

US-Russia Relations on Cyber Security



By: - Amarakoon Rajapaksha Wasala Mohotti Mudiyanseelage Poojika Buddhinee Amarakoon

Email: poojikabuddini@gmail.com

Masters in International Relations (in English)

SCHOOL OF INTERNATIONAL RELATIONS
SAINT-PETERSBURG STATE UNIVERSITY

The relations between United States and Russia are currently overshadowed with the cloud of distrust due to some certain tensions and pressing issues. Along with the mutual accusations both countries have imposed sanctions and this led to unstable the status of relations among these two great powers. However, the positive side of the relations among these two states is that despite these long term tensions, Russia and United States worked together in many areas extending their cooperation in certain critical areas, especially related to global security by following some measures to counter the threats to the stability of the world.

The current condition of relationship between Russia and United States is not in a good state where it got more worsen with the situation of accusation of Russian interference in the 2016 United States presidential election. The incident of Russia's annexation of Crimea and the southeastern Ukraine war (Donbass) along with the Russia's support to the Bashar-Al Assad regime in Syria and the opposite viewpoints of United States in that war condition has led to escalate the tensions in the relations between the two countries. Despite the fact that the President Trump determined to build up strong relations with Russia as he mentioned in his initial days of his presidency, the tough policies of United States congress has hindered these initiatives with imposing of sanctions and expelling of diplomats. However, being two nuclear superpowers United States and Russia have the responsibility in terms of world security and combatting global challenges like terrorism. The persistent cooperation and competitive relationship among these two states need to discrete in a way which is effective to address the eminent challenges.¹ In the present day, unlike the prevailed bipolar world condition, along with the tectonic shift of global power, Russia and United states do not remain as the sole great axis powers whereas it already transferred the bipolar world into a multipolar world system. The revolution of information and the rise of cyberspace has become a game changer and a unique phenomenon which directly affect to both domestic and international systems. This made the way to borderless interaction among the actors in the international arena while challenging the very idea of sovereignty.

Accordingly, cyber security is such kind of a pressing global issue where both United States and Russia needs to advance its cooperation through important dialogues and conversations which needs to be maintained on long term basis. In this field both countries share number of

¹ Stent.A, APRIL 27, 2020, Why are US-Russia relations so challenging?, Accessed 28/07/2020, <https://www.brookings.edu/policy2020/votervital/why-are-us-russia-relations-so-challenging/>

key interests and advancements in related to this field in terms of their national agendas as well. When considering about a brief recap of the condition of cyber security in the world today, it is a field of a must cooperation for the both countries due to intense technological development in the 21st century. The development of cyber space governance and unpredictable threats ignite the spark of the need of common approach and to rethink of new ways of inflicting the significant damages that will occur by cyber related issues to the national and international security grids. One of the most controversial episode in the current days in United States and Russia relations is the U.S accusation to Russia of involvement of hacking with regards to the 2016 US presidential election made a harmful effect to the efforts of restoring relations regarding the technological aspects and issues. However, it does not mean that the two state are not working on to keep their relation in that area. In past recent years the two countries have made several approaches in developing its relations regarding technology, information dissemination which are directly or indirectly related the cyber field.

Brief recap of historical cyber space relation between Russia and US is as follow: Since the United States recognized the Russian Federation as the successor of Soviet Union by December 25, 1991, the two countries formally established the diplomatic relations on December 31, 1991.² After that, by making a strength to the relationship between two countries the cyberspace integration approaches began roughly by 1998 with the Russia proposal to UN to develop a system to enhance the security of global information and telecommunication system which help to combat information terrorism and criminality. Then under a Group of Government experts(GEE) committee both Russia and US started the long process of discussions to develop norms of responsible state behaviour, confidence building measures, and actions to build cyber security capability on a global basis. The support from Russia on multilateral confidence building measures (CBMs) which were agreed in the Organization for Security Cooperation in Europe (OSCE) ultimately led to an agreement on cyber security between Russia and the United States in 2013 and 2016. The 2013 agreement was part of a broader bilateral effort to cooperate on counterterrorism and WMD where the leaders of the two countries identified the seriousness of cyber risks and agreed to establish national centers with a “hot line” as a mutual warning mechanism with related to cyber incidents which raise national security concerns and also regarding the cyber exercises of each countries which can be misperceived as an attack.³

² Bureau of European and Eurasian Affairs, 22July 2020, US Relations with Russia. Accessed 28 July 2020 <https://www.state.gov/u-s-relations-with-russia/>

³ Lewis J.A, 2017,Cyber Security: A U.S perspective, Report- A roadmap for U.S Russia Relations, Russian International Affairs Council

Moreover, according to the U.S government archives, the two countries took measures in exchanging of white papers where the militaries were examining the implication of ICT for planning and operations which in turn gives predictability and understanding of political-military environment, in a circumstance where both Russia and United States shared unclassified ICT strategies and other relevant studies in mutual manner.⁴

Both United States and Russia are making their ways of cooperation in combatting terrorism. In the cyber sphere the access to information and misuse of information and freedom of expression especially in social media, are the issues that come up in the context of cyber security. So, both countries need to extend their cooperation despite the fact of existing differences in terms of content and expressions within the cyberspace. Accordingly, several challenges which leads to hinder the cooperation between the two countries in the cyber space can be identified: The foremost challenge is that the two countries are skeptical about the sincerity of cyber operations where US officials are accusing Moscow for ransomware attack which tried to infiltrate US election. Then the disagreement of both parties on the nature of cyber conflicts which hinder the shared norms is also occurred as a result of Russia's skepticism on US with the incident of Panama papers. Moreover, Russian experts are in the view that cyber-attacks will make an effect which is equal to WMD (Weapons of Mass Destruction) whereas the United States is in the position that international norms and agreements needs to embed the legitimate use of cyber-attack in the framework of international law, which in turn accepts the use of cyber-attacks if it is guided by principles and norms of the laws of armed conflict that nations are obliged to follow.⁵ Along with this contrasting perception of cyber-attacks, more tensions are there in between Russia and US on issues related to content and expression. This disagreement was visible when Russia and China made the "International Code of Conduct for Information Security" with the support of Shanghai Cooperation Organization (SCO).⁶ The two different perspectives on the expression and content by the Russia and US is another challenging factor. The restriction on the use of social media or online speech, especially by groups like ISIS drives the interplay between rights and restriction on the

⁴ The white House, 2013 June, FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>

⁵ Grigsby. A, 2018 August, Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? <https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no>

⁶ Lewis J.A, 2017, Cyber Security: A U.S perspective, Report- A roadmap for U.S Russia Relations, Russian International Affairs Council

two different viewpoints of the two countries. So, it is quite clear that the clouds of suspicion and skepticism abided with not having a common understanding about certain cyber related norms has been the major root causes to hamper the initiatives on cooperation in cyber space.

Nevertheless, both Russia and United states face common threats to its cyber security from the third parties. Both states still does not have a common approach and joint efforts in solving these issues. Apart from that, neither Russia nor United states have a common perception on the elaboration of two different terminologies of cybercrime and cyberterrorism while there is no any identification of a clear agreed list of cybercrimes committed for which the mutual assistance has been requested and identified. Apart from that, in general, some critical global problems in the cyber space includes: not having a proper international mechanism to address the cybercrimes which will prosecute, investigate and punish those cyber criminals. The problem of distinction and characterizing a cyberattack and the problem of proper retaliation against a cybercrime where it needs to be proportionate to the crime committed and if not the further escalation of a cybercrime may expanded to involve into a non-cyber tools which can leads to cause catastrophic results.

Accordingly, the persistent threats such as hacking and DDoS attacks which takes place every day is a threat to the national security where Russia and United States needs to cooperate on investigating and prosecuting these incidents while assisting each other to share information about international cyber threats. Since both Russia and United States are working on combatting terrorism, the NGOs, civil society organizations, public diplomacy institutions of each country can work together in the process of information sharing to mitigate and counter the terrorist intelligence activities. The two countries need to continue the dialogue on cyber warfare while addressing the issues and challenges by initiating discussions with the academic experts in the field to make an understanding about the persistent problems. Then eventually the two countries can establish some sort of a cyber position through building norms to prevent the offensive use of cyber means to conduct activities, especially in the military sphere. Also, it can take cooperative actions to protect critical infrastructure facilities such as hospitals, electrical grids, nuclear facilities (by being states who possess great nuclear power capabilities) through dialogues and partnership. When considering about building norms, Russia and United States needs to continue discussions on building Universal Internet Governance rules with related to the security issues discussed above and in turn this will leads to develop a cyber security regime where the regulations and specificities will address the military, political, legal, economic and social issues that erupt in the cyber sphere. This establishment of code of

conduct by the cooperation of two countries will be able to address the key problems of effective government information policy to maintain a proper balance between the government controls over the cyber space and to detect malicious conduct by the parties which can emanate a threat to the national security of each state.

In a circumstance where both Russia and United states will not have agreed common norms with regards to the cybercrimes and cyberterrorism where their positions will converge into responsible state behavior, it is essential that two countries needs to approach in the form of Track II diplomatic channels to focus on these problems. Accordingly, as a first step for that, the both states needs to work on tracking and seeking common understanding about major issues in both national and international levels in the cyber space through broader discussions in government, think tanks and expert levels. By these discussions it needs to seek and establish confidence building measures as a way to turn these tenacious cybersecurity dialogues into the form of cooperation approach. It will be a joint venture of two states to articulate a concrete cyber posture that addresses the key issues in the context of mutually agreed norms for the use of cyber means that disrupt critical infrastructure which in turn a violation of international law and as well as the offensive use of cyber means, especially in military sphere which in turn will be a broader arms control paradigm among the two countries. In this, the most immediate issue that the two countries face with regards to the START Treaty on strategic offensive weapons, the successor of SALT (Strategic Arms Limitation Talks) Treaty which has been signed among the two countries in 1972 will expire by 5th February 2021.⁷ The new treaty can be extended up to five more years, where the two states needs to consider about the advent of new cyber capabilities and hence the modernization of weapons, when setting up the norms, principles and rules in the upcoming arms control treaties.

Another direction of cooperation are joint efforts in combatting terrorism and extremism in the cyberspace. Being two states which are in the avenue of beating the efforts of terrorists, United States and Russia can work together to counter the use of internet as a propaganda tool by the extremist terrorist organizations and also can make endeavors to share best practices in countering their soft power on the internet. For that the ICT companies of both countries can work together under common norms and principles with regular testing of systems and by

⁷ Stent. A, April 27, 2020, Why are US-Russia relations so challenging?, Accessed 28/07/2020, <https://www.brookings.edu/policy2020/votervital/why-are-us-russia-relations-so-challenging/>

maintaining regular warning system in potentially dangerous activities which threatens the national security.

Despite the prevailing negative vibes between relations of United states and Russia, if these initial steps and such efforts will be undertaken by both parties, it would be a successful path to rebuild the foundation of dialogues on cyberspace issues to enjoy the benefits of stability on behalf of the cyber security issues that will arise in the future which will affect to both nations.

Reference

Bureau of European and Eurasian Affairs, 22July 2020, US Relations with Russia. Accessed 28 July 2020 <https://www.state.gov/u-s-relations-with-russia/>

Grigsby. A, 2018 August, Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? <https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no>

Lewis J.A, 2017,Cyber Security: A U.S perspective, Report- A roadmap for U.S Russia Relations, Russian International Affairs Council

Policy Brief, May 2017, Suggestions on Russia-U.S. Cooperation in Cybersecurity, Russian International Affairs Council

Schmitt. M, June 18, 2019, U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?<https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/>

Stent.A, APRIL 27, 2020,Why are US-Russia relations so challenging?, Accessed 28/07/2020, <https://www.brookings.edu/policy2020/votervital/why-are-us-russia-relations-so-challenging/>

The white House, 2013 June, FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security<https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>