KnE Social Sciences

XXIII International Conference
Culture, Personality, Society in the Conditions of Digitalization:
Methodology and Experience of Empirical Research Conference
Volume 2020

Knowledge E
enriching | engaging | empowering

Conference Paper

The Digital Society in the 21st Century: Security Issue

D.M. Kovba and Y.Y. Moiseenko

Institute of Philosophy and Law of the Ural Branch of the Russian Academy of Sciences, Yekaterinburg, Russian Federation

Abstract

Digitalization is thought to be a key driver of recent economic, cultural, political, and society transformations, with these changes entailing both positive and negative consequences. The negative ones include various risks and threats for information security of both society and state. As a result, there has been growing impetus to rethink the concept of security in the digital age. In this paper the discourse of security is discussed in terms of dichotomy between soft and hard power in a digitalized society. This discussion involves the following issues to be considered: 1) how this soft/hard range of power can be applied to the security problem; 2) how different information threats could be countered within the discourse of the state security; 3) how the soft security could be implemented in a digitalized society. Structured analysis, discourse analysis and conceptual approach are mainly involved to provide research methodology for the discussion. It should be noted that our research is conducted within theoretical framework established by B. Buzan, J. Nye, with the acknowledgment of the results obtained from the previous studies of the authors of this paper. The concept of security was productively discussed in terms of soft and hard power vocabulary. As a result of this discussion, soft security was interpreted as the measure of protecting something from harm in invisible, unobtrusive ways, whether hard security was designed to oppose challenges and threats and it is traditionally associated with methods of force. It was particularly established that hard security measures are likely to be applied in the military sector, while soft security measures are commonly used in a non-military context. Due to the concept of soft security has not yet been clearly defined and has not received recognition as a scientific term, it is argued that further investigation is demanded. Within this investigation, information security is interpreted as a special category of soft security. The relevant distinction between information security and cybersecurity is made, with the different frequency of using these terms in official discourses of different states being explained. It is also considered that the problems of soft security insurance cannot be solved at the level of individual states due to the transnational nature of digital technology, so it requires international responses. Therefore, establishing the normative force (i.e. elaboration of international rules and institutions) can be an effective measure, while an international exchange of experience in countering information threats seems to be very useful. Educational programs aimed both at creating qualified personnel in the field of digital technologies, as well as at the general public (improving information literacy), also contribute to ensuring the safety of society and the state.

Corresponding Author:
D.M. Kovba
daria_kovba@mail.ru

Published: 21 January 2021

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the XXIII International Conference Conference Committee.

Keywords: information security, digital society, soft security, international relationships, cybersecurity.

1. Introduction

The digital revolution, which began in the 1980s, has led to fundamental changes in economics, culture, politics and other dimensions of society existence. Researchers tend to believe that it is currently problematic to determine exactly which technology exactly caused these changes. Nevertheless, there are at least five elements contributed to the digital revolution of the end of the XX century: 1) the conversion of the telephone exchanges to all digital technology and traffic with the conversion of speech to a digital stream at the exchange input; 2) optical fiber; 3) packet switched networks; 4) the advent of the personal computer; 5) large low cost memories of both semiconductor and magnetic [10, p. 262].

The widespread use of mobile devices and wireless Internet supplemented the digital revolution at the beginning of the XXI century by giving access to the network from almost anywhere in the world at any time. However, the changes having occurred appear to have both positive and negative consequences. M. Saksida writes: “If this revolution were put on trial, the defense would claim that everybody in the whole world is benefiting from it, while the prosecution would claim that, the defense is confusing the part of society which merely has exposure to or knowledge of the digital revolution with the part of society which actually benefits from it, and that this division is applicable in varying proportion to all nations, developing and developed alike” [10, p. 266]. It’s generally accepted that the intensive wide-spread of information and telecommunication technologies has brought advantages to the progress of modern societies, providing more developed countries with the opportunity to consolidate their already strong positions in the global geopolitical realm, and less developed countries to overcome several intermediate stages in their progress. Moreover, according to I. Kearns, “the digital society revolution is good for government, good for business and good for citizens” [3, p. 54].

Despite the obvious advantages, the development of new technologies throughout the world implies a number of negative consequences. For example, the actors of mass communications gain independence from power structures; users of new electronic network communities provide an unprecedented amount of information in open access, which apparently multiplies the risks of information security of society and the state. To be more precise, there is growing concern with difficulties of confrontation ideological fanaticism and radicalism, especially extremism and terrorism. Having become quite a frequent phenomenon, the cases of online recruitment of new terrorists should be mentioned here in the first place. Unfortunately, it is a well-known practice, when terrorist

organizations recruit young people into their ranks via Internet, alluring a number of them with “attractive”, but certainly phantom benefits. However, the values provided by these groups are always ascertained as simulacra, but not “real” or “potential” values, despite those misguided users may have considered [11, p. 130]. Another drawback of the digitalization is the digital gap problem, which outlines the correlation between the status of the state, e.g. its position in the international arena, and the level of its informatization. Developed and developing countries differ significantly in the degree of implementation and operational efficiency of information and communication technologies. So the digital gap often intensifies other types of inequality of states, e.g. economic, social inequality [7, p. 70].

Therefore, there has been growing concern for rethinking the concept of security in the digital age. That means the primary aim of this article is to study the security discourse in the new context of soft/hard power dichotomy in a digitalized society. This discussion involves the following issues to be considered: 1) how this soft / hard range of power can be applied to the security problem; 2) how different information threats could be countered within the discourse of the state security; 3) how the soft security could be implemented in a digitalized society.

2. Methodology and Methods

Structured analysis, discourse analysis, conceptual approach and the comparative method are involved to outline the research methodology. Discourse analysis describes the conceptual sphere of security and soft power. Conceptual approach provides the concepts of soft security and hard security lacking the generally accepted definition to be revealed. The comparative method makes the analysis of information security and cybersecurity, information warfare and cyber warfare possible, as well as identification of the reasons for distinguishing these terms in the official discourse of different states. It should be also noted that our research is conducted within theoretical framework established by B. Buzan, J. Nye, with the acknowledgment of the results obtained from the previous studies of the authors of this paper.

3. Results and Discussion

From soft power to soft security.

One important result of this study is the correlation between soft/hard power and the concept of security has been determined. Being a product of the two concepts

intersection, soft security describes a method of protection from harm in invisible and unobtrusive ways. Being its opposite, the concept of hard security challenges threats in terms of force. The multisectoral approach to security analysis proposed by B. Buzan [1, p.19] was also used in this paper, which recognizes challenges and threats through five separate interrelated sectors (military, political, economic, social and environmental one). In terms of the theory of B. Buzan, we propose that hard security measures are likely to be applied in the military sector, while the others will use soft security measures.

However, previous studies of the soft security has not resulted in its precise definition in any official international documents. It is only assumed that there is a common understanding that the concepts of soft power and soft security should be associated with a set of certain non-military social practices [2, p. 243]. A study on characteristics of the soft security discourse in EU law revealed that it could be described in two vectors. The first vector outlines certain risks and threats that can be eliminated by soft measures, focusing on: 1) dangers associated with the environment, nuclear weapon, drugs traffic, etc.; 2) the spread of infectious diseases, global warming, and environmental crisis. The second vector describes a certain combination of tools aimed to reduce, counteract or eliminate these harmful effects. Being a “soft security issues that need to be addressed,” or a “cooperation in the field of soft security,” it refers to different social practices. These practises are: 1) establishing and maintaining the peaceful environment (activities that do not involve military operations); 2) solving issues of soft security in cooperation with international forums and organizations; 3) reconciliation process, humanitarian assistance 4) good governance, human rights, sustainable development, social equality and poverty [2, p. 240].

The dichotomy between hard and soft security sectors can also be determined by threat orientation, e.g., hard threats are aimed at making an attack at the state literally, so they require a response from the defence enforcement agencies, while soft threats (such as drugs traffic, cyber terrorism, illegal migration and others) act indirectly, bypassing geographical boundaries. They, firstly, threaten the needs of individuals, and only then lead to general instability of society and the state.

It is almost certain that counteraction to international information and cyber threats has become one of the serious problems of modern society. However, few studies have been able to draw on any structured research on the topic how to differentiate the concepts of information security and cyber security.

Information security is to be defined as data security, dealing with issues of confidentiality, integrity and accessibility of information. These days data is mostly stored in electronic form on servers, personal computers, laptops, etc., but ten years ago, when

information has not yet been transferred to the Internet, it was hold in physical archives. Nevertheless, this method of data storage still exists. Information security experts are working to ensure that information is protected, regardless in what form it is stored. Therefore, it appears to be that the concept of information security is broader than the concept of cyber security.

Cyber security is to be defined as a protection method of data stored electronically. Thus, it is important for a specialist working in the field of information security to protect organization data from unauthorized access of any kind, while it is important for a cyber security specialist to protect data from unauthorized electronic access. The most reliable way to protect information is to store information in a safe at a military facility with complete restriction of access to it. This method of protection is not the most optimal, therefore, security experts are occupied with the problem of finding the optimal balance between data security and data availability.

The findings of this study suggest that in the official discourse of different states the terminology differs. Depending on the current political course and ideology, either the concept of information security or cyber security is more often used.

According to the analysis of official documents and statements, Russian Federation adheres to a broad approach in terms of defining information security, with such definition implying both technical and ideological aspects. However, in international negotiations hold by Russia, information security is proposed to be the appropriate term. People's Republic of China maintains the similar approach. Western countries, especially the United States, use the term cybersecurity in diplomatic rhetoric, which involves taking into account exclusively information and technical problems, primarily ensuring stable operation of information networks and systems, as well as data protection [7, p. 71].

Russian Federation insists on the principle of non-interference in the information space of other countries. According to its official position, the object of security should not only be network equipment and software, but also social and humanitarian objects. Otherwise, the United States adheres to the use of the term cyber security in the official discourse, which implies the security of only computer networks [12, p. 237]. Thus, US officials prefer a private regulatory model, trying to avoid content regulation issues.

There is a similarity between the use of information war and cyber war terms. The term information war has predominantly an expanded interpretation being a form of interstate confrontation, and is used in a different perspective than in the US military and scientific circles. Western researchers tend to use the term cyber war, which is limited to the impact on computer systems. The terminological discrepancy is the reason why

there is still no universally accepted definition of information war today at the global level.

It is a widely held view that information threats should be a matter of concern of a modern state. In their extreme examples, these threats take the form of information terrorism or information wars. To protect against them requires applying both hard security measures (e.g., imposing sanctions) and soft measures, which should dominate, since the nature of modern threats in the field of information technologies is concealed.

We have identified the following ways to implement soft security:

1) using normative force, (i.e. the establishment of international institutions, norms and rules, set the necessary agenda).

An example of such normative force use is “The International Code of Conduct for Information Security” proposed by the SCO countries to the UN Secretary General on January 9, 2015 [5]. It formalizes the obligation to comply with international standards, respect for other cultural traditions, and prohibits the use of information technologies to interfere with internal affairs of other countries, whereas cooperation is encouraged bilaterally, regionally or internationally to prevent criminal activities in the sphere of cybernetic and information technologies.

2) contributing to bridging the digital gap, i.e. the situation when some states, having unlimited access to information and communication technologies, become able to manipulate public opinion.

3) educating and supporting the qualified personnel that would have a sufficient knowledge in the field of information technology; increasing the number of state-funded places and state support for young scientists and specialists.

4) exchanging experience in countering information and cyber threats in the format of international forums, symposia, conferences, schools.

5) state support for programs stimulating personal and group skills and safe conduct skills.

An example of such program can be the EU programs aimed to increase citizen “media literacy”, which involves the development of critical thinking and civic participation through the media, with culture of information security development being taken into consideration [11, p. 131].

4. Conclusions

The total computerization of public life, the ubiquity of mobile devices and the Internet is revealed to have led not only to a number of positive consequences for society development, but also to negative ones. In contrast to usual threats to society and to the state, being eliminated by hard security, these new threats aimed at society individuals' demand for soft security measures to counteract them. Predominantly due to the transnational nature of digital technologies, soft problems and challenges cannot be solved at the level of individual states — international level of opposing them is required. Therefore, the establishment of normative force (international norms and rules), the establishment of international institutions can be an effective measure to ensure soft security. Besides, an international exchange of experience in countering information threats seem to be fruitful. Educational programs aimed both at creating qualified personnel in digital technologies, as well as at improving information literacy also contribute to ensuring the safety of society and the state.

References

[1] Buzan, B. (1991). *People, States and Fear: An agenda for International Security Studies in the Post-Cold War Era* (2nd ed.). Hemel Hempstead: Harvester Wheatsheaf, p. 318.

[2] Kavaliunaite, S. (2011). Comparative Analysis of Concepts «Soft Security» and «Soft Power» in EU Legislation. *Public policy and administration*, vol. 10, issue 2, pp. 231–246.

[3] Kearns, I. (2002). Protecting the Digital Society. *The RUSI Journal*, vol. 147, issue 4, pp. 54–56, **doi.org/10.1080/03071840208446798**.

[4] Kovba, D. M. (2014). Resources and the Implementation of Soft Power. *Scientific journal "Discourse-Pi"*, vol. 1, issue 14, pp. 136–139.

[5] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. 2015. The Ministry of Foreign Affairs of the Russian Federation. Retrieved February 10, 2019 from https://www.mid.ru/documents/10180/882233/A+69+723+En.pdf/0cedaf3d-6aad-4d9f-aa70-f370bc78ce46.

[6] Moiseenko, Y. Y. (2017). Phenomenology of "Smart Power": Cratological Aspect. *Scientific Journal "Discourse-Pi"*, vol. 3-4, issue 28-29, pp. 150–154.

[7] Nezhelsky, A. A. (2018). Theoretical Foundations of the Study of Information Wars and the Information Security of the State. *Power*, vol. 6, pp. 70–74.

[8] Nye, J. (2004). Soft Power: The Means to Success in World Politics. Public Affairs, 191 pp.

[9] Nye, J. (2010). The Future of Power. Public Affairs, New York, 320 pp.

[10] Saksida, M. (1997). The Information Society in the 21st Century. *International Information & Library Review*, vol. 29, issue 3-4, pp. 261–267.

[11] Shchelina, L. A. (2016). Russia's Information Security Problem: Network Dispersion Factor. *Labor and Social Relations*, vol. 3, pp. 129–138.

[12] Zinovieva, E. S. (2016). Promising Trends in the Formation of an International Regime for Ensuring Information Security. *Bulletin of MGIMO University*, vol. 4, pp. 235–247.