Effects of 'Digital' Country's Information Security on Political Stability

Tuan Anh Nguyen[1,*], Kalybek Koblandin[2], Shukran Suleymanova[3] and Vladimir Volokh[4]

[1]*Faculty of Humanities and Social Sciences, Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation*
[2]*Department of Regional Studies, L. N. Gumilyov Eurasian National University (ENU), Nur-Sultan, Kazakhstan*
[3]*Department of Public Relations and Media Policy, Russian Academy of National Economy and Public Administration under the President of the Russian Federation (RANEPA), Moscow, Russian Federation*
[4]*Department of Public Administration and Political Technologies, State University of Management, Moscow, Russian Federation*
E-mail: anhnguyen3891@yandex.ru; tanguyen@rambler.ru; koblandin_kalybek@rambler.ru; sh_suleymanova@rambler.ru; volokh.vl547@rambler.ru
[*]*Corresponding Author*

Received 05 July 2021; Accepted 31 August 2021;
Publication 22 October 2021

Abstract

In this day and age, information security is becoming a priority not only in the system of international economic relations but also at the state level. This study aims to study the effect of a 'digital' country's information security on its political stability through quantitative analysis. The study is a mixed research design with a focus on the Russian Federation and the Republic of Kazakhstan. Its methodological basis is represented by the collection and analysis of data on the level and nature of cybersecurity threats (Global Cybersecurity Index, the number of cyber incidents) and on the level of political stability (Political Stability and Absence of Violence/Terrorism indicator

Journal of Cyber Security and Mobility, Vol. 11_1, 29–52.
doi: 10.13052/jcsm2245-1439.1112

of the Worldwide Governance Index). The results of the study show that Russia with a GCI 2020 score of 98.06 and Kazakhstan with a GCI score of 93.15 have relatively low levels of political stability. This is evidenced by their 45.7 and 25.7 percentile ranks on Political Stability and Absence of Violence/Terrorism and a high frequency of offenses using information and communication technologies. Findings suggest that with a high level of commitment to information security, the growth in cyber incidents will not necessarily affect political stability. The obtained findings provide countries an insight into cybersecurity within the national system as well as present a great deal of data on best practices to work through gaps in the national culture of cybersecurity at the state level. The results and methodology of this study can be used by officials to develop information security strategies and tactics, as well as by other researchers for quantitative analysis of the relationship between information security and political stability of different countries and regions.

Keywords: Cyberattack, cybersecurity, global cybersecurity index, political stability and absence of violence/terrorism, technology, worldwide governance indicators.

1 Introduction

The advent of technology, which renders the country's border space increasingly permeable, coupled with the rise of new arenas and sources of conflict (such as weak institutions, ethnic conflicts, and environmental threats) has expanded national security requirements. Our understanding of 'security' is limited to the traditional concern with territorial integrity or protection of vaguely defined but well understood national interests and does not include threats to the social fabric of society or threats posed by states with incomplete control over their territory, weakened legitimacy, or persistent interethnic conflicts. In addition to that, the growing irrelevance of territoriality and the continuing importance of jurisdictional sovereignty have made states vulnerable to these new categories of threat: national responses are no longer adequate, yet the division of political space into states jealously guarding their sovereignty inhibits collective responses to these diffused threats [1].

The modern world is interconnected and governments and businesses are often faced with the challenge of balancing the protection of information resources with the need to share information. This tension between the

expected benefits and the potential security risks inherent in the information sharing process exists in many areas, including the public sector, business, healthcare, law enforcement, military, and so on [2].

Emerging late in the 1960s out of government-funded Cold War defense research on a communication system capable of withstanding nuclear attacks, in the late 1990s, the Internet became widely perceived as a global commons, inaccessible to governments and supporting the free flow of information and communication at both national and transnational levels. In the 21st century, global society is changing rapidly, and the development of information and communication technologies (ICTs) makes the world more integrated and accelerates the process of communication [3]. With the advancement of technology, especially the development of communication channels, including instant messengers and social media, the Internet has acquired the capacity to permit the speed and ease of public discourse and civic organizing. It became possible to use Internet-based tools to foster new forms of public discourse and civic engagement, to solve shared problems, and in mass protest movements or revolutionary regime change events [4, 5]. Despite growing restrictions on online communication and government oversight of social media, the social media platforms continue to be a sustainable space for social interaction [6].

Once regarded as a great force for human empowerment, social media and related digital tools for sharing information have become a serious threat to democratic stability and human freedom. The key challenges faced by contemporary democracies are their growing vulnerability to Internet polarization and manipulation, the new threats to human rights and privacy in the digital age, the challenge of aligning the business model of social media companies with their responsibilities to a democratic society, and the challenge of reining in the efforts of authoritarians to advance and disseminate digital technologies of surveillance and control. In many cases, it is no longer possible to separate the spheres of online politics and offline politics because digital rights are human rights, and human rights are digital rights [7].

The use of advanced technology predetermines new clashes and social tensions. In the context of social transformation, restrictions, ethnopolitical tensions and conflicts, information technologies can act as an effective resource in reaching political goals and destabilizing the country or region. Recognizing the influence of information bombardment on the electoral behavior of society, many countries increasingly turn their attention toward threats to public stability and security emanating from the information space [8]. The ubiquity of 'political' technology along with the emergence

of bot farms has undermined public confidence in the reliability of digital media, posing new threats to political stability [6]. By giving citizens a possibility to create online forums for public discourse, organizing, and protest activity, modern technologies posed substantial challenges to states that seek to balance potential economic and social benefits with the risk of increasing political instability. The implications involve global-scale experimentation and adaptation processes [9].

Disruptions in routine operation of digital technology, also known as cyber incidents, occupy a prominent position in national and international security policies, and state actors are trying to find adequate solutions to the new threat. With each passing year, cyberattacks become more targeted, more expensive, more destructive and, in many cases, more political and strategic. To launch their attacks, cybercriminals normally take advantage of jurisdictions that lack comprehensive legal frameworks on cybersecurity. Therefore, there is a need for an integrated approach to cybersecurity governance [10, 11].

Cybersecurity governance can be characterized by these factors: an increase in the number of security actors; the spread of security threats that are simultaneously intangible, intransigent and unpredictable; and the development of complex, overlapping mechanisms (institutional, legal, and normative) of monitoring and regulation. These all require strengthening of the role of the state, the actor traditionally seen as the guardian of international order and the primary agent of security policy [12]. Considering the variety of security threats, the government institutions must undertake many interrelated measures to counter them, including political measures, economic measures, legal measures, diplomatic measures, administrative measures, criminal intelligence operations, and more. These measures should be implemented as a systematic, consistent, and continuous process [13].

Craig and Valeriano [14] hold that states are still the most dominant actors in the cyberspace. Although non-state actors and terrorists do play a role, their tactics are usually ineffective or used as cover for nation-states seeking to hide their actions. Since nation-states have all the resources to invest in manpower, research, development and education, which non-state actors are unlikely to rise, they remain in the most advantageous position to ramp up cyber attack capabilities [14].

Nation-states have developed different views regarding the challenges and threats related to the cyber domain and these differences stem from the conceptualization of cyberspace. For Russia, Kazakhstan and China,

the information space includes not only the digital networks, but also the political and social sphere. Therefore, the main threat comes from the ability of opponents (such as the United States) to destabilize these political environments and threaten their control over society, specifically by means of disinformation. The main threats to the cybersecurity of the members of the Commonwealth of Independent States (including in particular Russia and Kazakhstan) are as follows [15]:

- Using information and communication technology (ICT) for military and political purposes to undermine the sovereignty, violate the territorial integrity, or implement actions that impede the maintenance of international peace, security, and stability;
- Using ICT for terrorist purposes and attracting new supporters to terrorist activities;
- Using ICT to interfere in the internal affairs of sovereign states;
- Using ICT for criminal purposes, including the commission of computer crimes and various types of fraud;
- Using ICT for computer attacks on critical information infrastructure;
- Using ICT to monopolize the market in the context of increasing technological dependence on states dominant in informatization.

For the United States, cyberspace, by contrast, includes computer networks and the economic, industrial or military activities that depend on them. The threat is therefore more related to the ability of a competitor to use the high digitalization of these societies to gain an asymmetric advantage or cause catastrophic damage [16]. For example, cyber-intervention in the 2016 US presidential election resulted in mainstream Pearl Harbor references. The 'cyber Pearl Harbor' analogy was used to define massive cyberattacks against the US infrastructure that could lead to catastrophic doom scenarios [17]. Therefore, cyber threats and information security vulnerabilities are at the forefront of Americans' attention. For example, in an address to Congress in February 2015, the US National Intelligence Director James Clapper declared that cyberattacks were a greater threat to national security than Sunni extremists, the nuclear ambitions of Iran and North Korea, and foreign operatives trying to penetrate the national security community in the United States [18].

The vast majority of cyber conflicts occur between long-standing rivals seeking to harm each other, and often exist in the context of regional disputes. Mutual attacks, on the other hand, are rare, but possible. At the same time, cyber threats and security landscape cannot be considered without a

deep consideration of the international processes. One cannot understand the dynamics of the Sony hack by North Korea in 2014 without looking at the long history of rivalry and cultural conflict between the United States and North Korea [18]. In this context, Iran is also significant. This country shaped its politics of authoritarian Internet control in the international struggle with the United States. The U.S-dominated Internet freedom agenda has confirmed the Iranian government's view that media was as an instrument of foreign interference, and Western support for Internet activists and circumvention tools motivated state authorities to intensify surveillance and persecution of critical online activity and improve technical capabilities for Internet monitoring. Cyberattacks against critical state infrastructure have also spurred the development of Iran's offensive capabilities for attacks and infiltrations. They even provided Iran with an opportunity to learn from its adversaries. Iranian hackers conduct cyberattacks against a wide range of internal and external targets using a variety of tools and tactics. The small number of groups with shifting strategies and sophistication active in this area have evolved from amateurs to more state-oriented hackers. The direct involvement of the Iranian state in cyberattacks has been documented in only a few cases, but the choice of targets generally corresponds to the ideological and strategic parameters of the Iranian regime [19].

Unlike Iran, China dedicates more coordinated, more strategic, and more consistent efforts to advance the sovereign Internet agenda at home and abroad. These efforts are driven not so much by security threats as by the desire to gain absolute control over the digital experience of its population. The focus is on three dimensions: Internet governance, national defense and internal influence. Through its guidance of the Shanghai Cooperation Organization and creation of the World Internet Conference, normative collaborations with Russia and other states, and promotion of Internet sovereignty as benefiting developing states, the Chinese government is advocating for global recognition of the norm over the long term. However, the growing international support for Internet sovereignty could undermine transparency, accountability, and human rights, sparking new hot spots in the ongoing confrontation over digital norms [20]. While analyzing the state of affairs with regard to the balance between cybersecurity and freedom in digital space, Buryak [21] revealed that the achievement of balance in post-industrial societies is determined primarily by state goals and strategies. This is directly related to the fact that the full-fledged digitalization of activities in the post-Soviet space entails numerous risks, including unauthorized interference into the operation of critical infrastructure, the private sector, and the personal

lives of citizens. Precisely these risks necessitate a legal regime to regulate activities in the information space and ensure digital sovereignty further.

Cyberattacks against state security are not limited by hacker attempts to access computer systems and databases. Tenove et al. [22] note that external and internal perpetrators such as state and non-state actors, terrorist groups, hacktivists and extremist social movements, and more can use digital technologies to undermine critical elements of democratic elections: opportunities for citizen participation (voting, running for office, or participating in public debates); public deliberation; and key institutional actions by electoral commissions, political parties and other organizations. Attackers interfere in elections by exploiting systemic and institutional vulnerabilities: low digital literacy of the population; imperfect data protection; shortcomings in the design and policies of social media platforms; high levels of polarization in political cultures and media systems; and inadequate electoral regulation. Election interferences can have a substantial negatively effect on political stability, undermining government legitimacy, exacerbating social discord, or weakening citizens' trust in democratic institutions and each other. However, the degree of such effect is not completely clear [22].

Some tactics for digital election interference include: *hacking attacks* designed to modify or leak private information, violate campaign laws and regulations, and more; massive *disinformation* and *propaganda* campaigns; *online 'trolling' operations* to threaten, stigmatize, and harass individuals or groups; and *micro-targeted manipulation* [22]. Examining the proliferation of hoaxes and hate speech through websites and social media in Indonesia, Gunawan and Ratmono [23] found that hate has been politicized and hoaxes have been modified for economic and political interests. The consequences were the shift from freedom of speech to hate speech, especially on social media. Gunawan and Ratmono [23] concluded that the proliferation of hoaxes as a means of promoting specific political interests threatens national security and political stability.

The increasing attention to the effect of information security and political stability stems from the relationship between political stability and economic growth, implying that cyber threats to political stability are also threats to economic strength [24 ,25]. Although many studies agree on the association of cyber threats and political stability, there is no quantitative assessment of cyber challenges and their relationship with a quantitative expression of political stability.

This study aims to study the effect of 'digital' country's information security on its political stability through quantitative analysis. The focus is

on Russian Federation and the Republic of Kazakhstan. The objectives of the study are: (1) to quantitatively analyze the level and nature of cyber threats; (2) to quantitatively analyze each country's political stability; and (3) to determine the relationship between cyber threats and political stability.

2 Materials and Methods

The study integrates several research methods, including quantitative and qualitative research methods, comparative and descriptive analyses, and graphical elements. The quantitative framework involves the collection and analysis of data on cyber threats and political stability from these data sources:

– The 2020 Global Cybersecurity Index (GCI) survey [26].

The GCI index revolves around five pillars of the global cybersecurity agenda: legal, technical, organizational, capacity building and cooperation. These five pillars shape the inherent building blocks of a national cybersecurity culture [26, 27]. The GCI index is calculated every two to three years by the International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies. It combines 25 indicators into one benchmark to monitor the cybersecurity commitment of 194 ITU member states and the State of Palestine to the said pillars. For each of these pillars, questions were developed to assess commitment [24]. Since the GCI index is not evaluated annually, it does not provide a sufficient amount of data to analyze the cybersecurity dynamics of a particular country, and it therefore can only be exploited to determine the level of commitment the country had to cybersecurity preparedness at a certain point in time [28].

– Crime statistics reports from the Ministry of Internal Affairs of Russia published in 2012/2019 [29]. The cybercrime-related reports selected for analysis present data on the number and types of technology-aided criminal offenses (or cybercrimes) detected in Russia in 2019, on the total number of committed crimes in Russia in 2019, and on the share of illegal access/malware-related incidents reported within the same time frame.

– These annual infographics summarize cyberattacks detected in the Republic of Kazakhstan in 2019 [30].

– The Worldwide Governance Index 2019 (Political Stability and Absence of Violence/Terrorism) – according to World Bank Policy Research Working Paper [31].

Political Stability and Absence of Violence/Terrorism is one of the six dimensions of governance in Worldwide Governance Indicators (WGI) project by Daniel Kaufmann (Natural Resource Governance Institute and Brookings Institution) and Aart Kraay (World Bank Development Research Group). It captures perceptions of the likelihood of political instability and/or politically motivated violence, including terrorism. This measure includes, but is not limited to, the following variables: armed conflict, violent demonstrations, social unrest, international tensions or terrorist threat, political terror scale, security risk rating, intensity of internal conflicts, intensity of violent activities of underground political organizations, intensity of social conflicts (excluding conflicts related to land), (government stability, internal conflict, external conflict, ethnic tensions, protests and riots, terrorism, interstate war, and civil war. The country's score (−2.5 weak; 2.5 strong) is calculated based on the extensive survey of entrepreneurs, citizens and experts from around the world [24, 31, 32].

The study focuses on two countries in transition: the Russian Federation and the Republic of Kazakhstan. These countries both began their journey toward market economy in 1990 after the breakup of the Soviet Union, the economy of which was based on the centralized economic planning. Today, both countries exhibit a relatively high level of development when compared to the most developed economies. According to the World Bank, both countries have an upper-middle-income economy, with GNI per capita of more than 4.046 US dollars [33]. On the other hand, these economies remain heavily dependent on resources, with issues of economic digitalization and technology adoption at the forefront.

3 Results

In current times, many world states are characterized as highly dependent on digital interactions. Digitalization is key to the development of economies, societies, and governments relying on digital systems. In this connection, cybersecurity must be highly prioritized in public policy to provide a safe everyday Internet connection, which has become more reliant upon due to new working and living conditions resulted from the Covid-19 pandemic. Cybersecurity provides a so-called secure gateway covering numerous aspects: from managing participants in the online space to sharing documents. Consequently, in order to move forward, countries need to identify cybersecurity strengths and weaknesses and use their competitive advantages to develop shared cyberspace and promote health-related data in

Table 1 Global cybersecurity index 2020

Country	Rank	Score (from 0 to 100)
Ranking leaders		
US	1	100
UK, Saudi Arabia	2	99.54
Estonia	3	99.48
Rankings of the analyzed countries		
Russia	5	98.06
Kazakhstan	31	93.15

Source: [26].

the face of the pandemic. The GCI allows countries to begin this process to better understand countries' commitments to cybersecurity, identify gaps, and encourage the incorporation of best cybersecurity-oriented practices. Table 1 shows the results of the GCI 2020 global rankings for Russia and Kazakhstan as compared to the ranking leaders.

As follows from the data above, Russia and Kazakhstan take quite rightful positions among a total of 194 countries of the world. Hence, the Russian Federation ranks 5th with the score of 98.06 out of 100, whereas Kazakhstan takes 31st place with the score of 93.15. This confirms high (Russia) and above-average (Kazakhstan) levels of their readiness to counteract potential information environment threats. It is important to note that at present, Russia and the cybersecurity leading country (the US) are in a bilateral relationship, which has both shared cybersecurity goals (the desire to prevent the militarization of global cyberspace) and contradictions (different approaches to the development of information resources). The US sets an emphasis on the use of a public-private partnership approach, while Russia's national security culture relies upon state control in Internet regulation and, accordingly, global management of information space, which is perceived by the US government as a threat to national economic security. By means of such a strategy, Russia protects itself from espionage through information technologies of Apple, Microsoft, Google, Skype, and Facebook, from misinformation through content production, and from computer attacks on critical infrastructure.

In this context, it makes sense to consider the national culture of cybersecurity from the perspective of the following five main pillars of GCI:

1. Legal measures – measures based on the existence of legal frameworks dealing with cybersecurity and cybercrime (include legislation, regulation, and containment of spam legislation). They authorize a state to set up basic response mechanisms through investigation and prosecution of

crimes and the imposition of sanctions for non-compliance or breach of law.

2. Technical measures – measures based on the existence of technical institutions and cybersecurity dealing framework. They are responsible for the effective development and use of ICT within the country.
3. Organizational measures – measures based on the existence of coordination institutions, policies, and strategies for cybersecurity development at the national level. They cover the identification of cybersecurity objectives and strategic plans, as well as the formal definition of institutional roles, responsibilities, and accountabilities to ensure their implementation. Organizational measures are indispensable for endorsing the elaboration and implementation of an effective cybersecurity posture.
4. Capacity building measures – measures based on the existence of research and development, education and training programs, certified professionals, and public sector agencies fostering capacity building. They are an integral part of the first three pillars (legal, technical, organizational) and are essential in raising awareness, knowledge, and know-how across sectors, making systematic and appropriate solutions, and promoting the development of qualified professionals.
5. Cooperative measures – measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

Table 2 provides estimates and values for the main pillars of national security culture by analyzed countries as of 2020.

According to the results of the GCI 2020, the strengths of Russian national cybersecurity embrace legal, capacity building, and cooperative measures, while the weak sides are embodied in organization-related issues, and technical measures occupy an intermediate position. As for Kazakhstan, the strong points of its cybersecurity include legal and cooperative measures, the weak one relates to capacity building, and the intermediate positions are occupied by technical and organizational measures.

Table 2 GCI 2020 results for Russia and Kazakhstan

		Values for Main GCI Pillars				
Country	GCI Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Building Measures	Cooperation Measures
Russia	98.06	20.0	19.1	19.0	20.0	20.0
Kazakhstan	93.15	20.0	19.5	18.5	15.2	20.0

Source: [26].

Let us take a closer look at the information security statistics for the examined countries.

3.1 Russian Federation

According to the Ministry of Internal Affairs of Russia, there were 294.4 thousand cases of high-tech criminal activity in 2019, among which the majority were 'old-style' crimes (Figure 1), such as fraud (119.9 thousand cases), theft (98.8 thousand cases), and the production, sale or shipment of drugs (24.7 thousand cases).

As follows from Figure 1, the modern types of crime (those related to virtual activity) made up a relatively small portion of cases. Hence, illegal access to information systems represent 2.42 thousand cases, cyber fraud – 0.69 thousand cases, creation, use and distribution of malicious computer programs or malware – 0.46 thousand cases), public call for extremist activity – 0.26 thousand cases, and public call for terrorist activity via the

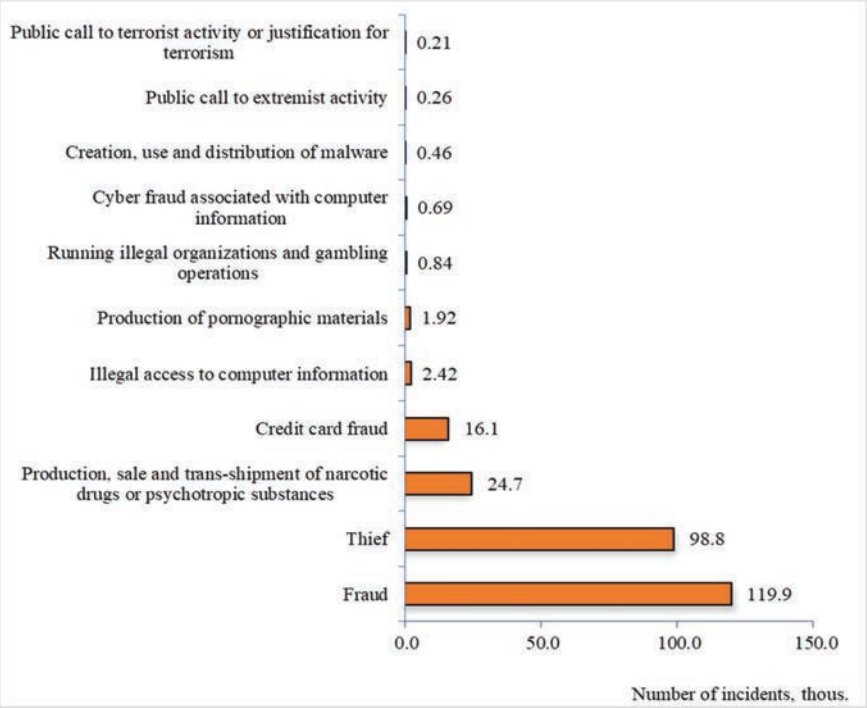


Figure 1 Types of cyber-events in Russia, adapted from crime statistics reports [29].

Internet – 0.21 thousand cases. Figure 2 below shows the number of crimes committed with the use of ICT tools in Russia.

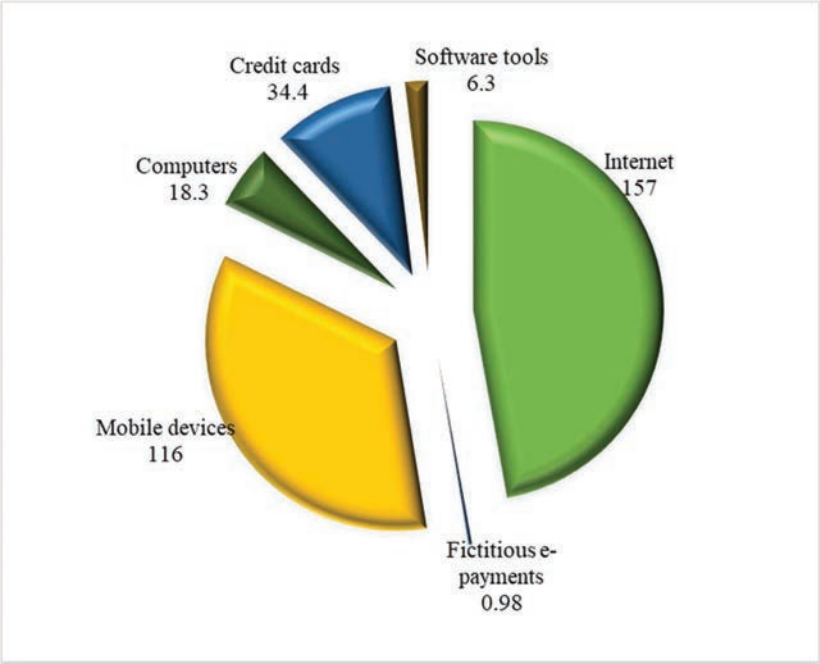


Figure 2 The summary of technologies and tools used in financial cybercrime in Russia in 2019 (number of cases), adapted from crime statistics reports [29].

The overwhelming majority of technology-aided criminal offenses in 2019 were committed using these technologies and tools (Figure 2): the Internet network (157 thousand cases), mobile devices (116 thousand cases), computers (18.3 thousand cases), and software tools (6.3 thousand). The thorough analysis of the above data allows the conclusion that common crimes are increasingly committed by modern methods using advanced ICT.

3.2 Republic of Kazakhstan

According to the National Computer Emergency Response Team of the Republic of Kazakhstan (KZ-CERT), the total number of cyber incidents in 2019 was 20.8 thousand cases (Figure 3). The largest number of incidents is related to the use of network botnets (17,300 cases), and the lowest – to the DoS and DDoS attacks (201 cases).

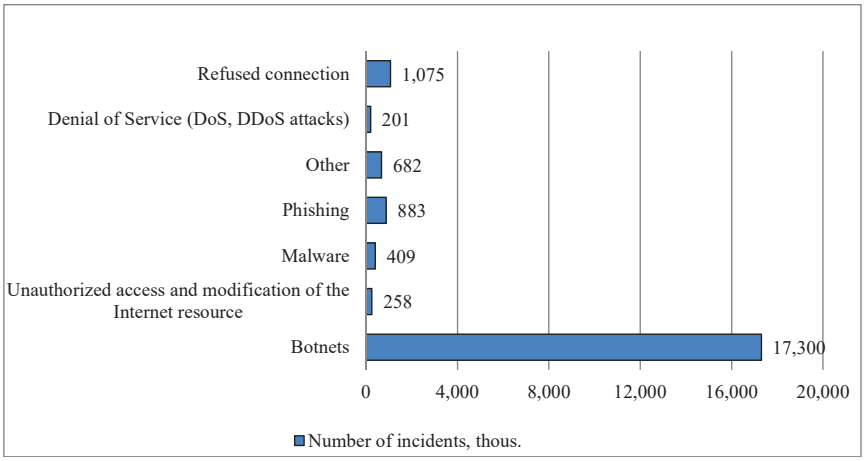


Figure 3 Types of crimes related to the use of computers and telecommunications technology, 2019 [30].

Figure 3 clearly shows that the use of botnets, refused connection to information resources, and phishing are the top three types of crimes related to the use of computers and telecommunications technology.

The analysis of the global cyber threats to critical state infrastructures conducted using the GCI and indicators of state-level crimes committed with the use of ICT suggests that the number of cyber threats is directly related to the country's political stability, which depends on governance and the institutions through which power is exercised. The six dimensions of governance cover the election process (voice and accountability), political stability and absence of violence, ability of the government to effectively formulate and implement sound policies, regulatory quality, the rule of law, and control of corruption. Within this framework, through the Worldwide Governance Index (WGI), quantitative indicators of political stability in Russia and Kazakhstan were analyzed (Table 3).

In contrast to the GCI 2020, Russia and Kazakhstan rank fairly low in the WGI. This fact is evidenced by their negative governance averages of -0.29 and -0.57 on the scale from -2.5 to 2.5. Political Stability and Absence of Violence/Terrorism indicator was not the exception as well – the percentile ranks of Russia and Kazakhstan correspond to 45.71 and 25.71 out of 100, respectively. These outcomes intimate that the analyzed states belong to the groups of countries with average (Russia) and below-average (Kazakhstan) levels of Political Stability and Absence of Violence/Terrorism (Table 3).

Table 3 WGI 2019 results for Russia and Kazakhstan: average value and values by six core WGI dimensions

Dimension	Country	Governance (from −2.5 to 2.5)	Percentile Rank (from 0 to 100)
Voice and Accountability	Russia	−1.21	14.78
	Kazakhstan	−1.10	18.23
Political Stability and Absence of Violence/Terrorism	Russia	−0.08	45.71
	Kazakhstan	−0.54	25.71
Government Effectiveness	Russia	0.12	57.69
	Kazakhstan	0.15	58.17
Regulatory Quality	Russia	0.14	61.06
	Kazakhstan	−0.43	36.06
Rule of Law	Russia	−0.43	36.06
	Kazakhstan	−0.72	25.00
Control of Corruption	Russia	−0.32	43.75
	Kazakhstan	−0.83	21.63
Mean	Russia	−0.29	40.71
	Kazakhstan	−0.57	30.80

Source: [31, 32].

The analysis of the relationship between the level of threats to political stability from the information environment was based on the total number of crimes committed using ICT on the one hand (in Russia, this figure is 294.4 thousand, and in Kazakhstan – 20.8 thousand) and WGI's Political Stability and Absence of Violence/Terrorism indicator on the other (in Russia it constitutes 45.71 points and in Kazakhstan – 25.71 points).

Figure 4 shows the scatter diagram, which provides a solid ground for formulating an assumption about the linear nature of the relationship between the number of cyber threats and political stability.

As evidenced by the diagram above, there is a relationship between the total number of crimes committed by means of ICT and the indicator of the Political Stability and Absence of Violence/Terrorism in the case of both Russia and Kazakhstan $(\mathrm{R}^2 = 1)$. The outcomes for the Russian Federation suggest that the high level of cybersecurity currently restrains the impact of cyber threats on its political stability. As concerns Kazakhstan, it is important to note that, despite an above-average position in the GCI 2020, the mechanism for countering potential cyber threats does not work here, and thus, there is a direct and strong impact of cyber threats on its political stability. Given the data obtained, the analyzed states are recommended to perform a systematic assessment of the information space in the sphere of cybersecurity, both at the national and international levels.

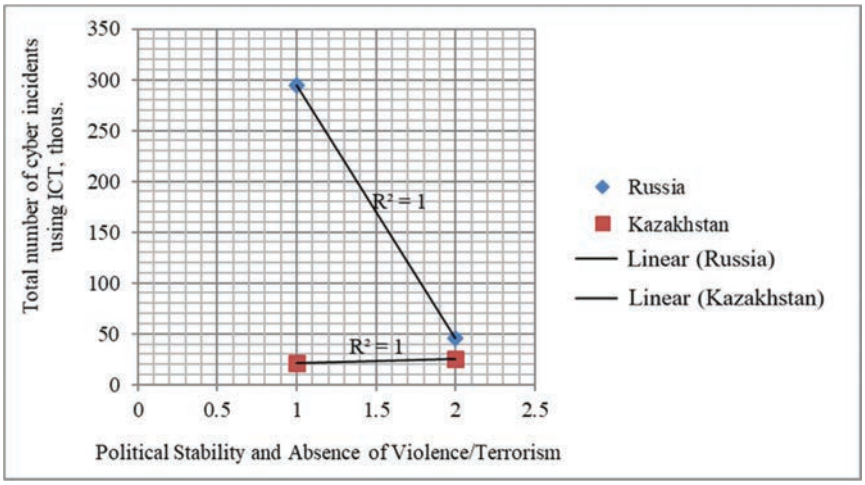


Figure 4 Scatter diagram: cyber threats – political stability.
Source: [26, 31].

4 Discussion

With the advancement of the Internet technology, the cyber risks will continue to grow. At the same time, the major threats to information security come from the inside. Attackers may interfere with critical infrastructure with the involvement of individuals who have inside knowledge of the company or industry (i.e., trusted employees) or people with access to protected information systems [7].

The essence of deliberate illegal actions is always the same, regardless of the type of cyber-event. What changes is the means of execution. Once again, technological developments designed to make life easier are used against us and now we are condemned to generate new escapes, rather than reap the fruits of civilization [5]. The increasing Internet penetration and technology adoption along with the increase in traffic leads to more information security threat [11]. The growth of cyber incidents in Kazakhstan and Russia only supports this suggestion.

The present analysis of the relationship between cyber threats and political stability suggests that with a high level of commitment to information security, the growth in cyber incidents will not necessarily affect political stability [12]. Of course, the massive targeted attacks (such as botnets, trolling, etc.) on democratic institutions and society at moments of vulnerability (elections, plebiscites, etc.) can cause significant damage. In this case,

cybersecurity measures are not by themselves a contributing factor in political stability. The maturity and strength of society and public institutions are also important [20].

According to estimates, the main information security trends of 2021 in post-Soviet countries, particularly Russia [34–36], will be associated with the expansion of the attack surface due to the mass transition to the remote work mode, the widespread emergence of distributed and disparate infrastructures, attacks on critical information systems, data leakage with the subsequent use of the information in phishing, social engineering, and some other forms of malicious activity. In such conditions, it is vitally important to use security software that meets the demands of practice, assure information security automation, and strengthen remote users' authentication. This study offers a systematic assessment of national cybersecurity culture at the national and international levels.

5 Conclusions

In order to determine the impact of national information security on political stability, the present study addressed the quantitative data on the Russian Federation and the Republic of Kazakhstan for 2019–2020. These data characterize the level and nature of cybersecurity threats or threats that come from the information space (such as GCI value and the number and types of cyber incidents). The study also explored the Political Stability and Absence of Violence/Terrorism data that reflects the level of political stability of states.

According to the analysis of GCI 2020 indicators, Russia is among the top five countries in terms of cybersecurity, and Kazakhstan belongs to the group of states with the above-average cybersecurity level. In contrast, the WGI 2019 results indicate that these states rank quite low and belong to the groups of countries with average (Russia) and below-average (Kazakhstan) levels of Political Stability and Absence of Violence/Terrorism. At the same time, both countries were found to have high levels of crimes carried out with the use of ICT(in Russia, the number of cases is 294.4 thousand, and in Kazakhstan – 20.8 thousand).

In summary, the collected data allows inferring that the high level of cybersecurity in Russia contains the impact of cyber threats on its political stability. However, with the GCI score of 98.15 and less, cybersecurity can not provide adequate and sufficient protection of the state, and, as a result, cyber threats can severely affect the political stability of the country. This fact was fully confirmed by the example of Kazakhstan.

The results and methods of this study can be used by Russian and Kazakh officials in developing information security strategies. Apart from this, the findings obtained can be benefited from by researchers engaged in quantitative analysis of the relationship between the level of cyber threats and political stability in a particular country or region.

This study is limited to statistics for two countries, the Russian Federation and the Republic of Kazakhstan. Another limitation is related to methodology. Future research will examine other countries through the integration of more indexes and methods of analysis.

Funding

This paper has been supported by the RUDN University Strategic Academic Leadership Program.

Competing Interests

The authors declare that they have no competing interests.

References

[1] J. Sperling, 'Eurasian security governance: new threats, institutional adaptations, in limiting institutions?', Manchester University Press, Manchester, 2018.

[2] C. Anderson, R. L. Baskerville, M. Kaul, 'Information security control theory: achieving a sustainable reconciliation between sharing and protecting the privacy of information', J. Manag. Inf. Syst., vol. 34, no. 4, pp. 1082–1112, 2017.

[3] Z. Syzdykova, N. Medvedev, S. Suleymanova, E. Nazarova, V. Volokh, 'Governance of cross-border migration in Asia', Space Cult. India, vol. 7, no. 4, pp. 264–273, 2020.

[4] R. Deibert, R. Rohozinski, 'Liberation vs. control: the future of cyberspace', J. Democr., vol. 21, no. 4, pp. 43–57, 2010.

[5] J. A. Kerr, 'Authoritarian management of (cyber-) society: Internet regulation and the new political protest movements', PhD Thesis, Georgetown University, Washington, 2016.

[6] E. Gaufman, 'Security threats and public perception', Springer, Switzerland, 2017.

[7] L. Diamond, 'The road to digital unfreedom: the threat of postmodern totalitarianism', J. Democr., vol. 30, no. 1, pp. 20–24, 2019.
[8] A. Salgiriev, V. Gaziev, M. Soltamuradov, S. Galbatsov, 'Information threats to the stability of political system in the northern Caucasus', Cent. Asia Caucasus, vol. 21, no. 4, pp. 25–32, 2020.
[9] J. A. Kerr, 'Information, security, and authoritarian stability: Internet policy diffusion and coordination in the former soviet region', Int. J. Commun., vol. 12, pp. 3814–3834, 2018.
[10] N. N. Schia, 'The cyber frontier and digital pitfalls in the Global South', Third World Q., vol. 39, no. 5, pp. 821–837, 2018.
[11] M. Dunn Cavelty, A. Wenger, 'Cyber security meets security politics: complex technology, fragmented politics, and networked science', Contemp. Secur. Policy, vol. 41, no. 1, pp. 5–32, 2020.
[12] J. Sperling, M. Webber, 'The European Union: security governance and collective securitization', West Eur. Politics, vol. 42, no. 2, pp. 228–260, 2019.
[13] V. Terziev, N. Nichev, S. M. Bankov, 'National security of the republic of Bulgaria', SSRN Electronic Journal, 2017.
[14] A. J. Craig, B. Valeriano, 'Realism and cyber conflict: security in the digital age', Realism Pract., vol. 85, pp. 85–101, 2018.
[15] B. Simis, 'Cybersecurity 2020–2021', Positive Technologies, 2021.
[16] S. Taillat, 'Disrupt and restraint: the evolution of cyber conflict and the implications for collective security', Contemp. Secur. Policy vol. 40, no. 3, pp. 368–381, 2019.
[17] S. Lawson, M. K. Middleton, 'Cyber Pearl Harbor: analogy, fear, and the framing of cyber security threats in the United States, 1991–2016', First Monday, vol. 24, no. 3, 2019.
[18] B. Valeriano, R. C. Maness, 'International relations theory and cyber security, in Oxford Handbook Intern. Pol. Theo.' Oxford, pp. 259–272, 2018.
[19] M. Michaelsen, 'Transforming threats to power: the international politics of authoritarian internet control in Iran', Int. J. Commun. (19328036), vol. 12, pp. 3856–3876, 2018.
[20] S. McKune, S. Ahmed, 'Authoritarian practices in the digital age the contestation and shaping of cyber norms through China's internet sovereignty agenda', Int. J. Commun., vol. 12, p. 21, 2018.
[21] V. Buryak, 'The problem of cybersecurity in the information society', Legal Fact, Vol. 32, pp. 25–31, 2018.

[22] C. Tenove, J. Buffie, S. McKay, D. Moscrop, 'Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy', Centre for the Study of Democratic Institutions, University of British Columbia, Vancouver, 2018.
[23] B. Gunawan, B. M. Ratmono, 'Social media, cyberhoaxes and national security: threats and protection in Indonesian cyberspace', Int. J. Netw. Secur., vol. 22, no. 1, pp. 93–101, 2020.
[24] M. A. Uddin, M. H. Ali, M. Masih, 'Political stability and growth: an application of dynamic GMM and quantile regression', Econ. Model., vol. 64, pp. 610–625, 2017.
[25] M. N. Azimi, M. M. Shafiq, 'Hypothesizing directional causality between the governance indicators and economic growth: the case of Afghanistan', Future Bus. J., vol. 6, no. 1, pp. 1–14, 2020.
[26] International Telecommunication Union, Global Cybersecurity Index 2020 (GCI 2020), 2021. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed 14 April 2021.
[27] R. Azmi, W. Tibben, K. T. Win, 'Review of cybersecurity frameworks: context and shared concepts', J. Cyber Pol., vol. 3, pp. 258-283, 2018.
[28] F. Bustamante, W. Fuertes, T. Tulkeredis, M. Ron, 'Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for Ecuador, in International Conference of Research Applied to Defense and Security', Springer, pp. 12–26, 2018.
[29] Ministry of Internal Affairs of the Russian Federation, Main Information and Analytical Center. Crime Statistics Reports for 2012-2019, 2019. https://мвд.рф/Deljatelnost/statistics. Accessed 14 April 2021.
[30] KZ-CERT, Cyber Incidents Infographics for 2012–2019, 2019. https://cert.gov.kz/press_club/infographics. Accessed 14 April 2021.
[31] D. Kaufmann, A. Kraay, M. Mastruzzi, The worldwide governance indicators: methodology and analytical issues. World Bank Policy Research Working Paper No. 5430, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1682130. Accessed 14 April 2021.
[32] The World Bank, The World Bank country and lending groups, 2021. https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups. Accessed 14 April 2021.
[33] United Nations, Standard country or area codes for statistical use (M49), 1999. https://unstats.un.org/unsd/methodology/m49/. Accessed 14 April 2021.
[34] World Bank and Natural Resource Governance Institute and Brookings, The Worldwide Governance Indicators (WGI 2012–2019), 2019. http:

//info.worldbank.org/governance/wgi/Home/Documents. Accessed 14 April 2021.

[35] FinCERT, Bank of Russia's Centre for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere. Review of transactions not authorised by customers for 2019, 2019, https://www.cbr.ru/eng/analytics/ib/fincert/. Accessed 14 April 2021

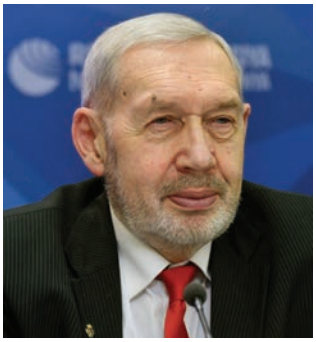
[36] N. Golovko, 'Cyber Threats and Information Security Forecast 2021', Anti-Malware, 2020, https://www.anti-malware.ru/analytics/Threats_Analysis/2021-Cyber-Threats-and-Information-Security-Forecast. Accessed 14 April 2021.

Biographies

Tuan Anh Nguyen is a Postgraduate of the Faculty of Humanities and Social Sciences at the Peoples' Friendship University of Russia (RUDN), Moscow, Russian Federation.

Kalybek Koblandin is a Doctor of Historical Sciences and Professor of the Department of Regional Studies at the L. N. Gumilyov Eurasian National University (ENU), Nur-Sultan, Kazakhstan.

Shukran Suleymanova is a Doctor of Political Sciences of the Department of Public Relations and Media Policy at the Russian Academy of National Economy and Public Administration under the President of the Russian Federation (RANEPA), Moscow, Russian Federation.



Vladimir Volokh is a Doctor of Political Sciences of the Department of Public Administration and Political Technologies at the State University of Management, Moscow, Russian Federation.