Russian International Affairs Council

EastWest Institute

POLICY BRIEF

Suggestions on Russia-U.S. Cooperation in Cybersecurity

Bruce W. McConnell,
Global Vice President, EastWest Institute
Pavel Sharikov,
Director, Applied Research Center, Institute for U.S.A. and Canada Studies, Russian Academy of Sciences
Maria Smekalova,
Coordinator of Russia-U.S. Dialogue on Cybersecurity project, Russian International Affairs Council

No. 11, May 2017

RUSSIAN INTERNATIONAL AFFAIRS COUNCIL

Editors:
Ivan Timofeev, Ph.D. in Political Science
Timur Makhmutov, Ph.D. in Political Science
Maria Smekalova
Bruce W. McConnell

Russian International Affairs Council (RIAC) is a membership-based non-profit Russian organization. RIAC's activities are aimed at strengthening peace, friendship and solidarity between peoples, preventing international conflicts and promoting crisis resolution. The Council was founded in accordance with Russian Presidential Order No. 59-rp "On the Creation of the Russian International Affairs Council non-profit partnership," dated February 2, 2010.

FOUNDERS

Ministry of Foreign Affairs of the Russian Federation

Ministry of Education and Science of the Russian Federation

Russian Academy of Sciences

Russian Union of Industrialists and Entrepreneurs

Interfax News Agency

RIAC MISSION

The mission of RIAC is to promote Russia's prosperity by integrating it into the global world. RIAC operates as a link between the state, scholarly community, business and civil society in an effort to find solutions to foreign policy issues.

The views expressed herein do not necessarily reflect those of RIAC.

EastWest Institute

Mission

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow, Dallas, Washington, D.C., San Francisco and Istanbul.

Legacy

With a legacy deeply rooted in the Cold War—hosting the first military-to-military dialogue between NATO and Warsaw Pact countries—to active engagement in the Balkans, the Middle East and East Asia, the institute continues to play a decisive role as a trusted facilitator in today's most contentious global conflicts.

Organization

To achieve our mission, EWI has three programmatic pillars: Global Security, Regional Security and Strategic Trust-Building. EWI operates both "above" and "below the waterline" to remain a public, yet discreet, force in the global arena.

Programs

- Global Cooperation in Cyberspace
- Economic Security
- Middle East and North Africa
- Afghanistan Reconnected
- Russia and United States
- Asia-Pacific

Global Cooperation in Cyberspace

The Global Cooperation in Cyberspace program seeks to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion. Working with government, business and civil society leaders from around the world, the institute's cyberspace program has highlighted three objectives to be pursued towards a safer and more secure Internet: enhance deterrence against malicious cyber activities; improve the security of Internet products and services; and maintain efficient information and technology flows across borders consistent with local values. The program is led by Global Vice President Bruce W. McConnell

The views expressed herein do not necessarily reflect those of EWI.

Suggestions on Russia-U.S. Cooperation in Cybersecurity

The current state of Russia-U.S. relations is marked by a high level of distrust. Tensions have been escalating for three years, both countries have imposed economic sanctions, disseminated propaganda, and exchanged accusations. The situation is unpredictable, the escalation may continue and destabilize the whole international system. The deterioration has touched all issues of Russia – U.S. relations, including cybersecurity.

Cooperation on cybersecurity is a relatively new problem, and probably has never been among the most prioritized, along with many other issues, including terrorism, Ukraine, Syria, economic sanctions, and many others.

While Russia and the U.S. feel the need to cooperate on settling pressing issues regarding cybersecurity, they seem to diverge over what should be done and over how international law could be applied.

In this context two parallel tracks should be promoted. The first one is cooperation on cybercrime prevention and counterterrorism measures. In part because they lack common terminology regarding cyberspace, Russia and the US fail to find common ground when talking about cybercrime prevention. What is more, the at times anonymous nature of cybercrime not only impedes the attribution process, but undermines the political stance in bilateral relations. The second track involves elaborating norms of behavior as well as protection of critical infrastructure from cyberattacks. Although work is being conducted by the United Nations Group of Governmental Experts (UNGGE), the most important issue has become how to make the norms actionable. Critical infrastructure, along with cybercrime, needs clear definition.

What is vital now is to continue dialogue and reach mutual understanding with the help of expert meetings and publications, technical cooperation, and balanced media participation and coverage, so that a more united approach may follow.

During the past year, Russian and U.S. experts in cybersecurity have been working together making important observations on existing problems in relations between the two countries in this area.

As a result of bilateral efforts, the Russian International Affairs Council (RIAC) and the EastWest Institute (EWI) are putting forward a number of challenges and proposals to promote cooperation in cyberspace between Russia and the United States.

The parties are hopeful that the suggested ideas, which appear at the end of this Policy Brief, will lay the groundwork for future cooperation. As a preface to those ideas, the brief provides contrasting perspectives from Russian and U.S. experts.

Russia and the U.S.: Frenemies in Cyberspace

Pavel Sharikov, Director, Applied Research Center, Institute for U.S.A. and Canada Studies, Russian Academy of Sciences

Prior to the current crisis, despite a number of contradictions on the topic, Russia and the U.S. managed to cooperate on building measures to raise mutual confidence, which included establishing a direct line between Moscow and Washington, agreeing on some issues of global internet governance, and some others.

Most of these confidence-building measures were agreed upon during the 2013 G8 summit in Ireland.[1] Unfortunately, all the success has been canceled due to the crisis. Many experts today agree that Russia and the United States are entering a Cold War 2.0. To some extent this definition is fair, given that both countries employ rhetoric similar to the “old Cold War” era, however using

AUTHORS:
Bruce W. McConnell,
Global Vice President, EastWest Institute
Pavel Sharikov,
Director, Applied Research Center, Institute for U.S.A. and Canada Studies, Russian Academy of Sciences
Maria Smekalova,
Coordinator of Russia-U.S. Dialogue on Cybersecurity project, Russian International Affairs Council

[1] Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0 .

modern technologies, including a wide range of cyber technologies.

With the tensions between Moscow and Washington growing deeper, people on both sides of the Atlantic agree that further deterioration is dangerous.

Probably the most disappointing fact is that instead of benefitting nations, expanded opportunities of information communication have led to the decrease of trust and confidence in international relations.

New Conditions

Information and cyber-related issues are game changers in the global system of international relations. Global cyberspace is a new phenomenon, which makes the new international system very much different from the bipolar world.

The "old Cold War" seems very explainable and predictable today, while the new Cold War is very much different.

The collapse of the Soviet Union, and the inevitable demise of the bipolar world destabilized the strategic balance of powers of the Cold War era. Additionally, other factors appeared. Many experts agree that as a result of the geopolitical shifts that happened due to the end of the Cold War, the concept of "strategic stability" developed a new meaning. The notion "strategic forces" is less defined by the capability to deliver nuclear weapons from one continent to another, because the balance of powers is no longer preserved by deterring the conflict between the two superpowers. Technological development led to the creation of new ways of inflicting significant damage, thus creating new threats to national and international security.

The Cold War was a unique period in the history of international relations. For the first and, so far, the only time the system of international relations was bipolar. The Soviet Union and the United States were the only superpowers, confronting each other for almost half a century. One way or another all other nations took part in this global confrontation between the two giant and incompatible economic systems – socialism and capitalism.

The collapse of the Soviet Union marked the triumph of liberal ideas, the bipolar order came to an end, and a new model of international relations started to evolve. Most experts in international affairs agree that the current system of international relations can be characterized as polycentric. The United States remains the most powerful nation in the world. And, while Russia inherited most of the Soviet legacy, it did not match the US in any power index except for nuclear weapons.

Security remains a significant issue in Russia – U.S. relations after the Cold War; however, Moscow and Washington are no longer the sole axis of the international system. Russia – U.S. relations in the field of security develop in accordance with the tectonic shifts in the world order.

The bipolar world is transforming into a multipolar world. The information revolution is a significant game changer in domestic politics as well as in international relations. Cyberspace is a unique phenomenon where domestic and international issues are interdependent to such an extent, that it is almost impossible to explore one without the other. The new system of international relations features new categories of actors and new forms of their interaction within the borderless cyber domain, thus challenging the very idea of sovereignty.

Non-state actors do not have military power, however, may pose a serious threat to other actors, including states. Hence states may not have an opportunity to inflict a retaliatory counter strike. Non-military factors of power are gaining more influence in the system of international relations. As the development of information technologies mainly took place in the private sector, dependence on information technologies make international relations actors vulnerable.

Ideological Confrontation or Information Warfare?

The old Cold War was about ideology. All domestic or foreign policy activities by both – the Soviet Union and the United States – have been compliant with either Communist (Marxist-Leninist) or Liberal democratic ideologies respectively. The Soviet Union and the United States belonged to oppositional ideological paradigms, incompatible with each other. This explains why the two countries were involved in ideological conflict.

What today looks like an ideological confrontation is in fact merely an odd form of information warfare – spread of propaganda through traditional and social media, internet, fake news, alternative facts, leaks etc.

Today Russia does not try to challenge American (or Western in general) world leadership in any way: Russian national interests consist in remaining an equal partner of the United States in addressing global challenges. With the collapse of the Soviet Union, there remained only radical forces who attempt to challenge the world order – like terrorist organizations or North Korea. And despite all the current political problems, ideologically modern Russian society is moving towards Western democracy, and is today closer than ever before.

While most of the problems mentioned above seem to lack direct connection with cyberthreats, all of them are related to cyberspace and information communication. The Russian government does admit that technical issues of security are inseparable from information contents.

Doctrines as a Base. A View from Russia

On December 5, 2016, President Vladimir Putin approved a new Doctrine of information security of the Russian Federation.[2] According to the new Doctrine, the Russian government remains a key player not only in providing information security, but also in developing information resources.

It's worth mentioning that the Russian government values both technological and humanitarian aspects of information. While the Western policies are mostly focused on providing technical security, Russian policymakers consider the contents of information more vital for security. In fact, the Internet is positioned as a basis for information infrastructure of the Russian Federation.

In general, the new Doctrine is consistent with the new official strategic position of the Russian government.

The new Doctrine builds on the trend towards further enhancement of government control of the Russian segment of the Internet and reinforcing national information sovereignty.

The new Doctrine also states that strategic deterrence and prevention of military conflicts is one of the main directions of information security. We are now awaiting the new U.S. document on cybersecurity prepared by the new Administration. Although some hints have already been given, a clear picture is yet to be provided. Hopefully, the two doctrines will have something in common, thus, allowing the two countries to find basis for cooperation.

It is true, that the security of the contents of information is as important as technical safety. The most debated episode of the recent Russia – U.S. confrontation in cyberspace is the hacking of the DNC during the U.S. 2016 presidential campaign, which serves as a clear example. The hacking itself was not as harmful for Hillary Clinton as the publication of the archive on Wikileaks, and the media coverage.

While the White House never made public any evidence for the involvement of the Russian government in the hacking, it uncovered some critical problems that urgently needed to be addressed.

First, the *problem of attribution of cyberattacks*. If a non-state actor executed the hacking, the U.S. sanctions against Russian officials fail to punish the real offender.

Second, the *inability of the international system to address cybercrimes*. There is no international mechanism that would provide the possibility to investigate, prosecute, prevent, or punish the criminals such as those who hacked the DNC server.

Third, there is a *problem of proper retaliation*. The response to a cyberattack would have to be asymmetrical, and must remain in the cyber realm. Further escalation may involve non-cyber tools, which may turn out to be very harmful.

All political contradictions aside, the leaders of Russia and the United States should admit

[2] Doctrine of Information Security of the Russian Federation / The Ministry of Foreign Affairs of the Russian Federation. URL: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

that the use of information tools against each other destabilizes the fragile equilibrium. With the political contradictions of the current crisis sooner or later going to be overcome, there is a high demand for raising mutual confidence and trust in bilateral relations.

Measures to Be Taken – Russia's Perspective

There are at least four fields of Russia – U.S. cooperation in cyberspace that are mutually beneficial, and in some sense vital for national security and the stability of international relations. Addressing these four issues in the near future would help to partly overcome the current crisis in bilateral relations.

The first pillar is countering cybercrime.

Cybercrime is probably the most persistent threat. Such incidents as hacking, DDoS attacks, and many others taking place every day, individually none of them can be considered a national security threat. That said, the governments must take urgent actions to decrease the scale and quantity of cyber incidents. Russia and the United States should cooperate on investigating and prosecuting these incidents, as well as on sharing information. Episodes like the DNC hacking should be subject to such type of cooperation. Russian and American law enforcement agencies should work out the mechanisms of joint investigation of cyber incidents, prosecution of cyber criminals, assisting each other in damage control, and share information about international cyberthreats.

The Second pillar is track 2 information sharing.

NGOs, civil society organizations, and public diplomacy institutions can work together to track and share information about terrorist activities on the net with intelligence agencies. Russian as well as American citizens have been repeatedly recruited through the Internet. While terrorists use the web as a tool for propaganda, countering such activity should be one of the directions of bilateral antiterrorist efforts, implemented by Russia and the United States through public diplomacy mechanisms. Creating a joint database of incidents could serve as a logical step in this direction.

Thirdly, the two countries should work on the cyber warfare posture.

Given the general negative environment in current Russia – U.S. relations, cooperation on cybersecurity should remain one of the positive examples. The governments of the two countries should definitely continue the dialogue, especially among the academic community, aimed at coming to common understanding of the problems. The governments of the two countries can publish some sort of cyber posture, declaring the norms of the use of offensive military cyber capabilities. Besides, the two countries need to harmonize their stances on protection of critical infrastructure (hospitals, electric grids, banks, nuclear facilities, etc.) even though the dialogue on this matter has been one of the more troublesome directions.

Finally, the issue of global Internet governance should be addressed.

Russia and the United States should continue discussions about the universal Internet governance rules with special regard to security issues. Any future international "cybersecurity regime" will be based on national regulations which are developed in accordance with the specifics of each nation's political, legal, economic, and social traditions. Certainly, one of the key problems of effective government information (cyber) policy is finding a proper balance between government control over cyberspace and freedom of information both on national and international levels.

In general, cybersecurity issues should be included in a broader range of the bilateral Russian-American relations agenda. Russia and the United States possess unique experience in arms control, which partly can be applicable to the cyber realm.

On the Need for Cooperation

Bruce W. McConnell, Global Vice President, EastWest Institute[3]

Conventional Cyber Threats

Much of the Western discussion about cybersecurity revolves around preventing and recovering from attacks on networks and networked information systems. Serious threat actors include organized crime groups out for financial gain, industrial competitors stealing proprietary information, and nation-states intent on espionage, intellectual property theft, or disrupting operations of military or other critical systems as an element of force projection during conflict.

Well-funded threat actors are constantly innovating. Take "ransomware," a variety of malicious software that installs itself on your computer and gets access to your data.

Ten years ago, the owner of the malware would contact the victim and threaten to release proprietary financial data it had accessed unless a ransom was paid. Today, the bad actor locks down the victim's computer and threatens to hold the data hostage until a ransom is paid. Hospitals have become particularly common victims. To combat these and other kinds of attacks, industry has focused its efforts on reducing vulnerabilities and promoting sound cybersecurity practices.

Unfortunately, preventing a determined attacker from getting in is impossible right now. If your valuable information is connected to the Internet, someone can get it.

An attacker will find an unpatched vulnerability, or an employee will open an infected attachment or click on a malicious link. A disgruntled system administrator can compromise systems without detection. Firms can, however, reduce the impact of these vulnerabilities through sound cybersecurity practices. And there are multiple guides available.

One that is gaining currency in the U.S. is the Cybersecurity Framework created by the National Institute of Standards and Technology, or NIST, which is part of the U.S. Department of Commerce. The framework lays out the basics of a cybersecurity program that all firms should manage to. It provides specific steps organizations can take to conduct basic cybersecurity activities: identifying risk, protecting systems and information, detecting attacks and failures, responding to those incidents, and recovering afterwards. The NIST framework is supplemented by other guidance, including EWI's "Purchasing Secure ICT Products and Services: A Buyers Guide." This guide recommends 25 questions that buyers can ask ICT suppliers to help them evaluate the security of the products and services that these suppliers deliver.

Internet Content and Terrorism

In recent years, security professionals have begun to pay more attention to content – information that is being transmitted and stored in cyberspace – and the implications for security of its propagation, corruption, and misuse. Law enforcement officials worldwide have long been combatting electronic information that depicts child exploitation, and nearly all countries and companies cooperate to remove that content from the internet when it is found and to track down and arrest its creators and purveyors. There is less unanimity when it comes to content that can be seen as political. Terrorist organizations use the Internet to advertise their beliefs, recruit new members, provide instruction on how to attack targeted individuals or institutions, plan operations, and incite violent attacks. International efforts to combat terrorist use of the Internet are often undercut by disagreement among nations as to what constitutes a terrorist organization and concerns in Western countries about the potential suppression of political speech by authoritarian regimes.

International Internet platform companies like Facebook and Twitter find themselves under increasing pressure to take down content that is objectionable in one or another jurisdiction.

[3] The views expressed do not necessarily represent the positions of the EastWest Institute or its Board of Directors.

Information Warfare

A major sticking point in promoting cybersecurity cooperation between Russia and Western countries has been a fundamental difference in focus on what is under attack and what is to be secured.

Western analysts tend to focus on network and systems security, and on criminal and terrorist use of the Internet. However the Russian view of information security encompasses protection against the use of the information space to attack Russia. For example, Secretary of State Clinton was seen as attempting to stimulate a "color revolution" in Russia by advocating for freedom of speech and promoting the use of Twitter as tool for dissidents. Similarly, the disclosure of the "Panama Papers" which implicated senior Russian officials in illegal financial transactions, and public accusations regarding the doping of Olympic athletes, were seen as Western attacks on the Russian nation.

Regardless of the accuracy of the allegations, the problematic use of the Internet as a tool to publicly attack a country or its people with negative information or attempt to destabilize a regime is increasingly a part of the cybersecurity conversation. Russian military doctrine acknowledges the importance of such tactics.[4] Such techniques are also used by Western militaries, where they are referred to as "influence operations."[5]

This dimension of cyberspace insecurity has been brought to the forefront in the public mind by cyber-enabled attacks designed to influence elections in the United States and Europe which have been attributed to Russian attackers.

Norms of Behavior

Malicious actors, both state and non-state, are engaged in an uncontrolled, global cyber arms race, led by the U.S., Russia, China and Israel, with over 30 other countries having established cyber offense units.

Cyber weapons have upsides: they are cost-effective, generally non-lethal and stealthy. However, continuing, ungoverned state-on-state skirmishes in cyberspace undermine terrestrial security and stability. As I testified at the House Homeland Security Committee in March, there is a growing risk of miscalculation and escalation that could spill over into direct physical harm to the citizens of the developed world. And, if fake news, political trolling and social media bots further degrade the credibility of cyberspace, it will become useless as a medium for commerce and governance. Consumers, afraid of victimization, are already leaving e-commerce.

A group of governmental cyber experts has worked at the United Nations for over 10 years to come up with an initial set of non-binding norms of behavior in cyberspace.

These include:

- Not allowing the use of information and communications technology, or ICT, to intentionally damage another country's critical infrastructure.
- Not allowing international cyber attacks to emanate from their territory.
- Responding to requests for assistance from another country that has been attacked by computers in the first country.
- Preventing the proliferation of malicious tools and techniques and the use of harmful hidden functions.

[4] The Russian military is charged with enhancing its "capacity and means of information confrontation (противоборства)," by "exerting simultaneous pressure on the enemy throughout the enemy's territory in the global information space . . . to create conditions to reduce the risk of [adversaries] using information and communications technologies for the military-political purposes to undertake actions running counter to international law, directed against sovereignty, political independence or territorial integrity of states or threatening international peace and security, and global and regional stability," including to counter "political forces and public associations financed and guided from abroad." Military Doctrine of the Russian Federation (as amended 2015) [Военная доктрина Российской Федерации (в редакции от 2015 г.) http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/976907, discussed at Roche, Edward M., Russian Cyber War Doctrine, https://cyberarmscontrolblog.com/2017/01/20/russian-cyber-war-doctrine.

[5] "Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counterpropaganda operations and public affairs (PA) operations." [U.S.] Air Force Doctrine Document 2-5, cited at http://www.au.af.mil/info-ops/influence.htm.

- Encouraging responsible reporting of ICT vulnerabilities and sharing associated information.
- Not harming the information systems of the authorized cybersecurity incident response teams.

On the private sector side, global ICT companies are beginning to step up to the responsibility that comes with their great power in cyberspace. For example, Microsoft recently issued a set of norms of industry behavior that global ICT companies should follow in their business practices.

Examples of the kinds of norms that companies are considering include:

- Creating more secure products and services.
- Not enabling states to weaken the security of commercial, mass-market ICT products and services.
- Practicing responsible vulnerability disclosure.
- Collaborating to defend their customers against and recover from serious cyber attacks.
- Issuing updates to protect their customers no matter where the customer is located.

This progress must be accelerated in order to prevent major accidental or intentional disruptions to global economic and political stability.

EWI has launched a new, global effort to develop rules of the road for state behavior in cyberspace, working with partners including the foreign minister of the Netherlands, the former foreign minister of Estonia, the former deputy national security adviser of India, the former secretary of homeland security, and various corporate sponsors. The Global Commission on the Stability of Cyberspace (GCSC) is a three-year effort to generate, evaluate and recommend state and non-state norms of behavior in cyberspace and propose policy initiatives for inclusion in wider dialogue. The GCSC will publish and advocate for detailed recommendations in capitals, corporate headquarters and with the general public worldwide. The first results—including a proposal that the core Internet infrastructure we all depend on should be off-limits for attacks—are expected in fall 2017.

Technical Cooperation

While diplomatic, policy, and political efforts are critical, cooperation is also needed at a more technical level.

One area has already been noted in the main part of this Policy Brief, which notes that "Russia and the United States need to regularly test a system of immediate mutual warning of potentially dangerous [cyber] activities." Regular exercise of the cyber hotline established between the two nations in 20xx would reduce the likelihood of miscalculation and overreaction.

Another approach involves private sector security cooperation. A group of cybersecurity companies recently founded the Cyber Threat Alliance, a group of cybersecurity practitioners from organizations that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries. Member companies[6] have worked together to produce private and public guides to improve cybersecurity on a global basis. Broadening the membership of the CTA to include more non-U.S. companies would be a useful step to improving international technical cooperation in cybersecurity.

Diffusing the Immediate Crisis

All these efforts take time. While progress is made in these areas, action is needed to reduce the likelihood of unintended consequences. Good communication among trusted parties is the key to success. Informal efforts such as the EWI/RIAC-sponsored dialogues should be encouraged and supported. The world depends too much on a safe and secure cyberspace to allow miscalculation and misinformation to deny its benefits to the world's peoples. Major powers like Russia and the United States must increasingly step up to their responsibilities in this area.

[6] Current members include: Check Point, Cisco, Fortinet, Intel Security, Palo Alto Networks, Symantec; and, Eleven Paths, IntSights, Rapid7, ReversingLabs, and RSA.

RECOMMENDATIONS

As a result of a number of joint meetings RIAC and EWI have outlined the following.

Challenges Regarding Cybercrime Prevention and Counterterrorism Measures:

- The broad global community lacks sufficient knowledge of cyberspace and cyber technologies.
- Countries face the urgent need to elaborate cyber terminology that would cover both cybercrime and cyberterrorism. Although neither Russia nor the U.S. is interested in bringing harm to each other, the parties have different perceptions on what should be considered an act of cybercrime.
- The most common cybercrimes include identity theft, financial fraud, denial of service attacks and intellectual property theft. Business suffers the most from cybercrimes, but law enforcement is unable to fully contribute to solving everyday cybersecurity issues that companies face.
- Unlike states, business is more interested in recovering from attacks than in trying to investigate them. The more time is spent on recovery, the more losses the business suffers.
- Communication between business and the government needs improvement. As IT companies tend to be international, they fall prey to the lack of contacts not only within their country of residence, but on an international level as well. In case of an attack they need to resort to contacting their partners abroad, where they face complex legal challenges.
- Anonymous nature of cybercrime. The investigators are sometimes able to track down the IP-address, not managing to go further. According to some experts, only 1 out of 10,000 crimes committed in the cyberspace are successfully investigated.
- International nature of cybercrime. As most of the attacks proceed from other countries, governments often fall short of conducting a proper investigation, as they cannot trace the criminals in other states.
- Russia and the U.S. have been unable to elaborate a joint strategy of behaving in cyberspace. Should an attack occur, the parties may accuse each other publicly. Such accusations lead to immediate further aggravation in relations.
- Russia and the U.S. face common threats in cybersecurity, proceeding from third parties. Still they lack joint efforts to investigate cybercrimes.
- There is no registered legal database of cybercrimes committed. Between Russia and the U.S., no agreed list of crimes is maintained for which mutual assistance has been requested.

Possible Measures to Be Taken:

- A global cyber forum should be organized to bring together all interested countries' representatives to work out cyber norms, primarily to find common ground regarding terminology and its interpretation. A new multistakeholder institution is needed.
- The governments need to start working closely with business representatives to elaborate ways of cooperation in cyberspace. The parties need to reach consensus regarding dual-use products and terms of their assembling and use.
- To make the fight against cyberattacks and cyberterrorism more effective, proper law enforcement mechanisms should be introduced.
- International cooperation to trace the attackers and elaborate efficient strategies to fight cybercrime is vital. It is crucial to establish streamlined and effective information exchange mechanisms both on bilateral and multilateral basis.

- On their part Russia and the U.S. should work out a bilateral agreement to determine their joint stance on the issue and prevent future cyber incidents. Trust is a primary thing to work on in bilateral relations.
- Russia and the U.S. need to regularly test a system of immediate mutual warning of potentially dangerous activities.
- ICT companies and governments should work together to reduce nation-state attacks. States should contribute to nonproliferation of cyber-related weapons (what has already been developed should be limited and precise), while the ICT companies should not traffic in cyber vulnerabilities or offensive purposes nor proliferate technologies leading to cyber vulnerabilities.

Challenges Regarding Cybersecurity Norms and Protection of Critical Infrastructure from Cyberattacks

- The precise applicability of international law to cybersecurity issues is still being debated. The established legal base does not deal adequately with the new threats including those in cybersecurity. Tangible results are impossible to reach in such situation.
- There is an emerging set of norms of recommended behavior in the cyber domain for business; and, the UNGGE is developing norms for states. Norms need to be actionable.
- Russia and the U.S. lack a mutual understanding of what critical infrastructure is and what objects can be regarded as such.
- Some countries do not have a tradition of mutual legal assistance should cyber incidents occur.
- In case of cyberattacks countries have to consult the counterpart's laws. States have conflicting legal frameworks, including different traditions as to how the police may work with law enforcement, policy makers and business.
- Laws often need to be translated, which creates additional hurdles for prosecution.
- Law specialists lack knowledge of IT, which makes it yet more difficult to elaborate adequate norms.

Possible Measures to Be Taken:

- There is a need for positive mindset: it's not about conflict, it's about finding a compromise. Trust issues need to be solved: countries should move from "information sharing" to "information exchange".
- Russian and U.S. experts have agreed that states should not attack each other's critical infrastructure. The terms remain unclear. An analysis of overlaps and gaps in Russia's and U.S.' critical infrastructure lists by the authorities needs to be done.
- The possible norms should be depoliticized. They will be introduced only once both countries have a strong will to collaborate on the issue. When common norms are introduced, there will be a win-win situation, for business representatives as well.
- The UN approval of cyber-related documents could give a necessary impetus to states to begin action. Eventually, some of the norms must be obligatory, and not only serve as a recommendation.
- Russia and the U.S. need to continue expert, business and diplomatic contacts to find common ground.

NOTES

facebook.com/
russiancouncil

twitter.com/
Russian_Council

vk.com/
russian_council

russiancouncil.
livejournal.com

flickr.com/photos/
russiancouncil

youtube.com/
russiancouncilvideo

slideshare.net/
RussianCouncil

linkedin.com/company/russian-international-affairs-council/
linkedin.com/groups/Russian-International-Affairs-Council-4473529

Tel.: +7 (495) 225 6283
Fax: +7 (495) 225 6284
E-mail: welcome@russiancouncil.ru
119180, Moscow, Bol. Yakimanka St., 1.

www.russiancouncil.ru