The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry

Juha Kukkola
Captain, Doctor of Military Sciences
Department of Warfare
Finnish National Defence University

Abstract: The Russian Federation is constructing a closed national network. If successfully completed, this state-controlled, technologically independent, and self-sufficient segment of the internet can be disconnected from the global internet by 2024. The segment is based on a national system-of-systems of information security and defence that will protect the Russian regime against internal and external information threats. It will also provide a source of power in the ever-continuing great power struggle and even a decisive advantage on a strategic level in the cyber domain. This chapter demonstrates that the Russian project is an effort to shape cyberspace through state action on a strategic level to gain an asymmetric military advantage. The advantage is based on the differences in freedom of action, common operational picture, command and control and resilience between one nation closing its networks and other nations leaving their networks open and their critical information infrastructure unprotected. These differences create strategic-level structural cyber asymmetry which can influence the way force is used in a state-to-state conflict. This chapter provides new insight on how a closed national network, or the Russian national segment of the internet, in particular, could change the balance of power and the rules of play in the future cyber domain.

Keywords: *Russian Federation, cyber defence, closed national network, asymmetry*

1. Introduction

The Russian Federation is constructing a national segment of the internet (*natsional'nyi segment interneta*) which can be disconnected from the global internet when certain threats materialise (FZ-90, 2019). This project is incorporated in the 2017 National Programme of the Digital Economy, which aims to achieve 'digital sovereignty' by 2024 (RP-1632, 2017). If successful, the programme will put the Russian part of the internet under the control of the Russian state. Although some commentators have argued that the Russian regime's project is mainly about authoritarian domestic political control over the internet, the project also has a military aspect that can affect the international balance of power (Soldatov, 2017; Ermoshina & Musiani, 2017; Vendil-Pallin, 2017; Nocetti, 2018). The concept of the Russian national segment of the internet is based on strategic-cultural Cold War-era Soviet ideas which carried with them a promise of an asymmetric advantage in great power relations (Kukkola, 2020). The project also contributes to the fragmentation of the internet along national boundaries, which is becoming ever more evident (Drake, Cerf & Kleinwächter, 2016).

Kukkola, Ristolainen and Nikkarila (2017) have argued that the Russian national segment of the internet will become a closed national network, which will provide an asymmetric advantage against states leaving their networks open. This advantage is based on the restructuring of cyberspace or, in military terms, the shaping of electronic battlespace on a strategic level. This chapter develops this argument further by arguing that the presence of structural cyber asymmetry can be analysed through the differences of freedom of action, common operational picture (COP), command and control (C2) and resilience between a nation closing its networks and nations leaving their networks open. These variables capture the essential characteristics of cyberspace on an operational-strategic level. At a strategic level structural cyber asymmetry will affect the way force is used in future state-to-state conflicts, contribute to the fracturing of cyberspace into national segments, and even promote a cyber arms race.

This chapter presents a case study where the Russian national segment of the internet and a theoretical open national network are analysed to explain the phenomenon of structural cyber asymmetry. In the first part, Russia's reasons for and means for constructing a national segment of the internet are examined. In the second, the concept of structural cyber asymmetry and related concepts of freedom of action, COP, C2 and resilience are explained. The third part examines the differences between the Russian segment, or a closed national network, and a Western open national network. In the fourth part, a qualitative analysis of Russia's closed network and a theoretical open network is conducted, examining the relative advantages and disadvantages of open and closed network nation defenders in the context of cyber conflict. Advantages and disadvantages are analysed to demonstrate the presence of structural cyber asymmetry and to understand its nature. Finally, the chapter will conclude with a discussion on the military-strategic implications of structural cyber asymmetry.

2. Why Russia is Pursuing Asymmetry in Cyberspace

To understand Russia's objectives and structural cyber asymmetry some basic concepts need to be introduced. First, a closed national network is a theoretical concept which describes a national network that can be disconnected from the global internet and still function normally in providing communications for the state administration, national economy, civil society and the military. An open national network is a theoretical state network based on the current Western way of managing the internet. Second, the Russian national segment of the internet is a real-life case of a closed national network. It consists of the internet infrastructure and other networks and systems residing in Russia and under its sovereign legal powers. It defines the borders of cyberspace and is a political, administrative and legal concept. Third, a unified information space (*edinnoe informatsionnoe prostranstvo*) is a strategic-cultural idea, which makes it understandable and reasonable for the Russia regime to develop the Russian national segment of the internet. The idea describes how this segment of cyberspace should be arranged according to cybernetic principles. Fourthly, a national system-of-systems of information security and defence is a collection of interconnected means and methods of the state to delineate, protect and control its national segment. The system-of-systems protects the state and its sovereignty and functions as a source of national power. In its ultimate state, as a manifestation of unified information space, it incorporates the whole national segment of the internet. All these concepts, except the first, are based on the thinking of Russian civilian and military academia. It should also be noted that the commonly used term, 'Russian internet' or 'RuNet', refers to the Russian-language social and cultural online environment which developed in the 1990s and 2000s without state interference. Its borders do not correspond to Russia's state borders and Russia is not currently claiming sovereignty over it.[1]

The Russian state began to build a national segment of the internet in the early 2010s because it was rational from the point of view of decision-makers (Kukkola, 2020; Nocetti, 2018; Kari, 2019). The idea of information sovereignty (*informatsionnyi suverenitet*) was present in Russian political discourse by the early 2000s and was promoted as a counterforce to a perceived American hegemony in internet governance and information technology superiority. Between 2009 and 2011 it became clear to the Russian regime that RuNet had transformed into an independent platform of political mobilisation. This was perceived as a threat to its authoritarian regime. Incidentally, the KGB-minded Russian security services had argued for the control of the internet since the mid-1990s (Thomas, 1998). After 2011 the regime began to implement political control and censorship of RuNet through laws and decrees. Meanwhile, it became apparent to Russian political and military elites that cyberspace would be militarised and that critical information in-

[1] For a more comprehensive discussion on these concepts see Kukkola, Ristolainen & Nikkarila, 2017; Ristolainen & Kukkola, 2019; Kukkola, 2020.

frastructure would be targeted in the next large-scale or regional war (Kukkola, 2020).

Autumn 2014 was a turning point for the Russian regime. A definite change in the strategic environment led the regime to pursue a centralised control of the internet under the guise of 'the national segment of the internet' which itself was a product of the ideas of information sovereignty and unified information space. According to these ideas, the state must control its information space and its borders to achieve information sovereignty.[2] Consequently, unified information space is a model for constructing such a space around vertically and horizontally integrated state-controlled networks and automated C2 management systems. This kind of national information system would provide an asymmetric response (*asimmetrichnyi otvet*) against an enemy by denying it an attack surface and making national systems more resilient while leaving Russia free to operate against an adversary (Kukkola, 2020; Pynnöniemi, 2018). The concept has its roots in the Soviet response to Reagan's Strategic Defense Initiative (SDI) in the 1980s (Hoffman, 2009). Arguably, Russian actions were influenced by multiple threats that seemed to materialise in 2014–2015. The global balance of power was changing as China rose to challenge the US while Russia's relations with the West became antagonistic. The Russian regime perceived itself to be vulnerable to 'colour revolutions' and to new technological threats in the information, cyber and space domains. Russia had also failed to create international cyber and information security norms to control its more advanced adversaries. The Russian strategic cultural ideas and the Chinese example of 'the Great Firewall' offered a possible solution that the Russian regime embraced.

Between 2015 and 2020 the Russian regime adopted multiple laws, strategies and programmes which were designed to establish a national segment of the internet, protect it from internal and external threats and create power. These policies have sought to establish a truly independent, self-sufficient, competitive, integrated, resilient and secure Russian national segment of the internet. The programmes have already produced several components: a national cyber incident management system (GosSOPKA), a national centralised system for monitoring and managing telecommunication networks (TsMUSSOP), a federal government information management system (Upravlenie), a national network of situation centres and other centralised management networks including national energy and defence industry manage-

[2] According to an official Russian definition information space or environment is 'a set of information resources created by subjects of the information sphere, means of interaction of such subjects, their information systems and the necessary information infrastructure' (Ukaz-203, 2017). The information sphere is a larger entity also encompassing the subjects of information sphere (i.e. users and organisations) and the rules and norms regulating their interaction (Ukaz-646, 2016). Conversely, according to US Joint Doctrine the information environment is the aggregate of individuals, organisations and systems that collect, process, disseminate or act on information. This environment consists of three interrelated and interacting physical, informational and cognitive dimensions (JP 3-13, 2014: p. ix-x).

ment systems (Kukkola, Ristolainen & Nikkarila, 2017; Kari, 2019; Kukkola, 2020). Russia aims to develop domestic hardware, software and artificial intelligence industries to a scale that will achieve 'technological sovereignty', or self-sufficiency in the ICT sector (Thornton & Miron, 2020). However, this ambitious programme has technological challenges (Dear, 2019). It has suffered from the resignation of the Russian government in January 2020, from the fall of global oil prices and the COVID-19 crisis. The resistance of civil society and the private sector has also been significant. Consequently, President Putin apparently agreed to postpone the programme until at least 2030 (Ukaz-474, 2020).

Russian state policies resonate with the ideas of Russian information warfare (IW) theorists who have argued for the development of a national information defence or management system since the early 2000s (Kukkola, 2020). These ideas are based on a shift in the Russian perception of the character of war, which has evolved incrementally towards a version where the borders between war and peace become increasingly blurred. The will of the population and its decision-makers and the national economy have become the primary military-political targets. This means that state control of the national information space is necessary for succeeding in the continuous great power, zero-sum struggle (Thomas, 2017; Jonsson, 2019; Kukkola, 2020). Thus, the shaping of cyberspace has a critical role in deterrence and strategic-level preparations of the battlespace. However, although the Western and Russian ideas about cyber security are converging, controlling the substance and flow of information is still the primary concern of the Russian concept of information security. During the late 2010s, Russia adopted the concept of critical information infrastructure as an object of national security. The concepts of integrity, resilience and security of the Russian part of the internet have been adopted to define the security of information-technological communication systems (FZ-126, 2003; Sheremet, 2019), and the Russian leadership routinely discusses cyber threats (Latukhina, 2018). If Russian policies and the ideas of IW theorists merge fully, the result will be a national system-of-systems of information security and defence which will protect and control the national information space from psychological and technological information threats—and incorporate that space altogether.

3. STRUCTURAL CYBER ASYMMETRY

Human action can change cyberspace in ways that it cannot change other domains. Cyberspace is an information technology-based man-made global domain governed by humans in the information environment. It is an environment in and through which power can be used in ways guided by ideas and beliefs. Through certain resources at their disposal, states can control and shape cyberspace and thus change its characteristics and properties. Cyberspace is a new and constantly evolving environment with unknown or poorly understood potential threats. Consequently, states shape cyberspace in distinct ways guided by strategic-cultural ideas and according to the resources at their disposal.

The military-strategic importance of the shaping of cyberspace through constructing closed national networks or real-world national segments is based on the possibility of creating asymmetry (Kukkola, Ristolainen & Nikkarila, 2017). Without asymmetry, national segments would only make sense as instruments of domestic political control and protectionist economic policies. However, the traditional view of cyberspace asymmetry based on either the difficulty of attribution, disproportionate capabilities of non-state actors, non-traditionality of cyber means, or the advantages of cyber offence over defence is too narrow (Liff, 2012; Gartzke, 2013; Rid & Buchanan, 2015). By contrast, structural cyber asymmetry is a property of cyberspace which emerges between two actors when the structure and rules of cyberspace are shaped so that one of them gains a disproportionate and exploitable defensive and offensive advantage.

Kukkola, Ristolainen and Nikkarila (2017) have argued that when a nation manages to close its networks and build defensive lines inside this national network it will gain an asymmetric advantage in Computer Network Attack and Exploitation operations (CNA/CNE) against a nation that leaves its national networks open in a state-to-state conflict. The argument is that it is easier for a nation closing its networks to attack and defend than it is for an open network nation. This is because the nation closing its networks can minimise its attack surface, build defence in-depth and control the network centrally while the nation leaving its networks open is vulnerable through multiple attack vectors.

In previous studies (Kukkola, Ristolainen & Nikkarila, 2017) the concepts of freedom of action, situational awareness and decision-making have been used to analyse the advantages and disadvantages of closed and open networks in CNA/CNE operations. This approach was based on a theoretical operational-strategic level analysis. Technical issues were not analysed, although practical issues of disconnecting national networks have been examined by others (Kukkola, Ristolainen & Nikkarila, 2019). This chapter argues that it is advantageous to replace situational awareness with a COP and decision-making with C2 when analysing structural cyber asymmetry. Freedom of action needs to be disconnected from its geographical connotations and resilience, understood as a property of cyberspace, should be added to complement this analysis. These modifications direct the analysis to the effects of the structure of cyberspace instead of the subjective processes of decision-makers—which in the context of national security are often unknowable to the temporary outside observer.

Freedom of action, COP, C2 and resilience are relative variables whose differences demonstrate the presence of structural cyber asymmetry. In the context of this chapter, these concepts refer to technological, organisational and functional properties of closed and open networks, not to the capabilities of national cyber forces. Freedom of action refers to the ability to act in a certain domain while at the same time possessing an ability to deny adversaries that same capability. In cyberspace, this ability is tied to user privileges and connections, not to geographical continuity (Kiviharju, Huttunen & Kantola, 2020). Moreover, traditional material calculations of the correlation of forces lose their meaning as 'forces' are not positioned against each other (Kallberg & Cook, 2017). Physical destruction is replaced by affecting the performance capacity of the targeted system (NATO, 2020). Thus, the objects of the analysis of freedom of action are the effects of the borders and internal structures and processes of closed and open networks on the ability of actors to affect systems, processes, or adversary's operations in either own or enemy networks.

Because the concept of situational awareness refers to a personal and unique comprehension of the situation (Endsley, 2015), it is difficult to capture when analysing strategic-level cyber conflict. However, because information superiority is based on accurate and current situational awareness, it is necessary to somehow capture its effects in the analysis of structural cyber asymmetry. The ability to detect and be aware of the situation in both one's own and in adversary networks is central to cyber warfare as the ability to know is the precondition of the ability to act (Brantly, 2016). The COP can be defined as analysed, organised and continuously updated information about the situation in an area of operations that is available to one or more actors (Kuusisto, Kuusisto & Arminsted, 2005). Consequently, when analysing COP as a precondition of national cyber situational awareness in the context of structural cyber asymmetry, the objects of analysis are the structures, processes, information content, models and flows related to offensive or defensive cyber operations (MNE7, 2012). Advantages in these factors facilitate faster, more efficient and effective decision-making (Simon, 1997).

Analysis of decision-making at the operational-strategic level is difficult because, like situational awareness, it is a partly cognitive, partly social phenomenon, emphasising subjective agency and competence and, in the case of cyber operations, it is also highly secretive (Howard & Abbas, 2015). However, the concept of C2, defined as a process of planning, preparing, decision-making, executing, directing, coordinating and evaluating to achieve a certain objective in the context of certain technological and organisational systems and structures, can be used to examine the presence of structural cyber asymmetry with the evidence available (Hayes & Alberts, 2005; Elbanna, 2006). Because the characteristics of cyberspace directly influence C2 (Brantly, 2016; Chen, 2019), the object of analysis is not the process of decision-making according to some specific model but rather the systems of information management, decision support and execution and the structures of the national networks (O'Brien & Marakas, 2011). Thus, structures, processes and technologies are evaluated according to their effects on the speed of decision-making, the exactness of execution and overall control interpreted as effectiveness.

Resilience, as the last variable used to analyse the presence of structural cyber asymmetry, directs the attention to the infrastructure of cyberspace.

Although resilience is a somewhat contested concept (Humbert & Joseph, 2019), cyber resilience can be defined as 'the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source' (Ross et al., 2018: p. 1). While freedom of action is used in this chapter to analyse the active ability to affect the adversary's systems or protect own systems, resilience captures the passive protective, risk-minimising and continuity-enabling policies and systems affecting the properties of the information infrastructure (Libicki, 2016). Thus, the object of analysis in the case of resilience are those systems and policies that ensure the continuity of the critical information infrastructure on a national level and its adaptation to new threats.

4. Closed and Open National Networks

Based on the writings of Russian theorists and official policy documents, the Russian closed national network, or the Russian segment of the internet, is approached in this chapter as a national system-of-systems of information security and defence. A system-of-systems is composed of multiple subsystems, the interactions of which enable the achievement of a goal which no individual subsystem can achieve alone (Ackoff, 1971). The goal, in this case, is national information security, which is understood as protecting the state from external and internal information (technological and psychological) threats to ensure its sovereignty, territorial integrity, economic development, defence and security (Ukaz-646, 2016). For Russia, and incidentally also for China, information threats are categorised into the military-political use of information weapons, terrorism, crime, the efforts to use a dominant position in the information space to cause damage to others, disseminating harmful information to the political, social, economic, spiritual and cultural systems of other states, and threats to the global information infrastructure (SCO, 2009; RP-788, 2015). The system is a complex system-of-systems as its subsystems have their own functions and management mechanisms that are somewhat independent. Subsystems can function in unpredictable and inefficient ways (Thurner, Hanel & Klimek, 2018). The subsystems should be understood as political, governance, normative, organisational, economic, technological and security and military entities. They have been formed through soft systems methodology and are thus observation-based theoretical constructs (Checkland, 1993). The subsystems are explored more comprehensively elsewhere and here it is only possible to offer a summary of each.[3]

There are seven subsystems in the Russian system-of-systems, which are classified according to borders (parts), functions, principles or rules and ob-

[3] The original model was presented in Kukkola (2020). It has been modified for this text by introducing 'active counter measures' subsystem and incorporating a previous subsystem of cyber diplomacy into it. On active counter measures, see Blank, 2013; Giles, 2016; and Ajir & Vaillant, 2018.

jectives.[4] The first is the scientific-industrial basis of the state. It is based on import substitution policies and significant state investment in technology and science. Direct state ownership of strategic assets is common. This subsystem's objective is to produce the scientific-technological and knowledge aspects of a state's cyber power.[5] The subsystem contributes to the goal of national information security by directly shaping cyberspace, protecting the supply chain and providing security through obscurity and transparency as Russian produced hardware and software (HW/SW) are accessible to security services and the military through backdoors.

The second subsystem is state authentication and encryption. It is based on domestically produced and operated services and algorithms that are controlled directly or indirectly by the state. Use of the subsystem is mandatory for public services and state corporations, and it is forced on the private sector and private users. The subsystem's objective is to make all data traffic inside Russian borders transparent to the security services and the military and to protect data from foreign exploitation.

The third subsystem consists of the administrative and technological processes of blacklisting and content management through removal and restriction. The state publishes a database of unwanted sites and addresses and service and content providers are legally bound to restrict access to those on this blacklist. This system includes vigilante groups and self-censorship. The objective of the system is political control through the removal of subversive information.

The fourth subsystem consists of the targeted surveillance systems and the massive internet data traffic localisation and retention conducted by the internet Service Providers (ISP) as ordered by the state. The subsystem is based on massive, distributed data centres and networked monitoring systems and provides a collection of information and its analysis. It is highly centralised and its objectives are mainly counterintelligence, law enforcement and political control. The second, third and fourth subsystems contribute to information security by making the flow and content of data accessible to security services and the military.

The fifth subsystem consists of the Critical Information Infrastructure (CII) and the regulations and policies related to it. The subsystem is based on state ownership or indirect control of CII and legal obligations on private actors to protect it. It includes backups of top-level domain name servers, routing registers and internet Exchange Points (IXP). The subsystem enables the functioning of the national segment and its disconnection from the global

[4] Military networks and systems are separate but interdependent parallel system, which are not discussed in thischapter. They are a subcomponent of CII.

[5] Cyber power is an ability that empowers an actor to influence others in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences. Resources of power consist of human knowledge, technology, regulations and organisations (Kukkola, 2020).

internet, thus contributing to information security.

The sixth subsystem is based on active information-technological and information-psychological countermeasures. The subsystem is managed by state-controlled or affiliated news services and educational, patriotic and religious institutions. It also includes dedicated cyber diplomacy organisations and cyber espionage and warfare units of the security services and the military. It controls the domestic information environment by controlling the substance of information and conducts external overt and covert espionage, influence and cyber operations abroad to prevent possible threats from emerging. The subsystem also increases information security by attempting to norm-bound (entangle) potential adversaries and, thus, restricting the information superiority of advanced adversaries. If successful, it might for example create taboos concerning the offensive use of cyber capabilities.[6]

The seventh subsystem consists of feedback, monitoring, control and management systems. It is managed by the state and security services and includes national-level cyber training ranges and exercises. This subsystem provides the vertical control and horizontal integration of the closed national network. The different systems penetrate all nationally significant networks. The subsystem provides information on the national segment and the whole society, in essence a real-time analysis of all information threats, not just cyber, and enables control of information flows in the segment and at its borders. Its objective is to ensure national information security through monitoring, controlling and defending the national segment of the internet.

These subsystems are based upon the Russian project to construct a national segment of the internet. Conversely, a generic open national network is, in this chapter, loosely based on the way the internet was governed in the technologically advanced Western countries in the mid-2010s.[7] This time and region were chosen as the basis of the open national network because Russia formed the basic principles of its project to build a national segment in contrast to the way the internet was managed in the West at that time. The Russian project is a response to the weaknesses and strengths perceived in those Western models at the time of writing of the information security doctrine and the National Programme of the Digital Economy in 2015–2016. Although, the US is the most obvious competitor and even an adversary of Russia, the open national network model is not solely based on the US example of a national network. This is due to the US's unique relationship to the internet, and the US's disproportionate economic and scientific-technological power in relation to other Western powers.

Therefore, using the US model of national network as an example would obscure the fact that the other Western countries are dependent on US software

[6] On the dissuasive, soft or diplomatic use of cyber power, see Nye (2017).

[7] Sources used to induce the properties of an open national network: include ITU, 2015; ENISA, 2015; Hitchens & Goren, 2017; European Commission, 2020; NATO CCD COE, 2020 and; Tikk & Kerttunen, 2020.

and hardware. Thus, the comparison offered below is designed to highlight the potential asymmetric effects of the policy pursued by Russia vis-à-vis regional Western powers if they do not drastically change their internet governance policies. Structural cyber asymmetry affects both small and great powers and can affect great powers through their allies. It is, however, recognised that after 2016 the Western cyber security strategies and capabilities have begun to change (e.g. NATO, 2016) and this will be noted and discussed below.

Although an open national network is arguably not a system-of-systems in the sense of a national information security and defence system, it is approached below through the subsystems of the Russian national system. These subsystems capture almost all technological, administrative, economic, normative, political and security aspects of a territorially delimited part of cyberspace. This approach helps to conceptualise national networks as more than just a technological phenomenon and to compare them even when they differ from each other. Moreover, when national networks are modelled as systems their interaction, competitive or confrontational, can be analysed. There is, therefore, an element of simplification explicitly present in the model but its function is to underline the differences between two types of networks. Table I shows the main differences between a closed and open national network.

Table I: Closed and Open National Network

Subsystems	The Type of Network	
	Closed National Network	Open National Network
1. Scientific-technological basis	• State-led • Closed markets, corruption and red tape • State ownership of strategic assets - foreign ownership highly regulated • Domestic SW/HW ecosystem • Primarily proprietary source code • Few international interdependencies • Limited international cooperation in cyber security	• State participation varies • Open markets • Privatization of strategic assets - foreign ownership regulated • Few domestic SW/HW • Fractured field of international and domestic services suppliers • Significant foreign interdependencies (supply-chains)
2. Authentication and encryption	• Primarily domestic SW/HW solution • State certification required for all cryptography • State able to decrypt all traffic without administrative process	• Limited domestic solutions • State provides certification for official use and recommendations • Slow decryption because of political and legal issues

Subsystems	The Type of Network	
	Closed National Network	Open National Network
3. Blacklisting and content restrictions	• Centralised system • Widespread state censorship and self-censorship • Vigilante groups	• No centralised system • No state censorship, some self-censorship • Little voluntary action
4. Targeted surveillance and data retention	• Widespread and unsupervised • Massive data collection • Localisation of critical data of companies and citizens based on national security	• Restricted and supervised • No massive data retention for security purposes • Data protection and localisation based on privacy issues • Significant portion of critical data abroad
5. Critical information infrastructure	• Owned by the state and private sector • Legal obligation to categorise, maintain and protect • CII mostly state-controlled and duplicated • Ability to disconnect the national network from the global internet	• Owned by the private sector • Protection guided by market economy factors • Some government regulation and certification • No state-level duplication of CII • No ability to disconnect national network
6. Active countermeasures	• State-controlled media • Strict laws to regulate foreign media and foreign ownership of media assets • State-supported religious and patriotic institutions • Dedicated cyber diplomacy organisation with clear national objectives • Overt propaganda, covert and disruptive information operations • Obfuscation of IW capabilities	• State and commercial media • Few restrictions for foreign media companies • Cyber diplomacy part of common foreign policy with diverging interests among allies • Soft power, overt strategic communications and targeted information operations • Official IW forces operating according to law

Subsystems	The Type of Network	
	Closed National Network	Open National Network
7. Management, monitoring, control and feedback	• Multiple centralised information management and incident response systems • Nationally controlled threat response (both technological and psychological) • Directed by the security services • Limited international cooperation and information exchange	• Only a limited national incident response system • Concentrates on cyber crime • National computer incident response team (CSIRT) coordinates and administratively stove-piped CSIRTs execute cyber security • Developing international cyber security cooperation

5. Comparison of Advantages and Disadvantages between Networks

Kukkola, Ristolainen and Nikkarila (2017) have argued that 'cyber asymmetry' favours a nation closing its networks when the analysis of asymmetry is based on examining attack-vectors. The refining of concepts and the addition of resilience do not significantly change the results of this analysis. Therefore, the analysis below takes prior results as a starting point and adds to them by examining the internal attributes of the networks. The analysis uses the concepts of freedom of action, COP, command and control and resilience to compare open and closed national networks through the seven subsystems of the national system-of-systems of information security and defence. For the sake of clarity, the results are presented from the perspective of the defending nations.

The scientific-technological basis of a closed national network provides a definite advantage in defence through proprietary HW/SW solutions. The basis limits the freedom of action of the attacker who must engage in comprehensive intelligence gathering and reverse engineering. Conversely, the defender knows most of the HW/SW solutions which need to be protected. COP and C2 benefit from domestically produced and integrated systems and cyber resilience is enhanced by a domestically produced and state-controlled ecosystem where observed vulnerabilities can be repaired quickly. The diverse SW/HW solutions of open national networks hinder the freedom of action of the defender. The defender's COP is limited due to legal issues and incompatible technologies while C2 lacks integrated support systems. Resilience is highly dependent on the commercial risk calculations of independent service providers.

The national authentication and encryption system of a closed national network provides a definite advantage in freedom of action and COP to the defender. All traffic is in principle transparent and there are no connections or networks that are closed to the defender. Conversely, the defender of an open national network is limited in its ability to decrypt traffic. The private sector and citizens use solutions closed to the defender. Additionally, domestic encryption solutions are used only in some systems and their quality is mixed although the use of multiple encryption and authentication systems might increase resilience through diversity and redundancy and encryption used in government networks is likely to be tested and certified.

The blacklisting and content restrictions provide a definite advantage for the closed national network defender in freedom of action. Freedom of action of an attacker using information-psychological and technological attacks can be denied by removing resources and platforms from the national cyberspace. Vigilante and similar groups also provide an advantage in COP. A centralised censorship system enhances the speed and effectiveness of C2. The resilience of the whole network is improved as the blacklisting system is tested and operated constantly. Defenders of open networks are disadvantaged in all these categories. They are not impotent, but processes related to blacklisting and restrictions are slow and have legal, political and economic limitations and consequences.

The targeted surveillance and data retention system of a closed national network provides the defender significant advantage in its COP and provides direct access to all public and private networks and their content, thus providing an advantage in freedom of action. As this subsystem is connected to the national centralised management and monitoring systems it also provides an advantage in C2 by providing timely and exact data on cyber and information incidents. The localisation of data to national data centres also enhances resilience. As open national networks officially lack this kind of subsystem they are again disadvantaged. However, once there is enough evidence of a hostile act in the network, open network defenders usually automatically have a mandate to start surveillance and counteractions.

The CII of a closed national network provides the defender advantage in all four categories. The law guarantees freedom of action in private systems and many critical systems are state-owned and controlled. The CII is connected to centralised monitoring and control systems, which gives an advantage in COP and C2. Resilience is high as the CII is constantly monitored, duplicated and protected. The whole national network or parts of it can be disconnected to enable recovery. Although open national network defenders are somewhat disadvantaged, much depends on the policies of those responsible for the CII. Centralised national systems mainly provide COP. Many of the existing systems are administratively stove-piped.

The active information-technological and information-psychological countermeasures provide the closed network defender with a definite advantage in freedom of action by manipulating information and destabilising opponents. Constant domestic monitoring and foreign espionage operations provide COP, but the advantage in C2 depends on how well actions are co-ordinated at the state level. Media control and patriotic education provide a definite advantage in information-psychological resilience. The open network defender is somewhat handicapped concerning the overt manipulation of information because of the need to coordinate actions with allies, domestic regulations and international law. This does not, however, mean that it lacks the necessary capabilities when needed. Democracy and transparency might also provide psychological resilience.

The management, monitoring, control and feedback system of a closed national network provides the defender with an advantage in all categories. Interconnected state-controlled systems enable freedom of action and provide national-level COP. The attacker's freedom of action is denied by centrally controlling the structure of the network. Support systems and centralised and hierarchical organisations provide superior C2. Resilience is enhanced as CII is continuously monitored, threats countered and personnel trained. The open national network defender is disadvantaged because of administrative stove piping. The defender might have an advantage in COP through international cooperation and voluntary public-private cooperation but only if the acquired information can be properly collected, analysed and quickly acted upon.

Although this comparison seems to favour closed national networks, this is not necessarily so. Closed national networks are dependent on state participation and, thus, on budgets and administrative efficiency. Domestic encryption solutions and the use of proprietary code do not automatically translate to better security. Politically motivated censorship breeds resistance and disillusionment and, at worst, increases the insider threat. Data retention creates troves of information that can be exploited by foreign hackers. Bureaucratic control of the CII creates overheads, disincentivises innovation and, ironically, produces target lists for the adversary. Authoritarian overtures are hard to mask in cyber diplomacy and create negative feedback from the international community. Citizens recognise propaganda and become disenchanted and passive as a result. Centralised and automated management and control systems are themselves the target of offensive cyber operations and can become victims of bureaucratic infighting and corruption. Despite these reservations, this analysis demonstrates that structural cyber asymmetry is also present when closed and open national networks are analysed based on their internal properties. The addition of resilience as a category of analysis just strengthens the argument.

6. Strategic Implications

The analysis presented in this chapter strengthens the argument that the Russian national segment of the internet, if successfully constructed, will lead to structural cyber asymmetry against nations leaving their networks open. This asymmetry will provide both defensive and offensive advantage. Thus, the strategic effects of structural cyber asymmetry seem obvious. The mechanisms and consequences of those effects are less obvious. Future developments might also challenge the presumption that any state will risk leaving its networks open. Russia's search for 'asymmetric responses' in the constant great power struggle might accelerate the fracturing of the internet into nationally controlled segments protected by military cyber forces.

Russian national system-of-systems of information security and defence should not be considered only as a 'kill switch'. If successfully deployed, it will be a system-of-systems constructed to control and manage the national information space in a continuum of interstate relations. These relations cover peaceful and intensified competition, conflict, the initial period of war, and war. The system is a response to all kinds of threats from terrorism, internal disturbances, revolutions and regional wars up to a total great power war fought with nuclear weapons. The system enables the flexible adjustment of control of the national information space. The national segment can even fragment along territorial lines into separate and internally functioning parts. A nation that can protect itself or at least ensure the continuity of the nation and state is in the position to perform a pre-emptive or even preventive attack and survive a counterstrike. Moreover, the system enables the creation of power through state-led innovation policies and a centralised management system of the information economy and society. It forms the information-technological basis for winning the constant measure-countermeasure struggle between great powers. The construction of the system in peacetime provides opportunities for exercising its full employment. Consequently, the elimination and mitigation of critical vulnerabilities and interdependencies are possible before a truly closed national network is deployed.

The decision on how to adjust the borders and internal functioning of a national segment of internet is a political question and depends on the perceived threat. The military-strategic implications of national segments are complex. The national segment will probably be disconnected in the case of a nation-wide insurgency or before the initial period of war in a regional or great power war. A flexible increase in control of the information space is enough to counter other kinds of threats. To be militarily effective, the disconnection must be conducted as soon as and as surprisingly as possible. However, economic and political reasons might delay the decision and hastiness could lead to cascading technical failure of the complex system. Outside a conflict situation, the ability to disconnect the national segment can be considered as part of deterrence by denial. The ability to conduct offensive operations from behind the protection of a national segment enables punishment. However, deterrence signalling can be misinterpreted for various reasons. A state closing its networks might be preparing the battlefield and considering a pre-emptive or even preventive attack, instead of just protecting itself from external information and cyber operations. Escalation management and control gains an additional dimension as states begin actively to manipulate their cyber and information space. Decision-makers might feel themselves secure behind the walls of national segments and engage in brinkmanship. The attacker might more readily use conventional or even nuclear force if cyber means are denied. However, if the defender feels that its strategic C2 systems are secure, it might lessen the pressure to conduct first strikes. Furthermore, national segments might still be reachable through or dependent on foreign assets despite all the efforts to achieve true technological self-sufficiency. It is possible that, if the defender wants to deny the freedom of action of the attacker, it must conduct operations against foreign networks and systems, which might escalate the conflict.

These arguments demonstrate that the panacea of structural cyber asymmetry might have unforeseen consequences, some of which already seem to be emerging. For example, the attributes and capabilities listed in Table I do not reflect the changes in Western policies during 2015–2020. During this period, the 5G and supply-chain security debate has led to the tightening of domestic market regulation. Many states pursue limited domestic HW/SW production and cryptography is increasingly seen as an issue of sovereignty. Military cyber forces are seriously considering ‘proactive deterrence’ instead of just defending their own networks. National data centres for domestic data and national cyber security centres are being built. Even the principle of territorial cyber sovereignty is being promoted by some Western countries.[8] These policies are a response to the evolving character of cyber conflict and the changing of great power relations. Open networks are becoming less open. From the viewpoint of 2020, it would seem that the asymmetric advantages of closed national networks are diminishing.

The self-evident military response to structural cyber asymmetry is to create one’s own closed national network to deter enemy attacks. It is likely that future wars are preceded by prolonged psychological operations to weaken the enemy already in peacetime, and in some cases countries can even achieve the same objectives as they would by launching kinetic attacks simply by delegitimising the regime in the eyes of its citizens through information operations. Disconnecting, or at least efficiently controlling the internet therefore makes sense for any government—authoritarian and democratic alike—in order to deter potential foreign information operations against its population. However, as the analysis of the Russian project presented in this chapter and research on the Chinese policies elsewhere (Inkster, 2016) have shown, a national segment of the internet is inherently an authoritarian project. Disconnecting the national network might not even produce the benefits sought. Moreover, the risks of closing national networks to the national and global information society and economy and the integrity of alliances, such as NATO, are real. Although NATO and its partners must find an answer to ‘asymmetric responses’, they should not follow the rules set by authoritarian states. Some scholars have proposed that democracies should join their socio-technical-economic systems to secure the existing substrate of cyberspace (Demchak, 2020). Others have argued that malign actors should be

[8] On these developments, see e.g. Tikk & Kerttunen, 2020.

challenged persistently and proactively in cyberspace (Fischerkeller & Harknett, 2019). Still others promote norm-building by the international community to defuse the ongoing cyber arms race (Tikk & Kerttunen, 2020). All these propositions have merit. However, perhaps the most important question is whether Western states should accept the idea of cyber sovereignty, or even information sovereignty. If the concept of sovereignty is adopted then the nature of 'cyber borders', the responsibilities of states concerning those borders and the role of the military in protecting them must be defined soon. The chosen definitions have significant consequences as there is the possibility that in the effort to ensure national security in cyberspace the democratic states and alliances such as NATO and the EU end up hitting the 'kill-switch' on the global internet.

7. REFERENCES

Literature

Ackoff, R.L. (1971) Towards a System of Systems Concepts. *Management Science*. 17 (11), 661–671.

Ajir, M. & Vaillant, B. (2018) Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.

Blank, S. (2013) Russian Information Warfare as Domestic Counterinsurgency. *America Foreign Policy Interests*. 35 (1), 31-44.

Brantly, A.F. (2016) *The Decision to Attack. Military and Intelligence Cyber Decision-Making*. Athens, Georgia, University of Georgia Press.

Checkland, P. (1993) *Systems thinking, Systems Practice*. New York, John Wiley & Sons ltd.

Chen, J.Q. (2019) A Strategic Decision-Making Framework in Cyberspace. In: Sarfraz, Muhammad (ed.) *Developments in information security and cybernetic wars.* Hershey, PA, IGI Global, 64–75.

Dear, K. (2019) Will Russia Rule the World Through AI? *The RUSI Journal.* 164 (5–6), 36–60.

Demchak, C. (2020) Cybered Conflict, Hybrid War and Informatization Wars. In: Tikk, E. & Kerttunen, M. *Routledge Handbook of International Cybersecurity*. London and New York, Routledge, pp. 36–51.

Drake, W.J., Cerf, V.G. & Kleinwächter, W. (2016) *Future of the internet Initiative White Paper. internet Fragmentation: An Overview.* World Economic Forum, January 2016. Available from: https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/169 [Accessed 9th February 2018].

Elbanna, S. (2006) Strategic decision-making: Process perspectives. *International Journal of Management Reviews*. 8 (1), 1–20.

Endsley, M.R. (2015) Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*. 9 (1), 4–32.

ENISA. (2015) *Critical Information Infrastructures Protection approaches in EU*, July 2015. Available from: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf [Accessed 15th September 2020].

Ermoshina, K. & Musiani, F. (2017) Migrating Servers, Elusive Users: Reconfigurations of the Russian internet in the Post-Snowden Era. *Media and Commu-*

nications, 5 (1), 42–53.

European Commission. (2020) *Reports and Studies about Digital Economy and Society Index*. Available from: https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650 [Accessed 14th July 2020].

Fischerkeller, M.P. & Harknett, R.J. (2019) Persistent Engagement, Agreed Competition and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*. Special Edition International Conference on Cyber Conflict (CYCON U.S.) November 14 -15, 2018, 267-287.

Gartzke, E. (2013) The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*. 38 (2), 41–73.

Giles, K. (2016) *Handbook of Russian Information Warfare*. Fellowship monograph 9. Rome, NATO Defence College.

Hayes, R.E. & Alberts, D.S. (2005) *Power to the Edge. Command... Control... in the Information Age*. Washington D.C., CCRP.

Hitchens, T. & Goren, N. (2017) *International Cybersecurity Information Sharing Agreements*. Center for International & Security Studies. Maryland, University of Maryland.

Hoffman, D.E. (2009) *The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. New York, Anchor Books.

Howard, R. & Abbas, A.E. (2015) *Foundations of Decision Analysis*. London, Pearson.

Humbert, C. & Joseph, J. (2019) Introduction: the politics of resilience: problematising current approaches. *Resilience*. 7 (3), 215–223.

Inkster, N. (2016) *China's Cyber Power*. New York, Routledge.

International Telecommunication Union (ITU). (2015) *Global Cybersecurity Index & Cyberwellness Profiles, April 2015*. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf [Accessed 15th September 2020].

Jonsson, Oscar. (2019) *The Russian Understanding of War: Blurring the Lines between War and Peace*. Washington, D.C., Georgetown University Press.

JP 3-13. (2014) Joint Chiefs of Staff. *Joint Publication 3-13, 27 November 2012 Incorporating Change 1 20 November 2014*. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf [Accessed 14th September 2020].

Kallberg, J. & Cook, T. S. (2017) The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*. 5, 8126–8130.

Kari, M. J. (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, Jyväskylän yliopisto.

Kiviharju, M., Huttunen, M. & Kantola, H. (2020) Finnish View on the Combat Functions in the Cyber Domain. In: Eze, T., Speakman, L. & Onwubiko, C. (Eds.) *Proceedings of the 19th European Conference on Cyber Warfare and Security. A Virtual Conference hosted by University of Chester UK* 25-26 June 2020, pp. 186–194.

Kukkola, J. (2020) D*igital Soviet Union. The Russian national segment of the internet as a closed national network shaped by strategic cultural ideas*. National Defence University Series 1: Research Publications No. 40. Helsinki, National Defence University.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2017) *Game Changer: Structural Transformation of Cyberspace*. Finnish Defence Research Agency Publications 10. Riihimäki, Finnish Defence Research Agency.

Kukkola, J., Ristolainen, M. & Nikkarila, J-P. (2019) *Game Player. Facing the structural transformation of cyberspace*. Finnish Defence Research Agency Publications 11. Riihimäki, Finnish Defence Research Agency.

Kuusisto, R., Kuusisto, T., & Armistead, L. (2005) Common Operational Picture, Situation Awareness and Information Operations. In: Hutchinson, B. *Proceedings of the 4th European Conference on Information Warfare and Security*. Glamorgan, UK, 2005, pp. 175–185.

Latukhina, K. (2018) The President urged to work together to fight the cyber threat to protect digitalisation. *Rossiiskaia Gazeta*, 8.7.2018. Available from: https://rg.ru/2018/07/08/putin-nazval-borbu-s-kiberatakami-gosudarstvennoj-zadachej.html [Accessed 18 September 2020].

Libicki, M.C. (2016) *Cyberspace in Peace and War*. Annapolis, Maryland, Naval Institute Press.

Liff, A. (2012) Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*. 35 (3), 401–428.

Multinational Experiment 7 (MNE7). (2013) *Outcome 3 Cyber Domain Final Report February 2013. Cyber Situational Awareness Standard Operating Procedure.* Available from: https://www.hsdl.org/?view&did=760553 [Accessed 31st July 2020].

NATO. (2016) *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation, 16th December 2016*. Available from: https://www.nato.int/cps/en/natohq/official_texts_138829.htm [Accessed 15th September 2020].

NATO. (2020) *Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 13th July 2020].

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). (2020) *Strategy and Governance*. Available from: https://ccdcoe.org/library/strategy-and-governance/ [Accessed 14th July 2020].

Nocetti, J. (2018) Cyber Power. In: Tsygankov A.P. *Routledge Handbook of Russian Foreign Policy*. London and New York, Routledge, 2018, pp. 182–198.

Nye, J.S. Jr. (2017) Deterrence and Dissuasion in Cyberspace. *International Security*, 41 (3), 44–71.

O'Brien, J. A. & Marakas, G. M. (2011) *Management Information Systems (10th edition)*. New York, NY, McGraw-Hill, Irwin.

Pynnöniemi, K. (2018) Russia's National Security Strategy: Analysis of Conceptual Evolution. *The Journal of Slavic Military Studies*, 31 (2), 240–256.

Rid, T. & Buchanan, B. (2015) Attributing Cyber Attacks. *The Journal of Strategic Studies*. 38(1-2), 4–37.

Ristolainen, M. & Kukkola, J. (2019) Closed, safe and secure – the Russian sense of information security. In: Benson, Vladlena & McAlaney, John (Eds.) *Emerging Cyber Threats and Cognitive Vulnerabilities*. London, Academic Press, pp. 53–71.

Ross, R., Graubart, R., Bodeau, D. & Mcquaid, R. (2018) Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. *Draft NIST Special Publication 800-160 Volume 2, 2018*. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 1st May 2020].

Simon, H. (1997) *The New Science of Management Decision*. Englewood Cliffs, NJ, Prentice Hall.

Shanghai Cooperation Organisation (SCO). (2009) *Agreement between the governments of the member states of the Shanghai Cooperation Organisation on cooperation in the field of ensuring international information security, 16th June 2009, Ekaterinburg*. Available from: https://base.garant.ru/2571379/ [Accessed 29th March 2019].

Sheremet, I. A. (2019) Ensuring cybersecurity in the context of the development of the digital economy [In Russian]. *The Bulletin of the Moscow University*. Series 25: International relations and world politics, 11 (1), 3–9.

Soldatov A. (2017) The Taming of the Internet. *Russian Social Science Review*, 58 (1), 33–39.

Thomas, T.L. (1998) Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The Journal of Slavic Military Studies*, 11 (1), 40–62.

Thomas, T. (2017) *Kremlin Kontrol: Russia's Political-Military Reality*. Fort Leavenworth, KS, FMSO.

Thornton, R. & Miron, M. (2020) Towards the 'Third Revolution in Military Affairs'. *The RUSI Journal*, 165 (3), 12–21.

Thurner, S., Hanel, R. & Klimek, P. (2018) *Introduction to the Theory of Complex Systems*. Oxford, Oxford University Press.

Tikk, E. & Kerttunen, M. (Eds.) (2020) *Routledge Handbook of International Cybersecurity*. London and New York, Routledge.

Vendil-Pallin, Carolina. (2017) Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 33 (1), 16–33.

Legislation

FZ-126. (2003) Federal law 07.07.2003 No 126-F3 (updated 07.04.2020) *'On Communications'* [In Russian]. Available from: http://www.consultant.ru/document/cons_doc_LAW_43224/ [Accessed 18th September 2020].

FZ-90. (2019) Federal law 01.05.2019 No 90-FZ *'On the changes to the Federal law on communications and the Federal law on information, information technology and information security'* [In Russian]. Available from: http://www.consultant.ru/document/cons_doc_LAW_323815/ [Accessed 8th May 2020].

RP-788. (2015) Degree of the Government of the RF 30.4.2015 N 788-p *'On the signing of an Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security'* [In Russian]. Available from: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#0463235836450268 [Accessed 18th September 2020].

RP-1632. (2017) Degree of the Government of the RF 28.07.2017 N 1632-r *'On the approval of the program 'Digital Economy of the Russian Federation'* [In Russian]. Available from: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed 23rd January 2018].

Ukaz-646. (2016) Order of the President of the RF 5.12.2016 N 646 *'On the approval of* *the doctrine of information security of the Russian Federation'* [In Russian]. Available from: http://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-05.12.2016-N-646/ [Accessed 21st March 2019].

Ukaz-203. (2017) Order of the President of the RF 09.05.2017 No 203 *'On the Strategy of the development of information society in the Russian Federation in the period 2017-2030'*. Available from: https://www.garant.ru/products/ipo/prime/doc/71570570/ [Accessed 18thth September 2020].

Ukaz-474 (2020) Order of the President of the RF 21.7.2020 N 474 *'On the national goals of development of the Russian Federation in the period to 2030'* [In Russian]. Available from: http://publication.pravo.gov.ru/Document/View/0001202007210012 [Accessed 1st November 2020].