The European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.05.295

SCTMG 2020

International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism»

COMPARATIVE ANALYSIS OF NATIONAL INFORMATION SECURITY POLICY IN THE CONTEXT OF GLOBALIZATION

Andrey Petrovich Koshkin (a), Andrey Vadimovich Novikov (b)*, Aleksandr Sergeevich Yablochkin (c)
*Corresponding author

(a) Plekhanov Russian University of Economics, 36, Stremyanny per. Moscow, 117997, Russia 160957@mail.ru,
(b) Plekhanov Russian University of Economics, 36, Stremyanny per. Moscow, 117997, Russia camouflage@yandex.ru,
(c) Plekhanov Russian University of Economics, 36, Stremyanny per. Moscow, 117997, Russia alexander7985@bk.ru

Abstract

Nowadays there is a certain tension between the concept of transparency of public administration and the need to protect socially significant information. The article discusses what types of information governments protect for reasons of national security, as well as what arguments they use. As a result of studying many national information security strategies, it is becoming clear that governments are seeking to limit the flow of information. Since there are various reasons for this process, but these reasons do not always correlate with the type of political regime that exists in the country. In other words, sometimes democracies and authoritarian countries limit the same types of information problems. Politics and political discussions depend on many persons and on which characters have the most powerful influence now, which most often leads to a gradual change in policy and its implementation mechanisms. Throughout the policy development process, tensions may arise between participants and stakeholders: politicians, interest groups, private sector representatives, citizens and independent experts. To understand these competing political interests, several examples of information security policies were examined. Examples are cases from all regions of the world, covering the period from 1998 to the present. In general, this article illustrates the paradox that democracies, which should be most interested in protecting information, under certain conditions will misuse information just like any other.

Keywords: Politics, information security, globalization, democracy.

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

In a globalized, web-based world with a high information density, information security is critical for nations. The combination of factors and persons, including various political and economic interests, policy development processes, types of governments and technical knowledge, together create disparate information security policies in different states. In the literature on information security, little attention is paid to the important issue of the differences in information security policies between states, especially the differences between policies in authoritarian and democratic states, and how different policy development processes contribute to these differences. Do authoritarian and democratic governments consider information security policies in the same or different ways, and whether tensions between different actors and stakeholders are considered under different types of regimes?

2. Problem Statement

There are two problems in understanding how states deal with information security policies. Firstly, there are many persons, both public and private, interested in how the information security policy works. However, these people do not work in a vacuum. They are limited by political, ideological and institutional factors. This leads to a second problem, which is that the institutional nature of government (whether democratic or authoritarian) also affects how it addresses these issues. While decision makers and private characters in both democratic and authoritarian countries interact to ensure that what they consider to be vital information is secure, these interactions may vary depending on the type of regime. Consequently, the policy development process may be reminiscent of a “tug of war” in countries where the power to develop policy is blurred. In these countries, the interaction between politicians and private actors “pulls” politics in one direction or another, depending on the political and ideological climate. In such an environment, one rarely finds that an information security policy is completely subordinate to one way of thinking. However, this is less true for cases of concentration of decision-making powers, as is the case in authoritarian governments. Even though several persons are interested in this, they are less able to influence politics, which accordingly becomes less like a “tug of war” and is more focused on the state’s own interests.

3. Research Questions

The national strategies and decisions investigated in this work are not randomly distributed events. Countries that have created an information security policy have it, because the circumstances are such that this policy has enough support, and that it can be adopted through the existing institutional process. The main sources of information collection were news and political databases, as well as banks of parliamentary documents of countries.

4. Purpose of the Study

The aim of the work was to compare national information security policies and analyze them based on three questions. First, what type of information is protected or restricted by government? The answers

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

were supposed to represent the field of political decision making. But keep in mind that some laws intersect between different categories. Secondly, what is the rationale that governments use to ensure the security or information restriction? The answer includes policy objectives, although they are not always clearly stated. Third, what are the circumstances around which policy is formulated? This is the most difficult question, because situations are not always explicitly stated in news articles or legislative archives. But where possible, this context can provide a deep understanding of the extent to which governments seek to ensure the security of information.

5. Research Methods

To understand these competing political interests, several examples of information security policies were examined. Examples represent all regions of the world, covering the period from 1998 to the present. Although some laws and examples may seem outdated, the importance of this project is to analyze the policy over time, and not just its relevance to current events. The article used the method of comparative and historical analysis.

6. Findings

National Information Policy. While some information policies are designed to free up the flow of information – for example, consumer protection laws or freedom of information laws – others are designed to restrict, ensure security, or control the flow of information. The types of controlled information are divided into the following categories: external threats (national security issues), internal threats (anti-government information), infrastructure information, personal or individual information, commercial information and media information.

External threats (national security issues). National security policy issues have always been the objectives of a policy of restricting information flows. Harold Innis argues that control over information (what he called "monopolies of knowledge") was indispensable in creating empires (Innis, 2007). Protecting national priorities from external threats is the most obvious and often the most acceptable reason for restricting the flow of information within the country. However, external threats, such as war and some forms of international terrorism, are different from internal threats, such as anti-government protests and armed acts of disobedience.

For example, the Patriotic Act gave the US government access to some information that it did not have before. While the U.S. military uses the Internet and other media to communicate with the public and create a positive image and intelligence information (Sandoval, 2006). It also limits the use of certain types of media by soldiers who may want to blog or comment on the war, justified by the argument that such communication could potentially expand the capabilities of enemies or create disunity.

In addition to enabling governments to expand the scope of the information they monitor and regulate; external threats can reveal new vulnerabilities. The war between countries also provides a powerful incentive to develop information security policies that can protect against foreign invasion. Tensions between Russia and Georgia have demonstrated the need to protect computer networks (both civilian and military) in the event of an armed conflict.

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Such lessons are not unique to interactions between government entities. After September 11, 2001, increased attention was paid to the role of non-state actors. The external threat of terrorism plays a significant role in shaping the types of information security policies that have emerged over the past decades. Al-Qaeda attacks have prompted other countries to develop their own information control policies.

Internal threats (anti-government and anti-stable information). Limiting information is relatively common when considering threats to the country's internal stability. Laws of incitement to rebellion of 1798 in the United States criminalized treason. More recently, changes in Russian media legislation in the 2000s, as well as in 2016, in connection with the adoption of the “Spring Package” and the 2019 “criticism of power” law, have created a wide discussion that people opposed to the current government can become more susceptible to prosecution.

In addition, Singapore’s experience in the field of electronic interaction between citizens and government is widely recognized. The government said it wants to be a “paperless” society. However, in 2003, parliament passed a law on the misuse of computers, which interpreters called the response to the Internet as "weapons of mass destruction". Similar new laws can be used as a “tool of oppression” by the government (Singapore Cyberterrorism, 2003).

For China, the fight against threatening information flows is an implicit policy. For both companies and individuals, the understanding of Chinese online political censorship is complicated by the secrecy with which it is shrouded. Officials usually deny that it exists at all. But senior executives left no doubt that control of the Internet is a political priority (Zhang & Zhu, 2019).

Infrastructure Information. The development of information infrastructure around the world has traditionally been a combination of public and private initiatives, with some countries leaning towards one or another option. Those who are inclined to implement government-funded programs can do this with the intention of controlling information passing through these networks.

For example, in 2006, Kenya, Uganda and Tanzania began the process of adopting harmonized cybersecurity laws in order to create opportunities for e-government and e-commerce programs. Relevant governments have recognized the cross-border flows of information that are already taking place and would like to ensure that they will have some control (and possibly revenue) from these existing links (Schia, 2018). This type of control is not necessarily negative. The authorities just want to know what is happening.

Another example of infrastructure control is the discussion about the responsibility of private Internet providers for the flow of information transferring through their networks. Internet service providers, organizations or companies that provide channels through which most of the Internet information passes can be in public or private management. The problem is that, although there is a technology for monitoring information that passes through their networks, many Internet providers, especially private ones, do not. Governments engage in political debates with them over infrastructure control.

For example, according to the Indian Information Technology Act of 2000, Internet service providers are not liable for criminal activity on their networks (Chaturvedi et al., 2014). But, full autonomy, as a rule, is not possible. Subsequently, the law states that the police have the right to enter any

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

institution and search in its electronic records, if the situation requires it. The United States is addressing the same issue by updating the Foreign Surveillance Act of 1978. Although US lawmakers hesitate to protect Internet providers in the name of civil liberties.

Personal information. Confidentiality of personal information has long been a subject of debate in national parliaments, especially in more democratic societies. Some countries have passed the laws, while others have not. Since confidentiality is understood from different perspectives in different cultures, it can be difficult to classify laws on this topic. The difference in the culture of privacy is easily apparent in discussions related to information between the US and the European Union (Rogerson & Strauss, 2002). In order to formulate and implement a privacy policy or a specific program, governments must somehow control the information. Usually restricting information that may be collected or stored by governments and private enterprises. For example, the European Union Convention on Cybercrime recognizes the right to privacy: taking into account the right to protection of personal data, as enshrined, for example, in the 1981 Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Christou, 2018). This issue is not always resolved unambiguously and in other countries, information about individuals does not receive the same level of protection. For example, Kazakhstan has passed the Law on the Protection of State Secrets of the Republic of Kazakhstan, which removes the emphasis from personal secrets in favor of more official information.

Commercial information. Countries may also have policies related to commercial information, i.e. financial transactions, electronic commerce, taxation on the Internet, etc. In some cases, such policies may be deregulatory and may be aimed at stimulating growth in accordance with the principles of the free market. In other cases, regulation may be stronger to provide incentives or cash infusions into the region. The East African Community has launched a program called the Electronic Legislation Policy Initiative (Bin Muhaya, 2010). This program recognizes both the nature of information for border crossing and the desire of governments to participate in the development of the project and, thus, have some control over the information that passes through the newly created networks.

Media coverage. An information policy can also be an initiative to restrict media freedom. For example, the Russian government tried to control coverage of the conflict with the separatist province of Chechnya based on existing media laws (Mukhina, 2005). Some countries have media laws that specify the types of information that should or should not be published or broadcast. Few countries have laws on freedom of speech and press like those contained in the US Constitution.

Computer viruses. Finally, there is a category of laws that target hackers and those who maliciously send viruses through information networks. For example, after large-scale hacker attacks from other states in 2003, Japan passed a law criminalizing this activity, even if it is only preparatory in nature. In addition, he created a monitoring center to track offenders (Bin Muhaya, 2010).

Justification of the need to ensure the safety of information. The issue is to determine the rationale for the declared or proposed adoption of the law or the implementation of the policy. They fall into three categories: a) protection of national interests, b) protection of citizens and c) facilitation of cross-border exchange of information.

Protection of national interests is the largest category and has several components. There is always an interest in using military and defense interests as a justification for restricting the flow of

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

information. Countries want to protect intelligence during conflicts so that the "enemy" does not discover secret information and protect, as far as possible, those who conduct ground battles. In 2006, Chinese government officials published a report entitled “National Defense of China,” which states that the PRC is pursuing a three-stage development strategy to modernize its national defense and armed forces, which includes the creation of “information armed forces capable of winning information wars” by 2050 year (Zhang & Zhu, 2019).

Also, in the arena of security issues is maintaining control within borders. Again, the Chinese government has a reputation for following censorship of communication and information via the Internet, although this is not the only country that does this (Kalathil & Boas, 2003).

While the Great Chinese Firewall protects the government from outside information attacks, another system (also known as the Golden Shield) is used internally. The vaguely worded laws against any opinion that is considered seditious, superstitious, or simply “harmful to public order” give officials wide powers to punish those who publish or post confidential content. But the main burden of routine censorship rests with Internet and content providers (Zhang & Zhu, 2019).

And, since the latter groups can be targeted by government repression as easily as individuals, they are often voluntary participants. Without completely suppressing the opposition, China succeeded in limiting the influence of certain social groups through this censorship and monitoring, which led to public agreement with the policies of the ruling party.

The protection of citizens is the second rationale. This could be a defense against cyber threats, as in the Japanese example above. But it can manifest itself in the form of regulation of annoying factors, such as spam (unsolicited commercial email), as is the case with the CanSpam Act of 2003 in the United States. But the language of defense is also used more widely. In South Africa, Parliament passed a bill on electronic communications and transactions, which was designed to protect citizens from cyber terrorism. Given the broad wording of the bill, criticism was inevitable:

> *The new law has been sharply criticized, especially by the Democratic Alliance party, which voted against it, as well as by organizations for the freedom of the Internet and private firms. The law allows the Minister of Communications to appoint inspectors to monitor the telecommunication networks and their content that they are authorized to capture*. (Kalathil & Boas, 2003, p. 73)

In one case, the policy clearly reflected the damage done to citizens. In April and May 2007, the Estonian government was subjected to a series of DoS attacks on the country's Internet infrastructure. This event disabled banks and government agencies (Štitilis et al., 2017). In the fall of that year, the Estonian parliament responded by voting to amend the country's criminal code. “A computer attack becomes an act of terrorism if it is carried out with the same goals as a regular terrorist attack. According to the current legislation, crimes of terrorism are crimes whose purpose is to seriously violate or destroy the country's political, constitutional, economic or social order” (Štitilis et al., 2017, p. 1152). The resulting reaction of Estonians to the bill, especially technical experts, provided orientation towards protecting citizens in subsequent political decisions.

https://doi.org/10.15405/epsbs.2020.10.05.295
Corresponding Author: Andrey Vadimovich Novikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In early 2012, the negative reaction of American citizens to the Law on Combating Piracy on the Internet (SOPA) and the Law on the Protection of Intellectual Property (PIPA) led to several politicians changing their minds about how they perceive the legislation. At least some of the merits in this change were attributed to a citizen protest, which drew attention to what initially seemed to be a slight change in legislation (Schmitz, 2013). This is a clear example of the role that public opinion has, and not just political figures.

The third category of explanations for information security policies is that it ***facilitates cross-border information exchange***. As can be seen from the examples of Kenya and the East African community, there is a desire to take advantage of existing networks and connections in the interests of the state. One reason is the exchange of information on criminal activity. The East African community "has begun to harmonize its laws to prosecute cybercriminals operating across national borders" (Schia, 2018, p. 822). It is not always easy to get information about hackers or other cybercriminals who do not live within national borders. For example, the EU Convention on Crime focuses on tracing those who distribute child pornography, which is the only offense related to the content of the convention. Chapter III of the convention is fully devoted to international cooperation and information exchange. At the same time, the Convention allows countries to take individual decisions on bilateral agreements with each other.

7. Conclusion

This article reveals the paradox: democracies that should be most interested in protecting information under certain conditions will misuse information just like any other country. Although this analysis has illustrated some of these conditions, these findings certainly do not represent the last word. Rather, they provide concepts that can highlight some of the nuances in developing an information security policy. Throughout the policy development process, tensions can arise between participants and stakeholders: politicians, interest groups, private sector representatives, citizens and "technical elites", those practitioners who understand how the technology works. Some of these persons, especially policy makers, may have difficulty understanding the nuances of information security policies or even information policies in a broader sense. on a wider level, information security policies are also an example of tension between decisions made in response to very specific situations, but the consequences of which may be unforeseen. These two frictions inspire a potentially rich research program on the dynamics of information technology and the resulting security and / or transparency requirements.

References

Bin Muhaya, F. T. (2010). Dominant factors in national information security policies. *J. of Comput. Sci., 6*(7), 808–812.

Chaturvedi, M., Singh, A.N., Gupta, M.P., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transform. Governm.: People, Process and Policy, 8*(3), 374–397.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *Europ. Politics and Society, 19*(3), 355–375.

Innis, H. (2007). *Empire and communications.* Lanham, MD: Rowman and Littlefield

Kalathil, S., & Boas, T.C. (2003). *Open networks, closed regimes: The impact of the Internet on authoritarian rule.* Carnegie Endowment for Int. Peace.

Mukhina, I. (2005). Islamic Terrorism and the Question of National Liberation, or Problems of Contemporary Chechen Terrorism. *Studies in Conflict & Terrorism, 28*(6), 515–532.

Rogerson, K., & Strauss, J. (2002). Policies for online privacy in the United States and the European Union. *Telemat. and Inform., 19*, 175–209.

Sandoval, G. (2006). *Now playing on the Net: War propaganda.* CNET News.com. https://www.cnet.com/news/now-playing-on-the-net-war-propaganda/

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly, 39*(5), 821–837.

Schmitz, S. (2013). The US SOPA and PIPA - a European Perspective. *Int. Rev. of Law, Comput. & Technol., 27*, 213–229.

Singapore Cyberterrorism (2003). Singapore cyberterrorism law raises fears of abuse. *The Hindustan Times*. http://www.crime-research.org/news/2003/11/Mess2401.html

Štitilis, D., Pakutinskas, P. Malinauskaitė, I., & Secur, J. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security J., 30*(4), 1151–1168.

Zhang, Y., & Zhu, X. (2019). Multiple mechanisms of policy diffusion in China. *Public Managem. Rev., 21*(4), 495–514.