THE POLITICAL CULTURE IN THE CYBERSPACE. PROFILING THE CYBER SECURITY

Cosmina Moghior
National University of Political Studies and Public Administration
Bucharest, Romania
cosmina_moghior@yahoo.com

Abstract:
Concepts like *cyberspace*, *cyber security, cyber war* and other words from the same family are increasingly brought to attention either in media, public discourses or in everyday life. Probably the main reason is the high interconnection of what we call *cyberspace* with the *real space*, our everyday life. We are living a double life, one in the virtual space and the other in the physical one. But what would be the role of the state in this constellation? Are the characteristics of a state influencing the level of cybersecurity? Our aim in this article is to identify some of the factors that have an impact in the cyberspace. We will proceed by presenting the approaches on cyberspace in the selected countries. After that, we will continue with selecting the data for the chosen variables and we will effectuate the preliminary analyses of the selected data. Afterwards, we will move to the individual interpretation of the results, correlations and graphics.

Keywords
Cyberspace, cybersecurity, political culture, personal freedom, democracy, ICT

1.INTRODUCTION

The cyber domain is evolving, and the international society is increasingly dependent on the cyber sector. Along with the opportunities, we are also

witnessing the emergence of new security challenges in the cyberspace. The cyber-attacks can affect the targeted entities in a wide range of ways, from information leaks to physical damage. The importance of the cyberspace had been recognized by a great number of states by extending the security sector to the cyberspace. The states had become so dependent on the cyberspace that in some cases, the security cannot be viewed separately from the cyber security.

The concept *cyber security* tends to appear more and more often in the political discourses, media, academia and even in daily conversations. But what is the meaning of this concept? And what are the factors that are contributing to the cyber security? We are looking to answer to those questions in the present research through a comparative research, using statistics. We selected People's Republic of China, Netherlands and Russian Federation as subjects for the present research. In the first section of our research, we will focus on depicting the main characteristics of the cyber security strategies of the states that we chose as a reference for our study. In the second section we will develop the methodology of our research, where we will discuss in-depth on the variables selected for our study, the hypothesis, the processed, corroborated and analysed data, the primary statistical analyses and the graphics of correlation between the variables. In the third section, we will discuss the primary interpretation of the results for each country. Finally, in the last section we will compare the results and we will verify if there is a general factor that influences the cyber security of the states that we had selected. In the conclusion will confront the hypothesis set in the beginning of our study with the actual results.

2.CYBER SECURITY STRATEGIES

When we talk about cyberspace, we often reflect on issues like cyber security, cyber-terrorism and cyber-attacks. Amos Guiora made a clear distinction between *cyber-attacks* and c*yber security*. The first refers to the *action* of harming the state's critical infrastructure, while the former illustrates the states' contractual *duty* to protect the individuals from any attacks. If we are posing the

question '*Cyber security for whom?*', Guiora's answer would be: civilians, public infrastructure and overseas assets, public and private (Guinora 2017, 17).

As the interest and the impact of cyberspace grew, many states recognized it as an extension of their national security the domain and many states formulated a cyber-security strategy. Depending on their culture, political regime, the perception of threats in the cyberspace, the strategies contain the appropriate objectives, concepts and required resources for achieving the objectives (Yarger 2008, 43-49).

China declared the cyberspace as a subject of sovereignty. China refers to sovereignty, as stated in the UN Charter: the states have equal sovereignty and the right to choose their own path of development without foreign intervention in the internal affairs. Next to sovereignty, for China the other main principles of cooperation in the cyberspace are: peace, shared governance and shared benefits. China stands for the regulation of the cyberspace, in a form agreed by all the states, to protect the individuals' rights and interests and to promote the Digital Economy and the cultural exchange (Shaohui 2017). Although China condemns all the cybercrimes, the means of responding those acts are unclear, since China stated that it opposes "all forms of hacking", but aims to tackle them through legal instruments. China believes that the arms race in the cyberspace is one of the main threats for the international security and stability, contradicting the principle of peaceful use of cyberspace. To defend itself from these threats, China introduced a backup force for the cyberspace (China National Cyberspace Security Strategy 2016).

The Dutch cyber security strategies are concentrated on evaluating and reducing the vulnerabilities and tend to have a military connotation. The Defence organization has the duty to eliminate the cyber threats. Netherlands perceive the development of the cyberspace as an opportunity to enhance its national security, by incorporating the cyber instruments in the military and intelligence capabilities. As the cyberspace has a very dynamic character, the Defence organization needs to be continuously informed. In this regard, the Defence Cyber Expertise Center was created for knowledge development, retention and dissemination and also a close cooperation with research institutions and businesses, as well as organizing trainings and simulations for the personnel.

The internal cyber security strategy was designed in a three-party model, through the cooperation between the public, the government and the private sector (businesses). At the international level, NATO and EU are the main cyber security guarantors and partners for Netherlands (The Defence Cyberstrategy 2012). The second cyber security strategy is focused on a procedural approach, by clarifying the roles, the relations between the actors involved in the cyberspace (the Government, the citizens and the businesses) and the methods used for assuring the cyber security(National Cyber Security Strategy 2: From awareness to capability 2013).

For the Russian Federation, the concept of cyberspace is too narrow to cover all the aspects of cyber security. The cyberspace is only a fraction of the *information space* puzzle, which deals with the technological communication: the internet and other telecommunication networks. Also, because the cyber activity has a trans-national extension, Russia believes that the formulation of the cyberspace regulation is almost impossible. In the Cyber Security Strategy, Russia established a set of priorities, principles and measures with the purpose of protecting the individuals, the organizations and the state. The first priority in the Russian cyber security is to create the necessary mechanisms to protect from the cybercrimes. In this regard, one of the private parties' duties is to support the state in assuring the cyber security. Other priorities are the creation of the appropriate mechanisms required to protect the critical information infrastructure and the government information resources, the development of a public-private partnership, to increase the digital literacy of citizens. Russia believes that it is important to develop the international cooperation to formulate a global system of cyber security (Концепция Стратегии Кибербезопасности Российской Федерации [The Strategic Concept of Cyber Security of Russian Federation 2014).

3.METHODOLOGY

Cyberspace is a multi-face domain, with unclear borders, with minimal rules. Even so, it bears a great importance for our everyday life, sometimes with

repercussions in the physical world, not only in the virtual one. The quest we set for in this research is a challenging one, but it might help us understand better the certain aspects of the cyberspace. In this section we will unpack our research questions, by selecting three case studies, the dependent and independent variables and set the research hypothesis. Afterwards we will select the data for each variable, which will then be processed through statistical calculation. The results will be the subject of a preliminary analysis of the cybersecurity performance in each state.

3.1.The theoretical framework of the research

This paper aims to identify the factors that are influencing the cyber security in People's Republic of China, Netherlands and Russian Federation. We had chosen the Personal Freedom Index, the Democracy Index and the ICT Development Index (IDI) as our independent variables, respectively the possible factors that might influence the cyber security. It is important to mention that our selection of independent variables (factors which might influence the dependent variable) is not exhaustive. The explanation is not that we do not intend to realize a global study of cyberspace, but it is that it would be impossible, since cyberspace is such a dynamic domain.

The selected states have different national and foreign policies, levels of technology development and organizations responsible for the cyber security. They all focus on different matters and perceive the cyberspace in a different manner. In order to identify the factor of cyber security, we proposed to test in our research the following hypotheses:

A. The relation between personal freedom and the risk of malware infection:

H_0: There is no relation between personal freedom and the risk of malware infection.

H_1: The highest the personal freedom is, the highest is the risk of malware infection.

H_2: The highest the personal freedom is, the lowest it the risk of malware infection.

B. The relation between the democracy index and the risk of malware infection:

H_0: There is no relation between the democracy index and the risk of malware infection.

H_1: The highest the democracy index is, the highest is the risk of malware infection.

H_2: The highest the democracy index is, the lowest it the risk of malware infection.

C. The relation between the ICT development index and the risk of malware infection:

H_0: There is no relation between the ICT development index and the risk of malware infection.

H_1: The highest the ICT development index is, the highest is the risk of malware infection.

H_2: The highest the ICT development index is, the lowest it the risk of malware infection.

We translated the cyber security in the concept of *risk of malware infection*. *Malware* is a software that has a malicious intent and/or effect. The malware family includes threats like Trojan horses, viruses, worms, adware, backdoor, spyware and others (Aycock 2006, 2). In our research we focused only on the web-based attacks (online threats). The figures used to reflect the risk of online threats resulted from the frequency of encountered detection verdicts on users' machines in each country, by the Kaspersky Lab's web antivirus. The value illustrates the percentage of users from a certain country who experienced a malware infection (Garnaeva et.all 2015). The risk of malware infection will be our dependent variable.

Personal Freedom Index measures the degree in which individuals enjoy the civil liberties (freedom of speech, religion, and association and assembly). Personal Freedom Index has a double dimension: one reflects the legal protection and security (rule of law and security and safety), while the other is concentrated around the specific personal freedoms (movement, religion, association,

assembly and civil society, expression and relationships). The freedom of expression is one of the universal human rights. It has many components, but the relevant one for our research is the state 'control over Internet Access'. The use of internet has a tremendous importance as it is one of the main instruments to inform, express and interact with the other individuals (Vásquez, Porčnik 2017, 9-14).

The *Democracy Index* illustrates the level of democracy worldwide. Over a half of the countries declared that their political regime is democracy. But in the light of the certain events and evolutions in the last years, we can observe a concerning development of the level of democracy worldwide. Terence Ball and Richard Dagger are defining democracy (liberal) as a society type of organization and ruling, where the power is located in the hands of the majority of the people only if the majority does not intend to deprive the individuals of their fundamental civil rights. Furthermore, democracy (social) provides an equal power on governance to all the individuals ("a man, a vote" principle) (Ball, Dagger 2000, 53). But even if this definition covers the idea of democracy that we accept today, it still has a lapidary character. A true democracy has to protect the basic freedoms and liberties of its citizens, has an efficient government functioning, independent media and judiciary system and isolated anomalies. Given the events which took place lately and the evolution of the foreign policy and the political discourse that can be identified in some states, the number of full democracies is decreasing (Democracy Index 2016 Revenge of the 'deplorables'" 2017, 52).

The *ICT Development Index (IDI)* is combining 11 indicators for monitoring the level, the progress, the differences and the development potential of the ICTs in different countries. There are three factors of development of the ICT: access, use and the skills. All of these variables combined create an outcome, or an impact, which is the level of ICT development level in that specific case. The values resulted from combining those indicators reflect the stage of development of the information society ("Measuring the Information Society Report" 2014, 36-37).

3.2.The processed, corroborated and analysed data for the research

We have selected secondary data, gathered through desk-based research from various sources. The Personal Freedom Index was collected from the *Human Freedom Index 2017* (Vásquez, Porčnik 2017, 212-301) a report issued by CATO Institute. The *Democracy Index (2017, 25-27)* was collected form the report issued by The Economist. The *ICT development Index* was collected from different reports issued in 2012 (Measuring the Information Society 2012, 21), 2014 (Measuring the Information Society 2014, 42) and 2016 (Measuring the Information Society 2016, 13) by the International Telecommunication Union. Finally, the *Risk of Malware Infection* was collected from the annual statistics issued by Kaspersky Lab in the beginning of 2012 (Namestnikov 2012a), the end of 2012 (Namestnikov 2012b), 2013 (Funk, Garnaeva 2013), 2014 (Garnaeva et.all 2014) and 2015 (Garnaeva et. al., 2015).
Hereinafter is the preliminary data selected for each country:

Year	Personal Freedom	Democracy index	ICT development index	The risk of malware infection
2011	5.25	3.14	3.88	41.4
2012	5.12	3	4.39	38.4
2013	5.12	3	4.64	32.2
2014	4.81	3	4.8	30.1
2015	5.62	3.14	5.19	33.12

Table 1: Preliminary data from People's Republic of China

Year	Personal Freedom	Democracy index	ICT development index	The risk of malware infection
2011	9.37	8.99	8.34	37.1
2012	9.34	8.99	8.95	23.9
2013	9.36	8.84	8.93	27.3
2014	9.45	8.92	8.36	26.4
2015	9.37	8.92	8.46	18.7

Table 2: Preliminary data from Netherlands

Year	Personal Freedom	Democracy index	ICT development index	The risk of malware infection
2011	6.12	3.92	6	55.9
2012	6.06	3.74	6.48	58.6
2013	6.06	3.59	6.7	54.5
2014	6.13	3.39	6.79	53.81
2015	5.63	3.31	6.95	48.9

Table 2: Preliminary data from Russian Federation

At the methodological level we opted for a quantitative data analyses. The present research aims to do a radiography of the three selected states, People's Republic of China, Netherlands and Russian Federation based on the statistical distribution of the variables indicators. The model we are proposing will indicate the relation between the dependent variable the Risk of Malware Infection and the independent variables Personal Freedom, Democracy Index and ICT Development Index. The quantitative results on each country are the following:

Variables	X average	M_e	M_0	Q_1	Q_2	Q_3	A	A_{iq}	σ2	σ	CV
Personal Freedom	5.18	5.12	5.12	4.96	5.12	5.43	-0.44	0.47	0.08	0.26	5.12
Democracy index	3.05	3	3	3	3	3.14	0.14	0.14	0.005	0.06	2.24
ICT development index	4.58	4.64	0	4.13	4.64	4.99	1.3	0.8	0.23	0.43	9.51
The risk of malware infection	35.04	33.12	0	31.15	33.12	39.9	11.3	8.75	21.97	4.19	11.96

Table 3: Descriptive statistics: China

Variables	X average	M_e	M_0	Q_1	Q_2	Q_3	A	A_{iq}	σ2	σ	CV
Personal Freedom	9.37	9.37	0	9.35	9.37	9.41	0.08	0.06	0.001	0.041	0.4
Democracy index	8.93	8.92	8.99	8.88	8.92	8.99	-0.07	0.11	0.003	0.05	0.62
ICT development index	8.6	8.46	0	8.35	8.46	8.94	0.12	0.59	0.09	0.27	3.18
The risk of malware infection	26.68	26.4	0	21.3	26.4	32.2	10.7	10.9	45.11	6.007	22.51

Table 4: Descriptive statistics: Netherlands

Variables	X average	M_e	M_0	Q_1	Q_2	Q_3	A	A_{iq}	σ2	σ	CV
Personal Freedom	6	6.06	6.06	5.84	6.06	6.12	0.01	0.28	0.04	0.03	3.12
Democracy Index	3.59	3.59	0	3.35	3.59	3.83	-0.43	0.48	0.06	0.22	6.22

ICT development index	6.58	6.7	0	6.24	6.7	6.87	0.95	0.63	0.13	0.32	4.99
The risk of malware infection	54.34	54.5	0	51.35	54.5	57.25	2.09	5.89	12.62	3.17	5.84

Table 5: Descriptive statistics: Russian Federation

The indicators used show show a mixture of high and low Risk of Malware Infection in all the three countries. With a high statistical deviation of σ= 6 and a mean of M_e= 26.4, the Risk of Malware Infection in Netherlands tends to oscillate from a low level of cybersecurity (37,1 in 2011) to a high level of cybersecurity (18,7 in 2015). In the case of China, the general level of cybersecurity is between the other two countries. Although, with a statistical deviation of σ= 4.19 and a mean of M_e= 33.12, the Risk of Malware Infection has the tendency towards high values, which implies mostly low levels of cybersecurity. The situation is different in the case of Russian Federation, where the general level of cybersecurity is low, as the indicators shows high levels in the Risk of Malware Infection. On the other hand, in Russia the statistic deviation is lower compared with the other countries, with a value of σ= 3.17 and a mean of M_e= 54.5. From this we can assert that in Russia, although the level of cybersecurity is constant, it is however quite low.

4.INDIVIDUAL INTERPRETATION OF MEASUREMENT INDICATORS

China, Netherlands and Russia have all different cyber profiles, due to their political culture, security perceptions and objectives in cyberspace. We tested in each case the correlation of three variables: Personal Freedom, Democracy Index and ICT Development Index. The aim of our study was to identify the factors that influence the risk of malware infection.

For *China*, the relation between Personal freedom (independent variable - I. V.) and Risk of Malware Infection (dependent variable - D. V.) shows a weak positive correlation, with a value for Pearson coefficient of R= 0.25.

The influence between those variables can be seen figure 1, where we can observe that risk of malware infection decreases when the personal freedom is also decreasing. Although, the low correlation is caused by the fact that the Personal Freedom has a low statistical deviation of σ= 0.26, while the statistical deviation for the Risk of Malware infection is high (σ=4.19).

The second set of variables, the Democracy Index (I. V.) and the Risk of Malware Infection (D. V.) are correlated as well, but the Pearson coefficient shows a weak correlation of 0.43. The correlation graphic (see figure 2) shows that the decrease of the Democracy

FIGURE 1

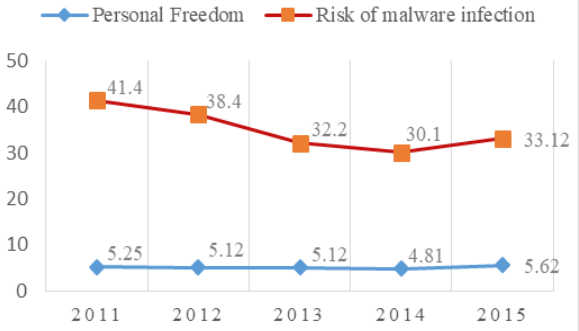


FIGURE 2

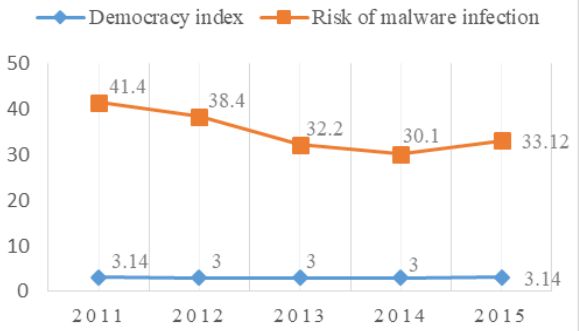
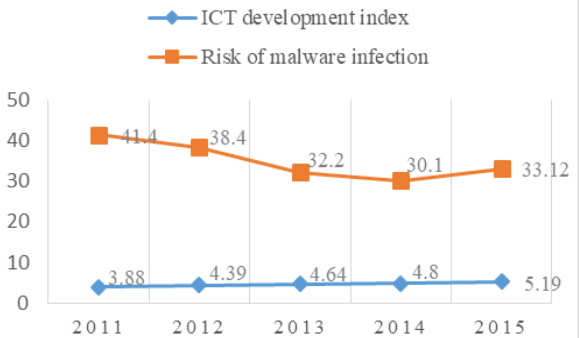
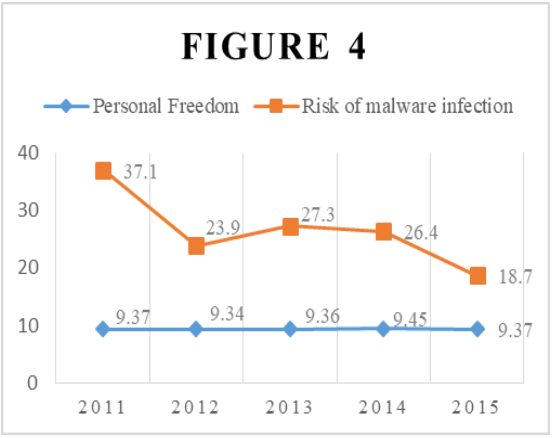


FIGURE 3

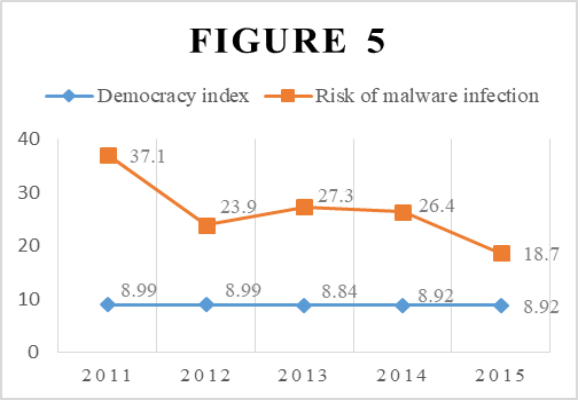


Index between 2012-2014 leads to a lower Risk of Malware Infection. If we look at the graphic, particularly in 2015, how the increase of democracy led the rise of insecurity.



The last set of variables, the ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) have a strong and negative correlation of R= -0.82. In figure 3 we can observe that the increase of the ICT Development Index generally leads to a decrease of the Risk of Malware Infection, with an anomaly in 2015, when the Risk of Malware Infection increased, even though ICT Development Index increased as well. China is one of the countries which stand for development of the infrastructure, use and skills of the ICT instruments. We can also see this tendency on the graph, where the ICT Development Index has an increasing and steady evolution.

For *Netherlands*, none of the variables have a significant correlation with the Risk of Malware Infection. The first set of variables, the Personal Freedom (I. V.) and the Risk of Malware Infection (D. V.) indicates a correlation of R= 0.04, close to 0, which indicates that there is almost no statistical correlation.



The relation between the Democracy Index (I. V.) and the Risk of Malware Infection (D. V.) shows a poor, but positive correlation of 0.29. If we look at the graphic (figure 5), we can observe that in 2013 the Democracy index decreased, and the risk of malware infection increased. The next year the Democracy index increased, and the risk of malware infection decreased. At a closer inspection, we can identify the tendency of the Risk of Malware Infection to decrease during the stagnant periods: 2011-2012 and 2014-2015.

The last variables, the ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) have a poor and negative correlation of R= -0.27. On the graph we can observe how the Risk of Malware Infection decreased with the increase of the ICT Development Index in 2012 and 2015. In 2013 and 2014 we can identify a reversed evolution.

In *Russia*, the strongest

FIGURE 6

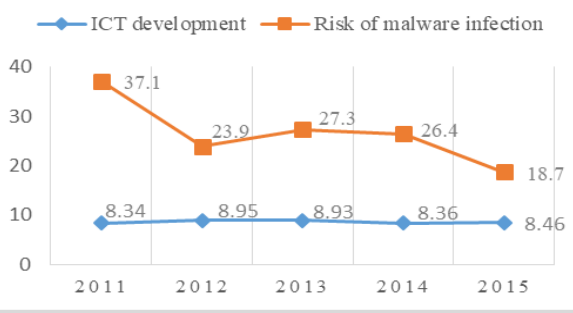


FIGURE 7

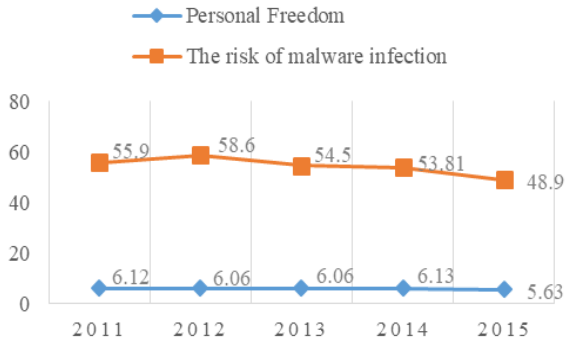
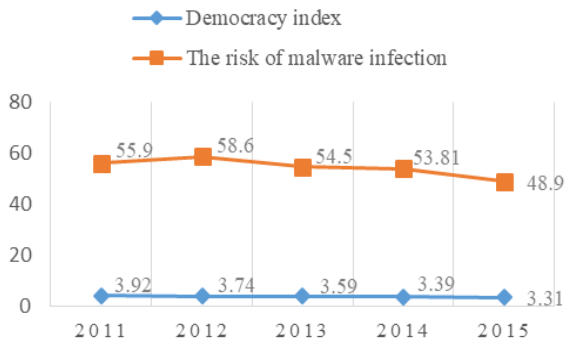
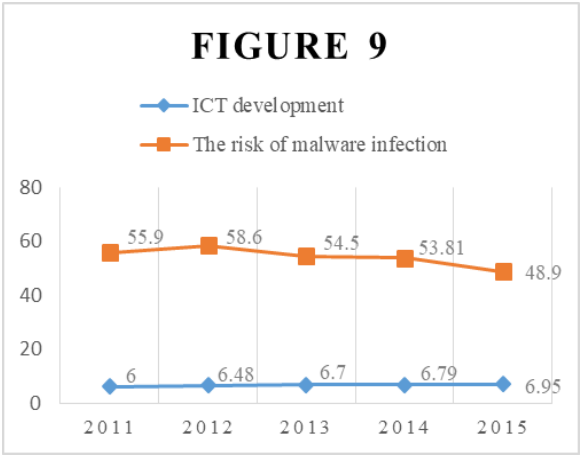


FIGURE 8



correlation is between the Personal Freedom (I. V.) and the Risk of Malware Infection (D. V.) with R= 0.8. The increase of the Personal Freedom between 2014 and 2015 led to the decrease of the Risk of Malware Infection. In the previous years we can observe that the decrease of the Personal Freedom between 2011 and 2012 led to the increase of the Risk of Malware Infection.



The second strongest correlation in Russia is the Democracy index, where the Pearson coefficient if R= 0.78. On the graph we can identify a concerning evolution of the Democracy Index, which had a continuous decrease between 2011 and 2015. On the other hand, we can observe a decrease of the Risk of Malware Infection between 2012 and 2015. Surprisingly or not, this indicates that the decrease of the democratic performance leads to a higher cybersecurity, as defined in our article.

The last set of variables, ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) are strong and negatively correlated with R= -0.65. The relation between the two variables is mixed. In general, the increase of the ICT Development Index leads to the decrease of the Risk of Malware Infection, with an anomaly in 2012, where we can observe that the Risk of Malware Infection increased, although the ICT Development Index increased.

5.FURTHER CONSIDERATIONS

The objective of our research was to identify the factors that are contributing to the cyber security in China, Netherlands and Russia. We could not find a general factor that influenced all the countries in similar manners. However, the

democracy index did correlate positively in all the cases, but not in the same ways. In China and Russia, the decrease of democracy is creating a stronger cyber security. On the other hand, in Netherlands we had observed the contrary: the strong democracy creates a safer cyberspace.

The results made us conclude that the factor which influences the cyber-security is the political culture. All the states selected in our study have a different political culture. Netherlands have a strong Western democracy and the citizens are enjoying the Western values. Russia has the soviet and Slav heritages. China is still influenced by its ancient Chinese culture, along with its present popular democracy. On top of that, each country perceives the cyberspace in a different manner. Therefore, like the other security sectors, the cyber security reflects a country's political culture. Each country has a unique profile which matches the needs and the interests of that nation.

However, we expected that the ICT development would have a strong impact on the cyber security. But it did not correlate positively in none of the selected countries.

6.CONCLUSIONS

Cyberspace is very dynamic and for this reason we couldn't find a global answer to our initial questions. Even though it is being advocated that it transcends the national borders and exceeds the state's expertise, cyberspace bears a tremendous importance for the national security. The design of the security strategy in the traditional security domains (air, sea, land) is closely connected to the characteristics of the state, notably its political culture. Cybersecurity is being shaped by culture, analogous to the traditional security. If we compare the nature of the cybersecurity between two countries with contrasting societies, we can discover that the issues are framed in different manners. And this is one of the reasons why studying the cyberspace from a cultural perspective is so captivating. Culture is so powerful that managed to influence even an inherently technical aspect.

The objective of our research was to identify the factors that are contributing to the cyber security in China, Netherlands and Russia. We could not find a general factor that influenced all the countries in similar manners. However, the democracy index did correlate positively in all the cases, but not in the same ways. In China and Russia, the decrease of democracy is creating a stronger cyber security. On the other hand, in Netherlands we had observed the contrary: the strong democracy creates a safer cyberspace.

The results made us conclude that the factor which influences the cyber-security is the political culture. All the states selected in our study have a different political culture. Netherlands have a strong Western democracy and the citizens are enjoying the Western values. Russia has the soviet and Slav heritages. China is still influenced by its ancient Chinese culture, along with its present popular democracy. On top of that, each country perceives the cyberspace in a different manner. Therefore, like the other security sectors, the cyber security reflects a country's political culture. Each country has a unique profile which matches the needs and the interests of that nation.

The culture factor is also illustrated in our study, where the variables from each country correlated in such a different manner with the variable representing the Risk of Malware Infection (the cybersecurity index in our research). A notable correlation with the Risk of Malware Infection was registered in relation to the Personal Freedom in the Russian Federation, where the increase of the Personal Freedom would lead to the decrease of the Risk of Malware Infection. This confirms the hypothesis 'the highest the personal freedom is, the lowest it the risk of malware infection' (A. H_2). Despite the fact that the cyberspace have been created without security in mind, it quickly became impetuous to adopt certain security measures, which also implied certain types of control. As the state is sharing its prerogatives with the private parties, it can only control a certain section of the cyberspace, notably the regulation and monitoring activities[1]. The Personal Freedom is only an element of the state control constellation in the

[1] Johan Eriksson, Giampiero Giacomello, "Who Constrols What, and Under What Conditions?", *International Studies Review*, 2009, 206-210, p. 209.

cyberspace. Many states, both democratic and totalitarian are already "controlling what their citizens can and cannot do on the Internet"[1]. Our study showed that the control over the internet does not serve only to consolidate the state power, but it also increases the cybersecurity. On the other hand, in the other two cases the correlation is weak for China and close to null in the case of Netherlands. China is known for its censorship practices on the Internet and the use of private companies in its surveillance operations. But in our research, it seems that the two variables do not correlate, question which is subjects of further research.

The Democracy Index has a positive correlation across the three cases, with a strong correlation the case of Russia and a weak one in the other two. We discovered an interesting aspect in our research, namely the manner in which the democracy correlates the Risk of Malware Infection in China and Russia. In those two countries, the increase of the Democracy Index leads to the increase of the Risk of Malware Infection, which confirms the B. H_1 hypothesis. Probably this result is due to the nature of their political regimes, namely authoritarian regimes[2]. On the other hand, Netherlands has a long history of well-established democratic institutions, having acquired a full democracy[3] level of development. This aspect is also illustrated in our research, where we showed that for Netherlands the highest the Democracy Index is, the lowest it the Risk of Malware Infection, confirming the B. H_2 hypothesis.

The correlation that did not turned out as we expected is the ICT Development Index, which has a negative correlation across all the states selected for our study. In the case of China and Russia, we registered a strong a negative correlation, while in the case of Netherlands it was only a weak one. However, we have observed in the graphics that the three states recorded a continuous growth of the ICT Development Index in the period selected for our research,

---

[1] Myriam Dunn Cavelty, " Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Center for Security Studies*, pp. 1-15, p. 8.
[2] The Economist Intelligence Unit, "Democracy Index 2017. Free Speech under attack", *The Economist*, London, New York and Hong Kong, 2018, p. 8.
[3] *Ibidem*, p. 5.

which confirms once more that the cyberspace is becoming increasingly developed, interconnected, interdependent. Moreover, we also observed in the graphics that while the ICT Development Index had a continuous growth, the Risk of Malware Infection registered occasional decreases. Still, it would be a major fallacy to draw hasty conclusions on the relation between those two indices in the present research, reason why we recommend further research on the actual impact of the ICT Development over the cybersecurity level in various countries.

REFERENCES

- Aycock, John, *Computer Viruses and Malware*, Springer, Calagary, 2006.
- Ball, Terence; Dagger, Richard, *Ideologii Politice şi idealul democratic*, Polirom, Iaşi, 2000.
- Funk, Christian; Garnaeva, Maria, "Kaspersky Security Bulletin 2013. Overall Statistics for 2013", *Securelist*, 10th of December 2013, accessed 30th of May 2017,https://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/#04.
- Garnaeva, Maria; Chebyshev, Victor; Makrushin, Denis; Unuchek, Roman; Ivanov, Anton, "Kaspersky Security Bulletin 2014. Overall statistics for 2014", *Securelist*, 8th of December 2014, accessed at 30th of May 2017, https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/.
- Garnaeva, Maria; Wiel, Jornt van der; Makrushin, Denis; Ivanov, Anton; Yury, Namestnikov, "Kaspersky Security Bulletin 2015. Overall statistics for 2015", *Securelist*, 15th of December 2015, accessed 30th of May 2017, https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/.
- Guinora, N. Amos, *Cybersecurity. Geopolitics, law, and policy*, Routledge, London and New York, 2017.

- "Measuring the Information Society", *International Telecommunication Union*, Geneva, 2012.
- "Measuring the Information Society Report", *International Telecommunication Union*, Geneva, 2014.
- "Measuring the Information Society Report", *International Telecommunication Union*, Geneva, 2016.
- Namestnikov, Yury, "Kaspersky Security Bulletin. Statistics 2011", *Securelist*, 1st of March 2012, accessed 30th of May 2017, https://securelist.com/analysis/kaspersky-security-bulletin/36344/kaspersky-security-bulletin-statistics-2011/.
- Namestnikov, Yury; Maslennikov, Denis, "Kaspersky Security Bulletin 2012. The overall statistics for 2012", *Securelist*, 10th of December 2012, accessed 30th of May 2017, https://securelist.com/analysis/kaspersky-security-bulletin/36703/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/.
- "National Cyber Security Strategy 2: From awareness to capability", *National Coordinator for Security and Counterterrorism*, 2013.
- "National Cyberspace Security Strategy", *China Copyright and Media*, 27th of December 2016, accessed 28th of May 2017, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.
- Shaohui, Tian (Ed.), "International Strategy of Cooperation on Cyberspace" (unofficial translation in English), *News Xinhuanet*, March 1st 2017, accessed 28th of May 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.
- "The Defence Cyberstrategy", *Ministry of Defence* (Netherlands), 27th of June 2012.
- The Economist Intelligence Unit, "Democracy Index 2016 Revenge of the 'deplorables'", *The Economist*, London, New York and Hong Kong, 2017.
- Vásquez, Ian; Porčnik, Tanja, "The Human Freedom Index 2016. A Global Measurement of Personal, Civil, and Economic Freedom", *Cato Institute*, Washington, 2016.

- Yarger, R. Harry, "Toward a theory of strategy: art Lykke and the U.S. Army War College Strategy Model", *U.S. Army War College Guide to National Security Issues,* 2008.
- "КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ" [The Strategic Concept of Cyber Security of Russian Federation], 2014.