Unofficial translation

Main International Information Security Challenges

(Outline of the Report by President of the National Association
of International Information Security Vladislav Sherstyuk)

The 6th China Internet Security Conference
2 September 2018, Beijing (the People's Republic of China)

Dear Forum hosts,
Dear Forum participants,
Ladies and gentlemen,

1. We are most grateful to the Forum organizers for the opportunity to take part in such a meaningful event held to discuss Internet security challenges.

Russia and China have truly friendly and brotherly ties in the field of ensuring international information security (IIS). Intergovernmental agreement on ensuring security in the field of IIS between our countries, concluded in 2015, moved cooperation in this area to a fundamentally new level. Not distorting soul I can say that positions of our countries on the issues related to ensuring IIS and combating cybercrimes are practically identical and Russian and Chinese delegations closely coordinate work at international venues and forums. Special impulse to this cooperation is given by regular meetings of our national leaders Vladimir Putin and Xi Jinping. We are sure that this tendency will be continued during their upcoming meeting at Vladivostok. That is why for me it is especially pleasant to present Russian position on organization of international cooperation in this field on Chinese soil.

As you know, the 2000 Okinawa Charter on Global Information Society marked, in effect, the beginning of the new era of the humankind development. This is the epoch of the intensive development of the global information and communication technologies (ICT) environment, the core of which is global information infrastructure, and, in particular, Internet. So much hope for positive changes and unlimited prospects of the humankind development we had when entering the digital age!

However, now we come to realize that the new ICT environment that indicated the nascence of the new space for social interactions both at national and international levels is not able to change human nature and patterns of international relations. It only creates new opportunities for showing both virtues and vices inherent in the human mental world.

As Russian President Vladimir Putin noted during his speech at the International Cybersecurity Congress organized by *Sberbank* in July 2018, "today, active introduction of digital technologies in many ways determines progressive development of every State and very likely of the world at large. Artificial intelligence, robotics and the Internet of Things lay the foundation for economic growth, and digital platforms and electronic document management dramatically increase the openness and efficiency of authorities, companies, business, social and educational institutions".

At the same time, the ICT environment is not only a new factor of sustainable society development but also a factor of higher social danger of actions related to the implementation of criminal intentions and terrorist activity, and a new space for international disputes and conflicts.

The pernicious nature of new international security challenges has been repeatedly highlighted both by political leaders of various States of the world and the UN General Assembly.

According to the Russian President, "today, security of global information space requires special attention. We see that the number of threats and risks in

this area is growing. The World Economic Forum reports that losses caused only by cyber-attacks in the world in 2017 amounted to around a trillion USD, and experts say that the damage will be much bigger in the absence of effective and efficient measures. Like other countries, Russia also faces such challenges. For example, in the first quarter of 2018, as compared with the same period of the previous year, the number of cyber-attacks against Russian resources increased by a third". The Russian President expressed his conviction that neutralizing those threats "and ensuring cybersecurity in general is a national objective whose achievement requires united efforts of law enforcement agencies, business circles, social organizations and citizens themselves".

Russian politicians and specialists share the opinion that sustainable operation of the ICT environment and its safe use by persons, societies and States may be ensured only on the basis of international cooperation in countering existing and potential threats.

The main platform for such cooperation should be the UN, which unites virtually all existing States of the world and is able to create conditions for maintaining international peace and security. The important role in facilitating this process is played by such regional associations as the SCO, BRICS, the CSTO and others.

In our view, this is the only means to reduce the risk of disturbing trends that have been formed in the ICT environment in recent years and indicate the existence of rather dangerous threats to peace.

2. We believe that such threats include primarily **the rapid transformation of the ICT environment into space for inter-State confrontation** through the hostile use of information and communication technologies. We all understand that in current circumstances countering this threat is one of the essential aspects of preventing international conflicts.

Methods of possible use of information technologies for force action against the opposing side keep increasing in number. Until recently, among such

methods experts included, above all, the use of malicious software and hardware for disrupting the operation of critical information infrastructure and other facilities that have significant impact on societal life, and the illegal acquisition of restricted information.

Currently, areas of the use of information technologies for military and political purposes have augmented significantly. Specialists pay growing attention to exploring ways of implementing artificial intelligence systems in weapons systems and military hardware. Ways and means of creation and modus operandi of autonomous military robots across land, sea and air and in information infrastructure are actively studied. Methods of using information technologies to enhance capability of means of armed struggle at all stages of conflict are being actively developed. At the same time, State infrastructure facilities multiply, and their destruction can lead to a conflict. Now, beside State's military infrastructure they often include social and economic facilities as well.

The experts of the Organization for Security and Cooperation in Europe believe that about 50 States of the world actively implement programmes to build military malware. They include 10 States with the most impressive military budgets. The unprecedented growth of the 2019 US military budget, which mounts up to the astronomical sum of US 716 billion dollars, should be emphasized.

In this context, we also take into account repeated media reports about significant volumes of budget investments of the US government in exploring technologies for producing malware and methods of their use to exert hostile pressure on opposing States.

The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security noted in its 2015 report that "a number of States are developing ICT capabilities

for military purposes. The use of ICTs in future conflicts between States is becoming more likely. "

The development of means of conducting military actions in the IT environment seems to increase the risk of conflicts that can disturb international peace and security.

This argument is proved by a series of unprecedented decisions taken in the United States recently. First of all, this is the National Security Strategy of the United States of America (December 2017). Among the main threats the document mentions China and Russia, which "seek to challenge American influence, values and wealth", and Iran and the DPRK, which "sponsor terrorism and threaten American allies".

Besides, on 23 March 2018, President Trump signed the Clarifying Lawful Overseas Use of Data Act or the "CLOUD Act". Its main purpose is to expeditiously ensure law enforcement and special services' across-the-border access to personal data of users suspected of committing crimes regardless of where such data are stored.

This Washington's initiative is another attempt to anchor the Anglo-Saxon superiority in the digital space and get full license there. The "exclusive" status is aimed to legitimize any military actions of the US-British alliance in this area. In doing so they declare the following principle: "what is permissible for the Internet country founders – the USA and UK – is not permissible for others".

3. The second devastating threat to the international information security is the **use of global media environment** and, particular, social networks, **to justify strong-arm approaches to resolving international disputes and to interfere in the internal affairs of sovereign States.**

This was the case in Yugoslavia in 1999. This was the case in Iraq in 2003. This was the case in Libya in 2011. And this is the case in Syria today.

Abuse of the freedom of the media by some states for the purposes of promoting their ideological superiority and special historical mission is

becoming a serious problem nowadays. Reliable information disseminated in the media by those states is being mixed with false information (fake news).

As demonstrated by the example of a mythical Russian trace in the so-called "Skripal case", interested states create chains of fake news, thus forming a kind of "fake chains". In such "fake chains", one fake story is supported by another. These chains are created to deliberately manipulate public opinion at both national and international levels, posing a real threat to international peace and security.

A good illustration in this context is the attempt of the US legislative and executive authorities to bridge the divide in the American society that followed the dramatic struggle between the Democrat and Republican presidential candidates by picturing Russia as an enemy, whipping up anti-Russia hysteria at home and globally. The absence of any facts whatsoever does not bother American politicians and even bolsters their confidence.

To see how much the Russian-American relations have degenerated, one only has to look at the quote by Senator Lindsey Graham – one of the co-sponsors of the new draconic bill on anti-Russia sanctions – who, according to Reuters, said: "Our goal is to change the status quo and impose crushing sanctions and other measures against Russia...."

Do I have to comment? I will just say that Russia has to actively advance its military assets, as described by President of the Russian Federation Vladimir Putin in his address to the Federal Assembly on 1 March 2018, and strengthen international cooperation with all sensible stakeholders only to avoid such a scenario and prevent American politicians from deluding themselves that this bold, but not very original idea could actually be implemented.

4. Before concluding the theme of the use of ICTs for military and political purposes, I would like to draw your attention to the fact that cyberspace, as Russian experts see it, is not some sort of special aspect of strategic stability. It is closely integrated with other aspects of the strategic

stability maintenance system. Therefore, the idea of treating cyberstability as a separate dimension of strategic stability is somewhat contrived. Maintaining strategic stability is a comprehensive task that requires consideration of all factors and use of a variety of means.

Maintaining strategic stability is an important component of ensuring international peace and security. This task should be fulfilled based on the application of norms and principles of international law to ensure regulation of international relations in the field of ICT use.

As pointed out in the 2013 and 2015 reports of the Group of Governmental Experts, international law is applicable to the ICT environment; however, we encounter certain difficulties when it comes to practical implementation of this conclusion.

In our opinion, these difficulties are primarily due to the characteristics of the ICT environment which make it different from the traditional environments of interstate interaction, i.e. land, air, water areas, subsoil assets, and space.

The differences are the following.

First of all, it is the *artificial nature of the ICT environment*, whose existence depends entirely on activities of people, private organizations and government entities. Together, they create conditions for operation and development of the ICT environment, for its use in all spheres of public life. One of the consequences of the artificiality of the ICT environment is the absence of state borders therein. This creates certain difficulties in terms of application of international law for regulating international relations in the field of ICT use. As noted by the UN Secretary-General in his foreword to the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations."

Practical implementation of the principle of sovereign equality of states is significantly hindered by the lack of defined limits of the state sovereignty in the ICT environment. It also hinders objective monitoring of states' compliance with their international obligations in the ICT environment.

We are not talking about borders in the conventional sense of the word, but rather about zones of states' responsibility for observing international treaties and respecting international custom rules and general principles of law recognized by civilized nations.

Another important difference of the ICT environment from the traditional spheres of international relations is the *virtuality of the processes of information transmission, processing and storage*, which are carried out by means of computers and communication devices and networks. The fact that these processes are virtual makes it impossible for concerned subjects of international law to ensure visual monitoring of threats emerging in the ICT environment and collect reliable information on incidents that could compromise international peace and security based on the presumption of trust in the law enforcement agencies of a state that alleges to have been a victim. The lack of such information poses a serious obstacle to the fulfillment of the requirements under Article 2(3) of the UN Charter in relation to peaceful settlement of international disputes.

Last but not least, what makes the ICT environment different is the *dual nature of ICTs*. On the one hand, ICTs, which are defined as a combination of methods and tools for processing and transmission of information, are not a weapon. On the other hand, experts recognize that malicious use of ICTs can, under certain conditions, turn non-military devices and mechanisms into weapons and inflict great suffering on citizens of individual states and humanity as a whole.

Essentially, we are trying to apply international law to ensure regulation of international relations in a fundamentally new environment of human

presence. The lack of mechanisms for applying international law to regulate international relations in the ICT environment *per se* creates additional threat in terms of preserving strategic stability.

5. We believe that the only *way out of this situation* is to step up international cooperation aimed at adapting and adjusting international law to the ICT environment.

It was in this vein that, in 2003, the Russian Federation suggested establishing the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which is to report to the UN Secretary-General. Practical value of this initiative has been recognized by the vast majority of states.

In 2015, long years of experts' work culminated in the consensus adoption of a report to the Secretary-General which in many ways can be called historic.

The sides agreed on a whole range of breakthrough ideas:

Firstly, prioritizing the prevention of the use of ICTs for military and political purposes;

Secondly, refraining from accusing states of cyberattacks without solid evidence, which is often the case nowadays;

Thirdly, using ICTs solely for peaceful purposes;

Fourthly, prohibiting the use of harmful functions hidden in the ICT products, which can turn different devices and mechanisms into weapons;

Fifthly, the sovereign right of states to manage the ICT infrastructure in their territory and determine their policy in the field of international information security.

It is very unfortunate that the 2016–2017 Group of Governmental Experts could not sustain the momentum and failed to achieve consensus on the draft final report to the UN Secretary-General. This circumstance, however lamentable it may be, should not be viewed as a reason to reconsider the role of

the United Nations in ensuring international information security and take the discussion of this issue to regional and bilateral levels.

Today, given the serious aggravation of the international situation, experts from many states believe that continuing work towards the adoption of norms, rules and principles of responsible behavior of states in the ICT environment will help lower the risk of conflicts arising from hostile and malicious use of ICTs by states as a means of settling interstate disputes.

The Russian Federation and other member States of the Shanghai Cooperation Organization have the intention to present a new draft resolution at the upcoming session of the UN General Assembly. The draft will contain norms and rules which have been revised to better reflect the realities of the modern international relations in the ICT environment.

The draft proposes that norms, rules and principles of responsible behavior of states be established in the following areas:

observing human rights and freedoms;

ensuring stable functioning and security in the use of the global information infrastructure through internationalization of Internet governance, consolidation of security of critical information infrastructure, prohibition of hostile or malicious use of ICTs;

strengthening guarantees for non-interference in the internal affairs of sovereign states and in the processes of their political and social development;

ensuring security in the use of ICT products;

employing peaceful means of dispute resolution in the ICT environment;

implementing confidence-building measures.

A 2016 study by the MSU Institute for Information Security Issues shows that introduction into the law enforcement practice of norms, rules and principles of responsible behavior of states in the ICT environment which were recommended for consideration by states in the 2015 report of the Group of Governmental Experts may require additional efforts.

As a matter of fact, an international group of experts came to the same conclusion after conducting a similar study in 2017. In 2018, drawing on the results of these studies, a compendium of commentaries to the norms, rules and principles of responsible behavior of states in the ICT environment was prepared and issued with support of the UN Department for Disarmament Affairs. It appears to us that it provides conditions for the next step, which is to identify problems of practical implementation of the norms of "soft law" in this field and prepare recommendations for their resolution.

In 2018, the International Information Security Research Consortium, which was established at the initiative of the Lomonosov Moscow State University, launched an international project to study the practicability of norms, rules and principles of responsible behavior of states designed to facilitate an open, secure, stable, accessible and peaceful ICT environment. The project is run by an international group of experts that comprises members of organizations from the Russian Federation, the USA, Estonia, South Korea, and Switzerland. Preliminary results of their work are expected to be submitted for consideration by the International Consortium in December 2018.

6. The international community is also faced with an increasingly difficult issue of countering criminal use of ICTs, which, in terms of its scale and comprehensiveness, has long grown into a global threat afflicting both developed and developing states.

It is no surprise that the main theme of the recent session of the UN Commission on Crime Prevention and Criminal Justice (Vienna, 14–18 May 2018), for the first time in its history, was the fight against cybercrime. In his address to the meeting, UN Secretary-General António Guterres assessed the damage to the world economy from this threat at USD 1.5 trillion annually. According to an estimate by field experts, the damage to the world economy from cybercrime is expected to reach USD 6 trillion per year by 2021, which would be commensurate with the total profit from the use of ICTs.

Unfortunately, for today, the international community has no common approach to addressing this problem. The situation is further compounded by the lack of a full-fledged international legal framework for cooperation or at least unified terminology.

At the regional level, a number of organizations have elaborated and adopted relevant documents. For example, the agreement on cooperation of CIS countries to combat crimes in the sphere of computer information (of 1 June 2001), the 2001 Council of Europe Convention on Cybercrime (of 23 November 2001; the so-called Budapest Convention), the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security (of 16 June 2009), the Convention on Combating Information Technology Offences signed by the members of the League of Arab States (of 21 December 2010), the African Union Convention on Cyber Security and Personal Data Protection (of 27 June 2014).

Such "regionalization" resulted in fragmenting positions at the international level, which prevents us from developing a common understanding of key aspects of countering illegal activities in the information sphere. We firmly believe that, faced with a global problem of such scale, we need to launch political discussion at an appropriate level – within the United Nations.

For that reason, the Russian Federation and other SCO states plan to introduce a draft resolution entitled "Countering criminal use of ICTs" at the upcoming 73rd session of the UN General Assembly. It pursues a simple objective and has a technical character. The operative part contains three paragraphs.

In the first paragraph, the UN General Assembly invites all Member States to convey their views and assessments regarding the issues of countering criminal use of ICTs. In the second, the UNGA requests the UN Secretary General to present a report to the General Assembly at its 74th session. In the third paragraph, the UNGA decides that the provisional agenda for its 74th

session should include an item entitled "Countering criminal use of information and communication technologies".

It is our hope that this draft resolution will give momentum to the international discussion on combating cybercrime and contribute to a transparent negotiation process in that field with due regard for equitable geographical representation within the UN General Assembly. Thus, all countries will have a chance to express their views on the matter, which will create conditions for achieving global compromise.

In our view, a convention drawn up under the aegis of the United Nations on countering crimes related to the use of ICTs that would take into account the realities of all states without exception and be based on the principles of sovereign equality of the parties and non-interference in the internal affairs of states may become a solution to the problem. The idea of drawing up such a document was first reflected in the outcome declaration of the 12th United Nations Congress on Crime Prevention and Criminal Justice (Brazil, April 2010). It could be based on the provisions of both the existing regional instruments and, for example, Russia's draft universal convention on cooperation in countering cybercrime, which meets modern standards and, on 28 December 2017, was given the status of an official UN document.

7. **Cyberterrorism** is the fourth among the most serious threats to international information security, and it is growing more and more closely linked to computer crime, undermining security in the use of critical information infrastructure.

The report of the UN Group of Governmental Experts noted that "threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging". The Group concluded that "the most harmful attacks using ICTs include those targeted against a State's critical infrastructure and associated information systems. The risk of harmful ICT attacks against critical infrastructure is both real and serious".

From this perspective, it is important to improve mechanisms for public-private partnerships in field of ensuring security of critical information infrastructure and security in the use of ICTs for exercising human rights and freedoms and engaging in economic, social, political, cultural or other activities.

Given the multifaceted nature of international information security, government authorities should concert their efforts to counter cyberterrorism with the activities undertaken by non-governmental stakeholders.

Particularly noteworthy are the initiatives launched by businesses to ensure security in the use of the ICT environment. Thus, at the 11th Forum in Garmisch-Partenkirchen (Germany, 2017), Russia's Norilsk Nickel put forward an initiative to draw up a charter for information security of critical industrial facilities. Norilsk Nickel is a global, systemically important Russian company which greatly contributes to the social and economic development of Russia's regions. Over the past year, the representatives of the company worked intensively to prepare a draft charter, arrange discussion of the document by stakeholders, and reflect on the comments received. As we all know, Microsoft and Sberbank undertook similar initiatives. It is therefore important that a mechanism be devised for using the potential of businesses, non-governmental organizations and citizens to consolidate efforts of the entire society in countering threats to sustainable functioning of the global information infrastructure and security in the use of ICTs.

8. In April 2018, the National Association for International Information Security was established in the Russian Federation to facilitate the development of public-private partnerships in field of ensuring security in the use of ICTs.

The Association is expected to work proactively, addressing most problematic issues related to ensuring international information security and thereby forming a basis for the government authorities' positions at negotiations.

As part of its statutory tasks, the Association is ready to cooperate with stakeholders from the People's Republic of China, as well as other states, to strengthen peace and security.

Thank you.