Finnish Defence Research Agency
Research Bulletin 01 – 2018

10.04.2018

New guidance for preparing Russian 'digital sovereignty' released

Captain Juha Kukkola
National Defence University

This paper analyses the latest developments of the Russian project to build 'digital sovereignty'. More precisely it examines how the Program of Digital economy of Russian Federation (*Tsifrovaia ekonomika Rossiiskoi Federatsii*)[12] is being planned to be implemented in the light of the action plans approved in January – February 2018.[3] This paper focuses on 'directions' (*napravlenie*) of 'information security' (*informatsionnaia bezopasnost'*) and 'information infrastructure' (*informatsionnaia infrastructura*) of the 'Digital economy'. Furthermore, 'directions' are approached through the concepts of shaping of cyberspace, controlling the national segment of Internet, and digital sovereignty.[4] These concepts connect 'Digital economy' and its 'directions' to the project started by the Russian government in 2014 to create self-sustained national Internet.[5] This paper stresses that Russian 'digital' socio-economic plans have also a military strategic character.

Strategic planning and digital economy

The Digital economy of Russian Federation (*Tsifrovaia ekonomika Rossiiskoi Federatsii*)[6] is a government program based on the Strategy of the development of information society in Russian Federation in 2017-2030 (*Strategii razvitiia informatsionnogo obshchestvo v Rossiiskoi Federatsii na 2017-2030 gody*)[7] and, to a lesser extent, Information Security Doctrine of Russian Federation (*Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii*)[8 9]. They are both part of the strategic planning process of the state defined in the Law on Strategic planning (*O strategicheskom planirovanii v Rossiiskoi Federatsii*).[10] The strategic planning consists of goal-setting, forecasting, planning, and developing programs for social-economic progress and national security of the Russian federation and its subjects. In the context of strategic planning, all the above-mentioned documents have both socio-economic and (military) security aspects. For example, the Strategy of the development of information society declares, in addition to socio-economic issues, as its objectives the protection of critical information infrastructure and the securing of the unity of communication networks for defence purposes.[11] Similarly, Information Security Doctrine combines strategic deterrence and prevention of conflicts arising from the use of information technology with innovation and economic competitiveness.[12]

The Program of Digital Economy takes its guidance from the Strategy and Doctrine and sets its objectives and tasks in the context of five directions (*napravlenie*): normative regulation, cadres and education, research and technical reserves, information infrastructure and information security. The last two are of interest when examining how Russia is shaping cyberspace and trying to achieve 'digital sovereignty'. In the Program, information infrastructure is intertwined with information security. Objectives and tasks are based on external and internal challenges and threats (the emphasis is clearly on adversary state actors) the main objective being: "ensuring the unity, stability and security of information-telecommunication infrastructure of the Rus-

[1] Note on transliteration and translation: Russian words are transliterated according to the Library of Congress system. The titles of documents and specific noteworthy concepts are given in translated form with transliterations.

[2] The Government of the Russian Federation. *Programma "Tsifrovaia ekonomika Rossiiskoi Federatsii" No. P-1632-p* 28 July 2017 [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed 22 September 2017].

[3] The Government of the Russian Federation. *O "dorzhnykh kartakh" po napravleniiam programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"* Official webpage, 9 February 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed 22 March 2018].

[4] Shaping of cyberspace is understood as state efforts to influence the structure of cyberspace by technological, administrative and political means to gain, for example, military advantage. Controlling of the national segment of Internet is understood as projecting state power and authority to cyberspace through information infrastructure located in its territory. Digital sovereignty is understood as projecting state sovereignty to cyberspace. It is the ultimate objective of controlling the national segment of Internet.

[5] Golitsyna, Anastasiia, Ser'gina, Elizaveta and Kozlov, Petr. "Gosydarstvo khochet kontrolirovat' marshruty internet-trafika v strane." *Vedomosti*, 11 February 2016 [Online]. Available: https://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane [Accessed 24 March 2018].

[6] The Government of the Russia Federation, Programma "Tsifrovaia ekonomika Rossiiskoi Federatsii."

[7] The President of the Russia Federation. *Ukaz "O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody" No. 203* 9 May 2017 [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf [Accessed 22 September 2017].

[8] The President of the Russian Federation. *Ukaz "Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii" No. 646* 5 December 2016 [Online]. Available: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf [Accessed: 12 September 2017].

[9] Another important document is the Strategy of Scientific-Technological Development of the Russian Federation (The President of the Russian Federation. *Ukaz "O Strategii nauchno-tekhnologicheskogo razvitiia Rossiiskoi Federatsii" No. 642* 1 December 2016 [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=207967&fld=134&dst=1000000001,0&rnd=0.03632307878975349#02745814856013906 [Accessed: 22 March 2018].)

[10] Federal'nyi zakon. "*O strategicheskom planirovanii v Rossiiskoi Federatsii" N. 172-F3* 28 June 2014 (amended 31.12.2017) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_164841/ [Accessed: 22 March 2018].

[11] The President of the Russian Federation, "*O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody*."

[12] The President of the Russian Federation, "*Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii*."

sian Federation on all levels of information space".[13] Like previously mentioned Strategy and Doctrine, the Program also combines security with economy by emphasising the use of domestic software, hardware, and cryptographic solutions. Most interestingly, the Program presents a 'road-map' which states that in 2020 Russia will ensure its 'digital sovereignty' (*tsifrovoi suverenitet*) and by 2024 it will be one of the leading states in information security. In connection to this, according to the Program in 2024 only 10% of internal traffic of the 'Russian segment of Internet' (*Rossiiskii segment seti "Internet"*) will be routed through foreign servers.[14]

In December 2017 'Government commission on the use of information technology to improve the quality of life and business conditions' (*Pravitel'stvennaia komissiia po ispol'zovaniiu informatsionnykh tekhnologii dlia uluchsheniia zhizni i uslovii vedeniia predprinimatel'skoi deiatel'nosti*) approved actions plan for four of the five 'directions' of Program of the Digital economy.[15] The fifth, cadres and education, was approved in February 2018.[16] According to the action plans the total budget of 'Digital Economy' will be 522 billion roubles (8,9$ bn) for the period of 2018-2020.[17] The responsibility for implementing 'directions' of 'information infrastructure' and 'information security' was given to Minkomsviaz' (Ministry of Telecom and Mass Communications of the Russian Federation) and a non-commercial organisation 'Digital Economy' (*ANO Tsifrovaja Ekonomika*) was created to coordinate public and private activities and to monitor the realization of the state program.[18] Currently, 'Digital Economy' organization includes representatives from the Russian government and all the leading Russian IT-firms.[19] It should be noted that the official presence of security and military institutions in this organization is light.

Information infrastructure

Practically all state security ministries and agencies are listed as responsible actors for 'the direction of Information infrastructure'.[20] The same applies to major IT-companies which are listed as participating contractors. The main objectives of 'the direction' are: Sufficient communication network; domestic infrastructure for data storage and processing which provides affordable, sustainable, safe, and cost-effective services; and sufficient digital platforms for the needs of citizens, business and the government.

In practice, the first objective includes, for example, creating normative base for the use of information technology[21], high-speed Internet (100Mb/s) to almost every household and government institution by 2024[22], speech and data connection to all priority objects of transport infrastructure[23], the implementation of 5G technology by the economy[24], developing state-wide narrow-band IoT network (LPWAN), and state wide (including EEZ) satellite services[25]. The second objective includes, for example, the establishment of federal data-centres (eight by 2024)[26] and unified cloud services for the government. The third objective includes, for example, e-government services and their management systems, space based remote sensing system and geodetic control network, and services based on these systems. 'The direction of information infrastructure' is the most expensive one and amounts to circa 436 billion roubles (7,6$ bn). FSB, FSO and FSTEK have a definite role in planning these projects but implementation is left to state corporations and private sector.

[13] The Government of the Russia Federation, Programma "Tsifrovaia ekonomika Rossiiskoi Federatsii".

[14] Ibid. For the background of this project cf. Ristolainen, Mari. "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security Between Russia and the West," *Journal of Information Warfare*, vol. 16, no. 4, pp. 113-131, 2017.

[15] The Government of the Russian Federation. *O "dorzhnykh kartakh" po napravleniiam programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii."* Official webpage, 9. February 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed: 22 March 2018].

[16] The Government of the Russian Federation. *Utverzhen plan meropriiatii po napravleniiu "Kadry i obrazovanie" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii."* Official webpage, 21 February 2018 [Online]. Available: http://government.ru/news/31428/ [Accessed: 22 March 2018].

[17] Only aprox. 130 billion roubles (2,2$ bn) will be funded from the federal budget. Federal spending was 3974 billion roubles in 2017. (Tishina, Iuliia and Zukova, Kristina. Otsifrovannye milliardy - Pravitel'stvo utverdilo proekty "Tsifrovoi ekonomiki." *Kommersant*, 10 January 2018 [Online]. Available: https://www.kommersant.ru/doc/3515334 [Accessed: 22 May 2018]; Trading Economics. Russian government spending. Webpage, 9 April 2018 [Online]. Available: https://tradingeconomics.com/Russia/government-spending [Accessed: 9 April 2018].)

[18] The Government of the Russian Federation. *Postanovlenie "O sisteme upravleniia realizatsiei programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"" No. 1030* 28 August 2017 [Online]. Available: http://static.government.ru/media/files/zutOPH6TyKz2ciJAFcn74orvpb89UCMa.pdf [Accessed: 22 May 2018].

[19] Tsifrovaia ekonomika. "*Tsifrovaia ekonomika*." Official webpage, 22 March 2018 [Online]. Available: https://data-economy.ru/ [Accessed: 22 March 2018].

[20] Federal Security Service (FSB), Federal Protective Services (FSO), Ministry of Interior (MVD) and Ministry of Defence (MOD) are mentioned. Also listed are Federal Service for Technical and Export Control (FSTEK) and The Federal Service for Supervision of Communications, Information Technology and Mass Media (Rozkomnadzor) and Rossviaz' (Federal Communications Agency). The main partners are Skolkovo foundation, M. V. Lomonosov Moscow university, Higher School of Economics, all the major IT-firms and the Central Research Institute of Communications (FGUP TsNIIS) (which is responsible for the development of SORM) (Government commission. "*Plan meropriiatii po napravleniiu "Informatsionnaia infrastruktura" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"."* Appendix N. 3 to the minutes of the meeting 18 December 2017 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_287865/ [Accessed: 22 March 2018]; TsNIIS. "SORM" Official webpage, 22 May 2018 [Online]. Available: https://zniis.ru/focus/sorm [Accessed: 22 March 2018].)

[21] The participation of Ministry of Defence in this project implies the use of Wi-Fi and other radio frequency based technologies to create backbone connections and the need to coordinate the use of electro-magnetic spectrum.

[22] Rostelekom is designated as the main provider. FSO is responsible for the networks of federal organizations and supervises their connections.

[23] This consists of, for example, highways and railroad lines.

[24] This includes Russian software, encryption, and SIM cards. FSB, FSO and MOD have a significant role in this task. Technology is based on 5G/IMT-2020 with SDN/NFV virtualization, Cloud RAN and Virtualized backhaul. Planned frequencies are: 694-790 MHz; 3,4-3,8 GHz; 4,4-4,99 GHz, 5,9 GHz, 24,25-29,5 GHz, 30-55 GHz, 66-76 GHz, 81-86 GHz.

[25] This includes 'GIMSS' 'Global multifunctional info-communication satellite system' (*Global'noi mnogofunktsional'noi infokommunikatsionnoi sputnikovoi sistemy*) which might be a LEO satellite system analogous to OneWeb (Balashova, Anna, Sidorkova, Inna and Kolomychenko, Mariia. "Pravitel'ctvu predlozat sozdat' global'nuiu set' za R299 mlrd." *RBC*, 22. November 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/22/11/2017/5a159bdb9a79476a55456d2b?from=center [Accessed: 22 March 2018]). LPWAN means Low-Power Wide-Area Network and EEZ Exclusive Economic Zone.

[26] Situated in Central (*Tsentral'nii*), North-Western (*Severo-Zapadnii*), Uralskii (*Ural'skii*), Siberian (Sibirskii), Privolzhzkii (*Privolzhkii*) and Far-Eastern (*Dal'nevostochnii*) federal districts (*federal'nyi okrug*) and probably in two more to ensure resiliency of the system.

Information security

'The direction of information security' does not, somewhat surprisingly, include Ministry of Defence in its list of responsible actors, although, it is consulted in some of the projects.[27] All the other security ministries and agencies are present.[28] The main objectives of information security are: Ensuring the unity, stability and security of information-telecommunication infrastructure of the Russian Federation on all levels of information space (*informatsionnoe prostranstvo*)[29]; ensuring organizational and legal protection of the individual, business and state interests in the framework of the digital economy; and the creation of conditions for Russia's leading position in the export of information security services and technologies; as well as the integration of national interests in the international documents on information security issues.

The first objective is defined by its indicators to mean decreasing the percentage of routing domestic traffic through foreign servers to 10% by 2024, the almost total replacement of foreign produced hardware and software by domestic versions in federal and local administrative organizations, state corporations and corporations connected to state, and the comprehensive implementation of Russian standards of information security by those same actors by 2024. In practice, the stability and security (*ustoichivost' and bezopasnost'*) of 'the unified telecommunications network of RF' is guaranteed, firstly, by defining the vulnerabilities of networks.[30] Based on the analysis and normative work, a 'centralized system of monitoring and managing the public communication networks' is to be established. This is an organizational and technological project, which is managed by a designated operator, and includes the Ministry of Defence. It functions in cooperation with National coordination centre of computer incidents (NKTsKI).[31] The system should be up and running by 2020. Stability and security includes also the creation of standards for domestic cloud, fog computing, and quantum technology, and for systems of augmented reality and artificial intelligence.

The manageability and reliability (*upravliaemost' and nadezhnost'*) aspect of the first objective concentrates on the 'Russian segment of Internet' and 'circuiting' (*zamykanie*)[32] its network traffic exclusively inside the territory of the Russian federation. Software component of this project consists of following subsystems: register of routing-address information (Internet Number Registry), monitoring of routing information (Internet Routing Registry), nationally controlled DNS root-servers, blocking of unlawful content, cooperation with NKTsKI, and national certificate authority centre.[33] The subsystems should be managed by a designated operator. Furthermore, the technological independence and security of data processing infrastructure and systems should be guaranteed. This is connected to import-substitution and domestic production of hardware and software. Objectives are achieved, on the one hand, with encouraging innovation and government projects and, on the other hand, with regulation.

Security in the context of 'Digital economy' is not only understood as 'cybersecurity'[34] but also in the context of national interests, among others national defence. Security is not only a technological issue but also a normative one: Cloud service provider's use of data should be regulated, security standards for big data (*bol'shie dannye*) management should be enforced, criminal code should be updated, and users of communication networks should be identified. The significance of the last, quite minimally described, task should not be under estimated. It is 'hidden' among the tasks defining the rules for managing personal data. Identification of users would, in practise, erase anonymity from RuNet. Interestingly, there is also a plan to enforce domestic antivirus software on all personal computers in Russia. 'Digital economy's' security concept also reflects Russian understanding of information threats by including the prevention of the dissemination of 'unlawful information' (*protivopravnaia informatsiia*).

In this context, security seems to be connected to multiple different systems of information sharing between officials and private citizens, and to the filtering of traffic. Such a system of systems should provide indicators of harmful activity to National and Regional Computer Incident Response Centres (NKTsKI and RKTsKI). Although this is not stated directly, the arrangement seems to refer to GosSOPKA[35] system. It could also refer to 'the

[27] Government commission. "*Plan meropriiatii po napravleniiu "Informatsionnia bezopasnost'" programmy "Tsifrovaia ekonomika Rossiiskoi Federatsii"*." Appendix N. 4 to the minutes of the meeting 18 December 2017 [Online]. Available: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf [Accessed: 22 March 2018].

[28] The main partners include, for example, Cryptographic academy of the Russian federation and a group of lesser known corporations and institutions.

[29] "A set of information resources created by the subjects of the information sphere, the means of interaction of such subjects, their information systems and the necessary information infrastructure" (The President of Russian Federation. "*O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody*.")

[30] This includes stability of public communication networks, vulnerability of mobile networks (SS7 and Diameter protocols), vulnerability of transit traffic, vulnerabilities arising from the use of foreign technology, and vulnerabilities caused by cybercrime.

[31] This is a suborganization of the FSB designated to manage GosSOPKA [see footnote 35] and to coordinate actions involving critical information infrastructure (The president of the Russian Federation. *Ukaz "O sovershenstvovanii gosudarstvennoi sistemy obnaruzheniia, preduprezheniia i likvidatsii posledstvii komp'iuternykh atak na informatsionnye resursy Rossiiskoi Federatsii" No.620* 22 December 2017 [Online]. Available: http://kremlin.ru/acts/bank/42623 [Accessed: 22 May 2018]; FSB. Law project "*O Natsional'nom koordinatsionnom tsentre po komp'iuternym intsidentam*" (prepared by FSB 26.12.2017) 23 January 2018 [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/56640460/ [Accessed: 22 March 2018].) Interestingly, FSTEK, which is under MOD, is the federal agency responsible for the security of critical information infrastructure (The President of the Russian Federation. *Ukaz "Vobrosy Federal'noi sluzhby po tekhnicheskomu i eksportnomu kontroliu" No. 1085* 16 August 2004 (amended 25.11.2017) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_14031/ [Accessed: 22 March 2018].)

[32] This term seems to refer to Internet backbone architecture based on circuit switching. The document does not specify what OSI layer level is being discussed.

[33] Cf. Roskomsvoboda. "*Kitaizatsiia" Runeta vkhodit v aktivnuiu fasu i nachnetsia s tochek obmena trafikom*. Webpage, 18 August 2017 [Online] Available: https://roskomsvoboda.org/31224/ [Accessed: 24 March 2018].

[34] The project mentions domestic biometric authentication, multifactor authentication, digital identification, cryptographic authentication, trusted third party authentication, TLS with Russian crypto algorithms; and, also, operating systems, database management systems, and office software (i.e. national application family i.e. 'The Resource').

[35] The GosSOPKA (*Dosudartsvennia Sistema obnaruzheniia, preduprezdeniia i likvidatsii posledsvii komp'iuternykh atak*) is "[…] a single territorially distributed complex, including forces and means designated to detect, prevent and eliminate the consequences of computer attacks and respond to computer incidents" (Federal'nyi zakon. "O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii" No. 187-F3 26 July 2017 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed: 1 November 2017].) The project of building GosSOPKA was initiated in 2013 by president Vladimir Putin (The President of the Russian Federation. "Vypiska iz kontseptsii gosydarstvennoi sistemy obnaryzeniia, preduprezdeniia i likvidatsii posledstvii komp'iuternykh atak na informatsionnye resursy Rossiiskoi Federatsii" No. 1274 12 December 2014

centralized system of monitoring and managing the public communication networks' which was mentioned in 'the information infrastructure direction.' In any case, both are managed by FSB.

The third objective of information security is connected to the creation of export markets for Russian IT-solutions but includes also wider foreign policy goals. This becomes clear when the term 'cyberphysical' (*kiberfizicheskii*) system is introduced and it is connected to IoT (Internet of Things) and to critical information infrastructure. The term's definition is left open, but it is preliminarily put into a legal-normative framework where unauthorized interference of 'cyberphysical' systems should be proscribed. This new term has a clear connection to the previous Russian endeavour in the United Nations to ban cyber weapons.[36]

Foreign policy character is emphasized in how Russian information security standards should be harmonized with international ones, but only with the participation of Russian experts in defining international ones and keeping them in line with Russian interests. This includes the promotion of Russian, mainly cryptographic, solutions abroad. One of the main spheres of action in this regard is Eurasian Economic Union.[37] Finally, 'the Concept of secure functioning and development of the Internet' is to be prepared and presented to international organizations (it may include multiple sub-concepts and normative initiatives). This policy initiative includes provisions on: Information, technological, and economic state sovereignty in national segments of Internet; confidentiality of data and security of users[38]; and equal participation of members of world community to the governance of global information network. This project should be completed, in accordance with Russian interests, by the end of 2020. All the objectives of information security should be achieved with 34 billion roubles (600$ million).

Self-sustained national Internet by 2024?

The program of 'Digital economy' might seem overly ambitious. Then again, Rostelekom and other IT-companies have already produced impressive results in building up Russia's IT-infrastructure and the state has invested significantly in domestic hardware and software production.[39] Rostelekom has also gained control of many of the subsystems mentioned in the documents.[40] Additionally, FSB and FSTEK already have the normative base for taking control of Russia's critical information infrastructure.[41] Furthermore, the Russian state is openly challenging the freedom and openness of Russian Internet – and winning.[42] And, after the fall of UN GGE process[43], Russia is preparing to push its normative view of state sovereignty in cyberspace through different venues.[44]

'Digital economy' brings together policies and projects which have already been in progress for some time. Moreover, although the program relies heavily on extra-budgetary funds and is financially quite modest – planned budget for state armament program for 2018-2027 is 300$ mrd[45] – many of its objectives can be achieved through legislation, reorganization and reallocation of resources. This could mean that some parts of 'Digital sovereignty' are achieved quite rapidly and effortlessly. Of course, Western sanctions and the development of global economy might have adverse effects on the program. It is also important to note that 'the directions' of 'Digital economy' have planned funding only to 2020. There are many economic and political variables, including the development of international relations and the Russian presidential elections in 2024, which could affect the realization of a self-sustained national Internet by 2024.

Discussion

The program of Digital economy is much more than a plan to push Russia to information age. It is both an economic and a national security project. It aims to shape the cyberspace by creating a self-sufficient and territorially based island of Internet where Russian state sovereignty is normatively and technologically undisputed. This subspace is based on domestically produced software and hardware infrastructure. It is controlled centrally by security services and its content and processes are sub-

[Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=181661&fld=134&dst=1000000001,0&rnd=0.556811797145774#046144179472131297 [Accessed: 24 March 2018].). It has been envisioned as a centrally controlled national SIEM (Security Information and Event Management system) (Solar Security. "*Reshenie po cozdaniiu tsentrov GosSOPKA ot Solar JSOC*." Official Webpage. https://solarsecurity.ru/upload/pdf/Solar_JSOC_GOSSOPKA.pdf [Accessed: 24 March 2018].

[36] Kavanagh, Camino. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. UNIDIR 2017 [Online] Available: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf [Accessed 24 March 2018].

[37] In this context common normative regulation and standards, joint exercises, and 'a zone of digital trust' (including the use of blockchain technology) are mentioned.

[38] The document explicitly states that confidentiality and security categorically exclude anonymity of users, irresponsibility of users and 'the impunity of offenders' (*beznakazannost' pravonarushitelei*). This definition follows the observed Russian state policy to restrict privacy in Internet. (Freedom house. *Freedom on the Net 2017 – Russia*. 2017 [Online]. Available: https://freedomhouse.org/report/freedom-net/2017/Russia [Accessed: 9 April 2018].)

[39] The Federal Agency for Press and Mass Communications. *Internet v Rossii 2016 gody: Sostoianie, tendentsii i perspektivy razvitiia*. Москва, 2017 [Online]. Available: http://www.fapmc.ru/rospechat/activities/reports/2017/teleradio/main/custom/00/01/file.pdf [Accessed: 24 March 2018].; RAEK. *Ekonomika RuNeta 2017*. [Online] Available: http://raec.ru/upload/files/deitogi_booklet.pdf [Accessed: n24 March 2018].; Minkomsviaz'. *Godovoi otchet o khode effektivnosti gosydarstvennoi programmy Rossiiskoi Federatsii "Inoformatsionnoe obchshestvo (2011-2020 gody)*" 25 April 2017 [Online]. Available: http://minsvyaz.ru/uploaded/files/otchet2016.pdf [Accessed: 24 March 2018].

[40] Balashova, Anna and Kanev, Petr. "Rostelekom" stal operatorom reestra domenov .ru i .рф. *RBC*, 23 January 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/23/01/2018/5a675ab29a79473a982cd704 [Accessed: 24 March 2018].

[41] The President of the Russian Federation, "Dokrina informatsionnoi bezopasnosti Rossiiskoi Federatsii."

[42] Li, Irina. Bez Telegram: 4 voprosa o vozmozhnoi blokirovke messendzhera v Rossii. *RBC*, 21 March 2018 [Online]. Available: Россииhttps://www.rbc.ru/technology_and_media/20/03/2018/5ab0f8439a794710eb5972ac?from=center_5 [Accessed: 24 March 2018].

[43] UN Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International Security. For more about this process cf. Tikk, Eneken and Kerttunen, Mika. *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute, 2017 [Online]. Available: cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf [Accessed: 9 April 2018].

[44] The Russian ministry of foreign affairs. *Vystuplenie Zamestitelia Sekretaria Soveta Bezopasnosti Rossiiskoi Federatsii O.V. Khramova na mezhdunarodnoi konferentsii OBSE po kiberbezopasnosti, g..Vena, 3 noiabria 2017 goda*. Official webpage 3 November 2017 [Online]. Available: http://www.mid.ru/web/guest/foreign_policy/rso/osce/-/asset_publisher/bzhxR3zkq2H5/content/id/2938933 [Accessed: 24 March 2018].

[45] Bocharova, Svetlana and Nikol'ckii, Aleksei. Putin soobchshil o priniatii novoi gosprogrammy vooryzhenii. *Vedomosti*, 24 January 2018 [Online]. Available: https://www.vedomosti.ru/economics/articles/2018/01/24/748864-putin-vooruzhenii [Accessed: 9 April 2018].

jugated to the interests of authoritarian state – in the name of security. Controlling national segment of Internet means government control over traffic, services, and users.

There is no doubt that 'Digital economy' is a foundation for digital sovereignty. It is openly stated in the documents discussed in this paper. This sovereignty is based on censorship, monitoring, filtering, controlling, and domestic production and ownership of the information infrastructure. In the best case for Russia, economic benefits will flow from this project and Russia will be able to sell its version of Internet (and domestically produced technology with it) to its allies. If this fails, Russia will ensure national cyber defence and resiliency of its networks based on the disconnection of its national segment from the global Internet and achieves authoritarian control of its (cyber) civil society.

Still, the worst case would be for Russia to remain outlier of global cyber community – as a pariah state relying on domestic, subpar solutions with inefficient IT-sector. 'Digital economy' is reminiscent of Soviet style five-year plans or a more recent state armament program. Neither of these produced the sought objectives 100%. Creation of information society based on a vertically controlled government program will have its pitfalls. Be as it may, it should be kept in mind, that the military strategic part of 'Digital economy' (security) will cost only 1/10 of the creation of information society (infrastructure). This, when all is said and done, is 'a military strategic idea that promises cost-effective solution for strategic deterrence against perceived threat'.[46]

Additional information

Captain Juha Kukkola serves as a research officer at Finnish National Defence University and he is a member of a multidisciplinary research group of cyber defence in the Information Technology Division at the Finnish Defence Research Agency. For further information, he can be contacted by email at juha.kukkola (at) mil.fi.

[46] Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka. *Game Changer. Structural transformation of cyberspace*. Riihimäki: Finnish Defence Research Agency, 2017 [Online]. Available: http://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398 [Accessed: 9 April 2018]. ISBN 978-951-25-2954-4.