for violations of any of the above rules.

To sum up, Russia has clearly created a highly regulated and top-down system to control CI in general (which mostly already was based on state-ownership), and CII in particular (which was a new phenomenon), in terms of their measures against safety and security threats. While malicious insider actions leading to the disruption of CI are naturally subject to criminal prosecution, the legislation is formulated in such a way that non-malicious omissions or neglect can easily become criminal acts as well. In practice, this regulation means that state agencies are closely connected to individual CI/CII companies' and facilities' safety and security measures at a very practical monitoring level. How this kind of system works in practice in Russia's allegedly corrupt system of governance and its interaction with profit-seeking companies cannot be concluded from the official documents, however.

7 Conclusions

This article took on the task of drawing a state-of-the-art picture of the CI policy in Russia. After setting some context, it started by asking what CI means for Russia. It became clear that in the Russian language the terminology is somewhat different from that in English, but basically refers to the same issues. It could even be argued that ‘critically important objects’ and ‘potentially dangerous objects’, the Russian equivalents of CI, as well as other sub-themes of the same subject matter, are much more facility-oriented or concrete than the sector-specific approaches cultivated in the West. In any case, one can conclude that the Russian approaches to the CI policy in Russia have, since the beginning of the 2000s, slowly but surely been evolving into a policy field, currently guided by laws, lower-level regulations and strategies, reflected in academic research, and been implemented on federal and regional levels.

What threats does Russia face in this field? It is noteworthy that Russian threat analyses are sweepingly drawn. The threats against CI range from normal natural disasters, technological catastrophes and terrorism to hostile foreign states and malicious (anti-regime) non-governmental organisations. Cyber security has in recent years emerged as a major object of interest in Russia, around which a regulatory system with its diversity of laws and institutions has been set up.

If in the Western CI policies and academic debates, the concept of resilience has been a formidable term for some time, this conversation seems to be slowly emerging in Russia, too. True, official documents and legislation do not yet show any conscious understanding about the concept, their focus being on CI protection. In the research literature, resilience has, however, become a topic, albeit with slightly different terms, and it is relatively easy to find articles and conference papers related to the subject.

Finally, what can we say about Russian CI policy-makers? A common phrase in all documents and regulations is the ‘unified state system’. Russia’s CI policy strictly adheres to the hierarchical structure of its general political system, and the only problem seems to be that of how to implement this rigorous control and regulation scheme as effectively as possible. Legislation has been drafted in such a way that CI operators are practically in direct relation to the authorities, the latter being equipped with the privilege of all the enforcement machinery. Monitoring has been attached with strict criminal penalties if operators fail to take responsibility.

While many of the challenges are the same, there are not many avenues where Russia and its Western neighbours could meet in this particular field in a constructive way. Safety and security of CI are in the very core of ‘hybrid threats’. In the conditions of geopolitical tensions and the competing socio-political systems, ‘learning from each other’ is not an option, except than learning to understand each other’s weaknesses and vulnerabilities. The one who knows these weaknesses better than the other party is on the winning side.

Funding Open Access funding provided by UiT The Arctic University of Norway.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Aradau C (2016) Security that matters: critical infrastructure and objects of protection. Secur Dialogue 41(5):491–514

Azanov SN et al (2015) Izmenenija v 2014 godu i puti sovershenstvovanija normativnoj pravovoj bazy po voprosam zashhity naselenija, kriticheski vazhnyh i potencial'no opasnyh ob''ektov. *Tehnologii grazhdanskoj bezopasnosti*,vol. 12, No. 3: 26–30. [Online] Available at: https://cyberleninka.ru/article/n/izmeneniya-v-2014-godu-i-puti-sovershenstvovaniya-normativnoy-pravovoy-bazy-po-voprosam-zaschity-naseleniya-kriticheski-vazhnyh-i

Azimov K (2020) Repatriation of Ex-jihadists: possible risks. *Russia Moslem World* 1(307):10–22

Ban'shhikova ZE, Nazarenko EK (2019) Realizacija gosudarstvennoj politiki v oblasti povyshenija zashhishhennosti kriticheski vazhnyh i potencial'no opasnyh ob''ektov ot ugroz razlichnogo haraktera. Tehnologii grazhdanskoj bezopasnosti, 16, 1(59): 54–58. [Online] Available at: https://www.elibrary.ru/item.asp?id=37112025

BBC (2019) Russia 'successfully tests' its unplugged internet. British Broadcasting Company. [Online] Available at: https://www.bbc.com/news/technology-50902496

Cimbanu C (2019) Russia to disconnect from the internet as part of a planned test. Russia's internet contingency plan gets closer to reality. Zero Day Net (11 February) [Online] Available at: https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/

Dodonov AG, Gorbachik ES, Kuznechova MG (2007) Zhivuchest' komp'juternyh sistem i bezopasnost' informacionnoj infrastruktury. Izvestija JuFU. Tehnicheskie nauki, No. 1. [Online, no page nos.] Available at: https://cyberleninka.ru/article/n/zhivuchest-kompyuternyh-sistem-i-bezopasnost-informatsionnoy-infrastruktury

EM-DAT Public (n.d.). The International Disaster Database. Centre for Research on the Epidemiology of Disasters—CRED. [Online] Available at: https://public.emdat.be/data

Federal'nyj zakon (1994) Federal'nyj zakon ot 11 nojabrja 1994 goda No. 63-FZ "O zashhite naselenija i territorij ot cherchvychajnyh situatsij prirodnogo i tekhnologichnogo kharaktera".

Federal'nyj zakon (1997a) Federal'nyj zakon 21 ijulja 1997 N 116-FZ "O promyshlennoj bezopasnosti opasnyh proizvodstvennyh ob''ektov".

Federal'nyj zakon (1997b) Federal'nyj zakon ot 21.07.1997 № 117-FZ "O bezopasnosti gidrotehnicheskih sooruzhenij".

Federal'nyj zakon (1998) Federal'nyj zakon ot 12 fevralja 1998 g. № 28-FZ "O grazhdanskoj oborone".

Federal'nyj zakon (2006) Federal'nyj zakon ot 06.03. 2006 № 35-FZ "O bor'be s terrorizmom".

Federal'nyj zakon (2010) Federal'nyj zakon ot 28.12.2010 № 390-FZ "O bezopasnost".

Federal'nyj zakon (2015) Federal'nyj zakon ot 8.03.2015 № 38-FZ "O vnesenii izmenenij i dopolnenij v Federal'nyj zakon ot 21 dekabrja 1994 g. № 68-FZ "O zashhite naselenija i territorij ot chrezvychajnyh situacij prirodnogo i tehnogennogo haraktera".

Federal'nyj zakon (2016) Federal'nyj zakon ot 06.07. 2016 goda n 374-FZ "O vnesenii izmenenij v federal'nyj zakon 'o protivodejstvii terrorizmu' i otdel'nye zakonodatel'nye akty Rossijskoj Federacii v chasti ustanovlenija dopolnitel'nyh mer protivodejstvija terrorizmu i obespechenija obshhestvennoj bezopasnosti".

Federal'nyj zakon (2017) Federal''nyj zakon ot 26 ijulja 2017 g. N 187-FZ "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii".

FinCERT (n.d.) The Financial Sector Computer Emergency Response Team. The Central Bank of the Russian Federation. [Online] Available at: https://old.cbr.ru/eng/fincert/

Ivanov AN, Ryzhko AS (2016) Aktual'nost' sovershenstvovanija processa upravlenija bezopasnost'ju kriticheski vazhnyh i potencial'no opasnyh ob''ektov v uslovijah vozrastanija terroristicheskoj ugrozy. Problemy obespechenija bezopasnosti pri likvidacii posledstvij chrezvychajnyh situacij, No.1–2 (5): 156–158. [Online] Available at: https://cyberleninka.ru/article/n/aktualnost-sovershenstvovaniya-protsessa-upravleniya-bezopasnostyu-kriticheski-vazhnyh-i-potentsialno-opasnyh-obektov-v-usloviyah

Jannikov IM, Telegina MV, Gabrichidze TG, Boltovskij AV (2018) Realizacija sistemy ocenki bezopasnosti kriticheski vazhnyh i potencial'no opasnyh ob''ektov. Izvestija Samarskogo nauchnogo centra Rossijskoj akademii nauk, 20.6–2: 395–400. [online] Available at: https://cyberleninka.ru/article/n/realizatsiya-sistemy-otsenki-bezopasnosti-kriticheski-vazhnyh-i-potentsialno-opasnyh-obektov/viewer

Kalashnikov AO (2013) Ensuring the security of critically important objects and trends in the development of information technology. World Appl Sci J 25(3):399–403

Kari MJ (2019) Russian Strategic Culture in Cyberspace Theory of Strategic Culture—a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. JYU Dissertations 122. Jyväskylä: University of Jyväskylä. [Online] Available at: https://jyx.jyu.fi/bitstream/handle/123456789/65402/978-951-39-78372_vaitos_2019_10_11_jyx.pdf?sequence=4#page=132

Klimov SM et al (2019). Metodika obespechenija ustojchivosti funkcionirovanija kriticheskoj informacionnoj infrastruktury v uslovijah informacionnyh vozdejstvij. *Voprosy kiberbezopasnosti*, 6(34): 37–47. [Online] Available at: https://cyberleninka.ru/article/n/metodika-obespecheniya-ustoychivosti-funktsionirovaniya-kriticheskoy-informatsionnoy-infrastruktury-v-usloviyah-informatsionnyh/viewer

Kravchenko M (2019) Russian anti-extremism legislation and internet censorship. Soviet Post-Soviet Rev 46(2):158–186

KVO (n.d.) Kriticheski vazhnyj ob''ekt (KVO). [Online] Available at: https://fireman.club/inseklodepia/kriticheski-vazhnyiy-obekt-kvo/

Kukkola J, Ristolainen M, Nikkarila J-P (2019) Game player. Facing the structural transformation of cyberspace. Riihimäki: Finnish Defence Research Agency. [Online] Available at: https://maanpuolustuskorkeakoulu.fi/documents/1948673/10330463/PVTUTKL+julkaisuja+11+Game+Player.pdf/9ff35e9b-3513-c490-c188-3e3f18e71bdd/PVTUTKL+julkaisuja+11+Game+Player.pdf#page=118

Kul'ba VV et al (2013) Upravlenie bezopasnost'ju i zhivuchest'ju ob''ektov infrastruktury zheleznodorozhnogo transporta na osnove indikatornogo podhoda. Teoreticheskaja i prikladnaja ekonomika 2:1–107

Lazari A (2014) European critical infrastructure protection. Springer, Heidelberg

Lilly B, Cheravitch J (2020) The past, present, and future of Russia's Cyber strategy and forces. In: 12th International conference on cyber conflict (CyCon), Estonia, pp 129–155. [Online] Avalaible at: https://ieeexplore.ieee.org/abstract/document/9131723

Malinin AM, Chistovich AS, Jemirov IH (2013) Energeticheskaja bezopasnost' i zhivuchest' sistem teplosnabzhenija.TTPS, No. 1 (23). [Online, no page nos.] Available at: https://cyberleninka.ru/article/n/energeticheskaya-bezopasnost-i-zhivuchest-sistem-teplosnabzheniya

Malyshev VP et al (2013) Razrabotka sistemy mer, napravlennyh na povyshenie ustojchivosti funkcionirovanija kriticheski vazhnyh ob''ektov Rossijskoj Federacii i ob''ektov zhizneobespechenija v uslovijah ugroz terroristicheskogo haraktera. Strategija grazhdanskoj zashhity: problemy i issledovanija, No. 2: 91–92. [Online] Available at: https://cyberleninka.ru/article/n/razrabotka-sistemy-mer-napravlennyh-na-povyshenie-ustoychivosti-funktsionirovaniya-kriticheski-vazhnyh-obektov-rossiyskoy-federatsii

Marten K (2019) Russia's use of semi-state security forces: the case of the Wagner Group. Post-Soviet Affairs 35(3):181–204

Massel' LV et al (2016) Kiberopasnost' kak odna iz strategicheskih ugroz energeticheskoj bezopasnosti Rossii. Voprosy kiberbezopasnosti 4(17):22–30

MChS (n.d.) Obespechenie zashhishhennosti kriticheski vazhnyh i potencial'no opasnyh ob''ektov ot ugroz prirodnogo i tehnogennogo haraktera. [Online] Not anymore available, retrieved 12 December 2019 from: https://www.mchs.gov.ru/upload/site1/gosdoklad/6_3_.pdf

Metodika (2012) Metodika otnesenija ob''ektov gosudarstvennoj i negosudarstvennoj sob'stvennosti i kritichei vazhnym ob''ektam dlja natsionalnoj bezopasnosti Rossijskoj Federatsii. Utverszhdeno MChS 17.10.2012, Moscow. Cancelled by EMERCOM 30 December 2019, N 43–7134–11.

Nuñez-Mietz FG (2019) Resisting human rights through securitization: Russia and Hungary against LGBT rights. J Human Rights 18(5):543–563

OECD (2019) Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. OECD Publishing, Paris.

Osnovye napravlenija (2012) Osnovnye napravlenija gosudarstvennoj politiki v oblasti obespechenija bezopasnosti avtomatizirovannyh sistem upravlenija proizvodstvennymi i tehnologicheskimi processami kriticheski vazhnyh ob'ektov infrastruktury Rossijskoj Federacii. Utverzhdeny Prezidentom Rossijskoj Federacii D. Medvedevym 3 fevralja 2012 g. N 803.

Osnovy (2006) Osnovy gosudarstvennoj politiki v oblasti obespechenija bezopasnosti naselenija Rossijskoj Federacii i zashishhennosti kriticheski bazhnyh i potentsialjeno opasnyh ob''ektov ot ugroz ot tehnogennogo, prirodnogo haraktera i terroisticheskih aktov. Utverzhdeny Prezidentom Rossijskoj Federatsii 28.09.2006 g. No Pr-1649.

Osnovy (2011/2017) Osnovy gosudarstvennoj politiki v oblasti obespechenija bezopasnosti naselenija Rossijskoj Federacii i zashhishhennosti kriticheski vazhnyh i potencial'no opasnyh ob''ektov ot ugroz prirodnogo, tehnogennogo haraktera i terroristicheskih aktov na period do 2020 goda. Utverzhdeno Prezidentom RF 15 nojabrja 2011 g. No Pr-3400. Later: Ukaz Prezidenta RF, 17.02.2017, No. N Pr-3400.

Petrova EG (2011) Natural factors of technological accidents: the case of Russia. Nat Hazards Earth Syst Sci 11:2227–2234

Pursiainen C (2018) Critical infrastructure resilience: a Nordic model in the making? Int J Disaster Risk Reduction 27:632–641.

Pursiainen C, Gattinesi P (2014) Towards testing critical infrastructure resilience. Luxemburg. Publications Office of the European Union, JRC Scientific and Policy Reports. Luxemburg: April.

Pursiainen C (2009) The Challenges for European Critical Infrastructure Protection. J Euro Integration, Issue 31/6, November: 721–739.

Pynnöniemi K, Busygina I (2013) Critical infrastructure protection and Russia's hybrid regime. Euro Security 22(4):559–575

Rudycheva N (2016) Kriticheskaja infrastruktura RF: segodnja otvetstvennyh net. Digital Report 06.12. [Online] Available at: https://digital.report/kiberbezopasnost-rossii-otvetstvennyih-za-sboi-net/

Romanova T (2017) Kategorija 'stressoustojchivost' v evropejskom sojuze. *Sovremennaja Jevropa*, Nr 4:17–28

Sayer P (2016) Spies planted malware on critical infrastructure, Russian security service says. Networkworld, 1 August, 2016. [Online] Available at: https://www.networkworld.com/article/3102232/spies-planted-malware-on-critical-infrastructure-russian-security-service-says.html

Sokolov BV et al (2015) Imitacionnoe modelirovanie zhivuchesti kriticheskih infrastruktur. Sed'maja vserossijskaja nauchno-prakticheskaja konferencija 'Imitacionnoe modelirovanie. Teorija i praktika', IMMOD, pp 162–167

Smekalova MV (2019) Evoljucija doktrinal'nyh podhodov SShA k obespecheniju kiberbezopasnosti i zashhite kriticheskoj infrastruktury. Vest. Mosk. Un-ta, Ser. 25: Mezhdunarodnye otnoshenija i mirovaja politika. No 1:147–168

Sputnik (2017a) Russia's Federal Security Service will shield the key objects, using domestically-developed components only. 27.01.2017 [Online] Available at: https://sputniknews.com/military/201701271050065224-fsb-cyberattacks-russia/

Sputnik (2017b) Russian Critical Infrastructure Avoids Serious Damage in Global Cyberattack. 21.05.2017. [Online] Available at: https://sputniknews.com/russia/201705211053839984-russian-infrastructure-avoids-wannacry/

Stepanova E (2010) Terrorizm kak ugroza kriticheskoj infrastrukture. Svobodnaja mysl' 4:33–48

Strokin VV (2014a) Pravovoe regulirovanie dejatel'nosti territorial'nyh organov MVD Rossii po zashhite potencial'no opasnyh i kriticheski vazhnyh ob''ektov. *Problemy v rossijskom zakonodatel'stve*, No 2:301–303

Strokin VV (2014b) O nekotoryh aspektah unifikacii ponjatija 'Potencial'no opasnye i kriticheski vazhnye ob''ekty'. Biznes v zakone, No.4: 16–18. [Online] Available at: https://cyberleninka.ru/article/n/o-nekotoryh-aspektah-unifikatsii-ponyatiya-potentsialno-opasnye-i-kriticheski-vazhnye-obekty

Tass (2017) The digitalisation of critical infrastructure and strategic consortia. May 29, 2017. [Online] Available at: https://tass.com/sp/948368

The Moscow Times (2017) 4000 Russians Now Fighting in Syrian Insurgency, Says Putin, 23 February 2017. [Online] Available at: https://themoscowtimes.com/news/4000-russians-now-fighting-in-syrian-insurgency-says-putin-57259

Turovsky D (2017) Moscow's cyber-defense. How the Russian government plans to protect the country from the coming cyberwar. Meduza, 19 July 2017. [Online] Available at: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense

Ukaz (2013) Ukaz Prezidenta Rossijskoj Federacii ot 15 janvarja 2013 g. N 31s g. Moskva "O sozdanii gosudarstvennoj sistemy obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak na informacionnye resursy Rossijskoj Federacii".

Ukaz (2015) Ukaz Prezidenta Rossijskoj Federacii ot 31 dekabrja 2015 goda N 683 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii".

Ukaz (2016) Ukaz Prezidenta RF ot 20.12.2016 N 696 "Ob utverzhdenii Osnov gosudarstvennoj politiki Rossijskoj Federacii v oblasti grazhdanskoj oborony na period do 2030 goda".

Zaharchenko RI, Korolev ID (2018) Metodika ocenki ustojchivosti funkcionirovanija ob#ektov kriticheskoj informacionnoj infrastruktury funkcionirujushhej v kiberprostranstve. Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli, 10(2): 52–61. [Online] Available at: https://cyberleninka.ru/article/n/metodika-otsenki-ustoychivosti-funktsionirovaniya-obektov-kriticheskoy-informatsionnoy-infrastruktury-funktsioniruyuschey-v/viewer

Østbø J (2017) Securitizing "spiritual-moral values" in Russia. J Post-Soviet Affairs 33(3):200–216

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.