Секция «Международная безопасность: новые вызовы и угрозы»

Cybersecurity in bilateral relations of Russia and the U.S.

Научный руководитель – Добросклонская Татьяна Георгиевна

Голикова Анна Александровна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра информационного обеспечения внешней политики, Москва, Россия
E-mail: annagolikova2107@gmail.com

Obstacles that preclude Russia and the U.S. to negotiate a joint agreement in cyber sphere

Introduction

A brief background of the topic

Cybersecurity is a critical area of modern society, which is only becoming more important due to the continuous development of technologies that bring both benefits and multiple threats. Back at the end of the 20th century, it was difficult to imagine that after some time the cyber realm would become a threat to national and international security. Thus, in 1985 the United Nations published the UN Study on concepts of security and in the chapter «problems and threats in international security» information threats were not mentioned at all.[1] However, since the early 1990s, the Internet has become widespread and crucial technology. Despite the fact that almost all countries are currently involved in the digital sphere, which is especially evident in the era of Covid-19, there are countries whose position on cybersecurity is particularly important - Russia and the United States.

Outline the aims of the essay

In order to understand the specifics of the approaches of Russia and the United States to cybersecurity, and why these countries should be identified as key actors, the following aims are set out in this essay:

- To explain the specifics of the cybersphere and the complexity of its regulation;
- To analyze the background of Russian-U.S. bilateral relations and figure out why previous attempts to come to a common agreement were unsuccessful;
- To examine the current situation and the nascent aspects that are influencing the cyber realm: the emergence of new actors, anonymous threats, the intervention of corporate interests and the strengthening of new regional blocs (BRICS, SCO, EU).

A suggestion of the conclusion the essay will reach

The current situation in the field of cybersecurity requires urgent development of a common agreement, but while critical actors such as the United States and Russia have contradictory approaches, and new, often underexplored, threats and actors only increase their influence, its elaboration and legal enforcement is unlikely. An analysis of all the subtleties of the cybersphere and the players that influence it will help us identify the steps we need to begin with.

The specifics of the cyberspace

At the beginning, it should be said how cyberspace differs from all areas of international relations and why this field requires a very specific approach. Despite the fact that the Internet was originally created as a military project APRANET, which in 1969 united four scientific institutions, just as part of the confrontation between the United States and the USSR during the Cold war, when it became widespread, it began to be seen as a source for the free exchange of ideas and opinions, and, thus it was believed that it cannot be subject to regulation. However, it soon became apparent that the Internet could be used by malicious actors in their interests, and even turn into a weapon of non-conventional warfare.

As the form of cyber danger significantly differs from traditional threats to strategic security, it creates more complications in the attempts to develop a legally-binding framework. Lucas Kello writes in his article «The meaning of the Cyber Revolution: Perils to Theory and Statecraft», our society is facing «a delay in the strategic adaptation to cyber realities».[2] At the moment, technological development is ahead of our ability to comprehend the problem and take measures. Countries and their citizens all around the world are increasingly vulnerable to cyber threats: in the first half of 2020 alone, the number of cyberattacks rose by almost a quarter.[3] The rapid development of technology in the modern world and our inability to keep up with its changes greatly complicates our understanding of cyberspace and its threats.

Moreover, if we consider the possibility that cyber conflict can escalate even to the scale of a military threat, we are increasingly faced with the problem of attribution. As H. Lin writes, there are no evidentiary norms effective at the international policy level[4],and for governments it is extremely difficult to determine what the actor had proceeded with the attack. Attribution problem is mainly connected with the opportunities that modern technological development provides - an ability to access networks from almost anywhere in the world. For example, in 2014 the Obama administration blamed North Korea for the 2014 Sony Pictures hack, however, the government did not provide any solid evidence, supporting the charges.[5] Closely linked to this problem is the fact that States cannot provide evidence that could jeopardize their own control programs for the protection against cyber threats.

This problem also makes it necessary to create a single mechanism for decision-making and dialogue between countries. And despite the fact, that there were attempts to create a legal basis to address cybersecurity issues, such as the Council of Europe Convention on Cybercrime (2001), and the adoption of numerous UN Resolution on the cyber-related agenda, we have not seen a significant progress on this issue, but rather, on the contrary, the contradictions between the world actors are only intensifying.

Russian-U.S. bilateral relation on cybersecurity

The United States, as the country where the Internet appeared, and Russia, as the successor to the Soviet Union, the main enemy of the Cold war era, are among the most important actors involved in the formation of cyber realm. Bilateral relations between Russia and the United States on cybersecurity issues are of particular importance, since these countries, are also permanent members of the Security Council, significantly influence decision-making on the adoption and development of the legal framework. Disagreements and deterioration in relations between Russia and the United States on cybersecurity issues create obstacles to developing a strategy to regulate cyberspace.

The U.S. and Russia have previously attempted to work out a joint position: in 1998, countries provided their share view on «Common Security Challenges at the Threshold of the 21st century», where they recognized the importance of cyber sphere. Russia also proposed to sign a statement at the presidential level, in which countries were to develop a joint definition of cyberthreats.[6] During Obama's presidency, in 2011, the International Strategy for Cyberspace was published, which outlined the US commitment to international cooperation in the cybersphere[7], in 2013 Russia and the US even signed the Joint Statement a New Field of Cooperation in Confidence Building and outlined mechanisms for reducing cyberthreats[8].

However, already in 2018, in the National Cyber Strategy of the US, Russia, along with China, Iran and North Korea, was named as a country that uses «cyberspace as a means to challenge the United States»[9]. This reflects that bilateral relations between the US and Russia have deteriorated over the past few years and now reaching a joint solution to develop a unified strategy to combat cybercrime and cyberterrorism will be particularly difficult. Moreover, the United States and Russia accused each other of cyberattacks, and one of the most notorious cases was the accusation of Russia interfering in the 2016 US presidential election. Even after

Special Prosecutor Mueller's report was released in 2019 denying the Kremlin-Trump link, relations have not improved, since the report did indicate that the IRA, International Research Agency, was involved in attempts to influence the opinion of voters using social media accounts. In February 2020, the United States accused Russia of a broad cyberattack against the republic of Georgia in October that took out websites and interrupted television broadcasts and many even then began to talk about the threat of Russian interference in the 2020 elections.

The nascent aspects of the cyber realm

In the XXI century, we are seeing the strengthening of new states that seek to influence the information sphere, such as China, Iran, and North Korea. One of the most significant actors is undoubtedly China, another permanent member of the Security Council. The field of cybersecurity came to the attention of the Chinese authorities in the second half of the 1990s.[10] One of the incentives for the development of legislation in this area was the creation in 1999 of the e-government system (Government Online Project, GOP).[11] The National People's Congress adopted the Chinese cybersecurity law on November 7, 2016 and it has become a precedent in Chinese law: according to it, official Beijing has the right to control events taking place in the Chinese segment of the Internet at the legislative level.[12] In this aspect, China's policy is approaching the Russian model, while China retains its specifics and keeps a distance, while increasingly entering into a confrontation with the United States, trying to approve its agenda.

The region of the Middle East, and first of all, Iran, which the US calls the «rogue state», is a region vulnerable to cyberattacks and is becoming a field for unleashing new cyber wars. The events surrounding Iran's nuclear program and the «Arab spring» have demonstrated the role of the information factor in strengthening the asymmetry of modern conflicts, domestic and international, which have threatened the sovereignty and territorial integrity of a number of countries. Iran promptly, in few years after Stuxnet attack, managed to create a national cybersecurity system.[13] In 2012, Iran signed an extensive agreement with North Korea on scientific and technical cooperation, including combining the efforts of the two countries in the fight against the «common enemy in the digital space».[14]In 2013-2015 Iran has been credited with executing hundreds of targeted cyberattacks on military installations, energy and water supply systems, and the banking sector of the United States, Israel, and several Middle Eastern countries. The US compared the threat posed by Iran to China.[15] The appearance of so many countries trying to use the cyber sphere for their own benefit, and their ability to join alliances, including with Russia, against the United States, clearly contributes to the polarization.

A significant obstacle is both the corporate interest and the international nature of the activities of companies that control the information sphere, but at the same time their physical and legal attachment to a certain territory. Internet companies, such as Facebook and Google, were established on the territory of the United States, and their key offices are located there, as well as, they report their activities to the U.S. government, while carrying out its activities all around the world. Another example is Huawei, the Chinese-based global telecommunications company, that in November 2019 even published the Position Paper on Cyber Security[16], still has to consider the position of the Chinese government in decision-making. The interference of corporate interests and their close relationship with the governments of the countries where they are located affects the agreement on cybersecurity issues.

+ regional blocks

Conclusion

Every year, the confrontation in the cyber sphere only increases - and Russia and the United States are no longer the only players in this area. The international community must come to an understanding of the threats posed by unregulated cyber sphere, and begin to develop a single agreement on cybersecurity, which is directly related to the issue of Internet regulation. Russia and the United States, having overcome their differences over how to treat the issue of regulation, will be able to change the situation and influence other states on the world stage, thereby reducing tensions. It is important to note that all questions concerning Internet governance could be solved only by involving all parties: private sector, represented by corporations, technical and academic community and governments. Russia and the U.S. must take into account all strategic changes, occurring in world politics, as well as the specific peculiarities of cyber domain, in order to make a significant progress towards the creation of safe international regulatory system.

[1] UN Study on concepts of Security, A/40/553, 26 August 1985

[2] Kello, Lucas, «The meaning of the Cyber Revolution: Perils to Theory and Statescraft» (International Security Journal, 2013)

[3] Аналитика. URL: https://www.ptsecurity.com/ru-ru/research/analytics/

[4] Lin H. Attribution of malicious cyber incidents: from soup to nuts. J. Int Affairs 2016; 70; 75-106.

[5] Hacker Lexicon: What Is The Attribution Problem? //https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/

[6] Gady, Franz-Stefan, and Austin, Greg. "Russia, the United States and Cyber Diplomacy, Opening the Doors." *Journal* of *EastWest Institute* (2010): 1.

[7] White House. "International Strategy for Cyberspace, 2011." Accessed August 17, 2020. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

[8] Karasev, Pavel. "New U.S. Cybersecurity Strategies, 2018." Accessed August 17, 2020. https://russiancouncil.ru/en/analytics-and-comments/analytics/new-u-s-cybersecurity-strategies/

[9] White House. "National Cyber Strategy of the United States of America, 2018." Accessed August 17, 2020. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[10] Bi, J. 2001. The Internet Revolution in China: The Significance for Traditional forms of Communist Control. *International Journal* 56(3): 421-441.

[11] Dong, F. 2012. Controlling the Internet in China: The real story. *Convergence: The International Journal of Research into New Media Technologies* 18(4): 403-425.

[12] Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты. Journal «Bulletin Social-Economic and Humanitarian Research», № 7 (9), 2020, e-ISSN 2658-5561 file:///C:/Users/Anna/Downloads/strategiya-kitaya-po-obespecheniyu-informatsionnoy-bezopasnosti-politicheskiy-i-tehnicheskiy-aspekty.pdf

[13] Developments in Iranian Cyber Warfare 2013-2014 // Institute for National Security Studies. August 2014 [Electronic resource]. URL: http://www.inss.org.il/uploadImages/systemFiles/ SiboniKronenfeld.pdf

[14] Iran and North Korea Sign Technology Treaty to Combat Hostile Malware // V3.CO.UK. September 3, 2012 [Electronic resource]. URL: http://www.v3.co.uk/v3-uk/news/2202493/iran-andnorth-korea-sign-technology-treaty-to-combat-hostile-malware#

[15] Cyberthreat Posed by China and Iran Confounds White House // The New York Times. September 15, 2015 [Electronic resource]. URL: http://www.nytimes.com/2015/09/16/world/asia/ cyberthreat-posed-by-china-and-iran-confounds-white-house.html?r=0

[16] Huawei's Position Paper on Cyber Security//https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la><span style=