УДК 004.056.53:34(045)

Salome Mikiashvili,
PhD in American Studies

U.S.-RUSSIA RELATIONS IN THE SPHERE OF CYBERSECURITY

International Black Sea University
2, David Agmashenebeli Alley, 13th km. Tbilisi, 0131, Georgia
E-mail: mikiashvilisalome@gmail.com

Purpose: *the purpose of the study is to critically evaluate US cyber security policy using a qualitative and comparative approach, the disadvantages that the country faces in the sphere of Cyber Security and identify what mechanisms and developments will Improve Cyber Security Policy to help overcome the challenges in response to Russian Cyberaggression.* ***The methodological basis*** *of the research comprises philosophical, ideological, general scientific and special methods.* ***Results:*** *cybercrime is recognized as the most threatening and dangerous crime of the 21st century, the more the consumer relies on information and communication technologies, the more cyber threats increase thus becoming greatest threat for countries national defense. Also there is lack of regulation in cyberwar that constitutes global threat. The author exemines the effectivness of the measures taken by the US and EU countries taken during or after the attacks.* ***Discussion:*** *improvement of the National Cyber defense strategy, search for actions to be taken while dealing with cyber attacks.*

Keywords*: Cyber security; Cybercriminal; Cyberaggression; national defense, strategy.*

Problem statement and its relevance. In the 21st century, where information and communication technologies are being rapidly developed, it's almost impossible to live daily life without cybersecurity. Cybercrime has become one of the major worldwide threats. It poses itself as the biggest challenge modern countries development and stability has to face.

Analysis of research and publications. The issue of U.S.-Russia relations in the sphere of cybersecurity was studied by K.H. Jamieson, P.A. Johnson, B.W. McConnell, P. Sharikov, M. Smekalova.

Purpose of the article: to explore the mechanisms that US is using to combat the cyber threats that are coming from Russia an whether these tools are effective or not and to observe the nature of defense that these countries are using.

The presentation of the main material. Crimes committed using the latest technologies can do great harm to national defense and security, to the economic system and to the welfare of society.

Unlike land, sea, air and space, cyberspace is a human-made digital network that is used to generate, modify, store or transmit information.

Cybersecurity means a combination of prevention, detection, response and restoration measures that ensure the confidentiality, integrity and accessibility of information stored and transmitted electronically.

The more the consumer relies on information and communication technologies, the more cyber threats increase. Cyber criminals use unauthorized access to the victim's computer system through malicious software. Steal, destroy, change information or use it to commit other, more serious crimes. Through viruses and malware, the malicious software spreads freely across the systems, making it easier for cybercriminals to access the victim's computer, its information, and remotely control it.

Thus, cybercrime is recognized as the most threatening and dangerous crime of the 21st century. Gaps exiting in Cyberdefence of the NATO and European Union countries became one of the main points of the discussion of the Warsaw 2016 summit. "Allies pledge to strengthen individual nations' and

collective cyber defenses, and recognize cyberspace as a new operational domain" [1].

The NATO and European Union have clarified their positions about Russia's aggressive actions. We see from the Warsaw summit communiques 5th article that the NATO's vision about the cyber and hybrid war is the same as the military activity or terrorism (at least in the written or stated form) "The Alliance faces a range of security challenges and threats that originate both from the east and from the south; from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks" [6].

Despite the clear stance of the EU and NATO on cyber-aggression, there have been numerous attacks on member states since the 2016 summit.

In 2017, security researchers sounded the alarm about Russian hackers infiltrating and probing United States power companies; there was even evidence that the actors had direct access to an American utility's control systems [2].

Two days before France's presidential runoff in May, hackers dumped a 9GB trove of leaked emails from the party of left-leaning front-runner (now French president) Emmanuel Macron. The leak seemed orchestrated to give Macron minimal time and ability to respond, since French presidential candidates are barred from speaking publicly beginning two days before an election [12].

At the end of May, officials warned about a Russian hacking campaign that has impacted more than 500,000 routers worldwide. The attack spreads a type of malware, known as VPNFilter, which can be used to coordinate the infected devices to create a massive botnet.

On March 7, WikiLeaks published a data trove containing 8,761 documents allegedly stolen from the CIA that contained extensive documentation of alleged spying operations and hacking tools [11].

And of course the list provided above is just a drop in the ocean. If a large-scale cyber-attacks, are considered in the context of warfare, then according to the norms of the international law, the response should be proportionate and relevant to the inflicted damage.

Which in reality is less likely to be implemented, because the union is acting in accordance with democratic norms and principles and the response measures cannot be implemented, before the conduction of investigation that will determine, whether the attackers where acting in the interests of an enemy country and they received fundings directly from the enemy state to carry out these actions or they are independent hackers, that are not associated with any political actor [4].

While these hampers the ability of democratic states to respond promptly to cyber-attacks, some political actors are taking radical steps and countering cyber-attacks with military confrontation.

The Israeli Defense Force claimed that it bombed and partially destroyed one building in Gaza because it was allegedly the base of an active Hamas hacking group. The assault seems to be the first true example of a physical attack being used as a real-time response to digital aggression [13].

According to a lot of experts and sources U.N. still lacks clarity on the subject. "Recently, U.N. Secretary-General António Guterres, in acknowledging the growing incidences of cyberattacks, noted that the lack of regulation in cyberwar constitutes a global threat, especially as he thinks that it remains unclear even if the laws of the Geneva Conventions apply to cyberwar, or if cyberwarfare meets the threshold of armed conflict necessary to trigger international humanitarian laws" [3].

The united states in its national cyber defense strategy sends the message that it will no longer just defend itself when it is the target of the cyberattacks.

It says "As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners."

It says that "all instruments of national power are available," including military force, "both kinetic and cyber," and calls for imposing, "swift, costly, and transparent consequences when malicious actors harm the United States or our partners" [5].

Russia in its informational security doctrine is sending the messages of Managing the internet in Russia, thus taking care of the informational security and it's cyberspace.

"The first objective has a clear aim to establish full state control over the domestic information space. For this purpose, the doctrine envisions creat-

ing and fostering "IT bonds" — to supplement the infamous "Russian spiritual bonds" that the Kremlin propaganda hails as deriving from Russian culture, language, history and sacred texts — in order to "protect" the Russian citizens from harmful information.

The second objective is related to the Kremlin's growing despair over losing the benefits of its external propaganda, which cost a fortune and was designed to justify Moscow's unlawful actions at home and abroad to the world audience. Namely, the document expresses a serious concern about "the Russian mass media being subjected to open discrimination," claiming that "Russian journalists are not fully permitted to perform their professional activities" (Scrf.gov.ru, December 5) [10].

Apparently, this new turn may have stemmed from recent actions of Brussels and individual EU members taken against Moscow's aggressive anti-Western propaganda (See EDM, December 7).

The final objective highlights Moscow's growing concerns that Russia is lagging behind other key players in the domain of IT and cyber security. Among the most noticeable shortcomings, the document points to Russia's dependence on the external IT market, the low effectiveness of Russia's scientific research, the weak ties between science and business, and the inadequate number of specialists working in this critical area. As a remedy, the doctrine sets a goal that envisages a drastic increase of IT's overall contribution to the national GDP and total exports [8].

The doctrine also calls for "liquidating the dependence of domestic industries on foreign information technologies" and ensuring information security by developing effective Russian technologies.

As US and NATO countries fail to address the drastic measures, the question is how can these states' cyberpolitics achieve effectiveness by adhering to democratic norms?

According to the bbc news, as a result of Russia's cyberattack on the US in 2016, the US expelled 35 Russian diplomats from the country and closed two consulates. It is believed that the cyber espionage was carried out by a Russian hacker group FANCY BEAR, and as US security agencies stress Russia affiliated criminal group which acts in the Russia's state interests and is linked to the Russian Federal Security Service [9].

After the Russian alleged meddling in the United States political elections in 2016, US continued to pursue active cyberpolitics which manifest in legal, organizational, technical, and other areas.

However, although concrete steps have also been taken by the state to strengthen cyber security (the legislation has been amended and the law defining US response to cyberattacks), there still are pressing issues.

Despite the fact that the United States government has taken multiple steps to reinforce its cybersecurity, quotation from “National Cyber Security": “*The number of cyberattacks on the US is increasing daily*”.

Conclusion. A lot of yet unanswered questions come to mind like how effective the US cyber security foreign policy in relation with Russia? (Whether it is rigid or liberal) What mechanisms and methods does US use against cyber threats that are coming from Russia? What is cyber diplomacy in the sense of the US and why are the countries actions limited with only official statements.

While the US has tightened its cyber policy since 2016 and imposed aggressive sanctions on the attacker nation, the number of cybercrime is still increasing.

Against this background, it is particularly important to determine what key postulates the US cybersecurity policy is built on, and how the country’s cyber security policy affect US-Russian relations does and whether there is a real cyber conflict between the two countries.

References

1. 2016 Warsaw Summit. *Wikipedia*. URL: https://en.wikipedia.org/wiki/2016_Warsaw_summit.

2. Jamieson K.H. Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know / Kathleen Hall Jamieson. 2018. 336 p. (Oxford University Press). (Your library). URL: http://www.librarything.com/ work/ 22207603/ reviews/162989217

3. Ctech by Calcalist. What Israel's Bombing of Hamas Hackers May Mean for the Insurance Industry, 2019. URL: https://www.calcalistech.com/ ctech/ articles/0,7340,L-3762296,00.html

4. Johnson P.A. (2002). M.N. Schmitt, B.T. O'Donnell (Eds.). Is It Time for a Treaty on National Cyber Security Organisation: United states; Piret Pernik, Jesse Wojtkowiak, Alexander Verschoor-Kirss. URL: https://ccdcoe.org/ uploads/2018/10/CS_organisation_USA_122015.pdf

5. National Cyber Strategy of the United States of America 2018. URL: https://www. whitehouse. gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

6. North Atlantic Treaty Organization: Warsaw summit communique Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. URL: https://www.nato.int/cps/en/natohq/ official_texts_ 133169.htm

7. Preciado M. (2012). If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare. URL: http://www.jlcw. org/jlcw-volume-1-winter-2012-issue-1/

8. Refworld. Russia's New Information Security Doctrine: Fencing Russia from the «Outside World»? 2019. URL: https://www.refworld.org/ docid/5864c6b24.html

9. Russia. The United States, And Cyber Diplomacy Opening the Doors By Franz-Stefan Gady and Greg Austin. URL: https://www.files. ethz.ch/isn/ 121211/ USRussiaCyber_WEB.pdf

10. Suggestions on Russia-U.S. Cooperation in Cybersecurity by Bruce W. McConnell, Pavel Sharikov, Maria Smekalova. URL: https://www. eastwest. ngo/ sites/default/files/ RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-en.pdf

11. Wired. The Biggest Cybersecurity Disasters of 2017 So Far, 2017. URL: https://www.wired.com/ story/2017-biggest-hacks-so-far/

12. Wired. The Biggest Cybersecurity Disasters of 2018 So Far, 2018. URL: https://www.wired.com/ story/2018-worst-hacks-so-far/

13. Wired. What Israel's Strike on Hamas Hackers Means For Cyberwar, 2019. URL: https://www. wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Саломе Мікіашвілі

ВІДНОСИНИ США-РОСІЇ У СФЕРІ КІБЕРБЕЗПЕКИ

Міжнародний Чорноморський Університет
алея Давида Агмашенебелі, 2, 13 км, 0131, Тбілісі, Грузія
E-mail: mikiashvilisalome@gmail.com

Сьогодні особливої уваги потребує проблема злочинів, вчинених із використанням новітніх технологій, які можуть завдати великої шкоди національній обороні та безпеці, економічній системі та добробуту суспільства. У своїй статті автор зазначає, що на відміну від суші, моря, повітря і космосу, кіберпростір – це створена людиною цифрова мережа, яка використовується для генерації, зміни, зберігання або передачі інформації. Кібербезпека означає поєднання заходів щодо запобігання, виявлення, реагування та відновлення, які забезпечують конфіденційність, цілісність і доступність інформації, що зберігається та передається в електронному вигляді. У XXI столітті, де інформаційно-комунікаційні технології швидко розвиваються, жити щоденним життям без кібербезпеки майже неможливо. Кіберзлочинність стала однією з головних світових загроз, вона проявила себе як найбільший виклик, із яким стикаються безпосередньо сучасні країни та їх відповідна стабільність. Саме тому, на думку автора статті, кіберзлочинність визнана найбільш загрозливим і небезпечним злочином XXI століття.

***Метою** дослідження є надання критичної оцінки політиці кібербезпеки США, виявлення недоліків, з якими стикається країна у цій сфері, та визначення механізмів і розробок, які б покращили політику кібербезпеки для подолання викликів у відповідь на російську кіберагресію, від якої страждають багато країн. **Методологічну основу** дослідження склали філософські, ідеологічні, загальнонаукові та спеціальні методи. **Результатом** дослідження став аналіз кіберзлочинності як найбільш загрозливого і небезпечного злочину XXI століття. У своїй статті автор дійшов думки про те, що чим більше споживач покладається на інформаційно-комунікаційні технології, тим більше зростає кіберзагроза, тим самим стає більшою загроза для національної оборони країн. Крім того, як зазначає автор, в кібервійні немає регулювання, а це, в свою чергу, становить глобальну загрозу. Автор демонструє ефективність заходів, які вживають країни США та країни ЄС під час або після відповідних нападів. Також у статті **дискусія** торкається вдосконалення національної стратегії кіберзахисту, пошуку дій, які слід вжити під час боротьби з кібератаками. Автор наголошує й на тому, що хоча Сполучені Штати Америки посилили свою кібер-політику з 2016 року та ввели агресивні санкції проти нападників, кількість кіберзлочинностей все ще зростає.*

***Ключові слова:** кібербезпека; кіберзлочинність; кіберагресія; національна оборона; стратегія.*