Contemporary Chinese Political Economy and Strategic Relations: An International Journal Vol. 7, No. 3, Dec. 2021, pp. 1319-1352

Cybersecurity Cooperation between Russia and China: Prospects and Problems

Elizaveta S. **Sokolova**[*]
Financial University under the Government of the Russian Federation

Elnur T. **Mekhdiev**[**]
Financial University under the Government of the Russian Federation

Kanan K. **Dadashov**[***]
Moscow State Institute of International Relations (MGIMO University)

Kamilla K. **Dadashova**[****]
Moscow State Institute of International Relations (MGIMO University)

Abstract

The problem of cyberthreats is one of the global issues that can be solved only through cooperation between countries, which is due to the borderless nature of the Internet. Considering that cyberspace is based on non-material assets, which are hard to estimate, the authors put forward an index allowing the evaluation of the financial efficiency of state policy in the field of cybersecurity. The authors propose a differentiated approach to cybersecurity, divide it into three basic levels and offer a broader understanding of cybersecurity. Furthermore, the authors conduct a comparative institutional analysis of the cybersecurity systems in Russia and China.

Keywords: *China, cybersecurity, digitalization, Russia*

1. Introduction

Cybersecurity today is one of the most important issues that received prominent coverage. It is connected, for example, to the claims of Russian meddling in the results of US presidential elections, the US-China information war involving their multinational companies etc. The threats are obvious, and they are associated with falsification of information, and all of these have their roots in the cybersecurity sphere. Cybersecurity provides the basis for discussing cyber sovereignty, which is considered a new but very important part of national security.

This article is aimed at finding the best track available for Russia and China in order to avoid conflicts caused by cyberattacks and to create a secure cyberspace in Asia. The main hypothesis of the article is that the sphere of cybersecurity could be much wider than it is considered at present, and that Russia and China are on the way to partnership on a wide range of cyberthreats issues and form a common strategy of fighting cybercrimes with low cost but efficient measures, which exceed their national borders. The object of the study is the development of the similar or unified approaches to the cybersecurity, taking into account the contemporary theories of cybersecurity and implementing these finding to the Russian-Chinese partnership. In order to achieve this object, the following task are to be achieved: the proposition of the unified approach to the cybersecurity issues, the comparison of the Russian and Chinese institutions in the field of cybersecurity, the proposition of the major spheres of cooperation between Russia and China in this field and the development of the best strategy for cybersecurity cooperation. The main findings include: (1) institutional approaches to cybersecurity are similar in Russia and Chins; (2) these approaches are tightly connected with the main threats in Central Asia and national strategies on intellectual property protection. We propose a model of the cybersecurity development taking into account the Shanghai Cooperation Organization's capacity and bilateral treaties. The novelty of the article includes the use of an institutional approach to cybersecurity and the conduct of the research on three levels: (1) private and corporate; (2) financial; (3) governmental.

2. Literature Review

In comparing Chinese and Russian institutions from the cybersecurity point of view, we relied on studies that focus on legislative system in the field of cyberthreats. Qi *et al.* (2018) discussed main problems that

China, like any other country, faces in the fight for cyber sovereignty and assessed the impact of the new laws in this field on its economics and social sector. However, legislative initiatives were researched without reference to the state strategies and international cooperation, and thus our research may contribute to understanding of this issue.

At the same time, Kokas (2018) gave a wide overview on the US and China's controversial politics on the global cyber arena, but gave little attention to the Chinese strategies on national cybersphere. Cho and Chung (2017), analyzed international cooperation in the field of cybersecurity and stated that cyber power is hard to measure, because it has a non-material dimension. This statement forms the basis for the vision of the Sino-Russian cybersecurity partnership's future, allowing them to suppose that both countries tend to underestimate their cyber power.

Financial aspects of Russian cybersecurity system are of interest for our research, since financial possibilities of Russia are far more limited than the Chinese, and the regulatory institutions in the financial sphere are less developed. In this regard, we relied on the research of cybersecurity in Russia and the financial technologies' development by (Soloviev, 2018).

The historical aspects of the cybersecurity institutions development in Russia and partly in the post-Soviet area were covered by (Chim, 2018). In addition, we have used data by China Internet Network Information Centre, Carnegie Endowment and the reports of International Telecommunication Union (ITU).

3. Methods

First of all, we define what we mean by cybersecurity and cyberthreats. Cybersecurity is a set of measures to prevent and prosecute cybercrimes. According to common understanding, cybersecurity is seen as internet security aimed at fighting malware, piracy, spam and other illegal or malicious content on the Internet, including Internet-based services. In this regard, cybersecurity is a matter of personal interest of every Internet-user. We do not consider the mentioned issues as threats in themselves, but they can be used to undermine stability, security and peace in many countries.

However, there is a broader understanding of cybersecurity. We suggest that cybersecurity encompasses not only the above, but also countering terrorism, drug dealing, spread of crime and threats to national security through the Internet instruments, social networks and financial instruments provided by banks.

The methods used for estimating efficiency of Sino-Russian cooperation in cybersecurity are more empirical than statistical. Firstly, no long-term data is available to build reliable trends with econometric methods (the first legal document on the issue was signed in 2015). Secondly, the data is scarce and fragmented. Therefore, the only method available is to refer to international ratings and legal practices in the studied countries and compare them by the developed criteria. In this way, we estimate the similarity of Russian and Chinese policies in the field of cybersecurity to more precisely assess the future prospects and steps of both countries. In addition, we introduce an index (*Ics*) that aims at estimating the financial efficiency of the cybersecurity policy in the national economy (Equation 1).

$$Ics = FC/\Delta CL + (\Delta FDI * (1 - Reinv) + \Delta FPI * (1 + OF))/\Delta PO \quad (1)$$

where, FC – financial costs of carrying out the current cybersecurity policy, CL – estimation of gross losses from cybercrimes in the economy, FDI – foreign direct investment, FPI – foreign portfolio investment, (FDI and FPI create capital inflow in the national economy, so they can be summarized, if no special accuracy is required), Reinv – reinvested profits of corporate sector in the national economy, OF – portfolio investments received from offshore jurisdictions, PO – volume of financial operations considered as fraud operations or prohibited by banks or authorities.

The first fraction reflects the efficiency of cybersecurity in the sector of physical users, while the second one estimates the effect of government regulatory policy and the changes in regulations on the national financial and banking system in general. As a result of the implementation of this index the government authorities can estimate both cost efficiency of cybersecurity and the share of threats, coming from abroad.

There is one more dimension of cybersecurity that is important for most of the countries – the cyber sovereignty (Chu *et al.*, 2018). Today, cyber sovereignty is not a highly discussed issue outside of context of cyberattacks by government-sponsored hackers. We introduce this aspect in our research in order to specify the future prospects of Chinese-Russia partnership on institutional level. This aspect also allows us to build up another level of research – the research of international security organizations and bilateral treaties in the Asian region.

The comparison of the institutional structure of Russian and Chinese cybersecurity sector is based on the estimation of the major threats and regulators of the sector influence, while the proposition of the major spheres of the development of cybersecurity cooperation is based on the current processes in the economies of both countries.

4. Results

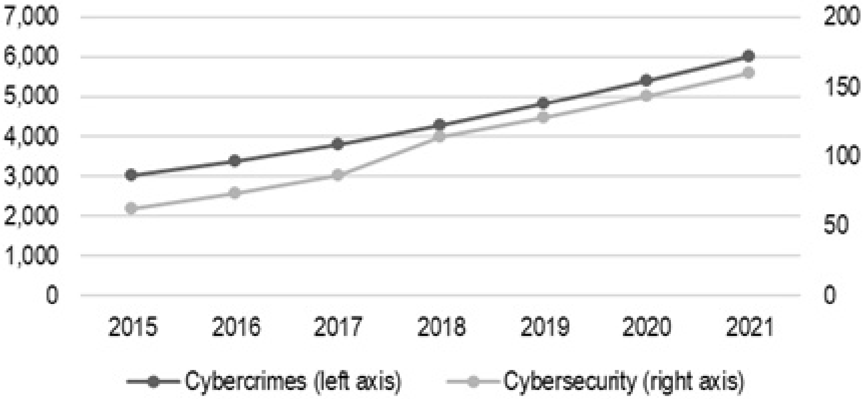
4.1. Classification of Cybersecurity Levels

Cybersecurity begins with a wide range of measures taken by regular Internet users. These are mostly commercial products provided by the specialists in private cybersecurity (Kaspersky Labs, Norton, etc.). Cybersecurity has two main circuits: "protection of" and "protection from". On this level, "protection from" circuit is represented by legal regulations and government agencies that control the sphere (in many countries these agencies may delegate their powers to Internet providers or special commercial commissions). This level is one of the most financially expensive (NortonLifeLock, 2018; Okonofua, and Rahman, 2018) but, at the same time, the most important levels, as it enables loosely connected individuals to form groups and/or to distribute illegal content. Most of the terrorist groups and illegal organizations conduct their activities on this level (United Nations, 2018; United Nations Office on Drugs and Crime, 2012).

The second level is a level of extensive financial control. It is mostly regulated by banks and banking authorities and is tightly connected to the lower level through internet transactions mechanisms, but not fully including it. On this level, the "protection of" and "protection from" circuits are integrated into one. It is important to develop this level prior to the higher level, since it allows the building of a viable strategic vision of national goals in the economic aspect of cybersecurity. In addition, the most of the cyberthreats are financial in nature and cost US$ 6 trillion annually (Cybersecurity Ventures, 2017). The investments in cybersecurity equal about US$200 billion annually, showing a negative efficiency. For every dollar spent on cybersecurity in 2017 (US$86.4 billion) and in 2018 (US$114 billion) (Cybersecurity Ventures, 2019) the losses from cybercrime were respectively US$43.94 and US$37.47, demonstrating efficiency growth (Figure 1), which should not be observed, according to forecast.

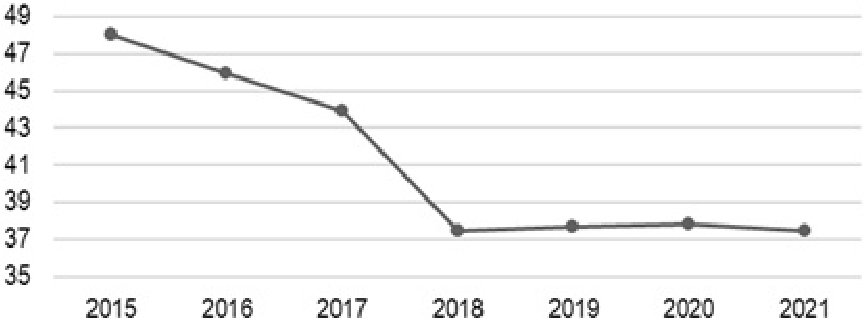
The higher speed of the investments in cybersecurity allows the conclusion that on the contemporary level its efficiency is not enough for the counteraction to the cybercrimes. The constantly and stably growing level of cybercrimes (at least in the financial sector and aspect) is indicating the same thing – the current system of cybersecurity does not provide enough defence for all the actors of the economy and public sphere.

Figure 1 Cybercrimes Dynamics (in US$ billions)



Source: Developed by the authors, based on Cybersecurity Ventures (2017).

Figure 2 Cybercrimes Counteractions Efficiency (the lower the value, the better) (in US$)

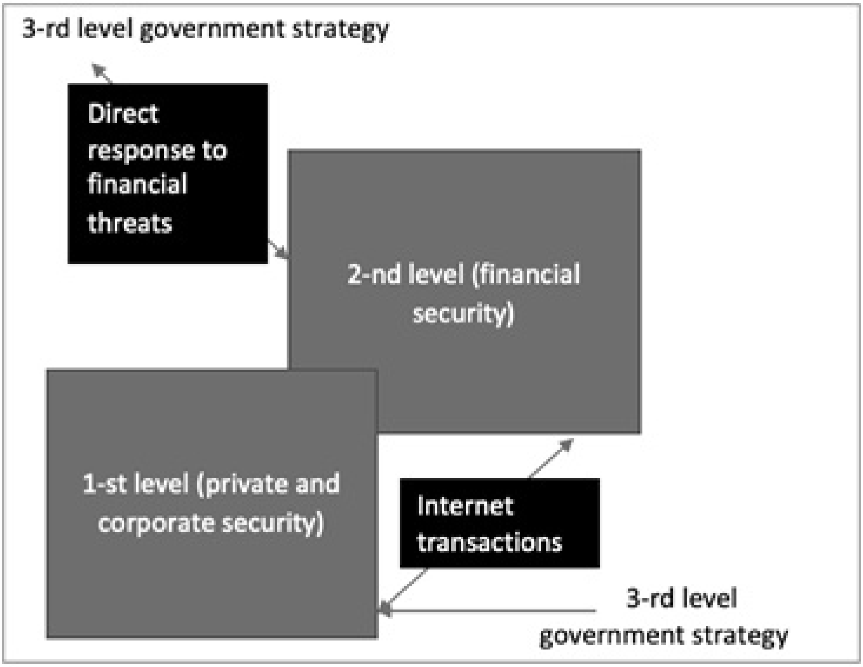


Source: Calculated by the authors.

Despite no statistics, Russia and China follow the main trend, because they are at the forefront of the cyberspace development. In Global Cybersecurity Index 2018 Russia ranked 26th (1st in regional rank), compared to 10th (2nd) in 2017. China took 27th (6th) place in 2018 and 32nd in 2017 (International Telecommunication Union 2017).

The third level is represented by national cybersecurity strategies that are interrelated to the previous two levels and form interaction between the national Internet segment and the global network. This level is shaped by national strategies of national security and the use of force against cybercrimes (Figure 3).

Figure 3 Levels of Cybersecurity on National Scale


3-rd level government strategy
Direct response to financial threats
2-nd level (financial security)
1-st level (private and corporate security)
Internet transactions
3-rd level government strategy

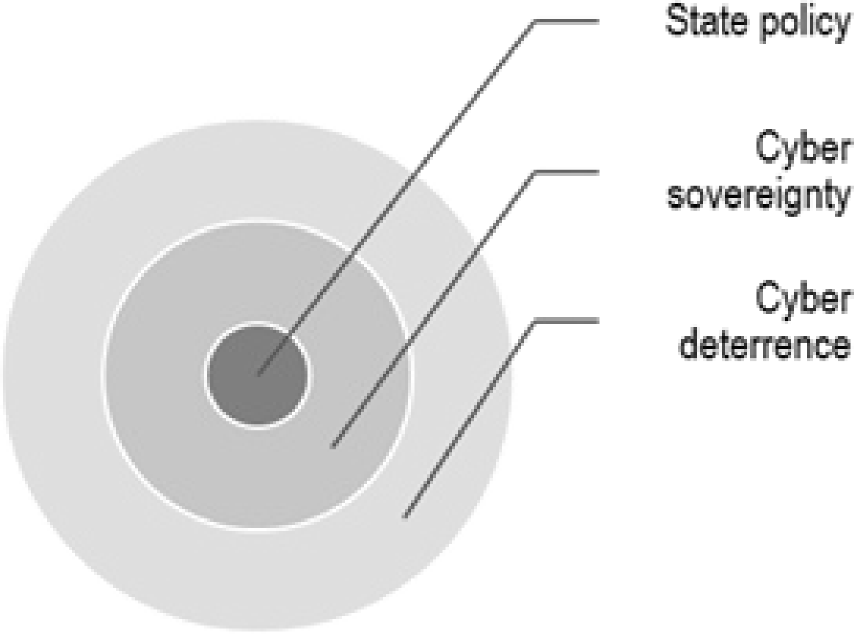
Source: Developed by the authors.

The government strategy is implemented by the state agencies responsible for data security. For Russia, they are the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor, 2014) and the financial authorities, namely the Federal Service for Financial Control and Monitoring (Rosfinmonitoring, 2019). In China, they are the China Internet Network Information Centre (China Internet Network Information Center, 2020) and the China Banking and Insurance Regulatory Commission (China Banking and Insurance Regulatory Commission, 2020).

All the mentioned aspects of cybersecurity lead to the formation of the most effective cybersecurity mechanisms in national visions. The leading countries of the world, such as the US, China, Russia, the United Kingdom and other countries that promote the development of high technologies and generate huge information flows in pursuit of leadership in this field, form a vision of cyber sovereignty, which generally means the independence of state policy from information interference from abroad. The most common example of conflicts on this ground is the accusation of Russian hackers of meddling in US elections in 2016 (the so-called Mueller investigation (*The New York Times*, 13th July 2018)). In this case, the United States accused Russia of violating its cyber sovereignty – a fact proven or forged is unclear, but the concept of cyberwar is coming to our near future. This case, like many cases with Chinese hackers, leads to a new understanding of state sovereignty in the digital age. This is no longer the problem of local violations in secret databases or espionage against politicians, the armed forces or technology, it is becoming the main national security problem.

In this regard, cybersecurity provides the basis for understanding deterrence policy. Today, cyber deterrence is becoming an important element of national security (Duggal, 2010; Tang and Zhang, 2010).

Figure 4 The Structure of the 3rd Level of Cybersecurity



Source: Developed by the authors.

Most of the charges of "political hacking" were brought against Russia and China; this leads to an important point for this study – in the modern world, cybersecurity is becoming a new tool of pressure with the concept of "highly likely" approach (Markov and Nevolina, 2018; Prier, 2017) in media coverage; the formation of cybersecurity mechanisms is impossible without the creation of information wars corps and politicized media covering cyberthreats and cybercrime cases in the way that is needed by their patron countries. The second important point is that today both Russia and China do not have enough influence in the world of information to create an effective system of cyber deterrence without restricting data traffic. Restricting and censoring data is the cyber deterrence policy of both countries.

These two spheres, cyber sovereignty and cyber deterrence, form the sub-level of state policy, which forms the structure of the 3rd level of cybersecurity, presented in Figure 4.

Figure 4 demonstrates that state policy provides only the basic directions for the development of cybersecurity, which, in turn, is aimed at ensuring the cyber sovereignty of the state. Cyber sovereignty today cannot be built on the basis of peaceful cooperation, especially in the case of the global powers mentioned above. The cyberwar field is not regulated by any international organizations, therefore, the behaviour of countries in this field is often carnivorous. Consequently, the external sphere of state policy in the modern world is defensive – it makes it possible to survive in case of attack from other parties.

At the same time, the corporate sector is also very vulnerable to the cyberthreats. The state companies and the multinational companies play a significant role in the development if the economy of the state of residency and in case of the multinational companies in the economies of the host country. In addition to that the amount of the financial resources they have and the activity they conduct in the financial sphere is comparable to the activity and resources of the countries. These factors lead to the necessity to develop cybersecurity on the corporate level, but at the same time, neither corporate, nor private security can’t be regulated by state, unless the company is state-owned or the citizen depends on the state (for instance, he or she is a public sector worker).

This sphere of cybersecurity is nearly impossible to regulate and to develop from a single centre and in order to provide a sustainable cybersecurity system, the state should concentrate on the minimization of risks in these two sectors. Today there is no effective instrument for that except for the financial instruments, such as subsidies and tax benefits. All in all, none of the mentioned sectors is well-protected from cyberthreats.

The state policy on cyberthreats today is based on the policy of the national security, but the characteristics of the cyberthreats leads to the necessity to unite the efforts of different countries in order to overcome them.

4.2. Russia-China Initiatives and Strategies on Cybersecurity

The legislative aspects of protection from cyberthreats in China and Russia are very similar. This follows from comparing the Chinese Internet Security Law adopted on 17 November 2016 (Creemers *et al.*, 2018) and the Doctrine of Information Security of the Russian Federation that came into force on 5 December 2016 (Ministry of Foreign Affairs of the Russian Federation, 2016) which:

1) provide that any personal data collected by whatever company should be stored on the territory of the country;
2) discuss the principles of cyber sovereignty;
3) define the main principles of a self-sufficient information infrastructure;
4) limit access to national data for the foreign companies;
5) impose new obligations on the Internet providers.

It is also provided therein that Russia and China aim to establish a system of international treaties, which will govern their relations in the field of cybercrimes. In this respect, the institutional matrices (Kirdina, 2014) of the cybersphere in both countries are similar. Table 1 presents the results of comparison.

Table 1 Comparison of Institutional Matrices

Criterion	Russia	China
Institutionalization of policy	Yes (see the Doctrine of Information Security).	Yes (see Internet Security Law).
Role of Government authorities	High. Roskomnadzor and Rosfinmonitoring have powers of creating safe Internet and monitoring financial flows on the Internet.	High, close to absolute. Internet Network Information Centre is empowered to limit access to any site without court decision. Banking and Insurance Regulatory Commission exercise control over all financial flows in the country regardless of their origin. This combination allows monitoring any financial activity on the web.
Role of providers	Medium. They comply with decisions of Roskomnadzor, but this does not work properly.	High. They are often affiliated with Internet Network Information Centre and obliged to implement its decision immediately. In addition, the Great Firewall blocks access to many resources automatically, but providers block it once again.
Limits of personal data use	High. No foreign provider can operate in this sphere; furthermore, there are strict banking regulations. Personal data leakages are often due to the low control capacity of Roskomnadzor and operational mistakes.	Extremely high. Any kind of personal data collection or use is controlled by Internet Network Information Centre. Personal data leakages are quite rare.
Cyber sovereignty program	Yes.	Yes. China was the first to put it forward.

Source: Developed by the authors.

Table 1 shows that approaches to the internet security regulations in both countries are similar. At the same time, the main difference in financial regulation is that Central Bank of Russia, which controls banking sector, also controls banking activity on the Internet. In addition, in Russia, there is no concept of national firewall; however, the new strategy involves creating infrastructure sufficient for operation of the national Internet segment in case of a deep conflict.

The other significant difference is the institutional structure of cybersecurity system of the two countries. The Chinese one is aimed at the isolation of the harmful information, while the Russian one at investigating its source and putting this source under block. The two approaches can correlate in case of the diversification of duties – the Chinese one serves as a firewall for the cyberthreats, while the Russian one as the analytical proactive system of prevention of them. In order to achieve such an efficient cooperation, the significant reforms in both states are needed, especially in the sphere of cooperation of the authorities and control organs, but in the long-run such system is possible to develop.

Nevertheless, the general view of cybersecurity as one of the spheres of national security tightly connected with the military potential is similar in both countries.

As a result, both countries can concentrate on the development of the national security programs, which will lead to the development of cybersecurity cooperation, but this process takes a long time and there is no guarantee, that the current state of being, where Russia and China are more rarely attacked in the cyberfield remains the same. With regard to the current information war of the USA and EU against Russia and the USA against China, the situation changes rapidly. The pandemics of the COVID-2019 significantly decreased the activity of all countries in the field of information war, but the situation with the Russian vaccine, which is very actively discussed in Europe, and the significant negative effects of Pfizer vaccine (CDC, 2021; Pfizer, 2020), which is promoted by its developers, leads to the conclusion, that the information war potential is insufficient in both countries to conduct the national security strategy. The same refers to the national institutions of both countries – they cannot manage the cyberthreats on the contemporary level.

4.3. The Strategy of Cybersecurity Cooperation between Russia and China: Main Issues and Advantages

The signing of a bilateral agreement (Reinhold, 2019), also known as a "nonaggression pact", in 2015 became the main milestone for the Sino-Russian cooperation in fighting cyberthreats. This agreement is formal in character, since it indicates general intentions, not commitments to an innovative or a deeper cooperation.

China avoids long-term agreements on a firm and comprehensive basis with temporary allies. In this respect, Russia is a temporary ally, because there exists no better variant. At the same time, Russia treats China as a dangerous partner, able to invoke economic and cultural risks. Nevertheless, it does not stop Russia from establishing strong ties with Chinese authorities, especially within international organizations. For now, in the strategies of the cyberspace development Russia and China do not treat each other as a rival. As a result of long talks, both sides agreed on the cooperation of intelligence services on the activities of CIA in the region. In near future Russia and China plan to be cautious partners in the field of cybersecurity, as they have the same goals and enemy – the US and its allies.

Cybersecurity authorities' cooperation on national security issues is a good point to begin, but this is a long way. The Russian "Big Eurasia" and the Chinese Belt and Road Initiatives, enlarged by the program vision of "a shared future for humanity", are under threat from crime in

Central Asia (Amer *et al.*, 2012: 244). The implementation of both initiatives is possible, if this problem is overcome. Due to the higher development of Russia and China in comparison with all the countries of Central Asia, most illegal actions are taken in more developed countries (this brings more profit when considering financial crimes and is more efficient in developed countries, if we talk about terrorism). In addition, the main drug transportation corridors pass through Russia, and many components of synthetic drugs are produced in China. As we have already mentioned, more and more criminal activities are migrating to the virtual realm, including organizing terrorist acts and drug trafficking.

China and Russia have rich experience in fighting crime, still their experience differs. Russia is capable of conducting efficient special forces operations and is a welcome partner in fighting crime in Central Asia (due to the history of the region). China possesses a much more developed system of cyber monitoring and control. When combined, these two approaches form a complex system of crime prevention activities.

In addition, China and Russia are home to many financial institutions (especially China) and special economic zones, which raises the issue of financial crimes. Although the studied countries tightened regulations on banks, the offshore finance is still a problem. Further steps of the cybersecurity strategy should necessarily include the measures aimed at cooperation in the financial sphere.

The important institution to start the development of the cybersecurity cooperation in real life, not on papers, is the Russian Direct Investment Fund (RDIF) (RDIF, n.d.). It promotes investments to Russia and from the country and has the significant influence of the foreign companies, which see the potential in the investments to Russia. The development of the cybersecurity cooperation in the current situation of stagnation of the Russian economy needs external financing, which will not be connected with the budget expenditures. This financial flow is to come from the commercial sector, especially those companies, which promote the use of their equipment in the institutions, which are involved in cybersecurity development. Such attitude allows attracting the companies, which seek a new market, in this regard, the Chinese companies will have special preferences and will help develop technological partnership between China and Russia, which both countries are interested in.

Both countries face a moral dilemma with regard to intellectual property. Intellectual property rights infringements are often and sometimes even encouraged by the countries' authorities in order to gain access to new technologies (intellectual espionage) (Ahammad *et al.*, 2018; Deorsola *et al.*, 2017). Hence, this does not allow citizens to form a respective attitude to intellectual property. The cybersecurity strategies include measures to fight this issue, but the balance between personal freedoms and state control is not achieved.

As we have already mentioned, one of the leading regional organizations in the field of security is the Shanghai Cooperation Organization. Despite that its instruments in the field of cybersecurity are not developed to the needed extent, the capacity of the Organization is vast, especially given the fact that its members tend to discuss security issues on the fields of the Organization's Summits, as well as make and implement decisions on them using its instruments. In this way, the Shanghai Cooperation Organization can facilitate overcoming cyberthreats in the region.

While speaking of Russian-Chinese partnership in the field of cybersecurity, it is necessary to figure out the major possible spheres of cooperation. The one of them, that we have been researching hereabove, is the financial cybersecurity. In the light of the current significant rise of crimes number in financial sector and the necessity to develop the national system of payments, Russia obviously faces significant difficulties, just as China with its high share of shadow banking operations (Chen and Chen, 2019). At the same time, these spheres form just a basement of the cybersecurity cooperation.

The following sphere is IT. It is widely known that China today has a strong IT industry, both hardware and software sectors. Russia tries to conquer the new heights in this sector (Kapranova, 2018). Both countries have introduced various services, which include personal data storage and collection, for instance, Gosuslugi in Russia. These services need a very strong proactive system of data defense, which both countries have to develop. The cooperation in this field, taking into account the high potential of the Russian specialists in IT and the Chinese technological base for it is a very useful sphere of partnership in cybersecurity.

The prevention of offline crimes is another sector. Huawei has the potential for the introduction of the system of monitoring of the new generation, which is implemented in China and in Russia. This system and its implementation are serious issues for the society, as it allows control over every person and lessens the extent of freedom and can even break human rights (PI and HKU, 2013; Ball and Edwards, 2009), but it's a powerful instrument for fighting crimes. The protection of this system and its development can boost the technological partnership with regard to the cybersecurity system.

The prevention of commercial data leakages is another interesting option for cybersecurity cooperation. Such leakages allow gaining personal data and commercial secrets, so in the situation of information war with the USA (Raychev, 2019; Gery *et al.*, 2017), such leakages are to be prevented. This sphere corresponds with the protection of private data.

The counteraction to the international terrorism is another sphere of high interest. We have already mentioned it, but this sphere is wider – it includes cooperation in the field of security, including cybersecurity as one of the major instruments of prevention of terrorism financing.

At the same time, we cannot miss out the effort of both countries to introduce the cybersecurity literacy in everyday life of its citizens. In Russia the major efforts are aimed at providing its citizens the basic financial literacy kevel through regular public-sponsored events, while in China the introduction of the system of personal scoring is aimed more at the development of law-obedience of its citizens. Such different approaches can lead to the collision of understanding of the cybersecurity, such as the one, described here above – the total control over citizens is unacceptable in Russia because of the specifics of the Russian mentality and national character (Szénási, 2016; Bulanov, 2016). This leads to the difficulties in coordinating the cybersecurity cooperation between China and Russia.

At the same time, Russia and China have different political systems, despite the fact that both countries cannot be named liberal, the multiparty electoral system in Russia cannot provide the long-run guaranty of the same course projection. It can be considered a risk for long-run partnership, but both countries have similar interests and geopolitical strategies in the field of stability and sustainable development of the SCO countries, despite competing in Central Asia. In this regard the history of the Russia-China relations with all its non-linearity adds up another reason for the partnership – the current fight with the common rival – the USA and its allies. The situation in Afghanistan and the Taliban regime in the country is another joint threat for Russia and PRC, which will make the cooperate even stronger.

5. Discussion

The results of the analysis of the institutional matrix of the Chinese and Russian approaches to cybersecurity and a broader classification of cybersecurity given above allow us to propose the most likely strategy of the future development of cybersecurity in China and Russia. The likelihood of systems and institutions and the differences in approaches and instruments forms an impressive cybersecurity cooperation future in case both countries manage to unite the cybersecurity systems, with no regard to the method -either through the SCO, or through the bilateral agreements. At the same time, it's necessary to mention, that the more countries participate in this system, the higher the benefits are, but the higher the risk are too. Taking it into account the two countries should start from the bilateral partnership, or by partnership, based on the SCO mechanisms and only afterwards to include new members in this cooperation framework.

This strategy, based on the current risks the countries face, features the following main points:

1) Integration of national mechanisms and mechanisms of the Shanghai Cooperation Organization will allow cutting the costs of the fight and improving the dissemination of best practices in Central Asian states. Especially if these practices are supported by recommendations of the Russian authorities, which have an influence in Central Asia due to historical, social and geopolitical reasons, and by the Chinese capital aimed at infrastructural development and overall better living conditions in Central Asia. Best practices should be disseminated through the Belt and Road instruments, Asian Bank for Infrastructure Investments and the future Bank of the Shanghai Cooperation Organization (China Global Television Network, 2018).

2) Creation, within the Shanghai Cooperation Organization, of an operation center for fighting cyberthreats. The center should be independent in its decisions and be under direct control of Rosfinmonitoring and the China Internet Network Information Centre. It will contribute to a more efficient decision-making and decision-implementing system.

3) Creation, within the Shanghai Cooperation Organization, of the special operations forces for a faster and stronger response to cyberthreats.

The above measures form the highest framework of Russia-China cooperation and represent the third level of cybersecurity strategy.

4) Unification of banking laws (which are already similar) (Vernikov, 2015), so that the banking authorities can form a common base of conspicuous transactions and share information on them. In addition, it is useful to formulate a similar approach to the development of national currencies and settlements in national currencies. The cryptocurrencies regulation should be also unified. Since neither Russia, nor China are at the forefront of integrating the cryptocurrencies into the monetary system, it is reasonable to formulate a cautious approach to their use in international transactions and follow the practice that any transaction in cryptocurrency is suspicious. It is important to ban use of cryptocurrencies in special economic zones, as it can lead to the formation of money laundering mechanisms.

5) Creation of a banking authority under the Bank of the Shanghai Cooperation Organization, which should be aimed at disseminating

financial practices in Central Asian countries by introducing a financial control regime equal to the national one in regard to financial flows of the companies, which are counterparties to the Russian and Chinese multinational and state-owned companies.

6) Development of a system of automatic financial control of cross-border financial flows. This system should work with all transactions of individuals and companies and form a database based on the analysis of big data of suspicious and regular transactions proposed above.

The level of private security is represented by numerous measures, many of which fall under the previously proposed measures (items 4, 5, 6), but there are some specific ones.

7) Promotion of a responsible attitude to information and personal data transmitted to and received from third parties. Today, the system of crimes in the Internet is based on that a) the criminal is anonymous, b) the victim does not apply for legal remedies, or c) witnesses of preparation of the crime or illegal actions do not take measures to prevent the crime or stop the criminal during the illegal act (Weulen Kranenbarg *et al.*, 2019) expressed similar ideas). A responsible attitude is to solve the second and third problems and reduce the first, especially crimes committed for the first time and for disorderly conduct. This measure can be implemented through extensive social work (in the education system and through work on cyber literacy of employers) and more efficient work of the police (special forces for fighting crimes in cybersphere should be created under the main part of the police corps).

8) Joint Sino-Russian corporations in the field of cybersecurity are one of the best instruments to start the transnational cooperation in economic aspects of cybersecurity.
9) Promotion of a responsible attitude to intellectual property using the measures proposed above. However, the measures should be taken in the national segment of the Internet, without prohibiting VPN and other traffic redirecting tools.

The overwhelming control that government cybersecurity agencies are gaining today in both China and Russia has a negative impact on personal freedoms. So, the course of these agencies to monitor the actions of individuals should be more in the field of intellectual property protection in the national segment of the Internet and work towards combating terrorism and drug trafficking through monitoring keywords in social networks. Both the Great Firewall in China and the widely discussed insult of government and VPN bans in Russia are rather examples of an extreme violation of personal freedoms in cyberspace. Since they are aimed at establishing control over information, and not at preventing illegal actions and protecting citizens (Akhmadieva *et al.*, 2018; United Nations, 1948).

On the other hand, such measures allow the countries to fight the attacks of the media under the patronage of their political rival countries, so this approach cannot be avoided in modern conditions. In order to improve the situation in the field of cyber sovereignty, the countries should pursue a common strategy of increasing informational influence and forming the image of victims, not aggressors, without taking into account the real situation (this area is not the subject of discussion, since, in this study, we did not find reliable evidence of the real situation and the history of the conflict between China and Russia and the Western world in the information sphere). The measures that both countries should take to achieve these goals are as follows:

1) Investments in the transparency of technological development. It is clear that the initial accusations arose as a result of intellectual property infringement, so creating the image of innovation developers can help create a new image of Russia and China in this field. To do this, countries should demonstrate the security of data storage by national leading companies in the field of ICT (for example, Huawei or Xiaomi in China or by national mobile operators, Beeline, Megafon or MTS, in Russia). Countries should also take part in international technology events.

2) Stimulation of the development of international media that will focus on the national interests of Russia and China and promote them at the international level. Well-known *RT* (Russia) or *People's Daily – Renmin Rìbao* (China) do not have sufficient authority on the international information arena, therefore, when the quality of information does not provide the potential to disseminate it, its quantity is necessary. The massive growth of international media, which should become a reliable and independent source of information, should be the goal for Russia and China. We propose joint ventures in this field, as the official positions of the two countries are often similar.

3) Stimulation of the counter-hacking measures imposed by national companies at all levels in order to ensure the security of the information flow into and out of the national segment of the Internet. This measure will ease the tension of China's Great Firewall and the restrictive measures taken in Russia. But at the same time, this is

unlikely, since they serve as an instrument of control over the population.

4) Creation of an agency on cybercrimes and cybersecurity at the international level outside of regional mechanisms – the creation of an independent court specializing in such cases for Member States. This idea is a long-term plan for countries, but it has the potential for development.

In general, cyber deterrence and cyber sovereignty have become a matter of high importance for both countries (in fact, this is true for any country that seeks to play an important role in the global economy and generate innovation or that seeks political power). The idea of cyber sovereignty has become a new sphere of national security, and its importance grows rapidly.

The SCO incorporates many other countries, including such a strong power as India, the cooperation between Russia and China for those countries has a high importance too, as many Central Asian economies suffer significantly because of terrorism, corruption and cyber threats too, so the more stable environment and the instruments of preventing such crimes on cost of the two major powers in Eurasia is a good and economically substantialised choice for these countries, especially in the current unstable conditions and threats from Afghanistan. Obviously, these countries and Afghanistan provide threats of other character than cyber threats, i.e. drugs, terrorism, corruption, radical Islam etc., but the cooperation in the field of cybersecurity within SCO proves useful for strengthening of security and partnership bonds in general, leading to a better and more cooperated answer for the above mentioned risks.

6. Conclusion

As we have demonstrated above, from the point of view of Russia and China, the cyberthreats are more than simply Internet threats. Moreover, the current national strategies in the field of cybersecurity are not wide enough and do not have the necessary tools to fight efficiently against these threats. In order to overcome the problem, Russia and China, worried about the general negative trends of development in cybersecurity and the situation in Central Asia, a strategically important region for them, took a number of steps to develop a common strategy to counter cyberthreats. All of the above confirms the hypothesis put forward in this study.

To overcome the insufficiency of the proposed strategy, it is reasonable to divide the cybersecurity into three interrelated levels and propose a set of measures for each of them. These measures should be implied simultaneously and supported by international organizations, such as the Shanghai Cooperation Organization.

The promotion of these measures through the Shanghai Cooperation Organization is less expensive, as it involves cooperative strategies with many Asian countries, all of which are interested in stable and secure development of Asia. It is important to plan and estimate the efficiency of the taken measures both on national and supranational levels. The developed index is an appropriate tool for national assessment.

The future development of the national economies of Russia and China highly depends on their ability to overcome the problems arising from cyberthreats, especially if the solution is efficient and less expensive. None of the two countries considers their current partnership as a long-term initiative, so they are cautious in their actions, that brings both benefits and losses.

The major spheres of cooperation in cybersecurity include the counteraction to terrorism, prevention of financial crimes, personal data protection, protection of commercial data, prevention of offline crimes, and information war instrument. Such a wide variety of options allows developing cybersecurity cooperation with little or no additional investments from the governments, due to the investment attractiveness of this sector for private investors.

At the moment, tactical actions of Russia and China against cybercrimes, including intellectual property infringements, are seen to be too strict and violating individual freedoms of their citizens. This model has no future; therefore, the state authorities should balance their actions in such a way so that the main goal is reached (i.e. terrorism and drug trafficking are defeated, and intellectual property rights are not infringed), but at the same time, the violation of human rights is reduced.

The issue of cyber sovereignty is important for both countries; they seek their way to secure it, but now they do not have sufficient resources in the sphere of international media influence and information dissemination effectiveness to ensure cyber sovereignty without restrictive measures on information flows in their national Internet segments. The rise of the propaganda efficiency of China and Russia at the international level can serve as a tool for cyber deterrence, so it is very important for both countries.

Notes

[*] Elizaveta S. Sokolova is a Doctor of Economics and Professor at the Department of State and Municipal Administration, Financial University under the Government of the Russian Federation. Her research interests cover the Asia region, Eurasian integration and Russian foreign policy. *<Email: sokolovaes65@mail.ru>* (ORCID 0000-0002-4237-548X)

[**] Elnur T. Mekhdiev is a PhD candidate at the Center for Analysis, Risk Management and Internal Control in Digital Space, Financial University

under the Government of the Russian Federation. His research interests cover the Asia region, Eurasian integration and Russian foreign policy. <*Email: e.mehdiev@gmail.com*> (ORCID 0000-0001-6248-6673)

*** Kanan K. Dadashov is a postgraduate at the Department of International Relations and Foreign Policy of Russia, Moscow State Institute of International Relations (MGIMO University). His research interests cover the Asia region, Eurasian integration and Russian foreign policy. <*Email: canan.94@mail.ru*> (ORCID 0000-0002-9265-3054)

**** Kamilla K. Dadashova is a postgraduate at the Department of International Relations and Foreign Policy of Russia, Moscow State Institute of International Relations (MGIMO University). Her research interests cover the Asia region, Eurasian integration and Russian foreign policy. <*Email: dadashova.kamilla@gmail.com*> (ORCID 0000-0002-7142-5298)

References

Ahammad, M.F., Z. Konwar, N. Papageorgiadis, C. Wang and J. Inbar (2018). R&D capabilities, intellectual property strength and choice of equity ownership in cross-border acquisitions: Evidence from BRICS acquirers in Europe. *R&D Management*, Vol. 48, no. 2, pp.177-194.

Akhmadieva, R., L. Ignatova, G., Bolkina, A. Soloviev, D. Gagloev, M. Korotkova and V. Burenina (2018). An attitude of citizens to state control over the Internet traffic. *Eurasian Journal of Analytical Chemistry*, Vol. 13, no. 1b.

Amer, R, S. Ashok and J. Ojendal (2012). *The security-development nexus: Peace, conflict and development*. London and New York: Anthem Press.

Ball, Rachel and Victoria Edwards (2009). Surveillance in public places: A human rights perspective. <*https://www.lawreform.vic.gov.au/sites/default/files/Submission%2B9%2BHuman%2BRights%2BLaw%2BResource%2BCentre%2BLtd%2B29.06.09.pdf*>

Bulanov, Yuriy (2016). Russian mentality: How does it influence leadership style? (Master's Thesis, Linnaeus University, Sweden.) <*https://www.diva-portal.org/smash/get/diva2:932581/FULLTEXT01.pdf*>

Centers for Disease Control and Prevention (CDC, United States) (2021). Possible side effects after getting a COVID-19 vaccine. <*https://www.cdc.gov/coronavirus/2019-ncov/vaccines/expect/after.html*>

Chen, Xu and Shuwen Chen (2019). The research on shadow banking system in China. *Journal of Economic Science Research*, Volume 02, Issue 04, pp. 31-35.

Chim, W. (2018). Russia's digital awakening. *Connections: The Quarterly Journal*, Vol. 17, no. 2, pp. 5-17.

China Internet Network Information Center (2020). <*https://cnnic.com.cn/AU/Introduction/Introduction/201208/t20120815_33295.htm*>

China Global Television Network (2018). SCO Development Bank: Prospects of the SCO Development Bank. <*https://news.cgtn.com/news/7a517a4d32454464776c6d636a4e6e62684a4856/share_p.html*>

China Banking and Insurance Regulatory Commission (2020). About the CBRC. <*http://www.cbrc.gov.cn/showyjhjjindex.do*>

Cho, Y. and J. Chung (2017). Bring the state back in: Conflict and cooperation among states in cybersecurity. *Pacific Focus*, Vol. 32, no. 2, pp. 290-314.

Chu, C.-P., T.-C. Liang and K.-C. Huang (2018). International security competition and debates on state sovereignty in the cyberspace and suggest plausible means. *2018 IEEE International Conference on Applied System Invention (ICASI), 13-17 April 2018*, pp. 1334-1337. <*https://ieeexplore.ieee.org/xpl/conhome/8379737/proceeding?pageNumber=12*>

Creemers, R., P. Triolo and G. Webster (2018). Translation: Cybersecurity Law of the People's Republic of China. <*https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/*>

Cybercrime Magazine (Cybersecurity Ventures) (13th November 2017). Cybercrime damages $6 trillion by 2021. <*https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*>

Cybercrime Magazine (Cybersecurity Ventures) (10th June 2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. <*https://cybersecurityventures.com/cybersecurity-market-report/*>

Deorsola, A.B., M.C. Martins Ribeiro Leal, M.D. Cavalcante, I.J. Schmidt and E.J. Braga (2017). Intellectual property and trademark legal framework in BRICS countries: A comparative study. *World Patent Information*, Vol. 49, pp. 1-9.

Duggal, P. (2010). Cyber deterrence: Legal perspectives (pp. 8-11). In: Andrew Nagorski (ed.), *Global cyber deterrence: Views from China, the U.S., Russia, India, and Norway*. New York: The EastWest Institute.

International Telecommunication Union (2017). Global Cybersecurity Index 2017. <*https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf*>

Gery, William R., SeYoung Lee and Jacob Ninas (2017). Information warfare in an information age. *Joint Force Quarterly* (*JFQ*) 85, 2nd Quarter 2017. Washington, DC: National Defense University Press. <*https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_22-29_Gery-Lee-Ninas.pdf*>

Kapranova, L.D. (2018). The digital economy in Russia: Its state and prospects of development. *Economics Taxes & Law*, Vol. 11, No. 2, pp. 58-69.

Kirdina, S.G. (2014). Institutional matrices theory, or X&Y theory: The main provisions and applications. *Journal of Institutional Studies*, Vol. 6, no. 3, pp. 13-33.

Kokas, A. (2018). Platform patrol: China, the United States, and the global battle for data security. *The Journal of Asian Studies*, Vol. 77, no. 4, pp. 923-933.

Markov, E. and A. Nevolina (2018). Russia as the main object of modern information wars. *Historia Provinciae – the Journal of Regional History*, Vol. 2, No. 3. pp. 12-48.

Ministry of Foreign Affairs of the Russian Federation (5th September 2016). Doctrine of Information Security of the Russian Federation. <*http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163*>

NortonLifeLock / Symantec (2018). 10 cyber security facts and statistics for 2018. (Written by a NortonLifeLock employee.) <*https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html*>

Okonofua, H. and S.S.M. Rahman (2018). Cybersecurity: An analysis of the protection mechanisms in a cloud-centered environment. *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. 12th IEEE International Conference on Big Data Science and Engineering* (*TrustCom/BigDataSE*), pp. 1955-1962.

Pfizer (2020). Pfizer-BioNTech COVID-19 Vaccine. (VRBPAC briefing document. Meeting date: 10th December 2020) <*https://www.fda.gov/media/144246/download*>

Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly*, Vol. 11, no. 4, pp. 50-85.

Privacy International (PI, London) and the Law and Technology Centre of the University of Hong Kong (HKU) (March 2013). The Right to Privacy in China (Stakeholder Report, Universal Periodic Review, 17th Session - China). <*https://www.uprinfo.org/sites/default/files/document/china/session_7_-_october_2013/js8_upr17_chn_e_main.pdf*> <*https://privacyinternational.org/advocacy-briefing/655/right-privacy-china*>

Roskomnadzor (16th March 2009). Statute on Roskomnadzor. <*http://eng.rkn.gov.ru/legal_information/*>

Rosfinmonitoring (20th April 2019). Legal basis. <*http://www.fedsfm.ru/en/normative-legal-base*>

Qi, A., G. Shao and W. Zheng (2018). Assessing China's cybersecurity law. *Computer Law & Security Review*, Vol. 34, No. 6, pp. 1342-1354.

Raychev, Yavor (2019). Cyberwar in Russian and USA military-political thought: A comparative view. *Information & Security: An International Journal*, Vol. 43, No. 3 pp. 349-361.

Reinhold, T. (2019). Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security of May 8, 2015. <*https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf*>

Russian Direct Investment Fund (RDIF) (n.d.). Overview – The Russian Direct Investment Fund (RDIF) is Russia's sovereign wealth fund with reserved capital of $10 billion under management. <*https://rdif.ru/Eng_About/*>

Soloviev, V.I. (2018). Fintech ecosystem and landscape in Russia. *Journal of Reviews on Global Economics*, Vol 7, pp. 377-390.

Szénási, Endre (2016). Putin's Russia: Russian mentality and sophisticated imperialism in military policies. *Proelium*, Vol. 7, No. 11, pp. 7-12.

Tang Lan and Zhang Xin (2010). Can Cyber Deterrence Work? (pp. 1-3) In: Andrew Nagorski (ed.), *Global cyber deterrence: Views from China, the U.S., Russia, India, and Norway*. New York: The EastWest Institute.

The New York Times (13th July 2018). 12 Russian agents Indicted in Mueller investigation. (Reported by Mark Mazzetti and Katie Benner.) <*https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html*>

United Nations Office on Drugs and Crime (6th July 2012). The use of the Internet for terrorist purposes. <*https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf*>

United Nations (26th December 1948). The Universal Declaration of Human Rights. <*https://www.un.org/en/universal-declaration-human-rights/*>

United Nations (4th October 1948). Illicit drug flows, organized crime grow as terrorism spreads across borders, Third Committee delegates stress amid calls for stronger justice systems. <*https://www.un.org/press/en/2018/gashc4228.doc.htm*>

Vernikov, A.V. (2015). Comparing the banking models in China and Russia: Revisited. *Studies on Russian Economic Development*, Vol. 26, no. 2, pp. 178-187.

Weulen Kranenbarg, M., T.J. Holt and J.-L. Van Gelder (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, Vol. 40, No. 1, pp. 40-55.