Rashid Ismailov –

Speech text (24/08/2022)

In general, for the business community, the most important component is the predictable and transparent conditions for fair competition. The commercialization of Internet opened the way for implementation of various business projects, sale of information, goods and services, however, with an essential downside like fraud, sales of illegal services, cyber-attacks, etc.

Furthermore, the line between cyber-attack and cyberwar is de facto blurring.

Paradoscal, the further technology advances, the more it increases damaging risks for users. For example, the deployment of 5G takes security to another level of criticality. Fraud will threaten not only subscribers' personal data. In solutions using the industrial Internet of things, it can threaten their life and health (for example, self-driving cars, telemedicine).

As a President of VimpelCom PJSC (brand - Beeline), Russian federal telecom operator, part of international group VEON, I must confirm that cyber-attacks on the civilian infrastructure of telecom operators have intensified many times over, if, for example, we compare year by year.

Our company had to develop scenarios of business continuity, reliable IT landscape, establishing protected perimeter & trusted HW/SW environment. The situation requires additional resources, and despite the fact, that so far professionals are capable to remain it under control, the general trend cannot be considered as encouraging.

Enhancing cybersecurity and protecting critical information infrastructures are essential to every nation's social and economic development.

In the digital age, trust is more than critical – trust is everything.

The intention to make technologies as accessible as possible should not shift focus from the human being, which creates tremendous controversial capacity.

How to respect all necessary digital rights of individuals and to adequately distribute roles of among all stakeholder of that process? This is about the role of states, transnational corporations and regulators. Each of them is trying to win a power game, getting more authorities by continuously growing its technological capabilities. How to arrange the digital interaction among states and to align operation of mutually beneficial initiatives on counteracting fraudsters and criminals in the digital space? How to align sharing of any data among e-government systems of different countries?

For example, total distrust still prevents us from giving up paper documents during trans-border interactions; it is paradoxical, but paper has remained the only factor of credibility and a safe haven. Digital technologies have already discredited themselves.

The sophistication of attacks is growing, which creates clear risks for business and the economy as a whole.

Many countries in the world are now seriously engaged to return of sovereignty. Because many countries have seen cross-border information flows as more of a threat than an opportunity, including a threat to their economies, finances, and cultures.

The global nature of Internet has begun to "bump" on national borders. States, including those that have always been the leaders of globalization, spoke about the need to control information flows, counteract the spread of distorted or false information, the need for protectionist programs to support national producers, and protect national information and cultural resources.

However, as for the Internet, sovereignty never existed. Due to its nature - transboundary, global technical infrastructure and methods of governance - the Internet does not follow the principles of territoriality and state control over cross-border exchanges.

Unfortunately, infrastructure, especially global infrastructure, almost inevitably becomes a factor of political influence and even political pressure. This is true for the internet just as it is for gas pipelines or the financial system.

For the vast majority of countries, the level of sovereignty does not allow them to claim an independent role in the global information space.

Today, ICTs have the same decisive impact on national and global development, they also determine the degree of sovereignty, like nuclear technologies in the 40s of the last century or rocket and space technologies in the 50s, 60s, and 70s.

Infrastructural sovereignty is first of all the ability of the network to operate even in the event of a catastrophic shutdown of the main cross-border channels. This is not isolation from the global network, this is insurance against problems.

Internet Threats may have a different nature: (1) May come from authorities (data corruption in the DNS root zone, distortion of objects in RIR databases, ect,); (2) Attacks on infrastructure (DDoS, BGP hijacking, fake digital certificates, etc.); (3) Threats at the content level. It has nothing to do with censorship. The technical possibility to block illegal content is only a part of sovereignty.

Unfortunately, the exclusively market principles of the functioning of the Internet give rise to a situation in which the global information space can be transformed into an environment harmful to users.

In this situation, states must act both from the considerations of preserving their own sovereignty and from an understanding of the global nature of the Internet and the information society.

In the absence of effective international law in the field of the Internet, it turns into a space of global information and cyber war without rules.

Users can benefit from the digital world if countries will support the free flow of information while respecting applicable domestic and/or international legal frameworks for privacy and data protection, and strengthening security in the use of ICT as well as transparency and consumer protection.

In the past, information flow was largely regulated domestically. In general, the only international rules that applied to some aspects of information flow were rules of customary international law, and their application was purely exceptional.

International legal framework supposed to be binding on States Parties. Like other universal instruments, such as the Universal Declaration of Human Rights, and some specific provisions, such as the principle of non-discrimination, have become part of customary international law and are considered binding on all States, even those that have not ratified a human rights treaty that embodies norms of customary law.

I believe that ITU's commitment to collaboration with industry associations and ICT organizations will leverage collective opportunities to build the capacity of emerging technologies and developments in Member States and enhance coherence among all stakeholders in the international community.

ITU has enormous standardization expertise that might be used to develop common approach to devices operation, technological level of automatic exchange of information, including the exchange of protocol standards.

International Telecommunication Union has a significant role to play by heading activities in technology standardization and development of recommendations for the broadest field of application.

It is a great honor for me to present myself in front of you as a candidate for the position of ITU Secretary-General.

Russia, as one of the founding countries of the Union, and I, as a candidate for the position of the ITU Secretary-General, feel highly responsible for strengthening and further developing ITU for the benefit of the global population

and committed to strengthening ITU's human resources and the efficiency of its work.

What is a role of ITU in this process? For example, through the standardization of the security parameters of IoT sensors. I believe that the participation of states is important here, it is rather shortsighted to give standardization to corporations.

Almost all of my professional activities have been devoted to the telecommunication and ICT industry.

17 years in total worked in international companies – telecom equipment vendor of (Ericsson, Nokia, Huawei).

I have experience of the public service in the position of Deputy Minister of Communications and Mass Media of the Russian Federation.

I have been associated with ITU for 6 years of collaboration as the head of Russian delegation and I warmly remember this experience:

I am convinced that my 30 years professional experience in the industry will enable me to lead ITU to new horizons ensuring ITU’s ability to face emerging challenges.

My programme “Five Steps to the ICTs Humanization” reflects solutions of these tasks.

I believe that in the context of the rapid development of information technologies, the International Telecommunication Union should remain the leading UN platform for agreeing collective approaches to solving urgent problems in the field of telecom and ICT development.

Spectrum remains a key to the implementation of the 5G capacity and an important driver for the industry.

The role of ITU to manage radio frequency spectrum and satellite orbits is central and to be further straitened. As well as in the development of globally agreed standards which are fundamental to ensure available and affordable telecommunications for everyone.

ITU has enormous standardization expertise that might be used to develop common approach to devices operation, technological level of automatic exchange of information, including the exchange of protocol standards.

We should not stop the progress, however we shortly should solve these issues, not only shape them. Despite today’s conditions of reduced international contacts and processes of mutual integration and cooperation.