УДК 342

МЕНЯЮЩАЯСЯ РОЛЬ ГОСУДАРСТВА В КИБЕРПРОСТРАНСТВЕ

Л. Галбаатар

Институт правовых исследований, информации и обучения
при Генеральном судебном совете Республики Монголия, Республика Монголия

galbaatar@judcouncil.mn

Поступила в редакцию 04.09.2018

Сегодня многие страны принимают и применяют стратегии кибербезопасности, это рассматривается как необходимый элемент для жизнедеятельности, работы и развития в киберпространстве. Несмотря на то что принятые стратегии ориентированы на реализацию в киберпространстве, можно говорить о том, что они не соответствуют роли государства в киберпространстве. Вне всякого сомнения, меняющаяся роль государства в киберпространстве потребует нахождения нового баланса между кибербезопасностью и «свободой» в киберпространстве. В статье рассматриваются текущая и меняющаяся роль государств в киберпространстве на основе анализа правовых и политических документов, отражающих содержание национальной политики кибербезопасности стран – членов НАТО и стран, не являющихся членами НАТО, а также доклады и рекомендации международных организаций, таких как Международный союз электросвязи и ЮНЕСКО.

Ключевые слова: киберпространство, баланс интересов, кибербезопасность, свобода, наблюдение, политика.

1. Introduction

Today, more than 70 countries have been adopting and implementing cybersecurity strategy documents. Such cybersecurity documents are now considered to be indispensable for working and developing the cyberspace. Even though cybersecurity strategy documents are being implemented, they don't match the role of states in cyberspace. For example, on June 5 2013, Edward J. Snowden disclosed some documents and came to the conclusion that online surveillance undertaken by the National Security Agency (NSA) violated international law on human rights. He also released information about NSA activities with the intelligence agencies of other countries [1]. In addition, by 2020, the 4th Industrial Revolution will have brought us new advanced technologies – robotics and autonomous transport, artificial intelligence, machine learning and the Internet of things (IoT) [2]. These developments will change the role of states in cyberspace. What is certain is that the changing role of states in cyberspace will need to find a balance between cybersecurity and liberty in cyberspace. Therefore, we need to examine the current and changing role of states in cyberspace which is referred to as national cybersecurity policy. We will look at legal documents of NATO and non-NATO member countries including Europe, Asia & Oceania, Africa, Americas, reports and recommendations of international or regional organizations such as International Telecommunication Union and UNESCO.

2. Sustainable development goals and cybersecurity

A. Countries' global ranking on e-governance and cybersecurity

In 2015, UN General Assembly adopted Sustainable Development Agenda-2030 with its 17 goals, and all of these goals are addressed to peoples and countries of the globe for reducing poverty, protecting the nature and encouraging sustainable development in all sectors of society [3]. According to Tomasz Janowski's presentation, 87 percent of the goals and all 169 provisions were related to and required the capability of e-government. Moreover, only less than 31 percent of UN member states have reached a development stage which was enhanced by e-government, but 55 percent have not reached it yet. It follows from this presentation that e-governance should play the main role in the implementation of Sustainable Development Agenda, but more than 69 percent of UN member states at the moment are affected by the differences between willingness (Sustainable Development Agenda) and capability (e-governance). To fully understand and efficiently resolve these differences, research work should be enhanced and conducted in relation to the countries which have made a commitment to change their policy environment [4]. With the purpose of clarifying the above research results, let us try to synthesize current ranks of the following 10 countries which have specific policies and regulations for cybersecurity [5].

Table I

Some countries' global rank on e-governance and cybersecurity

Region	Country	Global Rank /E–Government Development Index 2017/18/ [6]	Global Rank /Global Cybersecurity Index 2017/ [7]
Europe	UK	4	12
	Estonia	16	5
	Russia	32	10
Asia & Oceania	Australia	2	7
	China	65	32
	India	96	23
	R. Korea	3	13
Africa	S. Africa	68	58
Americas & the Caribbean	USA	11	2
	Panama	85	62

Table II

Some countries' security and liberty in cyberspace

Tiers/Country		Estonia	Russia	India
Cybersecurity index tiers-2017 [7]		Leading	Leading	Maturing
Liberty in cyberspace-2017 [8, 9]	Obstacles to access	0/25	11/25	12/25
	Limits on contents	3/35	23/35	9/35
	Violations of user rights	3/40	32/40	20/40
	Overall score	6/100 (free)	66/100 (not free)	41/100 (partly free)
Balance between security and liberty in cyberspace		Balanced	Not balanced	Not balanced

Table I shows that E-Government Development Index is irrelative of Cybersecurity Index on this comparative rating information of 10 countries, and one could conclude easily that ensuring cybersecurity has no direct correlation with the strengthening of e-governance. In other words, it seems that e-governance could not be a guarantee of cybersecurity, and the strengthening of cybersecurity could not help in all situations of e-governance. Therefore, strong capability of both e-governance and cybersecurity of such countries is currently an imperative need.

3. Balancing between cybersecurity and human rights in cyberspace

A. Security and liberty in cyberspace

This section will discuss how a country's duties with regard to cybersecurity could be changed and what type of changes will be needed in the future. For the purpose of clarification, it might be useful to analyze, as examples, the rating data of three countries, which have specific policies and regulations on cybersecurity.

The data of Table II is sourced from a report of the recognized international organization and a comparison is made of selected indicators regarding the cybersecurity and cyber liberty index in the three countries in 2016. This comparison proves that ensuring cybersecurity could be balanced with human rights in cyberspace, but some countries impose restrictions and violate human rights under the pretext of ensuring cybersecurity. Therefore, a country's obligations for cybersecurity need to be changed to avoid improper prohibitions or restriction of human rights and to provide a balance in cyber space.

B. Principles for governing the cyberspace

The previous part has mentioned the types of duties that should be addressed to the country in the cyberspace and how these duties have changed during the recent years. Moreover, it would be important to define or state the principles/rules which apply during the implementation of duties in cyberspace by countries. The UNESCO's study encompasses 52 declarations, guidelines, and frameworks from various international actors, as well as the documents dealing with internet governance principles. Here, these 52 documents can be summarized as follows according to their geographic origins:

- 28 documents stem from global institutions (or from several jointly acting regional institutions),
- 11 documents are based on regional initiatives,
- 13 documents have been developed by different bodies of civil society [10].

The following 10 documents out of 52 were connected to countries' duties in the cyberspace:

1. International Mechanisms for Promoting Freedom of Expression (2005);
2. Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace (2003);
3. Madrid Privacy Declaration (2009);
4. Code of Good Practice on Information, Participation and Transparency in Internet Governance (2010);
5. Joint Declaration on Freedom of Expression and the Internet (2011);
6. Declaration of Internet Freedom (2012);

Table III

Principles for governing the cyberspace

Principles	Documents mentioning the aspect (out of 52)	Documents addressing the aspect in more detail (out of 52)
Access	50	22
Openness	34	17
Freedom of Expression	41	21
Privacy	36	14
Multi-stakeholder Part.	39	19
Ethics	19	11
Gender Equality	18	8
Sustainable Development	24	6
Cultural Diversity	20	8
Science	6	6
Education	24	13
Accountability	28	2

7. Internet Governance – Council of Europe Strategy 2012–2015 (2012);

8. Promotion, Protection and Enjoyment of Human Rights on the Internet (2012);

9. Right to Privacy in the Digital Age (2013);

10. Recommendation on a Guide to Human Rights for Internet Users (2014).

Table III shows the 12 most popular principles of international cyber governance declarations, guidelines and frameworks (52 documents). Based on these experiences, each country should include provisions about the principles of access, freedom of expression, multi-stakeholder participation, privacy, and openness in its own regulations and activities in relation to cyberspace. This would ensure sustainable conditions for complete implementation of its functions in current cyberspace.

Conclusions

Most countries have stated their own commitments and responsibilities with regard to cyberspace in the national policy and regulations, but cyberspace is changing rapidly in multiple ways. Typically, these changes are related to the balance between ensuring cybersecurity and protection of human rights. Based on the compared results on E-Governance and Cybersecurity Indexes of the selected 10 countries, states should implement their duties of a balanced and sustainable development of both aspects at the same time. Furthermore, the duties of the states with regard to cybersecurity are changing in view of the need to implement the measures aimed at avoiding illegal restrictions and violation of human rights and ensuring the balanced state activities in cyberspace. In addition, states need to pay more attention to these changing duties and must adopt and implement internationally recognized principles of cyberspace regulation.

Список литературы

1. David P. Fidler. 2015. The Snowden Reader. Indiana University Press. ISBN 978-0-253-01738-3.

2. Alex Gray. The 10 skills you need to thrive in the Fourth Industrial Revolution. World Economic Forum. 19 Jan 2016. https://www.weforum.org/agenda/2016/01/the-10-skills-you-need-to-thrive-in-the-fourth-industrial-revolution/

3. Sustainable Development Goals. United Nations. http://www.un.org/sustainabledevelopment/sustainable-development-goals/

4. Tomasz Janowski. 2017. ICEGOV 2017 Keynote Lecture 4 by. March 9, 2017. https://www.youtube.com/watch?v=UeMydYZ4EOc&list=PLvQecBSGPKvk0-ZgIYAmL7itQhu7XaXNB&index=5

5. Cyber Security Strategy Documents. 2017. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/cyber-security-strategy-documents. html

6. United Nations e-Government Survey 2018. United Nations. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

7. Global Cybersecurity Index. International Telecommunication Union (ITU), 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

8. Freedom on the Net 2016. Freedom house, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2016

9. Freedom on the Net 2017. Freedom house, 2018. https://freedomhouse.org/report/freedom-net/freedom-net-2017

10. UNESCO Principles for Governing the Internet /A comparative Analysis. UNESCO Series on Internet Freedom, 2015.

THE CHANGING ROLE OF THE STATE IN CYBERSPACE

L. Galbaatar

Today, many countries adopt and apply cybersecurity strategies; this is seen as a necessary element for living, working and developing in cyberspace. Despite the fact that the adopted strategies are aimed at the implementation in cyberspace, we can say that they do not correspond to the role of the state in cyberspace. The changing role of the state in cyberspace will require a new balance between cybersecurity and "freedom" to be found in cyberspace. This article discusses the current and changing role of states in cyberspace, based on an analysis of legal and policy documents reflecting the content of the national cybersecurity policy of NATO member countries and non-NATO countries, as well as reports and recommendations of international organizations such as the International Telecommunication Union and UNESCO.

Keywords: cyberspace, balance of interests, cybersecurity, freedom, surveillance, policy.

References

1. David P. Fidler. 2015. The Snowden Reader. Indiana University Press. ISBN 978-0-253-01738-3.

2. Alex Gray. The 10 skills you need to thrive in the Fourth Industrial Revolution. World Economic Forum. 19 Jan 2016. https://www.weforum.org/agenda/2016/01/the-10-skills-you-need-to-thrive-in-the-fourth-industrial-revolution/

3. Sustainable Development Goals. United Nations. http://www.un.org/sustainabledevelopment/sustainable-development-goals/

4. Tomasz Janowski. 2017. ICEGOV 2017 Keynote Lecture 4 by. March 9, 2017. https://www.youtube.com/watch?v=UeMydYZ4EOc&list=PLvQecBSGPKvk0-ZgIYAmL7itQhu7XaXNB&index=5

5. Cyber Security Strategy Documents. 2017. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/cyber-security-strategy-documents. html

6. United Nations e-Government Survey 2018. United Nations. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

7. Global Cybersecurity Index. International Telecommunication Union (ITU), 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

8. Freedom on the Net 2016. Freedom house, 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2016

9. Freedom on the Net 2017. Freedom house, 2018. https://freedomhouse.org/report/freedom-net/freedom-net-2017

10. UNESCO Principles for Governing the Internet /A comparative Analysis. UNESCO Series on Internet Freedom, 2015.