International Journal on Emerging Technologies **11**(5): 150-154(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Digitalization and National Security: Economic and Political Aspects (implications for Russia and the EAEU)

Yana L. Gobareva[1], Olga Yu. Gorodetskaya[1], Marina V. Karp[2] and Irina V. Kolesova[3]

[1]Associate Professor, Department of Data Analysis, Decision-Making and Financial Technology, Financial University under the Government of the Russian Federation, Moscow, Russia.
[2]Professor, Department of Accounting, Audit and Taxation, State University of Management, Moscow, Russia.
[3]Associate Professor, Department of Banking and Finance, Sevastopol State University, Sevastopol, Russia.

(Corresponding author: Yana L. Gobareva)
(Received 15 June 2020, Revised 17 July 2020, Accepted 06 August 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Today, digitalization is one of the most serious transformational processes, which affects all spheres of life and carries risks that are difficult to assess because of their complexity. National security in the era of digitalization includes the cybersecurity issues that are rapidly developing. The new conditions of the digital economy and the new threats in the digital sphere require proactive measures to counter them. In this regard, the authors highlight the basic digitalization threats to national security and give recommendations on how to address them. The major challenge of the study is the lack of methods for the econometric assessment of the cybersecurity efficiency, which leads to an unclear situation in the field of national security efficiency estimation, therefore, the development of new approaches in this field is difficult. The major contribution of the article is the formulation of the concept of national and regional security in the digital space, proposals for ensuring it via the example of Russia and the EAEU, the empirical development of the system of filters for countering terrorism and the formulation of the economic vicious circle of cybercrime.

Keywords: Digitalization, national security, threats, society, cybercrime, EAEU.

Abbreviations: EAEU, the Eurasian economic Union; UN, the United Nations; US, the United States.

I. INTRODUCTION

The digitalization issue and its relationship to national security has been raised for a long time. Digitalization as a process creates significant risks for maintaining the current position in the national security system focused on physical threats. Most state security systems are based on risk prevention, on an attempt to predict it, to maximally localize the consequences if the problem cannot be eliminated.

A digital society is characterized by completely different approaches to the formation of threats: digital risks are intangible, it is possible to localize their consequences only in real time upon the occurrence of an event, and also it is practically impossible to create a system of such risks prevention, only protection, which will provide enough time for a response [1]. Thus, the system of digital threats and digital security require the development of new approaches aimed at preventing chaotic threats and creating sufficiently powerful protection to deter them until the moment of reaction.

These characteristic features determine not only the main differences between digital and material threats, but also indicate the imperfection of the modern system of fighting digital threats in the world as a whole. These problems determine the goals set in this article: to prove the reality and an increase in speed of the transformation of the society into a digital society, develop ways to counter digital threats, and assess main economic and political consequences of the inconsistency with modern realities. A study of the digitalization process suggests that its development is accelerating [2]; therefore, the fastest and most coordinated solution to the problems associated with digital threats is necessary at the global and national levels and is extremely relevant.

The issue of digitalization and the potential risks it carries has been actively discussed in recent years. The authors have studied numerous assessments of digitalization in business and its risks [3–6]. [7,8] highlighted the issue of cooperation in the digital field in order to overcome the risks of the modern world. These works contributed to the understanding of digitalization as an overwhelming process in our lives; in this study, the authors follow the same approach and include international cooperation in overcoming the risks associated with digitalization.

Mau [9] developed the idea of new integration processes and pinpointed the domination of national interests over global, putting forward the problem of Russian politics in a new era. [9] interconnected the global nature of digitalization and the national nature of its regulation. At the same time, previous studies did not focus on the consequences of digitalization for society, which are in focus of this study.

Due to the fact that Russia is a significant player in world trade, as well as the fact that digitalization has a significant impact on trade [10], the authors of this paper focus on the development of digitalization risks counteracting system in the EAEU and Russia. Study in this area is based on works revealing key specific points of the process in the EAEU [11] and identifying key features of the process in Russia [12].

[27, 28] focused on Russia's main goals in this new field.

This article puts forward an econometric model and develops an interconnected system of cybercrime consequences – the economic vicious circle of cybercrime.

II. MATERIALS AND METHODS

The authors begin the study of digitalization and its risks to national security with an understanding of what digitalization is. Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities [13] or the way in which many domains of the social life are restructured around digital communication and media infrastructures [14]. Thus, there is no single approach to the term. Within the study, the authors consider digitalization as an institutional transformation which is closer to the second definition.

To achieve these goals, the authors use a statistical analysis of data on the penetration of digital technologies into people's daily lives. Based on the analysis, the authors conduct a regression analysis ($f(x) \sim t + const$, since the dynamics trajectories of the studied indicators are linear, and R2> 0.95), on the basis of which they make a forecast until 2030 (the time horizon is not taken randomly, the UN sustainable development goals are for the same period). Having proved the existence of a digital society, the authors address its key risks, propose strategies for addressing them in Russia and the EAEU, and then indicate the economic and political consequences of inaction.

III. RESULTS AND DISCUSSION

Today, it is common to say that modern society is characterized by a high degree of digitalization [5, 15]. This thesis is in some way outdated, since it reflects only one side of the problem – that every day a person uses certain new generation technologies. It should be said a digital society, a digital person, because: a) all information about a person and his / her life and activity is stored on the Internet (from the purchase history to passport, credit card, etc. data [16]; b) a person does not only use the new generation technologies, he / she transforms them and can transfer a significant part of his / her life to digital space today [17]; c) government and business institutions also become digital, starting from the receipt of through special government services, to the fact that information about citizens and their activities is also stored by government agencies in digital form, often in cloud storage [18]. Thus, society becomes fully digital. These trends are presented in Fig. 1.

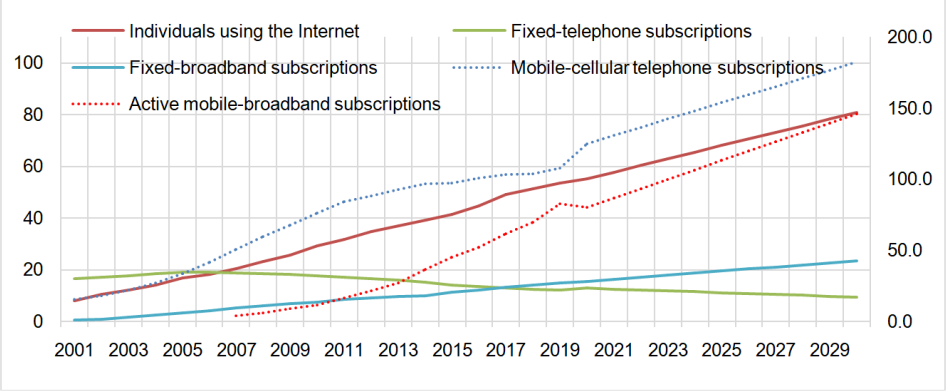

Fig. 1. Main digital society indicators – number per 100 people; dotted lines on the right axis (created by the authors, based on [19]).

As the forecast in Fig. 1 shows, by 2030, 80 out of 100 people in the world will use the Internet, and for one person there will be two mobile telephone subscriptions. In addition, the dynamics has a linear growth and has no tendency to decline in any indicator except fixed telephone subscriptions, since mobility is becoming another extremely important feature of the digitalized world. Further study of the data [19] shows that a significant share of the growth of indicators is in developing countries, which indicates their involvement in the digitalization process. The speed of these processes is very high, compared with the global GDP growth, for example, the growth of Internet users in the world is five times more. Control over economic risks is complicated due to the speed of processes in the modern economy and the significant involvement of the population in these processes, so digitalization processes are much faster than economic ones and imply a much greater involvement of the population, which gives a reason to think about how great the digital society risks and threats are.

The main threats of the new social organization are [20, 21]:

1) Digital terrorism;
2) Crime in a virtual environment;
3) Psycho-emotional insecurity of a person, lack of personal space in the digital environment;
4) Falsification of information;
5) The threat of national sovereignty in the digital space.

These five main threats cannot be considered without an integrated approach, since the most significant of them, digital terrorism, can often be provoked by a desire to violate the sovereignty of the state (for example, Russia is accused of this in the context of the US presidential election) [22]. At the same time, the existence of threats to the emotional and psychological health of a person on the Internet, although today does not represent such significant damage to both the

economy and political independence of the country, pose a significant problem in the future due to the massive use of digital technologies.

Thus, in order to create a system of protection against digital challenges, the state or the international community needs to create some kind of universal tool for filtering large amounts of information, which will cut off the flows that carry threats, but will not hinder or slow down the rest of the flow. This goal is obviously idealized and impossible, as it will require extremely large financial investments and political compromises (the use of digital pressure tools has become one of the most effective and inexpensive policy tools) [23, 24]. Therefore, the protection of the population, institutions and sovereignty in this area should be provided by individual states. Within this study, the authors propose ways to reduce the risks of digitalization for Russia and the EAEU [25].

With regard to the first risk, digital terrorism, it is necessary to fully understand what digital terrorism is and clearly distinguish it from the manifestation of freedom of expression. Digital terrorism always carries a threat; its consequences, both cybernetic and cyberkinetic, harm the economy, threaten the life and health of citizens, undermine law and public law institutions, create a mental load for citizens through the spread of panic and fear. At the same time, criticism of the state or officials, as well as other manifestations of a civil position that do not have the above features, are not terrorist acts. Having figured out what digital terrorism is, it is necessary to identify how to fight it.

The authors propose to introduce a filter system at the state level, based on who can stand behind the terrorist attack:

(1) Filter of mental or social health. Generally, individuals with mental disabilities, or terrorists' relatives, and children from dysfunctional families, are prone to terrorism. Introducing this filter significantly limits the range of constant monitoring of certain groups of people who are highly likely to participate in digital terrorism. In addition, it is possible to further limit the circle of people by education, as digital terrorism requires special skills.

(2) Filter of incoming traffic from abroad, especially from conditionally unfriendly countries. This will also limit the amount of constant monitoring and, consequently, the economic costs of the functioning of the system.

(3) "Honey pots" system (filter of knowledge / skills for a terrorist). This implies creating a number of targets for attacks that will serve as baits or disseminate false information, as for attacks by foreign structures subordinated to the government.

(4) Creation on the basis of the EAEU and Shanghai Cooperation Organization of situation or quick response centers on digital terrorism, which will have the authority to eliminate the threat or its source. This measure is aimed at creating an information filter on a wider space, which will allow the services of member countries to have greater capabilities and resources in the fight against digital terrorism. At the same time, these structures will be more efficient in the fight against digital terrorism, since they should include the counterterrorism services of member states and stimulate cooperation and information exchange between them. As mentioned earlier, a digital society is based on information and operations with it, therefore counterterrorism services should have a volume of information larger than a potential digital terrorist cell.

The second threat is the issue of personal security of each individual [29]. Nevertheless, at the national level, a competent and efficient service should be formed within the law enforcement agencies, which would have highly qualified specialists and could quickly respond to citizens' appeals (in particular, to appeals in the digital space). At the national level, it is also necessary to conduct information campaigns to fight against financial crimes, and develop cooperation between financial control authorities. This risk becomes a national threat with the proliferation of digital institutions. The same goes for the following two threats.

The third and fourth threats are also related to the individual's personal security, but they can significantly undermine the foundations of society and cause serious harm to the economy. Falsified information, in particular, deteriorates the productivity of employees and organizations, makes them spend resources on verifying the received data. If the state needs to direct efforts to protect a person in the digital environment (ensure the child Internet safety, protect citizens' data, create a safe environment for the digital society), it should introduce a voluntary content filtering system, then the second is a question of transaction costs of firms, and in the context of the formation of a digital society the state should not interfere in the information field.

The fifth threat is not obvious, but it arises from all the previous ones; the greater the impact of previous threats on the economy and politics of a country or a union of countries, the greater the probability of centrifugal trends. In fact, the society is being divided according to interests; that is, there are conditions for a new type of separatism – the separatism of digital preferences. To avoid such phenomena, it is necessary to turn to the creation of a unified national idea, which will be promoted by both state and public organizations in the digital environment. For Russia and the EAEU, this idea is obvious; it is the Big Eurasian space, the idea of integrating countries around the EAEU core, it is a kind of "second circle" of integration, which is already being formed today by signing agreements on free trade zones [26].

Despite the fact that the digitalization risks' problem for the countries' national security is global, the proposed solutions are practically universal. Since the nature of such a rapid growth of information flows with the understanding of the inefficiency of such an array of information is not obvious; modern measures to fight the digitalization threats should be based on the economy. The damage only from crimes in the digital environment was estimated at $ 3 billion in 2015, by 2021 it will grow to $ 6 billion [27]; this indicates the need to increase the effectiveness of the fight against this threat. If we consider other digitalization threats, the damage will increase significantly. Moreover, its assessment does not seem economically feasible, as there are a damage multiplier and a vicious circle (Fig. 2).

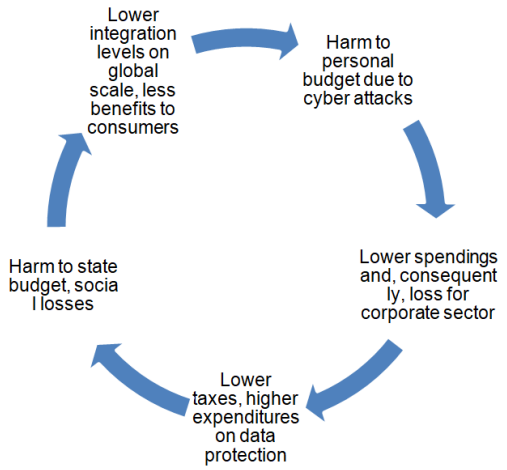

Fig. 2. Economic vicious cycle of cybercrime (created by the authors).

Thus, the lack of an adequate response to the digitalization threats leads to an increase in economic problems and destabilization of the political situation in the country.

IV. CONCLUSION

Digitalization is a process, which has been poorly studied from institutional perspective and poses a number of threats to national security. The massive penetration of digital technologies into everyday life makes any process risk a significant threat to society. In addition, the irreversibility of the digitalization process will not allow in case of unforeseen threats to exclude the national economy from the process.

The main threats to digitalization are digital terrorism and cybercrime due to the fact they already exist in an obvious form, and law enforcement agencies and the state have no effective tools and reliable protection for fighting them. At the same time, such threats as loss of national sovereignty, falsification of information, and the threat to the psycho-emotional health of citizens have been little studied and do not appear so vividly; therefore, their impact on society should not be ignored.

A system of the preventive fight against digital threats does not exist; the only option is to integrate filter schemes into national (regional) information dissemination systems, as well as create and accumulate a wide database of information from law enforcement agencies that would exceed the capabilities and scope of terrorist and criminal cells.

V. FUTURE SCOPE

The problem of national security in the new era of digitalization is not properly addressed. The problem tends to develop rapidly, however, the actions taken by national governments cannot stop the spread of cybercrimes. The article provides a basis for further research on the cybercrime dynamics and the impact of digital security problems on the national economy. Future researches may focus on the analysis and technological capability of filtering harmful content, especially in the context of freedom of information. The contemporary cybersecurity context does not reveal a very important issue – the efficiency of the conducted policies. The econometric analysis of measures taken to prevent cybercrimes and the economic losses caused by them, just as the development of methods for estimating losses in this field is another important issue for future research.

Conflict of Interest. No.

REFERENCES

[1]. Sheremet, I. (2018). Digitalization and national security. *The Free Economy Journal*. Retrieved from http://freeeconomy.ru/english/digitalization-and-national-security.html

[2]. Funabashi, Y. (2019). The digital transformation of national security. *The Japan Times*. Retrieved from https://www.japantimes.co.jp/opinion/2019/05/14/commentary/japan-commentary/digital-transformation-national-security/#.XsRgK2gzbIX

[3]. Deloitte. (2018). Managing Risk in Digital Transformation. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf

[4]. Markovitch, S., and Willmott, P. (2014). Accelerating the digitization of business processes. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/accelerating-the-digitization-of-business-processes

[5]. McKinsey Global Institute. (2019). Twenty-five years of digitization: Ten insights into how to play it right. Briefing note. Retrieved from http://tiny.cc/oodepz

[6]. UNCTAD. (2019). Digital economy report 2019. Value creation and capture: implications for developing countries. Overview. Retrieved from https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf

[7]. Afonasova, M. A., Panfilova, E. E., Galichkina, M. A., andŚlusarczyk, B. (2019). Digitalization in Economy and Innovation: The Effect on Social and Economic Processes. *Polish Journal of Management Studies*, *19*(2): 22–32. doi: 10.17512/pjms.2019.19.2.02

[8]. Rodina, L., and Nazarov, S. (2020). Systematization of the Activity Digitalization Risks: Economic, Cultural, Political, and International Aspects. *Proceedings of the "New Silk Road: Business Cooperation and Prospective of Economic Development" (NSRBCPED 2019)*. Presented at the "New Silk Road: Business Cooperation and Prospective of Economic Development" (NSRBCPED 2019), St. Petersburg, Russia; Prague, Czech Republic. doi: 10.2991/aebmr.k.200324.129

[9]. Mau, V. A. (2020). Economics and politics in 2019–2020: Global challenges and national answers. *Voprosy Ekonomiki*, (3): 5–27. doi: 10.32609/0042-8736-2020-3-5-27

[10]. Daniltsev, A. (2018). Risks and Challenges to Trade Within Digital Economy. *Trade Policy*, *4*(16): 125–131.

[11]. Voronina, T. V., Yevchenko, N. N., Yatsenko, A. B., andMadiyarova, D. M. (2018). Peculiarities of the Process of Digitalization of Economies in the Eurasian Economic Union States. *European Research Studies Journal*, *21*(Special issue 2): 1021–1033.

[12]. Korovin, G. B. (2018). Problems of industrial digitalisation in Russia. *Journal of New Economy*, *19*(3): 100–110. doi: 10.29141/2073-1019-2018-19-3-9
[13]. Gartner. (2020). Digitalization. In *Gartner Glossary*. Retrieved from https://www.gartner.com/en/information-technology/glossary/digitalization
[14]. Bloomberg, J. (2018). Digitization, Digitalization, And Digital Transformation: Confuse Them at Your Peril. Retrieved from https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/#208c1aed2f2c
[15]. Mühleisen, M. (2018). The Long and Short of The Digital Revolution. *Finance & Development*, *55*(2): 4–8.
[16]. Ross, R. (2017). Why Security and Privacy Matter in a Digital World. Retrieved from https://www.nist.gov/blogs/taking-measure/why-security-and-privacy-matter-digital-world
[17]. Dufva, T., and Dufva, M. (2019). Grasping the future of the digital society. *Futures*, *107*: 17–28. doi: 10.1016/j.futures.2018.11.001
[18]. Hanna, N. (2018). A role for the state in the digital age. *Journal of Innovation and Entrepreneurship*, *7*(1): 5. doi: 10.1186/s13731-018-0086-3
[19]. International Telecommunication Union. (2019). Measuring digital development: Facts and figures 2019. Geneva: International Telecommunication Union.
[20]. Credit Suisse. (2017). The Dark Side of Digitalization. Retrieved from https://www.credit-suisse.com/about-us-news/en/articles/news-and-expertise/the-dark-side-of-digitalization-201702.html
[21]. Kavanagh, C. (2019). New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? Retrieved from https://carnegieendowment.org/files/WP_Camino_Kavanagh___New_Tech_New_Threats1.pdf
[22]. Vovchenko, N. G., Ivanova, O. B., Andreeva, O. V., andKostoglodova, E. D. (2018). Conceptual Approach to the Development of Financial Technologies in the Context of Digitalization of Economic Processes. *European Research Studies Journal*, *21*(Special Issue 2): 11–20.
[23]. Doffman, Z. (2019). Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#a9ebd1f6758c
[24]. Lohrmann, D. (2020). State and Local Governments Face Iranian Hacking Threats. Retrieved from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/state-and-local-governments-face-iranian-hacking-threats.html
[25]. Khalin, V., and Chernova, G. (2018). Digitalization and Its Impact on the Russian Economy and Society: Advantages, Challenges, Threats and Risks. *Administrative Consulting*, *10*: 46–63. doi: 10.22394/1726-1139-2018-10-46-63
[26]. Frolova, E. E., Polyakova, T. A., Dudin, M. N., Rusakova, E. P., and Kucherenko, P. A. (2018). Information Security of Russia in the Digital Economy: The Economic and Legal Aspects. *Journal of Advanced Research in Law and Economics*, *9*(1): 89–95. doi: 10.14505//jarle.v9.1(31).12
[27]. Cybersecurity Ventures. (2020). Official Annual Cybercrime Report. Retrieved from https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
[28]. Mitrofanova, I. V., Pyankova, S. G., Ryabova, I. A., Ob'edkova, L. V., and Shcherbina, A. B. (2020). Digitalization of the Russian Economy (Target-Oriented Approach): First Results, Risks and Prospects. In T. Kolmykovaand E. V. Kharchenko (Eds.), *Digital Future Economic Growth, Social Adaptation, and Technological Perspectives* (pp. 485–497). Cham: Springer International Publishing. doi: 10.1007/978-3-030-39797-5_47
[29]. Stepanyan, T. M., Okhotnikov, I. V., Spektor, A. A., Yashkova, N. V., and Tumanov, E. V. (2019). Institutional and Legal Problems of Economic Safety. *Journal of Advanced Research in Law and Economics*, *10*(5), 1561–1569.

How to cite this article: Gobareva Y. L., Gorodetskaya, O. Yu., Karp, M. V. and Kolesova, I. V. (2020). Digitalization and National Security: Economic and Political Aspects (implications for Russia and the EAEU). *International Journal on Emerging Technologies, 11*(5): 150–154.